A Content Protection Method That Allows Commissioning of Editing Control Processing to a Third Party using a Proxy Signature

Tomohiro Kobayashi[1], Keiichi Iwamura[1] and Masaki Inamura[1,2]
[1]*Graduate School of Engineering, Tokyo University of Science, 6-3-1 Niijuku, Katsushikaku, 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, Proxy Signature, Billing.

Abstract: In consumer-generated media (CGM), 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 (K. Koga et al., 2015, T. Fujimoto et al., 2016) has been proposed that controls editing using digital signatures. We propose a method in which the author can securely provide individual editing permissions for content that has been editing-prohibited. 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

In recent years, it has become easier to generate and transmit content in the modern society where the Internet has developed. The distribution of content by general users has become popular, and this content is called User Generated Content (UGC). In UGC (YouTube, etc.), with the spread of content distribution services, new content is generated by secondary use of the published content. This creates content circulation by creating better content for viewers. In such an environment, copyright protection technology that protects the rights of authors without hindering the distribution of content is essential. In addition, technology that guarantees the copyright of the original content after secondary use is also required.

A copyright protection method suitable for UGC has been proposed (K. Koga et al., 2015, T. Fujimoto et al., 2016). In case of former, a content protection scheme using a Boneh-Lynn-Shacham (BLS) signature method (Boneh et al., 2001, Boneh et al., 2003) to achieve both editing control and rights inheritance has been proposed. Also, in case of later, we realized the composition control by the editor, which was the problem in (K. Koga et al., 2015). In addition, by using the ID-based signature method (Xun, 2003, Jing et al., 2005), a public key certificate is not required, and the work of verifying the signature of a content composed by many authors and editors has been reduced. As a result, the rights of authors once set to prohibit editing are protected without further editing.

In (T. Kobayashi et al., 2019), a content protection method has been proposed that implements the purchase and sale of content editing rights (supports billing) through financial transactions. In addition, an organization (third party) involved in buying and selling content has been newly established in order to reduce the time and effort required for authors to transfer editing rights. Therefore, we propose a method to outsource the processing related to billing on behalf of the author. As a result, it is possible to buy and sell editing rights for content for which editing is prohibited, which was not realized in the conventional method.

However, in (T. Kobayashi et al., 2019), the trouble of creating the signature of the content of the author is still significant problem. Therefore, in this paper, the Proxy signature scheme (Francesco et al., 2016) is newly adopted as the signature scheme. The purpose of this scheme is to further reduce the work of the author by entrusting the creation of the author's signature to a copyright protection organization (a third-party organization in the conventional method).

Kobayashi, T., Iwamura, K. and Inamura, M.
A Content Protection Method That Allows Commissioning of Editing Control Processing to a Third Party using a Proxy Signature.
DOI: 10.5220/0009871800980109
In *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020) - Volume 3: ICE-B*, pages 98-109
ISBN: 978-989-758-447-3

This paper is structured as follows: Chapter 2 describes the prerequisite knowledge and previous research that forms the basis of this method; Chapter 3 describes the proposed method and the algorithm; Chapter 4 describes conclusion.

2 RELATED WORK

In this section, we describe the previous research used in this method and the conventional method we have proposed.

2.1 Aggregate Signature based on ID-based Signature Scheme

In the ID-based signature method, a key is generated from an author ID indicating the author information newly set for each author. Therefore, there is no need to issue a public key certificate for signature verification. It uses a pairing function with hyperbolic characteristics on an elliptic curve. The algorithm of the ID-based aggregate signature that can aggregate multiple generated signatures into one signature is shown in (N. Yanai et al., 2017).

2.2 Proxy Signature

The Proxy signature method allows the signature authority to be transferred to a person called the Proxy signer without sharing the signature key itself. Most Proxy signatures use bilinear pairing of elliptic curve groups to satisfy identity-based properties. An example of the Proxy signature algorithm using ID-based signature is shown in (Francesco et al., 2016).

2.3 Editing Control using Digital Signature

A technology for controlling the secondary use of content using the BLS signature scheme (Boneh et al., 2001, Boneh et al., 2003) as follows is proposed in (K. Koga et al., 2015). The author divides the content into multiple partial content and pre-generates a digital signature (hereinafter referred to as an edit control signature) indicating whether editing is possible for each partial content. Then, the edit control signature is aggregated into one signature (hereinafter, aggregate signature), and the aggregate signature is made public for each content. The edit control signature of the partial content that is allowed to be edited is made public and deleted from the aggregate signature so that it can be replaced, and the edit control signature of the partial content that cannot be edited is kept confidential and cannot be replaced. This allows the author to control in advance whether editing is possible. In addition, the control data that is not displayed is set as empty data and the displayed data is set as actual data. This makes it possible to control addition (change from empty data to actual data) and deletion (change from actual data to empty data). The content playback device has a signature verification function: it always performs signature verification before playback, and if it does not have a valid digital signature or whose digital signature does not match, does not play content that as unauthorized content.

A content management station that verifies the originality of each partial content and issues a digital signature (hereinafter referred to as a management station signature) that authorizes the author is established. It is mandatory to set the management station signature for each partial content. As a result, each partial content is associated with its author (the content management authority associates the partial content with its author like a certification authority in PKI), and the author is not deceived in units of partial content (partial content without a management station signature is illegal). Only authors can set it as editable (the published edit control signature is always verified with the author's key specified by the management station signature). This prohibits editing that is not allowed by the author. However, after editing the partial content set to be editable, the editor can make it impossible to edit it further, including other partial content. For example, if the partial contents A and B are editable, the editor changes A to A ' and replaces it with a new signature, keeping both signatures private. As a result, the content can be made uneditable in both A and B thereafter. The uneditable partial content is checked with the key of the editor (hereinafter, bID) that is set to be uneditable. In other words, even if the author cannot edit the partial content at positions A and B, the editor can change the setting according to the editing circumstances.

Diversion control is realized by the same mechanism as above, using the content ID described later. However, even if the editor who diverts and uses the partial content that can be diverted makes it impossible to divert it after the diversion, there is no effect on the edited work. This is because changing the settings by the editor is meaningless as the original content has its diversion control signature published. Therefore, the applicability of the partial content can be determined only by the author (hereinafter aID) of the partial content. Therefore, since the diversion control signature is always checked with the aID key, the editor cannot change the setting.

The authors of the content (hereinafter cID) only can decide whether to perform composition control or not. Therefore, after the editor combines the contents a and b that can be combined, the combination of a and b is indispensable in the story; if you do not want to change it as one work, it cannot be realized.

In (T. Fujimoto et al., 2016), inheritance control is realized. A new signature is introduced that controls the change of copyright settings (hereinafter, setting control signature) to control inheritance. However, whether or not the inheritance is determined by the author who created the content, the signature is verified using the cID key. The cID is specified from the content ID. The content ID is the ID set by the cID, and only one content ID is set for the content. When the partial content is diverted, then the content is set with multiple content IDs. Since the start and end position signatures included in the aggregated signature are always private and are verified using the cID key, if the content ID is falsified, the signature will not match. In addition, whether or not editing is possible is controlled not only by publishing/unpublishing the edit control signature but also by control parameters. Therefore, the setting control signature includes parameters related to the controllability (p_s for setting, p_c for change, p_d for deletion, p_m for diversion, p_b for composition) in the hash value as follows:

$$h_{ijk} = H(IC_{ij} \parallel I_{ijk} \parallel H(A^*_{ijk}) \parallel p_s \parallel p_c \parallel p_d \parallel p_m \parallel p_b \parallel r) \quad (1)$$

Therefore, if $p_s = 1$ is set (inherited), after verifying the signature, the settings related to the editing of each partial content are checked; if the settings are different from the settings of the setting control signature, the contents are invalid. If $p_s = 0$, the settings for each edit are not verified.

2.4 Content and Partial Content and Aggregate Signature Structure

In (T. Fujimoto et al., 2016), Partial content is roughly divided into actual data and control data. Actual data is treated as the data displayed as content, and control data is treated as the data not displayed. The control data includes the start data indicating the beginning of the content, final data indicating the end, and empty data required to control addition / deletion. The content consists of start data, final data, and one or more partial contents created by the author. Also, as the author information, a content ID is set for the content, and a partial content ID is set for the partial content. As a result, in addition to addition / deletion / change control for each partial content within one content, it also controls the diversion of the partial content and the composition of the content.

2.4.1 Content Tree Structure

As mentioned above, an author ID is set for a content as author information. When an author creates a content A_{ij}, IC_{ij} is set as a content ID. When the content A_{ij} has m pieces of partial contents $A_{ij1} \sim A_{ijm}$, A_{ij0} is set as start data, A_{ijm+1} is set as final data, and $I_{ij0} \sim I_{ijm+1}$ are set as the content ID. ID_{ij} represents the positional relationship between the authors of the content. Considering the positional relationship shown in Fig. 1 as an example, the contents $A_{11} \sim A_{16}$ are the primary contents created by the authors $ID_{11} \sim ID_{16}$, respectively. The authors ID_{21}, ID_{22} combine the contents A_{21}, A_{22} with the primary contents to create secondary contents, and the author ID_{31} combines the secondary contents to create the tertiary contents A_{31}.

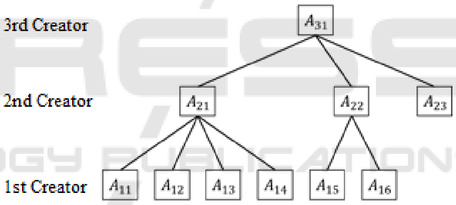

Figure 1: Content tree structure.

3 PROPOSED METHOD

In this section, the method proposed in this paper is described.

3.1 System Configuration

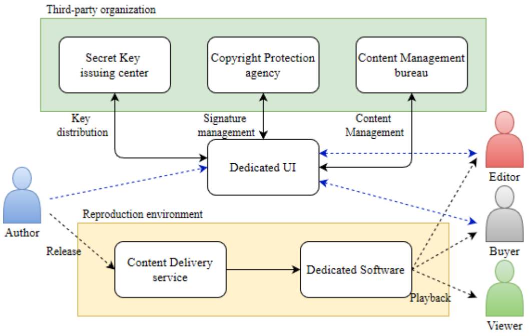

Figure 2: System configuration.

The following definitions describe a person, an institution, and the system constituting the present system configuration:

- Author (A)
  The person who creates the original content.
- Editor (E)
  The person who edits the content that is allowed to be edited in the distributed content.
- Buyer (B)
  A person who edits the content that is prohibited for editing but is compatible with billing in the distributed content.
- Viewer (V)
  People who watch the distributed content.
- Secret Key issuing center (SK)
  A trusted organization that issues and manages secure keys when using public key cryptography.
- Copyright Protection agency (CP)
  A reliable organization that manages the billing for content on behalf of the author in the proposed method.
- Content Management bureau (CM)
  A trusted organization that verifies the originality of each piece of content. The management station signature for partial content is created only when the originality of each piece of content can be confirmed.
- Dedicated UI (UI)
  A user interface that executes the necessary algorithms to implement the proposed method.
- Content Delivery service (CD)
  Service to distribute the created content.
- Dedicated Software (SO)
  A software to verify the signatures when playing the content.
- Administration Bureau (AB)
  A reliable organization that manages the dedicated UI and dedicated software.

3.2 Various Editing Controls

In the proposed method, the following editing controls are performed:

[Change]
The control related to content change is the change from real data to actual data, and this control is performed using the change control signature.

[Addition]
The control for adding content is a change from empty data to actual data, and this control is performed using the change control signature.

[Deletion]
The control for deleting content is a change from real data to empty data. However, in order to realize the control such as {changeable / non-deletable}, {non-changeable / deletable}, this control is performed using the deletion control signature.

[Diversion]
The control on the diversion of content indicates that the partial content in one content is diverted to another content, and this control is performed using the diversion control signature.

[Composition]
The control for compositing content indicates that one content is composited with another content, and this control is performed using a composition control signature.

[Inheritance]
This control introduces a new signature that controls the change of copyright settings (hereinafter, setting control signature) to control inheritance. Only the creator of the original content can create the setting control signature; the secondary and subsequent editors cannot change it. In addition, the setting control signature is verified using the hash value of the original partial content, and hence, it is necessary to link the hash value of the original content to the header portion of the edited partial content in advance.

3.3 Protocol of the Proposed Scheme

In the proposed method, the billing for the purchaser in the conventional method (T. Kobayashi et al., 2019) is entrusted to a third party using a Proxy signature to reduce the processing load on the author. Therefore, an editing control method suitable for the Proxy signature method is required. The specific editing control algorithm is described below.

3.3.1 Pre-processing

(1) Key Generation (A)(E)(B)⇔(SK)
The user ID_{ij} that generates the signature registers personal information using a dedicated UI. This is followed by applying to the private key issuing center to create a public key pair for the set ID. The secret key issuing center selects $g \in G_1$ as a generator, selects a random number $s \in Z_p^*$, calculates a public key $Q_{ij} = H_1(ID_{ij})$ from ID_{ij}, and substitutes $d_{ij} = sQ_{ij}$ with the signature key of the author ID_{ij} (secret key). The secret key issuing center publishes $g_{pub} = sg$. Here, s is the master secret key, which is secretly managed by the secret key issuing center.

(2) Proxy Key Generation (A)⇔(CP)

The author ID_{ij} entrusts the signature authority using a Proxy signature to a copyright protection agency using a dedicated UI. The proxy key generation protocol is shown below.

① Creating a Warrant (A)

The author ID_{ij} delegates his signing authority through a warrant w signed by the Copyright Protection agency $\mathrm{ID_{CP}}$. The warrant w contains information such as the ID of the author, the ID of the Copyright Protection agency, the time of the delegation, the validity of the period, and the nature of the signable message.

② Generating Delegation Values (A)

The author ID_{ij} randomly chooses $x_{ij} \in \mathbb{Z}_q^*$ and calculates:

$$S_{ij} = x_{ij} Q_{ij} \in G_1 \tag{2}$$

$$h_2 = H_2(w, S_{ij}) \in Z_q^* \tag{3}$$

$$T_{ij} = \left(x_{ij} + h_2\right) d_{ij} \in G_1 \tag{4}$$

The original signer O then sends $D = (w, S_{ij}, T_{ij})$ to the Proxy signer over a secure channel with T_{ij} as the delegated value.

③ Validation of Delegation Values (CP)

When the copyright protection agency receives the delegation value T_{ij} of the warrant w, it calculates the following and verifies that the equation holds.

$$\mathrm{Q_{ij}} = H_1(ID_{ij}) \tag{5}$$

$$h_2 = H_2(w, S_{ij}) \in Z_q^* \tag{6}$$

$$e\left(T_{ij}, g\right) = e(S_{ij} + h_2 Q_{ij}, g_{pub}) \tag{7}$$

If not, a new delegation value is requested or the protocol is terminated.

④ Proxy Key Generation

If the verification is successful, the Copyright Protection agency $\mathrm{ID_{CP}}$ generates a proxy signing key by calculating the following.

$$d_{P_{ij}} = T_{ij} + h_2 d_{CP} \tag{8}$$

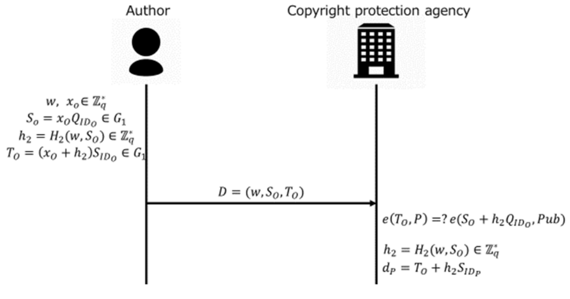
Author
Copyright protection agency
$w,\ x_o \in \mathbb{Z}_q^*$
$S_o = x_O Q_{ID_O} \in G_1$
$h_2 = H_2(w, S_O) \in \mathbb{Z}_q^*$
$T_O = (x_O + h_2) S_{ID_O} \in G_1$
$D = (w, S_O, T_O)$
$e(T_O, P) =? \, e(S_O + h_2 Q_{ID_O}, Pub)$
$h_2 = H_2(w, S_O) \in \mathbb{Z}_q^*$
$d_P = T_O + h_2 S_{ID_P}$

Figure 3: Proxy key generation protocol.

3.3.2 When Creating Original Content

① Decomposition into Partial Contents (A)

The author $\mathrm{ID_{ij}}$ decomposes the content created by them into a desired unit for editing control using a dedicated UI.

② Applying to Content Management Bureau

The author $\mathrm{ID_{ij}}$ asks the Content Management Bureau to check the originality of the partial content divided in ① and receives the signature of the Management Bureau.

③ Creating Start and End Data

Control data A_{ij0}^*, A_{ijm+1}^* is created to be added to the beginning and end of the content.

$$\begin{cases} A_{ij0}^* = IC_{ij} || I_{ij0} || \, d \\ A_{ijm+1}^* = IC_{ij} || I_{ijm+1} || \, d \end{cases} \tag{9}$$

$$\begin{cases} h_{ij0} = H(IC_{ij} || I_{ij0} || \, H(A_{ij0}^*) \parallel r) \\ h_{ijm+1} = H(IC_{ij} || I_{ijm+1} || \, H(A_{ijm+1}^*) \parallel r) \end{cases} \tag{10}$$

④ Editing Control Settings

The author $\mathrm{ID_{ij}}$ sets various edits (change, delete, divert, inherit) for each partial content divided in ①. Here, for the start data and the final data, various edits are set to be prohibited. In addition, whether composition control is possible or not is set.

⑤ Creating Control Data

Create control data A_{ijk}^* based on the partial content A_{ijk} (d for empty data).

⑥ Creating a Hash Value

The author $\mathrm{ID_{ij}}$ generates a hash value for each editing control of each partial content divided in ① using the dedicated UI. Here, $p = 1$ when editing is permitted, and $p = 0$ when editing is prohibited; r is a constant that changes for each edit: change: rc, delete: rd, diversion: rm, configuration: rs, and composition: rb.

Change / Delete / Divert:

$$h_{ijk} = H\left(IC_{ij} \parallel I_{ijk} \parallel H\left(A_{ijk}{}^*\right) \parallel p \parallel r\right) \tag{11}$$

Configuration:

$$\begin{aligned} h_{ijk} = H\big(IC_{ij} \parallel I_{ijk} \parallel H\left(A_{ijk}{}^*\right) \parallel p_s \parallel p_c \\ \parallel p_d \parallel p_m \parallel p_b \parallel \mathrm{p_p} \parallel r\big) \end{aligned} \tag{12}$$

($\mathrm{p_s}$: configuration, $\mathrm{p_c}$: change, $\mathrm{p_d}$: delete, $\mathrm{p_m}$: diversion, $\mathrm{p_b}$: composition, $\mathrm{p_p}$: billing)

Composition:

Pre-composition:

$$h_{ijf} = H\left(IC_{ij} \parallel I_{ij0} \parallel H\left(A_{ij0}{}^*\right) \parallel p \parallel r\right) \tag{13}$$

Post-composition

$$h_{ijb} = H\left(IC_{ij} \parallel I_{ijm+1} \parallel H\left(A_{ijm+1}{}^{*}\right) \parallel p \parallel r\right) \qquad (14)$$

⑦ Outsourcing the signature creation

The edit control settings and hash values of the various partial contents are sent to the copyright protection agency.

3.3.3 Signature Generation

①Creating Start and End Position Signatures (R)

α_{ij} and β_{ij} are created for each of change, deletion, and diversion. Here, r_{ij0} , r_{ijm+1} are random numbers generated by the copyright protection agency.

$$\begin{cases} \alpha_{ij} = (r_{ij0} + h_{ij0})d_{p_{ij}}, U_{ij0} = r_{ij0}g \\ \beta_{ij} = (r_{ijm+1} + h_{ijm+1})d_{p_{ij}}, U_{ijm+1} = r_{ijm+1}g \end{cases} \qquad (15)$$

② Creating an Edit Control Signature

The copyright protection agency calculates various editing control signatures for each partial content using the proxy key based on the received hash value as follows. Here, the random number r_{ijk} is different for each edit.

Change control signature:

$$\sigma_{ijk} = \left(r_{ijk} + h_{ijk}\right)d_{p_{ij}}, U_{ijk} = r_{ijk}g \qquad (16)$$

Delete control signature:

$$\tau_{ijk} = \left(r_{ijk} + h_{ijk}\right)d_{p_{ij}}, U_{ijk} = r_{ijk}g \qquad (17)$$

Diversion control signature:

$$\chi_{ijk} = \left(r_{ijk} + h_{ijk}\right)d_{p_{ij}}, U_{ijk} = r_{ijk}g \qquad (18)$$

Configuration control signature:

$$\omega_{ijk} = \left(r_{ijk} + h_{ijk}\right)d_{p_{ij}}, U_{ijk} = r_{ijk}g \qquad (19)$$

Pre-composition control signature:

$$\delta_{ijf} = \left(r_{ijf} + h_{ijf}\right)d_{p_{ij}}, U_{ijf} = r_{ijf}g \qquad (20)$$

Post-composition control signature:

$$\delta_{ijb} = \left(r_{ijb} + h_{ijb}\right)d_{p_{ij}}, U_{ijb} = r_{ijb}g \qquad (21)$$

③ Aggregate Signature for Content

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

Change aggregate signature:

$$\sigma_{ij} = \alpha_{ij} + \sum \sigma_{ijk} + \beta_{ij}, \quad U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1} \qquad (22)$$

Delete aggregate signature:

$$\tau_{ij} = \alpha_{ij} + \sum \tau_{ijk} + \beta_{ij}, \quad U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1} \qquad (23)$$

Diversion aggregate signature:

$$\chi_{ij} = \alpha_{ij} + \sum \chi_{ijk} + \beta_{ij}, \quad U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1} \qquad (24)$$

Configuration aggregate signature:

$$\omega_{ij} = \alpha_{ij} + \sum \omega_{ijk} + \beta_{ij}, \quad U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1} \qquad (25)$$

Composition aggregate signature:

$$\delta_{ij} = \alpha_{ij} + \delta_{ijf} + \delta_{ijb} + \beta_{ij}, U_{ij0}, U_{ijm+1}, U_{ijf}, U_{ijb} \qquad (26)$$

④ Signature Management

The copyright protection agency sends only the created signature and the individual signature of the part that the author can edit to the author and keeps the created signature secure.

3.3.4 Linking to Content

① Signature Verification (A)

After receiving the signature, the author ID_{ij} calculates whether the aggregate signature of the various edit controls is valid to confirm the validity of the various edit control signatures and verifies that the verification formula holds.

Change:

$$e\left(\sigma_{ij}, g\right) = \prod e\left(S_{ij} + h_2\left(Q_{ij} + Q_{CP}\right), U_{ijk} + h_{ijk}g_{pub}\right) \qquad (27)$$

Delete:

$$e\left(\tau_{ij}, g\right) = \prod e\left(S_{ij} + h_2\left(Q_{ij} + Q_{CP}\right), U_{ijk} + h_{ijk}g_{pub}\right) \qquad (28)$$

Diversion:

$$e\left(\chi_{ij}, g\right) = \prod e\left(S_{ij} + h_2\left(Q_{ij} + Q_{CP}\right), U_{ijk} + h_{ijk}g_{pub}\right) \qquad (29)$$

Configuration:

$$e\left(\omega_{ij}, g\right) = \prod e\left(S_{ij} + h_2\left(Q_{ij} + Q_{CP}\right), U_{ijk} + h_{ijk}g_{pub}\right) \qquad (30)$$

Composition:

$$e\left(\delta_{ij}, g\right) = \prod e\left(S_{ij} + h_2\left(Q_{ij} + Q_{CP}\right), U_{ijk} + h_{ijk}g_{pub}\right) \quad (k = 0, f, b, m+1) \qquad (31)$$

② Creating a Header

The author ID_{ij} creates a partial content, start data, and final data, and a header of the entire content using the signature received from the copyright protection agency.

Table 1: Content header.

Author aID(ID_{ij})	Content ID(IC_{ij})		Content (A_{ij})
Change aggregate signature			
Delete aggregate signature			
Diversion aggregate signature			
Composition aggregate signature			
Setting aggregate signature			
Warrant w	Delegation value S_{ij}	Other	

Table 2: Start and end data headers.

Author aID(ID_{ij})	Content ID(IC_{ij})	Partial Content ID(I_{ijk})	
Hash value of change control signature		pc	start data or end data (A_{ij0} or A_{ijm+1})
Hash value of delete control signature		pd	
Hash value of diversion control signature		pm	
Setting control signature		ps	
Composition control signature		pb	
or hash value			
identifier	Management station signature	Other	

Table 3: Partial content header.

Author aID(ID_{ij})	Content ID(IC_{ij})			partial Content
partial Content ID(I_{ijk})	original hash value(H(A^*_{ijk})			
Change control signature	Signature method	bID	pc	
or hash value				
Delete control signature	Signature method	bID	pd	
or hash value				
Diversion control signature	Signature method		pm	
or hash value				
Setting control signature			ps	
Purchase availability(p_p)	identifier	Management station signature	Other	

Table 4: Composition content header.

Structure data	Composition Content
Synthetic management signature	
ID of the composited editor	
Other	

③ Publishing Content

The author ID_{ij} publishes the content associated with the header created in 3.3.4 ② on the content distribution service.

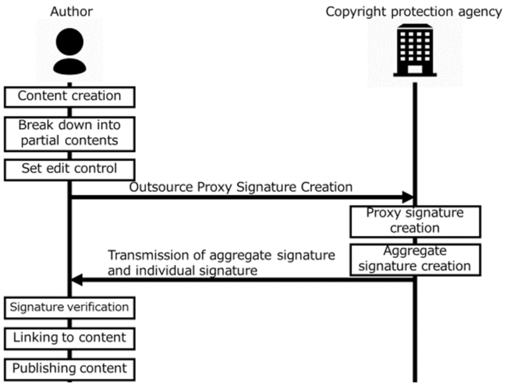
Author
Copyright protection agency
Content creation
Break down into partial contents
Set edit control
Outsource Proxy Signature Creation
Proxy signature creation
Transmission of aggregate signature and individual signature
Aggregate signature creation
Signature verification
Linking to content
Publishing content

Figure 4: Delegation of editing control signature creation.

3.4 Editing Content

3.4.1 Change / Add / Delete / Diversion Partial Content

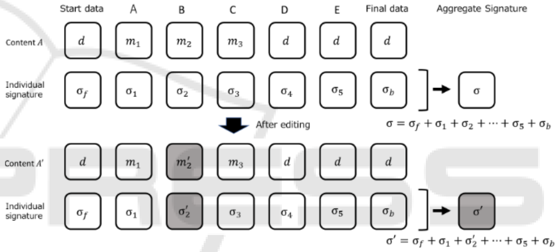

Figure 5: Edit control (change).

Consider a case in which an editor ID_{ab} edits (changes, adds, deletes, and diverts) a partial content A_{ijk} of a content A_{ij} to be a partial content A_{abk}. At this time, the editor ID_{ab} performs the following processes. When editing two or more partial contents, the same processes are repeated.

① Signature Verification of Secondary Use Content
The successful verification of the signature of content A_{ij} is confirmed. Here, partial content that is permitted to be diverted can be diverted. Also, the partial content A_{ijk} that is allowed to be changed, added, or deleted can be changed to the partial content A_{abk}.

② Generating Hash Values
The editor ID_{ab} creates control data A^*_{abk} from the edited partial content A_{abk} as in 3.3.2.⑤. After that, a hash value and a part of the control signature are created based on the constant p (representing the propriety) for each edit as in 3.3.2.⑥. However, if the inheritance is set, the value of p for A_{ijk} is inherited as it is; if it is not

necessary to inherit, p can be set at the discretion of the editor of A_{ijk}.

$$A^{*}_{abk} = IC_{ij}||I_{ijk}||A_{abk} \tag{32}$$

$$h_{ijk} = H\left(IC_{ij} \parallel I_{ijk} \parallel H(A_{abk}{}^{*}) \parallel p \parallel r\right) \tag{33}$$

③ Creating an Edit Control Signature
The following are calculated for the edited partial content. Here, the random number r_{abk} is different for each edit.
Change control signature:

$$\sigma_{abk} = r_{abk}h_{abk} + d_{ab}, U_{abk} = r_{abk}g \tag{34}$$

Delete control signature:

$$\tau_{abk} = r_{abk}h_{abk} + d_{ab}, U_{abk} = r_{abk}g \tag{35}$$

Diversion control signature:

$$\chi_{abk} = r_{abk}h_{abk} + d_{ab}, U_{abk} = r_{abk}g \tag{36}$$

Where d_{ab} is the signature key of editor ID_{ab} and r_{abk} is a constant generated by editor ID_{ab}.

④ Creating an Aggregate Signature
Editor ID_{ab} updates the aggregate signature as follows. However, if the aggregate signature for prohibited editing (change, deletion, diversion) cannot be updated. $U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1}, U_{abk}$ are different for each edit.
Change aggregate signature:

$$\begin{gathered}\sigma'_{ij} = \sigma_{ij} - \sigma_{ijk} + \sigma_{abk},\\ U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1}, U_{abk}\end{gathered} \tag{37}$$

Delete aggregate signature:

$$\begin{gathered}\tau'_{ij} = \tau_{ij} - \tau_{ijk} + \tau_{abk},\\ U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1}, U_{abk}\end{gathered} \tag{38}$$

Diversion aggregate signature:

$$\begin{gathered}\chi'_{ij} = \chi_{ij} - \chi_{ijk} + \chi_{abk},\\ U_{ij0}, U_{ij1}, \cdots, U_{ijm}, U_{ijm+1}, U_{abk}\end{gathered} \tag{39}$$

⑤ Linking to Content
The partial content that allows editing is associated with the edit control signature. In addition, for the partial content for which editing is prohibited, only the generated hash value and U_{abk} are linked to the partial content, and the editor ID_{ab} is linked as the editor bID for which editing is prohibited.

3.4.2 Compositing Content

The editor ID_{ab} combines the contents A_{ij} and $A_{mn}(A_{ij} \rightarrow A_{mn}$ order). Editor ID_{ab} composites the contents by the following procedure:

① Signature Verification of Secondary Use Content
Editor ID_{ab} checks whether the composite control signature of the contents A_{ij} and A_{mn} has been published. Editor ID_{ab} can compose A_{ij} and A_{mn} if the opposing sides are both permitted to compose when the composing order is decided. At this time, the composition order of A_{ij} and A_{mn} is recorded as structural data.

② Composition Management Signature
ID_{ab} fixes the relationship between the contents by creating a composite management signature between contents A_{ij} and A_{mn}. The composite management signature is created as follows:

I. The final position signature $\beta_{ij(ab)}$ and the start position signature $\alpha_{mn(ab)}$ are created using the editor's secret key $\mathrm{d_{ab}}$ for the final data of the content A_{ij} and the start data of the content A_{mn}. ($\mathrm{r_{ijm+1(ab)}}, \mathrm{r_{mn0(ab)}}$ are random numbers generated by editor ID_{ab}.)

II. A composite management signature is created using the post-composition control signature of the content A_{ij} and the pre-composition control signature of the content A_{mn}.

Composition management signature:

$$\delta_{(ij)(mn)} = \beta_{ij(ab)} + \delta_{ijb} + \delta_{mnf} + \alpha_{mn(ab)} \tag{40}$$

By configuring the aggregation signature as described above, the relationship between the two contents can be fixed.

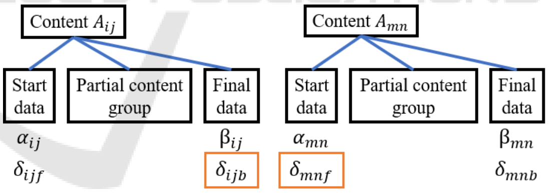

Figure 6: Compositing content.

3.5 Billing Support

Consider the case where the editing of content is prohibited and the transfer of editing rights by charging is permitted. Here, as an example, we explain the charging support in the change control.

3.5.1 Compositing Content

First, the purchaser confirms that the purchase of the target partial content is permitted by verifying the following expression using the header and the inheritance control signature of the partial content.

$$h_2 = H_2(w, S_{ij}) \in Z_q^{*} \tag{41}$$

$$h_{ijk} = H\big(IC_{ij} \parallel I_{ijk} \parallel H\big({A_{ijk}}^{*}\big) \parallel p_s \parallel p_c \parallel p_d \parallel p_m \parallel p_b \parallel \mathrm{p_p} \parallel r\big) \tag{42}$$

$$e\big(\omega_{ij}, g\big) = e(S_{ij}{+}h_2\big(Q_{ij} + Q_{CP}\big), U_{CP} + h_{ijk}g_{pub}) \tag{43}$$

Next, if the purchase is permitted ($p_p = 1$), the copyright protection agency is requested to purchase the partial content.

3.5.2 Transfer of Editing Rights for Partial Content

After receiving the purchase application from the buyer, the copyright protection agency performs the following:

① Create Buyer Data
Copyright protection agencies create buyer data A_{cpx} based on the buyer's registration information. A change control signature σ_{CPx} for the purchaser data is created using the Proxy key of ID_{ij} in the same manner as in 3.3.2 ⑤, ⑥ and 3.3.3. ②.

② Creating a Rights Transfer Signature
The copyright protection agency calculates the following using the change control signature σ_{ijk} of the partial content to be purchased, the change control signature of the purchaser dataσ_{CPx}, and the signature σ_{ijx} of the empty data included in the content to be purchased.

$$\sigma_{TR} = \sigma_{ijk} + \sigma_{ijx} - \sigma_{CPx} \tag{44}$$

③ Transfer of Editing Rights
The copyright protection agency sends the purchaser data created in ① and the rights transfer signature σ_{TR} created in ② to the purchaser using a secure channel.

3.5.3 Signature Update When Charging(P)

① Editing Partial Content
The buyer ID_{cd} edits the purchase target partial content and creates a change control signature σ_{cdk} for the edited partial content in the same manner as in 3.4.1. ② and ③.

② Adding Purchase Data
The purchaser adds the purchaser data received in 3.5.2. ③ by changing the null data specified by the copyright protection agency.

④ Updating Aggregate Signature
The purchaser ID_{cd} updates the change aggregate signature σ_{ij} using the rights transfer signature σ_{TR} received in 3.5.2. ③ and the individual signature $\sigma_{cdk}$of the edited partial content as follows.

$$\begin{aligned}\sigma'_{ij} &= \sigma_{ij} - \sigma_{TR} + \sigma_{cdk}\\ &= \sigma_{ij} - \big(\sigma_{ijk} + \sigma_{ijx} - \sigma_{CPx}\big) + \sigma_{cdk}\end{aligned} \tag{45}$$

⑤ Linking to Content
The purchaser ID_{cd} associates the signature with the edited partial content as inherited by the original author ID_{ij}. Here, if the signatures are not linked according to the author's inheritance, the verification of the setting control signature ω_{ij} does not match, resulting in unauthorized editing. As for the association of the signature with the purchaser data, since the purchaser data is basically prohibited from editing, only the hash value is associated. Here, since the purchaser does not have the individual signature of the purchaser data, it is impossible to link them in the first place.

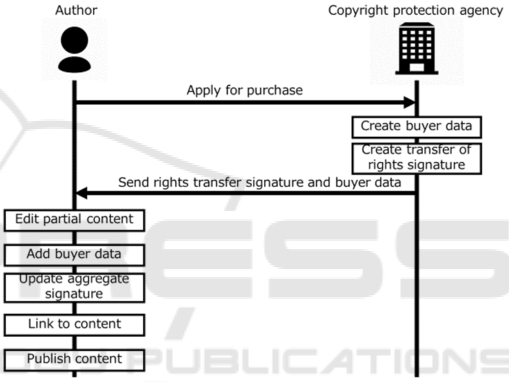
Author
Copyright protection agency
Apply for purchase
Create buyer data
Create transfer of rights signature
Send rights transfer signature and buyer data
Edit partial content
Add buyer data
Update aggregate signature
Link to content
Publish content

Figure 7: Protocol for billing.

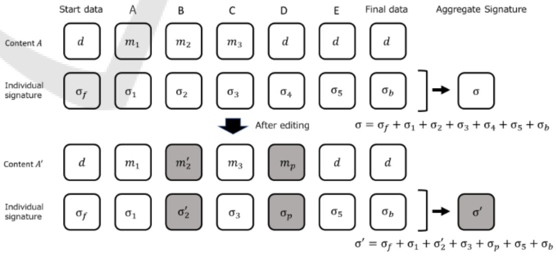

Figure 8: Editing control when billing is supported (change).

3.6 Watch Content

The mechanism of signature verification in dedicated software when viewers view content is described below. Here, by verifying the signature of the content, it is possible to confirm that the content is legitimate without any unauthorized editing, and it is possible to disable the reproduction of the illegal content.

3.6.1 Content Signature Verification

① Verification of the Management Station Signature

The dedicated software verifies that the management station signature of each partial content is valid. Inconsistent partial content without a management station signature or inconsistent content is considered illegal content.

② Verification of Composition Content

In the case of composite content, the composite data is separated into each content by referring to the structural data. If the structural data and the structure of the content do not match, the composite is illegal.

③ Verification of Composite Management Signature

The dedicated software verifies that the contents are correctly combined using the following verification formula (e.g. when synthesized in the order of $(A_{ij} \rightarrow A_{mn})$):

$$\begin{aligned} & e(\delta_{(ij)(mn)}, g) \\ & = e(g_{pub}, Q_{ab})e(U_{ijm+1(ab)}, h_{ijm+1}) \\ & \cdot e(S_{ij}+h_{2(ij)}(Q_{ij} + Q_{CP}), U_{ijm+1} \\ & \qquad + h_{ijm+1}g_{pub}) \\ & \cdot e(S_{mn}+h_{2(mn)}(Q_{mn} + Q_{CP}), U_{mn0} \\ & \qquad + h_{mn0}g_{pub}) \\ & \cdot e(g_{pub}, Q_{ab})e(U_{mn0(ab)}, h_{mn0}) \end{aligned} \tag{46}$$

④ Verification of Composite Control Signature

The dedicated software verifies that the contents are correctly composited using the public key Q_{aID} of the aID as follows.

$$e(\delta_{ij}, g) = \prod e(S_{ij}+h_2(Q_{ij} + Q_{CP}), U_{ijk} + h_{ijk}g_{pub}) \quad (k = 0, m+1, f, b) \tag{47}$$

⑤ Verification of Diversion Control

I. Verification of diversion control signature

The dedicated software verifies that each partial content is properly diverted using the aID's public key Q_{aID} as follows.

$$e(\chi_{ij}, g) = \prod e(S_{ij}+h_2(Q_{ij} + Q_{CP}), U_{ijk} + h_{ijk}g_{pub}) \tag{48}$$

II. Confirmation of content ID

The dedicated software checks whether each partial content has the correct content ID (content ID is unified). If it has a different content ID, following steps are taken for the target partial content:

i. When the diversion control signature is published:

Verify that the partial content diversion control signature is correct using the public key of aID as follows:

$$e(\chi_{ij}, g) = e(S_{ij}+h_2(Q_{ij} + Q_{CP}), U_{ijk} + h_{ijk}g_{pub}) \tag{49}$$

ii. When the diversion control signature is private:

Verify whether the generated and diverted hash values are equal.

⑥ Verification of Control Signature for Each Edit

The dedicated software verifies that each partial content has been correctly edited (changed / added / deleted). First, it confirms whether the empty data is changeable / deletable or not changeable / deletable, and the dedicated software generates a hash value for each edit. If the actual data does not have a change control signature, the dedicated software verifies that the generated hash value is equal to the change hash value. If the empty data does not have a deletion control signature, the dedicated software verifies that the generated hash value is equal to the deletion hash value. The dedicated software attaches the public key Q_aID of the aID (the public key Q_{aID}, Q_{bID} and the signature U_{aID}, U_{bID} if the change / deletion has been changed), the hash value of the generated partial content, and the partial content without signature. Collect the hash values and verify that the following equations hold:

Change:

$$e(\sigma_{ij}, g) = \prod e(S_{ij}+h_2(Q_{ij} + Q_{CP}), U_{ijk} + h_{ijk}g_{pub}) \tag{50}$$

Delete:

$$e(\tau_{ij}, g) = \prod e(S_{ij}+h_2(Q_{ij} + Q_{CP}), U_{ijk} + h_{ijk}g_{pub}) \tag{51}$$

⑦ Verification of configuration control signature

The dedicated software verifies each partial content by using the attached parameters $p_s, p_c, p_d, p_m, p_b, p_p$ according to the following formula. If it is verified correctly with $p_s = 1$, verify that the setting of each parameter and editing permission status of each partial content match for editing and composition.

$$e(\omega_{ij}, g) = \prod e(S_{ij}+h_2(Q_{ij} + Q_{CP}), U_{ijk} + h_{ijk}g_{pub}) \tag{52}$$

Those that have been correctly verified can be used as legitimate content.

3.7 Regarding Signature Verification after Secondary Use

In the proposed method, the signature creation of the original author is entrusted to a copyright protection agency, so the Proxy signature method is used. In contrast, since the signatures of the editor and the buyer are created individually, the usual signature method is used. Therefore, in the proposed method, two signature methods are mixed in the content after secondary use. In this case, since the signature verification algorithm is different, different verification formulas must be used for each. However, in the proposed method, an aggregate signature must be created for each content. In addition, if the proxy signature scheme is separated from the aggregate signature of the normal signature scheme, if the editor edits only one partial content, the individual signature will be found from the aggregate signature even if the individual signature is kept private. This is a problem. Therefore, it is desirable to have one aggregate signature. Therefore, in the proposed method, signature verification is performed as follows so that verification can be performed without any problem even with one aggregate signature. The algorithm for verifying the aggregate signature is shown below.

① Check Signature Scheme

Confirm from the header of the partial content whether the signature scheme used for various control signatures of the partial content is the normal signature scheme or the Proxy signature scheme.

② Preparation for Verification of Aggregate Signature

Calculates only the right side of the verification formula for partial content using the Proxy signature method and the normal signature method.

$$a_{ij} = \mathit{\Pi} e\left(S_{ij}+h_2\left(Q_{ID_{ij}} + Q_{ID_R}\right), U_R + h_3 g_{pub}\right) \tag{53}$$

$$b_{ij} = \prod e\left(g_{pub}, Q_{ID_{ab}}\right) e(U_i, h_i) \ \ (i \in \mathcal{J}) \tag{54}$$

③ Verification of Aggregate Signature

The validity of the aggregate signature is confirmed by verifying that the following equation holds.

$$e(V, g) = a_{ij} \cdot b_{ij} \tag{55}$$

3.8 Comparison with Conventional Method

Here, a comparison is made on the amount of calculation in the method proposed with the conventional method (T. Kobayashi et al., 2019). For the comparison, the amount of calculation by the author and the third party of each method is calculated and compared. At this time, the number of times is counted for each of the following calculation processes.

P: Bilinear pairing, H: Hash function used for mapping, SM: Scalar multiplication

Table 5: Preparation amount.

Method	role	Computational complexity
Conventional method	(A)	0
	(CP)	0
Proposed method	(A)	2SM+H
	(CP)	2SM+2H+2P

Table 6: Amount of calculation required for signature generation for each partial content (change control).

Method	role	Computational complexity
Conventional method	(A)	2SM+2H
	(CP)	0
Proposed method	(A)	H
	(CP)	2SM+H

Table 7: Calculation amount required for charging for each partial content (change control).

Method	role	Computational complexity
Conventional method	(A)	2SM+H
	(CP)	2SM+H
Proposed method	(A)	0
	(CP)	2SM+H

Table 8: Calculation amount per piece of partial content corresponding to billing.

Method	role	Computational complexity
Conventional method	(A)	4SM+3H
	(CP)	2SM+H
Proposed method	(A)	H
	(CP)	4SM+2H

Table 5 shows that the amount of computation required to prepare for signature creation is larger in the proposed method than in the conventional method. However, once the signature preparation has been performed, there is no need to do so afterwards, so the impact is considered to be small. From Table 6, it can be seen that, compared to the conventional method, the amount of calculation for the signature generation per partial content by the author is reduced in the proposed method. In addition, Table 7 shows that the author's calculation amount for charging for each partial content is reduced compared to the conventional method. As a result, it can be seen from Table 8 that the amount of calculation by the author was significantly reduced for each piece of content to be charged.

4 CONCLUSIONS

In this method, the Proxy signature scheme (T. Kobayashi et al., 2019) is newly adopted as the signature scheme. The purpose of this scheme is to further reduce the work of the author by entrusting the creation of the author's signature to a copyright protection organization (a third-party organization in the conventional method). Also, compared to the conventional method, the time and effort required for the author to create a signature has been greatly reduced. In this method, we propose a method in which the author can securely provide individual editing permissions for content that has been editing-prohibited. 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. Additionally, I want to continue my research in the future.

REFERENCES

"YouTube" https://www.youtube.com/ 2020/03/28

K. Koga, M. Inamura, K. Kaneda and K. Iwamura: "Content Control Scheme to Realize Right Succession and Edit Control", ICE-B2015.

T. Fujimoto, K. Iwamura and M. Inamura: "Content Protection Scheme to Realize Edit Control Including Diversion Control and Composition Control", ICE-B 2016.

Boneh D., Lynn B., Shacham H. "Short Signatures from the Weil Pairing" In: Boyd C. (eds) Advances in Cryptology —ASIACRYPT 2001.

Boneh D., Gentry C., Lynn B., Shacham H. "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps" In: Biham E. (eds) Advances in Cryptology — EUROCRYPT 2003.

Xun, Y., "An identity-based signature method from the Weil pairing" IEEE Communications Letters, 2003

Jing, X., Zhenfeng, Z., Dengguo, F., "ID-based aggregate signatures from bilinear pairing" CANS, 2005.

T. Kobayashi, K. Iwamura and M. Inamura "Content Protection Method to Control Editing by Billing",ICE-B 2019.

Francesco Buccafurri, Rajeev Anand Sahu and Vishal Saraswat "Efficient Proxy Signature Scheme from Pairings", ICETE 2016.

N. Yanai, T, Iwasaki, M, Inamura, K. Iwamura, Provably Secure Structured Signature Schemes with Tighter Reductions, Trans. Fundamentals of Electronics, Communications and Computer Sciences, Vol.E100-A, No.9, pp.1870-1881, IEICE, 2017.