Content Protection Method to Control Editing by Billing

Tomohiro Kobayashi[1], Keiichi Iwamura[1] and Masaki Inamura[2]
[1]*Faculty of Engineering, Tokyo University of Science, 6-3-1 Niijuku, Katsushika-ku, Tokyo, 125-8585, Japan*
[2]*Center for Research and Collaboration, Tokyo Denki University, 5 Senju-Asahi-cho, Adachi-ku, Tokyo, 120-8551, Japan*

Keywords: Copyright Protection, Content Protection, Edit Control, Digital Signature, Aggregate Signature, Billing.

Abstract: In consumer-generated media (CGM), where consumers themselves generate and transmit content, it is important to promote secure content circulation. Content circulation includes the editing of content, and it is desirable for content to become more abundant and varied. For copyright protection suitable for CGM, a technology (Katsuma et al., 2015, Tatsuya et al., 2016) has been proposed that controls editing using digital signatures, and guarantees the copyright of the original content even for secondary use. However, in those scheme, the content that the author has declared as editing-prohibited once is always kept as editing-prohibited thereafter, and the circulation of the content is stagnant from then onwards. Therefore, we propose a method in which the author can securely provide individual editing permissions for content that has been sent as editing-prohibited. Specifically, when an author wants to transmit content as editing-prohibited, and then an editor wants to view it and purchase the right to edit the content, this method offers a way to securely buy and sell the right to edit content in exchange for money. Therefore, this method is applicable to commercial content circulation. It is possible to promote content circulation while protecting the rights of the author by using the proposed method, even in scenarios where content circulation is stagnant with conventional methods.

1 INTRODUCTION

With the development of the Internet, it has become easy to generate and transmit content, and the distribution of content by general users has grown in popularity. The media created by consumer is called consumer-generated media (CGM). In CGM (YouTube, Nico Nico Douga, etc.), it is easy to browse and obtain published content with content distribution services, so that new content can be generated by secondarily using content. Content circulation is promoted by creating better content, so it is essential to have copyright protection technology that can protect the rights of the original author without interfering with content circulation. There is also a need for technology to guarantee the copyright of the original content.

A copyright protection method suitable for such CGM has been proposed (Katsuma et al., 2015) and (Tatsuya et al., 2016). In case of the former, content control that combined editing control and rights inheritance notation using a Boneh–Lynn–Shacham (BLS) signature method (Boneh et al., 2001, Boneh et al., 2003) was proposed. A method has been proposed: The content was divided into multiple content parts, and editing control was applied (change, addition, deletion) to each content part, as was control of appropriation of partial content to other content, and control of content composition. Also, in case of the latter, the use of ID-based signature methods (Xun, 2003, Jing et al., 2005) eliminated the need for public key certificates and reduced the time needed for signature verification in content produced by a large number of authors and editors. As a result, with regard to content for which the author has prohibited editing, the rights of the author are protected and the document is protected from further editing.

On the other hand, during content circulation, the author's rights are regarded as important, and this directly impacts the author's interests, that is, in a situation where the author's rights are guaranteed, the author can find profit and usually allows editing. It is possible that editing rights are bought and sold for content, so a technology is needed to allow the buying and selling of editing rights for content with a financial transaction. Therefore, in this paper, we propose a means to safely permit editing only to the purchaser in the above conventional method.

Kobayashi, T., Iwamura, K. and Inamura, M.
Content Protection Method to Control Editing by Billing.
DOI: 10.5220/0007959701960208
In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019)*, pages 196-208
ISBN: 978-989-758-378-0

In this paper, Section 2 describes previous research, Section 3 describes an outline and the algorithm of the proposed method, and Section 4 presents the conclusion.

2 PREVIOUS RESEARCH

2.1 Principle of Editing Control using Signature

A technique has been proposed to control the secondary usage of content using BLS signatures (Katsuma et al., 2015, Tatsuya et al., 2016). The author divides the content into multiple parts, generated a digital signature in advance (hereinafter referred to as an edit control signature) to indicate whether or not editing is possible for each part, and aggregate the edit control signature into one (hereafter referred to as an aggregate signature). In addition, the author disclose those aggregate signatures of each piece of content. The author could control in advance whether or not editing was possible by concealing the control signature of the partial content for which editing was not permitted, and protecting it from being deleted. In this way, the author could control in advance whether editing was possible. In addition, it was possible to control addition (change from empty data to actual data) and deletion (change from actual data to empty data) using control data that was not displayed as empty data, and data that was displayed as actual data. The content reproduction device had a signature verification function, which it used to perform signature verification before reproduction, and did not reproduce content that did not have a valid digital signature, or that did not match the digital signature (was considered illegal).

In addition, a content administration center would be established to verify the originality of each piece of partial content and issue a digital signature (hereinafter called the administration signature) to certify the author. Set the administration signature would be mandatory for partial content. With this signature, each piece of partial content is linked to the author, and it would be impossible to forge the author of partial content (partial content without an administration signature is considered to be illegal). In addition, the author alone can be given the right to edit (an edit control signature is always checked with the author's key specified in the administration signature), and any editing that the author does not permit can be prohibited.

In addition, diversion control is realized by the same mechanism described above, but using a content ID, which will be described later. Here, a diversion control signature is introduced to control diversion. It is meaningless for the editor to change the signature because the diversion control signature is authenticated by the author's key of the original content. Therefore, only the author (hereafter aID) of the piece of partial content can decide the propriety of diversion, and the diversion control signature is always checked along with the aID key, so the editor cannot change the setting.

In addition, composition control is control of content that incorporates partial content, while editing and diversion control is control of partial content. Therefore, the process of ordering and arranging multiple pieces of content, and considering it as one piece of content is called composition of content, and content generated by composition is called composition content. Here, we introduce a composition control signature to control the composition of content. The composition content is composed of structure data (control data representing the order of content and composition history) and a plurality of content constituting the composition content. In addition, only the author (hereafter cID) of the content can decide whether or not to combine content, and cannot be realized even if the author wants to leave the decision of whether to combine or not to an editor.

2.2 Content and Partial Content, and Structure of Aggregate Signature

Partial content is divided into two parts, real data and control data; real data is treated as data to be displayed as content, and control data is treated as non-displayed data. The control data includes start data representing the beginning of the content, final data representing the end, empty data for controlling addition/deletion, and structure data for controlling the composition of the content. The content consists of start data, final data, and one or more pieces of partial content created by the author. In addition, the content ID is set for the content as author information, and the partial content ID is set for the partial content. As a result, it is possible to perform change/addition/deletion control for each piece of partial content, and also diversion control within one piece of content, and also enable the composition control of content.

Also, an edit control signature is generated for each piece of partial content, and an aggregate

signature, in which the edit control signature is aggregated, is set for the content. The aggregate signature has the structure "start position signature + edit control signature group of partial content + final position signature." Here the start position signature and the final position signature are always non-disclosure. The structure of the start position signature and the final position signature will be described later. The aggregate signature is linked to the start data or the final data for each piece of content and disclosed, and content without an aggregate signature is treated as illegal content.

2.3 Content Tree Structure

When a certain author creates content A_{ij}, IC_{ij} is set as the content ID. Furthermore, when the content A_{ij} has m partial contents $A_{ij1} \sim A_{ijm}$, A_{ij0} is set as the start data, A_{ijm+1} is set as the final data, and $I_{ij0} \sim I_{ijm+1}$ is set as the content ID. (i, j) of ID_{ij} represent the position relationship of the content by the author, so taking the position relationship shown in Figure. 1 as an example, the content $A_{11} \sim A_{16}$ is by author $ID_{11} \sim ID_{16}$, respectively. It is the primary content created by $ID_{11} \sim ID_{16}$. Also, the author ID_{21}, ID_{22} refers to the author who combines primary content to make the secondary content A_{21}, A_{22}, and the author ID_{31} refers to the author who combines secondary content to create the tertiary content A_{31}. However, each piece of content is not necessarily created by different authors. For example, A_{11} and A_{12} may be by the same author. Therefore, the notation is ID_{11}, ID_{12}, but the actual IDs are the same.

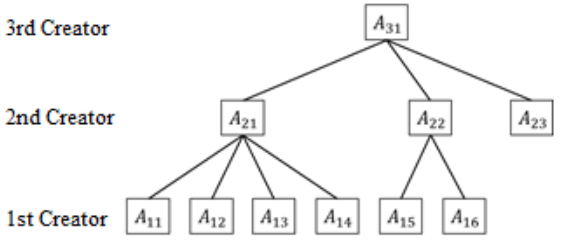

Figure 1: Content tree structure.

3 OUTLINE OF THE PROPOSED METHOD

3.1 Principle of Content Protection by Billing

To correspond about billing, it is necessary for the author of the original content to provide the purchaser with editing rights to the content individually for which editing is prohibited. The editing rights are controlled by the disclosure and non-disclosure of signatures, as described in 2.1. In other words, the signature of the target partial content is disclosed to give the purchaser a permission to edit. However, if the signature of the partial content for which editing is prohibited is disclosed to the purchaser, there is a risk that the signature may be leaked from the purchaser who obtained the signature. Therefore, we introduce a purchaser data as a control data which can specify the purchaser, and the signature of the purchaser data is aggregated in the signature of partial content which the editor wants to edit. If the purchaser is disclosed the signature of the partial content, the purchaser data is also disclosed. If the purchase data does not be added in the content, the aggregate signature not in agreement. Therefore, the purchaser who leaks the signature is determined. The purchaser data is shown in Figure.2.

3.2 Partial Content Configuration

In addition to the actual data, empty data, start data, final data, and structure data described in Section 2.2, purchaser data is introduced as new control data in order to control billing correspondence with the purchaser. The purchaser ID is inserted into the header of the purchaser data, and the information in the billing correspondence described later is specified in the partial content. Also, if the data is not purchaser data , the purchaser ID is not set.

Therefore, as shown in Figure. 2, partial content is associated with the original content author ID (aID), content ID, partial content ID, purchaser ID, identifier, administration signature, various edit control signatures (change/deletion), diversion control signature, composition control signature, etc. Here, the content ID is an ID set by the author cID of the content, and generally only one content ID (different content IDs only when diversion control is performed) is set to the content. However, the composition control signature of pieces of partial content other than start data and final data is not set. Also, if editing is not possible, the hash value at that time is linked to the bID (ID of the user who carried out edit when prohibited) that has been disabled. Also, if diversion is not possible, the hash value is associated at that time. However, the identifier identifies data types such as actual data, empty data, start data, final data, structure data, and purchaser data.

<table>
<tr><td colspan="2">Author aID</td><td colspan="2">Content ID</td><td rowspan="7">Partial content</td></tr>
<tr><td colspan="2">Partial content ID</td><td colspan="2">Purchaser ID</td></tr>
<tr><td colspan="3">Change control signature or Hash value</td><td>bID</td></tr>
<tr><td colspan="3">Deletion control signature or Hash value</td><td>bID</td></tr>
<tr><td colspan="3">Diversion control signature or Hash value</td><td></td></tr>
<tr><td colspan="3">Composition control signature</td><td></td></tr>
<tr><td>Identifier</td><td>Administration signature</td><td>Others</td></tr>
</table>

Figure 2: Partial content configuration.

3.3 Algorithm

Based on the algorithm proposed in (Katsuma et al., 2015) and (Tatsuya et al., 2016), the modified algorithm to support the proposed method is shown below.

3.3.1 Preparation and Key Generation

(1) **Generation of Signature Key and Public Key.**
Author ID_{ij} who generates the signature requests the secret key issuance center to generate the signature key. The secret key issuance center selects $g \in G_1$ as a generator, selects a random number $s \in Z_p^*$, and the public key $Q_{ij} = H_1(ID_{ij})$ is calculated from the ID_{ij}, and $d_{ij} = sQ_{ij}$ is issued as the signature key (secret key) of author ID_{ij}.

(2) **Publishing of g_{pub}.**
The secret key issuance center publishes $g_{pub} = sg$, where s is the master secret key, and the secret key issuance center keeps it secret.

3.3.2 When Creating Original Content

Author ID_{ij} define change / deletion / diversion availability of partial content , content composition availability and content ID and partial content ID (here, partial content $A_{ij1} \sim A_{ijk} \sim A_{ijm}$ is created, and those partial content ID are defined as $I_{ij1} \sim I_{ijk} \sim I_{ijm}$) and do the following. Here, let A_{ij1} be the partial content that corresponds to the credit for the work, and A_{ij2} be the partial content for commercial use judgment.

(1) **Creation of Start Data and Final Data.**
The control data A_{ij0}^*, A_{ijm+1}^* attached to the head and tail of the content are created, and the start position signature α_{ij} and the final position signature β_{ij} are generated for each of change, deletion, diversion and composition. Here, d is empty data, r_{ij} is a random number generated by author ID_{ij}, and r is a constant determined according to the process, and change is r_c, deletion is r_d, diversion is r_t, and composition is r_s.

$$\begin{cases} A_{ij0}^* = IC_{ij}||I_{ij0}||\,d \\ A_{ijm+1}^* = IC_{ij}||I_{ijm+1}||\,d \end{cases} \quad (1)$$

$$\begin{cases} \alpha_{ij} = r_{ij}H(IC_{ij}||I_{ij0}||H(A_{ij0}^*)||r) \\ \quad ,U_{ij0} = r_{ij0}g \\ \beta_{ij} = r_{ij}H(IC_{ij}||I_{ijm+1}||H(A_{ijm+1}^*)||r) \\ \quad ,U_{ijm+1} = r_{ijm+1}g \end{cases} \quad (2)$$

(2) **Creation of Control Data.**
Based on the partial content A_{ijk} (d in the case of empty data), control data A_{ijk}^* is created.

$$A_{ijk}^* = IC_{ij}||I_{ijk}||A_{ijk} \quad (3)$$

(3) **Creation of Edit Control Signature.**
A different constant r is created for each edit, and a hash value is generated.

$$h_{ijk} = H(IC_{ij}||I_{ijk}||H(A_{ijk}^*)||r) \quad (4)$$

Also, the following hash values are calculated to create the pre-composition and post composition control signatures, where the constant r is r_f for pre-composition, and r_b for post-composition.
Pre-composition control hash value:

$$\boldsymbol{h_{ijf} = H(IC_{ij}||I_{ij0}||H(A_{ij0}^*)||r_f)} \quad (5)$$

Post-composition control hash value:

$$h_{ijb} = H(IC_{ij}||I_{ijm+1}||H(A_{ijm+1}^*)||r_b) \quad (6)$$

The following is calculated for each partial content, where the random number r_{ijk} is different for each edit.
Change control signature:

$$\sigma_{ijk} = r_{ijk}h_{ijk} + d_{ij}, U_{ijk} = r_{ijk}g \quad (7)$$

Deletion control signature:

$$\tau_{ijk} = r_{ijk}h_{ijk} + d_{ij}, U_{ijk} = r_{ijk}g \quad (8)$$

Diversion control signature:

$$\chi_{ijk} = r_{ijk}h_{ijk} + d_{ij}, U_{ijk} = r_{ijk}g \quad (9)$$

Pre-composition control signature:

$$\delta_{ijf} = r_{ijf}h_{ijf} + d_{ij}, U_{ijf} = r_{ijf}g \quad (10)$$

Post-composition control signature:

$$\delta_{ijb} = r_{ijb}h_{ijb} + d_{ij}, U_{ijb} = r_{ijb}g \quad (11)$$

(4) **Aggregate Signature of Content.**

Aggregate signatures for various controls are created. Here, $U_{ij0}, U_{ij1}, \ldots, U_{ijm}, U_{ijm+1}$ are different for each editing.

Change aggregate signature:

$$\sigma_{ij} = \alpha_{ij} + \sum \sigma_{ijk} + \beta_{ij} \\ , U_{ij0}, U_{ij1}, \ldots, U_{ijm}, U_{ijm+1} \quad (12)$$

Deletion aggregate signature:

$$\boldsymbol{\tau_{ij} = \alpha_{ij} + \sum \tau_{ijk} + \beta_{ij}} \\ \boldsymbol{, U_{ij0}, U_{ij1}, \ldots, U_{ijm}, U_{ijm+1}} \quad (13)$$

Diversion aggregate signature:

$$\boldsymbol{\chi_{ij} = \alpha_{ij} + \sum \chi_{ijk} + \beta_{ij}} \\ \boldsymbol{, U_{ij0}, U_{ij1}, \ldots, U_{ijm}, U_{ijm+1}} \quad (14)$$

Composition aggregate signature:

$$\boldsymbol{\delta_{ij} = \alpha_{ij} + \delta_{ijf} + \delta_{ijb} + \beta_{ij}} \\ \boldsymbol{, U_{ijf}, U_{ij0}, U_{ijm+1}, U_{ijb}} \quad (15)$$

(5) **Linking to Partial Content.**

The partial content for which editing is permitted is associated with the generated edit control signature. For the partial content for which editing is prohibited, the hash value used for signature creation is linked to the partial content, and author bID links to the author of the original content.

3.3.3 Change, Addition, Deletion, Diversion of Partial Content

Consider the case where author ID_{ab} edits (changes, adds, deletes, diverts) the partial content A_{ijk} of the content A_{ij} and sets it as the partial content A_{abk}. At this time, author ID_{ab} performs the following process. When editing two or more pieces of partial content, the process is repeated.

(1) **Signature Verification of Secondary Use Content.**

Confirm that the signature of content A_{ij} is verified. Here, partial content for which diversion is permitted can be diverted, and partial content A_{ijk} for which change / addition / deletion is permitted can be changed to partial content A_{abk}.

(2) **Generation of Hash Value.**

Author ID_{ab} creates control data A^*_{abk} from the edited partial content A_{abk}, and creates a hash value and a part of the control signature as in Section 3.3.2 (3).

$$A^*_{abk} = IC_{ij} || I_{ijk} || A_{abk} \quad (16)$$

$$h_{abk} = H(IC_{ij} || I_{ijk} || H(A^*_{abk}) || r) \quad (17)$$

(3) **Aggregate Signature Update.**

Author ID_{ab} creates a control signature from A_{abk} in the same manner as in Section 3.3.2 (3), and creates each edit control signature from the signature key d_{ab} of author ID_{ab} and the constant r_{ab} generated by author ID_{ab}.However, if no change is permitted, it cannot be changed. The aggregate signature is updated as follows (U_{ijk} is replaced with U_{abk}).

Change aggregate signature:

$$\sigma'_{ij} = \sigma_{ij} - \sigma_{ijk} + \sigma_{abk} \\ , U_{ij0}, U_{ij1}, \ldots, U_{ijm}, U_{ijm+1} \quad (18)$$

Deletion aggregate signature:

$$\tau'_{ij} = \tau_{ij} - \tau_{ijk} + \tau_{abk} \\ , U_{ij0}, U_{ij1}, \ldots, U_{ijm}, U_{ijm+1} \quad (19)$$

Diversion aggregate signature:

$$\chi'_{ij} = \chi_{ij} - \chi_{ijk} + \chi_{abk} \\ , U_{ij0}, U_{ij1}, \ldots, U_{ijm}, U_{ijm+1} \quad (20)$$

Also, for prohibited edits (change / addition / deletion), the aggregate signature is not updated.

(4) **Linking to Partial Content.**

Partial content that permits editing is associated with an editing control signature. Also, for partial content that prohibits editing, only the generated hash value and U_{abk} are linked to the partial content, and author's ID_{ab} is linked as author bID for which editing is prohibited.

3.3.4 Content Composition

When author ID_{ab} combines content A_{ij} and A_{mn} as the front and back content, author ID_{ab} performs content composition according to the following procedure.

(1) **Signature Verification of Secondary Use Content.**

Author ID_{ab} checks whether the post-composition control signature of content A_{ij} and the pre-composition control signature of A_{mn} are disclosed, and verifies the aggregate signature.

If both A_{ij} and A_{mn} are permitted to be combined, author ID_{ab} can combine them, and at this time, record the combined order of A_{ij} and A_{mn} in the structure data.

If the content that composes the composition content is composable, the content side of the content front and back that is also composable, so it is possible to delete the content. Therefore, new content can be composited at that position. In

addition, even if the first or last piece of content in the composition content cannot be combined, even if the side without the content cannot be combined, if the side with the content can be combined, the content can be deleted and replaced.

3.3.5 Signature Verification

Content signature verification is always performed by the playback device when using content (viewing/secondary use). Here, the object that performs content signature verification is called a verifier, and the verifier performs the following processing.

(1) **Verification of Administration Signature.**
The verifier verifies whether the administration signature of each piece of partial content is valid. Partial content without an administration signature, or with inconsistent content is regarded as illegal content.

(2) **Verification of Composition Content.**
In the case of composition content, this refers to structure data and separates the composition content into pieces of content. If the structure of the structure data and the structure of the content do not match, the content is considered as illegal composition.

(3) **Verification of Composition Control Signature.**
The verifier verifies that each content is composited correctly as follows using the public key, Q_{aID}, of aID.

$$e(g, \delta_{ij}) = \prod e(U_{ijk}, h_{ijk}) e(g_{pub}, Q_{ij}) \quad (21)$$

(4) **Verification of Diversion Control Signature.**
I. The verifier verifies that each piece of partial content is correctly used and verifies the use of a public key Q_{aID} as follows.

$$e(g, \chi_{ij}) = \prod e(U_{ijk}, h_{ijk}) e(g_{pub}, Q_{ij}) \quad (22)$$

II. Confirmation of Content ID.
The verifier verifies whether each partial content has the correct content ID (content ID is unified). If they have different content IDs, the following is performed for the target partial content.

(i) **When the Diversion Control Signature is Disclosed:**
It is verified as follows using the public key Q_{aID} of aID whether the diversion control signature of partial content is correct or not.

$$e(g, \chi_{ii}) = e(U_{iik}, h_{iik}) e(g_{pub}, Q_{ii}) \quad (23)$$

(ii) When the Diversion Control Signature is not Disclosed:
It verifies whether the generated hash value and the diversion hash value are equal.

(5) **Verification of Control Signature of Each Edit.**
The verifier confirms that each piece of partial content is correctly edited (change / addition / deletion). First, it checks whether the empty data is in a changeable/deletable or non-changeable/non-deletable state, and the verifier generates a hash value for each edit. If the actual data does not have a change control signature, the verifier confirms that the generated hash value and the change hash value are equal. If the empty data does not have a deletion control signature, it confirms that the generated hash value and the deletion hash value are equal. The verifier uses the public key Q_{aID} of aID (the public key Q_{aID}, Q_{bID} and the signature U_{aID}, U_{bID} if the changeable/deletable has been changed), the hash value of the generated partial content, and the partial content without a signature to collect the hash values attached and verifies that the following equation holds true.

$$e(g, \sigma_{ij}) = \prod e(U_{ijk}, h_{ijk}) e(g_{pub}, Q_{ij}) \quad (24)$$

$$e(g, \tau_{ij}) = \prod e(U_{iik}, h_{iik}) e(g_{pub}, Q_{ii}) \quad (25)$$

3.4 Content Protection by Billing 1

In the proposed method, the signature of the partial content to be purchased is not disclosed independently as described above, but an aggregate signature is created and disclosed by aggregating the purchaser data described in 3.1 and the partial content to be purchased to the user.

First, the content created by the author of the original content is composed of partial content A_{110} ~A_{115} (A_{110}: Start data; A_{111}, A_{112}: Actual data with editing prohibited; A_{113}, A_{114}: Empty data; A_{115}: Final data). At this time, the billing mechanism for various editing controls is explained in Sections 3.4.1 to 3.4.3, taking the case where the purchaser purchases editing rights for editing partial content as an example.

In addition, by disclosing the signature to the purchaser as follows, it is possible to allow the purchaser to edit it without disclosing the partial content signature, and the purchaser can create a valid aggregate signature for the edited content.

In addition, the signature σ_{dID} of the purchaser

data A_{dID} in which the purchaser ID (dID) is inserted in the header is aggregated into the aggregate signature disclosed to the purchaser dID. By doing so, the purchaser must add purchaser data A_{dID} in order to properly edit the partial content. Therefore, in order to leak the aggregate signature σ_d received by the purchaser, it is necessary to pass the purchaser data A_{dID} aggregated together with the partial content signature. Therefore, because the leak source is known, it is possible to prevent the intentional signature leak by a malicious purchaser.

3.4.1 Content Protection by Billing 1 (Change / Addition / Deletion Control)

The algorithm for billing for various edit controls is shown below.

Change Control. In the change control, the content is controlled using the change control signature. The billing correspondence in the change control will be described below by taking an example of allowing change of the actual data A_{111}, in the content shown in 3.4 to actual data A_{211}. In addition, because it is necessary to add purchaser data simultaneously with the change of the partial content to be purchased in the proposed method, empty data A_{113} is also changed to purchaser data A_{dID} at the same time. Change aggregate signature of content σ_{11} is constructed as follows.

$$\sigma_{11} = \alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{113} + \sigma_{114} + \beta_{11} \quad (26)$$

(1) Author aID creates a purchaser data $\boldsymbol{A_{dID}}$ using a purchaser ID (dID), and creates a change control signature $\boldsymbol{\sigma_{dID}}$ for the purchaser data $\boldsymbol{A_{dID}}$.

(2) A change aggregate signature σ_d is created using the change control signature σ_{111} of actual data A_{111}, the change control signature σ_{dID} of purchaser data A_{dID}, and the change control signature σ_{113} of the empty data A_{113} that is used for the addition of the purchaser data A_{dID}.

$$\sigma_d = \sigma_{111} + \sigma_{113} - \sigma_{dID} \quad (27)$$

(3) Purchaser dID changes actual data $\boldsymbol{A_{111}}$ to actual data $\boldsymbol{A_{211}}$, and adds empty data $\boldsymbol{A_{113}}$ to purchaser data $\boldsymbol{A_{dID}}$, and then adds aggregate signature $\boldsymbol{\sigma_d}$, change control signature $\boldsymbol{\sigma_{211}}$ of actual data $\boldsymbol{A_{211}}$, and creates a post-edit change aggregate signature $\boldsymbol{\sigma'_{11}}$ using the pre-edit change aggregate signature $\boldsymbol{\sigma_{11}}$.

$$\boldsymbol{\sigma'_{11}} = \boldsymbol{\sigma_{11}} - \boldsymbol{\sigma_d} + \boldsymbol{\sigma_{211}} = \boldsymbol{\alpha_{11}} + \boldsymbol{\sigma_{211}} + \boldsymbol{\sigma_{112}} + \boldsymbol{\sigma_{eID}} + \boldsymbol{\sigma_{114}} + \boldsymbol{\beta_{11}} \quad (28)$$

Addition Control. "Addition" indicates a change from empty data to actual data. Therefore, it can be realized by performing control using a change control signature in the same manner as change control, and requesting the right to edit empty data A_{114} instead of actual data A_{111} in the above "Change control".

Deletion Control. Deletion indicates a change from actual data to empty data, but unlike the change / addition control, a deletion control signature is used to realize a state such as {changeable and non-deleteable or non-changeable and deleteable}. The billing correspondence in the deletion control will be described below by taking an example of allowing change of actual data A_{111}, in the content shown in 3.4, to empty data A_{211} and deleting it. In addition, because it is necessary to add purchaser data simultaneously with the deletion of the partial content to be purchased in the proposed method, the update of the change aggregate signature is also performed simultaneously. Therefore, empty data A_{113} is also changed to purchaser data A_{dID} at the same time. The change aggregate signature σ_{11} of content, and the deletion aggregate signature τ_{11} are configured as follows:

$$\sigma_{11} = \alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{113} + \sigma_{114} + \beta_{11} \quad (29)$$

$$\tau_{11} = \alpha_{11} + \tau_{111} + \tau_{112} + \tau_{113} + \tau_{114} + \beta_{11} \quad (30)$$

(1) Author aID creates purchaser data $\boldsymbol{A_{dID}}$ using a purchaser ID (dID), and creates a change control signature $\boldsymbol{\sigma_{dID}}$ and a deletion control signature $\boldsymbol{\tau_{dID}}$ for purchaser data $\boldsymbol{A_{dID}}$.

(2) **I.** A deletion aggregate signature τ_d is created using the deletion control signature τ_{111} of actual data A_{111}, the deletion control signature τ_{dID} of purchaser data A_{dID}, and the deletion control signature τ_{113} of empty data A_{113} that is used for the addition of purchaser data A_{dID}.

$$\tau_d = \tau_{111} + \tau_{113} - \tau_{dID} \quad (31)$$

II. A change aggregate signature σ_d is created using change control signature σ_{dID} of purchaser data A_{dID} and change control signature σ_{113} of empty data A_{113} that is used for the addition of purchaser data A_{dID}.

$$\sigma_d = \sigma_{113} - \sigma_{dID} \quad (32)$$

III. The deletion aggregate signature $\boldsymbol{\tau_d}$, the change aggregate signature $\boldsymbol{\sigma_d}$, and purchaser data $\boldsymbol{A_{dID}}$ created above are disclosed to the purchaser.

(3) The purchaser dID deletes actual data A_{111} by changing it to empty data A_{211}, and adds empty data A_{113} by changing it to purchaser data A_{dID}, and performs the following steps.

I. Update of Deletion Aggregate Signature.

A post-edit deletion aggregate signature $\tau_{11}{}'$ is created using the deletion aggregate signature τ_d, deletion control signature τ_{211} of empty data A_{211}, and pre-edit deletion aggregate signature τ_{11}.

$$\begin{aligned}\boldsymbol{\tau_{11}'} &= \boldsymbol{\tau_{11} - \tau_d + \tau_{211}} \\ &= \boldsymbol{\alpha_{11} + \tau_{211} + \tau_{112} + \tau_{dID} + \tau_{114} + \beta_{11}}\end{aligned} \quad (33)$$

II. Update of Change Aggregate Signature.

A post-edit change aggregate signature $\sigma_{11}{}'$ is created using the change aggregate signature σ_d and pre-edit change aggregate signature σ_{11}.

$$\begin{aligned}\sigma_{11}' &= \sigma_{11} - \sigma_d \\ &= \boldsymbol{\alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{dID} + \sigma_{114} + \beta_{11}}\end{aligned} \quad (34)$$

3.4.2 Content Protection by Billing 1 (Diversion Control)

Diversion means adding actual data from one content to other content. Therefore, in diversion, the piece of partial content for the diversion destination is changed and added, so the change aggregate signature is needed to be also updated simultaneously. In the explanation, the content shown in 3.4 is used as content 1 of the diversion source created by the author, and content 2 of the diversion destination is newly defined and used below. Here, content 2 of the diversion destination is the content composed of partial content $A_{120} \sim A_{124}$ (A_{120}: start data; A_{121}: actual data; A_{122}, A_{123}: empty data, A_{124}: final data). In addition the diversion control signature $\chi_{122}, \chi_{123}, \chi_{124}$ and change control signature $\sigma_{122}, \sigma_{123}, \sigma_{124}$ of empty data $A_{122}, A_{123}, A_{124}$ of the diverted destination are assumed to be disclosed. Diversion aggregate signatures, χ_{11}, χ_{12}, and change aggregate signatures σ_{11}, σ_{12} of Content 1 and Content 2 are configured as follows.

$$\chi_{11} = \alpha_{11} + \chi_{111} + \chi_{112} + \chi_{113} + \chi_{114} + \beta_{11} \quad (35)$$

$$\chi_{12} = \alpha_{12} + \chi_{121} + \chi_{122} + \chi_{123} + \beta_{12} \quad (36)$$

$$\sigma_{11} = \alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{113} + \sigma_{114} + \beta_{11} \quad (37)$$

$$\sigma_{12} = \alpha_{12} + \sigma_{121} + \sigma_{122} + \sigma_{123} + \beta_{12} \quad (38)$$

(1) Author aID creates purchaser data $\boldsymbol{A_{dID}}$ using a purchaser ID (dID), and creates a change control signature $\boldsymbol{\sigma_{dID}}$ and a diversion control signature $\boldsymbol{\chi_{dID}}$ for the purchaser data $\boldsymbol{A_{dID}}$.

(2) **I.** Diversion aggregate signature χ_d is created using diversion control signature χ_{111} of actual data A_{111}, and diversion control signature χ_{dID} of purchaser data A_{dID}.

$$\chi_d = \chi_{111} + \chi_{dID} \quad (39)$$

II. Change aggregate signature σ_d is created using change control signature σ_{111} of actual data A_{111}, and change control signature σ_{dID} of purchaser data A_{dID}.

$$\sigma_d = \sigma_{111} + \sigma_{dID} \quad (40)$$

III. Disclose diversion aggregate signature χ_d, change aggregate signature σ_d, and purchaser data A_{dID} created above to the purchaser.

(3) The purchaser dID diverts empty data A_{122} to actual data A_{111}, adds empty data A_{123} to purchaser data A_{dID}, and performs the following steps.

I. Update of the Diversion Aggregate Signature.

Post-edit diversion aggregate signature $\chi_{12}{}'$ is created using diversion aggregate signature χ_d, diversion control signatures χ_{122}, χ_{123} of empty data A_{122}, A_{123}, and pre-edit diversion aggregate signature χ_{12}.

$$\begin{aligned}\chi_{12}' &= \chi_{12} + \chi_d - \chi_{122} - \chi_{123} \\ &= \boldsymbol{\alpha_{12} + \chi_{121} + \chi_{111} + \chi_{dID} + \beta_{12}}\end{aligned} \quad (41)$$

II. Update of the Change Aggregate Signature.

Post-edit change aggregate signature $\sigma_{12}{}'$ is created using change aggregate signature σ_d, change control signatures $\sigma_{122}, \sigma_{123}$ of empty data A_{122}, A_{123}, and pre-edit change aggregate signature σ_{12}.

$$\begin{aligned}\boldsymbol{\sigma_{12}'} &= \boldsymbol{\sigma_{12} + \sigma_d - \sigma_{122} - \sigma_{123}} \\ &= \boldsymbol{\alpha_{12} + \sigma_{121} + \sigma_{111} + \sigma_{dID} + \beta_{12}}\end{aligned} \quad (42)$$

3.4.3 Content Protection by Billing 1 (Composition Control)

In the description, content 1 is defined as the author's created content, and content 2 is defined as the composition target content using content 1 and content 2, as in 3.4.2. Here, it is assumed that pre-combination control signature δ_{12f} of start data

A_{120} of content 2 is released.

(1) Author aID creates purchaser data A_{dID} using a purchaser ID (dID), newly creates start data A_{130} and final data A_{132}, and creates content that is composed of partial content A_{130}, A_{dID}, A_{132} (A_{130}: start data, A_{dID}: purchaser data, A_{132}: Final data) and this is called content 3. In addition, the various control signatures are created in the same manner as discussed in 3.3, and aggregate signatures for various edit controls of content 3 are created.

(2) Content 1 and content 3 are composed using post-composition control signature δ_{11b} of content 1, and pre-composition control signature δ_{13f} of content 3 so it is in the order 1 → 3 to create composition content 1‐3. At the same time, structure data is created so it is in the order 1 → 3. Then, Author aID disclose post-composition control signature δ_{13b} of composition content 1–3 and content 3 to the purchaser.

(3) The purchaser dID uses the post-composition control signature δ_{13b} of the content 3 and the pre-composition control signature δ_{12f} of the content 2 to compose the content 3 side of the composition content 1-3 and the content 2.

By disclosing the signature to the purchaser as described above, the composition control signature of content 1 is not disclosed, but the composition control signature of content 3 composed of purchaser data A_{dID} is disclosed to the content of purchaser 1. It is possible to indirectly allow the composition of content 2. Further, because content 1–3 includes the purchaser data A_{dID}, when the purchaser tries to leak the composition control signature of content 3 received, the leakage source is identified from the purchaser data A_{dID} of the content 3. Therefore, it is possible to prevent intentional signature leakage by a malicious purchaser.

3.5 Content Protection by Billing 2

In billing method 1 described in 3.4, the author of the content must perform the above processing each time a purchaser appears. Therefore, if the number of purchasers increases, the author's burden is large. Therefore, assuming that the purchaser performs the processing in advance assuming that the third party is the one that collectively manages copyrights such as JASRAC, the third party performs the processing at the time of the billing correspondence. We propose a method of entrusting to an institution as billing method 2.

First, in order to entrust the billing correspondence to a third-party organization, the author of the content discloses signature for the billing correspondence to the third-party organization in advance. At this time, there is also a possibility that the signature leaked from a third-party organization, so that the measures should be taken at the same time. The mechanism of the billing correspondence for various edit controls in billing system 2 will be described below in 3.5.1 to 3.5.3.

Also, by making the signature disclose to the purchaser via a third-party organization as follows, while the burden on the author is reduced, it becomes possible to allow the purchaser to edit as in the case of billing system 1. However, purchaser data A_{eID}, in which the third-party organization ID (eID) is inserted into the header is aggregated in the aggregate signature disclosed to the third-party organization eID. In order to edit partial content when doing so, it is necessary to add purchaser data A_{eID}, and when the third party tries to leak the aggregate signature σ_e received, it is integrated with the partial content signature. The leak source is identified from purchaser data A_{eID}. Therefore, it is possible to prevent intentional signature leakage by malicious third parties.

In addition, to realize editing permission by any purchaser for a third-party organization, aggregate signature σ_e is configured in advance so that the third-party organization can add purchaser data A_{dID} for the purchaser dID. As a result, the third party can construct an aggregate signature σ_d that includes purchaser data A_{dID} using aggregate signature σ_e received from the author. Therefore, to edit partial content, it is necessary to add purchaser data A_{dID}. Thus, to leak aggregate signature σ_d received by the purchaser, it is necessary to pass purchaser data A_{dID} aggregated together with the partial content signature. Because the leak source is known, it is possible to prevent the intentional signature leak by a malicious purchaser.

3.5.1 Content Protection by Billing 2 (Change/Addition/Deletion)

Below is an algorithm for billing method 2 for various edit controls (change, addition, deletion).

Change Control. The charge correspondence in the change control will be described below, taking the case of changing actual data A_{111} to actual data A_{211} as an example. The change aggregate signature

σ_{11} of the content is configured as follows.

$$\sigma_{11} = \alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{113} + \sigma_{114} + \beta_{11} \quad (43)$$

(1) Author aID creates purchaser data $\boldsymbol{A_{eID}}$ using a third-party organization ID (eID), and creates a change control signature $\boldsymbol{\sigma_{eID}}$ for purchaser data $\boldsymbol{A_{eID}}$.

(2) Change aggregate signature σ_e is created using change control signature σ_{111} of actual data A_{111}, change control signature σ_{eID} of purchaser data A_{eID}, and change control signatures $\sigma_{113}, \sigma_{114}$ of empty data A_{113}, A_{114} that are used for the addition of purchaser data A_{eID}, A_{dID}. In addition, disclose σ_e to a third party with the purchaser data A_{eID}.

$$\sigma_e = \sigma_{111} + \sigma_{113} + \sigma_{114} - \sigma_{eID} \quad (44)$$

(3) Third-party organization eID creates purchaser data $\boldsymbol{A_{dID}}$ using purchaser ID (dID) and creates a change control signature $\boldsymbol{\sigma_{dID}}$ for purchaser data $\boldsymbol{A_{dID}}$.

(4) Change aggregate signature σ_d is created using change aggregate signature σ_e and change control signature σ_{dID} of purchaser data A_{dID}, and is disclosed to the purchaser together with purchaser data A_{eID}, A_{dID}.

$$\begin{aligned} \sigma_d &= \sigma_e - \sigma_{dID} \\ &= \sigma_{111} + \sigma_{113} + \sigma_{114} - \sigma_{eID} - \sigma_{dID} \end{aligned} \quad (45)$$

(5) The purchaser dID changes the actual data $\boldsymbol{A_{111}}$ to actual data $\boldsymbol{A_{211}}$, and adds empty data $\boldsymbol{A_{113}, A_{114}}$ to the purchaser data $\boldsymbol{A_{eID}, A_{dID}}$, and then adds the change aggregate signature $\boldsymbol{\sigma_d}$ and the actual data $\boldsymbol{A_{211}}$. Create a post-edit change aggregate signature $\boldsymbol{\sigma_{11}}'$ using the change control signature $\boldsymbol{\sigma_{211}}$ and the pre-edit change aggregate signature $\boldsymbol{\sigma_{11}}$.

$$\begin{aligned} \boldsymbol{\sigma_{11}}' &= \boldsymbol{\sigma_{11} - \sigma_d + \sigma_{211}} \\ &= \boldsymbol{\alpha_{11} + \sigma_{211} + \sigma_{112} + \sigma_{eID} + \sigma_{dID} + \beta_{11}} \end{aligned} \quad (46)$$

Addition Control. As described in 3.4.1, addition control is performed using a change control signature, and this can be realized by exposing the editing right of empty data instead of that of actual data in 3.5.1 "Change control".

Deletion Control. The billing correspondence in deletion control will be described below by taking actual data A_{111} as empty data A_{211} and deleting as an example. It is assumed that the content change aggregate signature σ_{11} and deletion aggregate signature τ_{11} are configured as follows.

$$\sigma_{11} = \alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{113} + \sigma_{114} + \beta_{11} \quad (47)$$

$$\tau_{11} = \alpha_{11} + \tau_{111} + \tau_{112} + \tau_{113} + \tau_{114} + \beta_{11} \quad (48)$$

(1) Author aID creates a purchaser data $\boldsymbol{A_{eID}}$ using a third-party organization ID (eID), and creates a change control signature $\boldsymbol{\sigma_{eID}}$ and a deletion control signature $\boldsymbol{\tau_{eID}}$ for the purchaser data $\boldsymbol{A_{eID}}$.

(2) **I.** A deletion aggregate signature τ_e is created using the deletion control signature τ_{111} of actual data A_{111}, the deletion control signature τ_{eID} of purchaser data A_{eID}, and the deletion control signatures τ_{113}, τ_{114} of the empty data A_{113}, A_{114} that is used for the addition of the purchaser data A_{eID}, A_{dID}.

$$\tau_e = \tau_{111} + \tau_{113} + \tau_{114} - \tau_{eID} \quad (49)$$

II. The change aggregate signature, σ_e, is created using change control signature σ_{eID} of purchaser data A_{eID}, and change control signature $\sigma_{113}, \sigma_{114}$ of empty data A_{113}, A_{114} for adding purchaser data A_{eID}, A_{dID}.

$$\sigma_e = \sigma_{113} + \sigma_{114} - \sigma_{eID} \quad (50)$$

III. The deletion aggregate signature τ_e, the change aggregate signature σ_e and the purchaser data A_{eID} created above are disclosed to a third-party organization.

(3) Third-party organization eID creates purchaser data A_{dID} using purchaser ID (dID), and creates change control signature σ_{dID} and deletion control signature τ_{dID} for purchaser data A_{dID}.

(4) **I. Update of Deletion Control Signature.**
A deletion aggregate signature τ_d is created using deletion aggregate signature τ_e and deletion control signature τ_{dID} of purchaser data A_{dID}.

$$\begin{aligned} \tau_d &= \tau_e - \tau_{dID} \\ &= \tau_{111} + \tau_{113} + \tau_{114} - \tau_{eID} - \tau_{dID} \end{aligned} \quad (51)$$

II. Update of Change Control Signature.
A change aggregate signature σ_d is created using the change aggregate signature σ_e and change control signature σ_{dID} of the purchaser data A_{dID}.

$$\begin{aligned} \sigma_d &= \sigma_e - \sigma_{dID} \\ &= \sigma_{113} + \sigma_{114} - \sigma_{eID} - \sigma_{dID} \end{aligned} \quad (52)$$

III. The deletion of aggregate signature $\boldsymbol{\tau_d}$, the change aggregate signature $\boldsymbol{\sigma_d}$, and the

purchaser data $\boldsymbol{A_{eID}, A_{dID}}$ created above are disclosed to the purchaser.

(5) The purchaser dID deletes actual data A_{111} by changing it to empty data A_{211}, adds the empty data A_{113}, A_{114} by changing it to the purchaser data A_{eID}, A_{dID}, and performs the following steps.

I. Update of Deletion Aggregate Signature.

A post-edit deletion aggregate signature $\tau_{11}{}'$ is created using the deletion aggregate signature τ_d, the deletion control signature τ_{211} of empty data A_{211}, and the pre-edit deletion aggregate signature τ_{11}.

$$\begin{aligned}\boldsymbol{\tau'_{11}} &= \boldsymbol{\tau_{11} - \tau_d + \tau_{211}} \\ &= \boldsymbol{\alpha_{11} + \tau_{211} + \tau_{112} + \tau_{eID} + \tau_{dID} + \beta_{11}}\end{aligned} \quad (53)$$

II. Update of change aggregate signature.

A post-edit change aggregate signature $\sigma_{11}{}'$ is created using the change aggregate signature σ_d and the pre-edit change aggregate signature σ_{11}.

$$\begin{aligned}\sigma'_{11} &= \sigma_{11} - \sigma_d \\ &= \alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{eID} + \sigma_{dID} + \beta_{11}\end{aligned} \quad (54)$$

3.5.2 Content Protection by Billing 2 (Diversion Control)

In the explanation, content 2 similar to 3.4.2 is newly defined and used as the content 2 of the diversion destination. Here, content 2 of the diverted destination is content composed of partial content $A_{120} \sim A_{125}$ (A_{120}: start data; A_{121}: actual data; $A_{122}, A_{123}, A_{124}$ empty data, and A_{125}: final data). The diverted destination is empty It is assumed that diversion control signatures $\chi_{122}, \chi_{123}, \chi_{124}$ and the change control signatures $\sigma_{122}, \sigma_{123}, \sigma_{124}$ of data $A_{122}, A_{123}, A_{124}$ are disclosed. The billing correspondence in diversion control will be described below, taking the case where actual data A_{111} of content 1 is added to empty data A_{122} of content 2, and diverted. It is assumed that diversion aggregate signatures χ_{11}, χ_{12} and change aggregate signatures σ_{11}, σ_{12} of contents 1 and 2 are configured as follows.

$$\chi_{11} = \alpha_{11} + \chi_{111} + \chi_{112} + \chi_{113} + \chi_{114} + \beta_{11} \quad (55)$$

$$\chi_{12} = \alpha_{12} + \chi_{121} + \chi_{122} + \chi_{123} + \chi_{124} + \beta_{12} \quad (56)$$

$$\sigma_{11} = \alpha_{11} + \sigma_{111} + \sigma_{112} + \sigma_{113} + \sigma_{114} + \beta_{11} \quad (57)$$

$$\sigma_{12} = \alpha_{12} + \sigma_{121} + \sigma_{122} + \sigma_{123} + \sigma_{124} + \beta_{12} \quad (58)$$

(1) Author aID creates a purchaser data $\boldsymbol{A_{eID}}$ using a third-party organization ID (eID), and creates change control signature $\boldsymbol{\sigma_{eID}}$ and diversion control signature $\boldsymbol{\chi_{eID}}$ for purchaser data $\boldsymbol{A_{eID}}$.

(2) **I.** Diversion control signature χ_{eID} of purchaser data A_{eID} and diversion control signature χ_{111} of actual data A_{111} are used to create diversion aggregate signature χ_e.

$$\chi_e = \chi_{111} + \chi_{eID} \quad (59)$$

II. A change aggregate signature $\boldsymbol{\sigma_e}$ is created using a change control signature $\boldsymbol{\sigma_{eID}}$ of purchaser data $\boldsymbol{A_{eID}}$, and change control signature $\boldsymbol{\sigma_{111}}$ of actual data $\boldsymbol{A_{111}}$.

$$\sigma_e = \sigma_{111} + \sigma_{eID} \quad (60)$$

III. change aggregate signature $\boldsymbol{\sigma_e}$ and the purchaser data $\boldsymbol{A_{eID}}$ created above are disclosed to a third-party organization.

(3) Third-party organization eID creates purchaser data A_{dID} using purchaser ID (dID), and creates a change control signature σ_{dID}, and diversion control signature χ_{dID} for data purchaser A_{dID}.

(4) **I. Update of Diversion Control Signature.**

A diversion aggregate signature χ_d is created using diversion aggregate signature χ_e and diversion control signature χ_{dID} of purchaser data A_{dID}.

$$\begin{aligned}\chi_d &= \chi_e + \chi_{dID} \\ &= \chi_{111} + \chi_{eID} + \chi_{dID}\end{aligned} \quad (61)$$

II. Update of Change Control Signature

A change aggregate signature σ_d is created using the change aggregate signature σ_e and the change control signature σ_{dID} of the purchaser data A_{dID}.

$$\begin{aligned}\sigma_d &= \sigma_e + \sigma_{dID} \\ &= \sigma_{111} + \sigma_{eID} + \sigma_{dID}\end{aligned} \quad (62)$$

III. The diversion aggregate signature χ_d, the change aggregate signature σ_d, and the purchaser data A_{eID}, A_{dID} created above are disclosed to the purchaser.

(5) The purchaser dID diverts empty data A_{122} to actual data A_{111}, adds empty data A_{123}, A_{124} to purchaser data A_{eID}, A_{dID}, and performs the following:

I. Update of the Diversion Aggregate Signature.

After editing using the diversion aggregate signature χ_d, the empty data for adding content 2 $A_{122}, A_{123}, A_{124}$ is diverted to control signature $\chi_{122}, \chi_{123}, \chi_{124}$ and the pre-edit diversion aggregate signature χ_{12} to create the post-edit diversion aggregate signature $\chi_{12}{}'$.

$$\chi_{12}' = \chi_{12} + \chi_d - \chi_{122} - \chi_{123} - \chi_{124} = \alpha_{12} + \chi_{121} + \chi_{111} + \chi_{eID} + \chi_{dID} + \beta_{12} \quad (63)$$

II. Update of the Change Aggregate Signature.

Before editing, after change aggregate signature σ_d, change control signatures $\sigma_{122}, \sigma_{123}, \sigma_{124}$ of the empty data $A_{122}, A_{123}, A_{124}$ for addition of content 2 and the change aggregate signature σ_{12}, create the change aggregate signature σ_{12}'.

$$\sigma_{12}' = \sigma_{12} + \sigma_d - \sigma_{122} - \sigma_{123} - \sigma_{124} = \alpha_{12} + \sigma_{121} + \sigma_{111} + \sigma_{eID} + \sigma_{dID} + \beta_{12} \quad (64)$$

3.5.3 Content Protection by Billing 2 (Composition Control)

In the description, Content 1 is defined as the author's created content, and Content 2 is defined as the composition target content using Content 1 and Content 2 as in 3.4.3. Here, it is assumed that the composition control signature δ_{12f} of the start data A_{120} of content 2 is disclosed.

(1) Author aID creates purchaser data A_{eID} using a third-party organization ID (eID), and is composed of partial contents $A_{130}, A_{131}, A_{eID}, A_{133}$ (A_{130}: start data; A_{131}: empty data; A_{eID}: Purchaser data (eID), A_{133}: Final data). Furthermore, in the same manner as in Section 3.3.2, various control signatures for each partial content, and various aggregate signatures for content 3 was obtained by aggregating them.

(2) Composition content 1 and content 3 using the post-composition control signature δ_{11b} of content 1 and the pre-composition control signature δ_{13f} of content 3 so it is on the order of 1 → 3 to create the composed content 1–3 After that, the post- composition control signature δ_{13b} of the composited content 1–3, and content 3 and change control signature σ_{131} of empty data A_{131} of content 3 are disclosed to a third-party organization.

(3) Third-party organization eID creates purchaser data A_{dID} using a purchaser ID (dID), and creates change control signature σ_{dID} for the purchaser data A_{dID}. Then, using the change control signature σ_{131} of the empty data A_{131} and the change control signature σ_{dID} of the purchaser data A_{dID}, the change aggregate signature $\sigma_{13} = \alpha_{13} + \sigma_{131} + \sigma_{eID} + \beta_{13}$ before editing is updated. Therefore, the post-edit change aggregate signature σ_{13}' is created by adding the purchaser data A_{dID} to the content 3.Then, post composition control signature δ_{13b} of composition content 1–3 and content 3 is disclosed to the purchaser.

$$\sigma_{13}' = \sigma_{13} + \sigma_{dID} - \sigma_{131} = \alpha_{13} + \sigma_{dID} + \sigma_{eID} + \beta_{13} \quad (65)$$

(4) The purchaser dID combines the content 3 part of the composition content 1–3 with content 2 using post-composition control signature δ_{13b} of content 3 and precomposition control signature δ_{12f} of the content 2.

By disclosing the signature to the purchaser as described above, while reducing the burden on the author, it is possible to indirectly permit the composition of content 1 by disclosing the composite control signature of the content 3 composed of the purchaser data. Furthermore, because composition content 1–3 includes purchaser data A_{eID}, when the third party tries to leak the composition control signature of the content 3 received, the leak source of content 3 from the purchaser data A_{eID} is revealed. Therefore, it is possible to prevent intentional signature leakage by malicious third parties.

4 CONCLUSION

In this method, for content for which the author has prohibited editing, when an editor wants to have permission to edit the content appears, billing is performed as a content control method to allow the purchaser editing permission through a financial transaction. We proposed two response methods. The first was a method to correspond to billing between the author and the purchaser, but with the above proposal method, if the number of purchasers increase, the burden on the author would increase. The second problem is that a third party is assumed based on the measures taken when the burden of the author is considered to be a problem, and the author-third-party purchaser. However, even in the proposed method, copyright management is concentrated in one place, which leads to problems such as high risk when assuming an attacker. In the future, considering the proxy signature (Boldyreva et al., 2012, Xu et al., 2005) etc. to address the above problems, we will decentralize the agencies that billing correspondence and reduce the risk of attacks, etc. Additionally, we would like to perform research on technology.

REFERENCES

"YouTube"https://www.youtube.com/2019/04/19 6:50

"Nico Nico Douga" http://www.nicovideo.jp/2019/04/19 6:50

Katsuma Koga, Masaki Inamura, Kitahiro Kaneda and Keiichi Iwamura: "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, July 2015*.

Tatsuya Fujimoto, Keiichi Iwamura and Masaki Inamura: "Content Protection Scheme to Realize Edit Control Including Diversion Control and Composition Control," *ICETE 13th International Conference on e-Business (ICE-B 2016), pp.116-122, Lisbon, Portugal, 26-28 July, 2016*.

Keiichi Iwamura, Tatsuya Fujimoto "Content protection technology realizes inheriting copyright setting based on ID based signature" *Tokyo University of Science master's thesis, 2016*.

Boneh D., Lynn B., Shacham H. (2001) Short Signatures from the Weil Pairing. In: Boyd C. (eds) Advances in Cryptology — ASIACRYPT 2001. *ASIACRYPT 2001. Lecture Notes in Computer Science, vol 2248. Springer, Berlin, Heidelberg*.

Boneh D., Gentry C., Lynn B., Shacham H. (2003) Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Biham E. (eds) Advances in Cryptology — EUROCRYPT 2003. *EUROCRYPT 2003. Lecture Notes in Computer Science, vol 2656. Springer, Berlin, Heidelberg*.

Xun, Y., "An identity-based signature method from the Weil pairing" *IEEE Communications Letters, 2003, vol. 7, no. 2, p. 76-78*.

Jing, X., Zhenfeng, Z., Dengguo, F., "ID-based aggregate signatures from bilinear pairing" *CANS, 2005, vol. LNCS3810, p. 110-119*.

"JASRAC" https://www.jasrac.or.jp/

Boldyreva, A., Palacio, A. & Warinschi, B. J Cryptol (2012) 25: 57. https://doi.org/10.1007/s00145-010-9082-x

Mitsunari Shigeo "Applied cryptography for the Cloud." Shuwa System, 2015. 240 pp. ISBN-10: 479804413X, ISBN-13: 978-4798044132.

Xu J., Zhang Z., Feng D. (2005) ID-Based Proxy Signature Using Bilinear Pairings. In: Chen G., Pan Y., Guo M., Lu J. (eds) Parallel and Distributed Processing and Applications - ISPA 2005 Workshops. ISPA 2005. *Lecture Notes in Computer Science, vol 3759. Springer, Berlin, Heidelberg*.

Masaki Inamura, Keiichi Iwamura "An Expression of a Quotation Process in Contents with a New Tree-structure Aggregate Signature Scheme" *IPSJ Journal Vol.53 No.9 2267-2278 (Sep. 2012)*.

Naoto Yanai, Tomoya Iwasaki, Masaki Inamura, Keiichi Iwamura "Provably Secure Structured Signature Schemes with Tighter Reductions" *IEICE TRANS FUNDAMENTALS, vol. E100-A, NO.9 September 2017*.