COIN-BASED ANONYMOUS FINGERPRINTING SCHEME WITH AUTOMATIC IDENTIFICATION OF REDISTRIBUTORS

Shingo OKAMURA[†], **Maki YOSHIDA**[‡], **and Toru FUJIWARA**[‡]

[†]Cybermedia Center, Osaka University
okamura@cmc.osaka-u.ac.jp, +81-6-6879-4519
5-1 Mihogaoka, Ibaraki, Osaka 567-0047, Japan
[‡]Graduate School of Information Science and Technology, Osaka University
{maki-yos, fujiwara}@ist.osaka-u.ac.jp, +81-6-6879-4519
1-5 Yamadaoka, Suita, Osaka 565-0871, Japan

ABSTRACT

As the markets of digital contents over computer networks become more popular, illegal redistribution of contents by a buyer becomes the more serious problem. To deter illegal redistribution, various fingerprinting schemes have been proposed. The fingerprinting schemes enable merchants to embed information which identifies the original buyer to the purchased content. Identifying the original buyer from the confiscated content deters buyers from redistributing contents. To protect honest buyer's privacy, a certain type of fingerprinting schemes, called an anonymous fingerprinting scheme, allows the buyers purchasing fingerprinted contents anonymously. The anonymous fingerprinting schemes involve the registration center to which every buyer registers before purchasing contents. In most of the anonymous fingerprinting schemes, the merchant has to cooperate with the registration center to identify the buyer from the confiscated content. To identify the buyer speedily, it is desirable that the merchant needs not to cooperate with the registration center. This feature is called the automatic identification.

In this paper, an efficient anonymous fingerprinting scheme with automatic identification is proposed. To realize the automatic identification, personal information of the buyer is embedded correctly in the purchased content retaining the anonymity of the buyer. Then, the merchant can identify the buyer by himself/herself when a copy of the purchased content is confiscated. Compared with the previous anonymous fingerprinting scheme with automatic identification, although the proposed scheme requires more number of registrations, the total amount of computation is smaller than the previous schemes.

KEY WORDS

Digital contents distribution, Anonymous fingerprinting, Automatic identification, Digital coin, Privacy protection

COIN-BASED ANONYMOUS FINGERPRINTING SCHEME WITH AUTOMATIC IDENTIFICATION OF REDISTRIBUTORS

1 INTRODUCTION

With spread of computer networks, the markets of digital contents over computer networks become popular. It is important to prevent buyers from illegal redistribution of contents. However, preventing illegal redistribution perfectly is difficult. Therefore, as a deterrent against illegal redistribution, various fingerprinting schemes are proposed [1–8]. A fingerprinting scheme enables the merchant to embed information, which identifies the buyer, to the purchased content when the content is sold and to identify the original buyer of a redistributed content when the content is confiscated. This embedded information is called a fingerprint.

The basic security requirement for fingerprinting schemes is that the merchant can identify the original buyer of a confiscated content. It is also required that the merchant can prove the validity of the identification to others and the buyer can purchase fingerprinted contents from the merchant anonymously, because users' concerns over cheating and privacy have become stronger lately. Fingerprinting scheme which satisfies the above requirements is first proposed in [3]. Such fingerprinting scheme is called the *anonymous fingerprinting scheme.* In the previous anonymous fingerprinting schemes [3–8], in addition to a merchant and a buyer, a participant, called the registration center, is involved to enable any buyer to purchase fingerprinted contents anonymously. The buyer commits a secret information to the registration center together with his/her identifier before the purchase. The buyer purchases a content in which the secret information is embedded from the merchant without revealing the secret information. If the merchant confiscates a copy of the content, the merchant can extract the embedded secret information from the confiscated content. The merchant can identify the original buyer of the content and prove the validity of the identification to others using the embedded secret information and the help of the registration center.

In the previous anonymous fingerprinting schemes such as [3–5], the merchant has to cooperate with the registration center to identify the original buyer of the confiscated content. To identify the buyer speedily, it is desirable that the merchant can identify the buyer without cooperating with the registration center. This feature is called the *automatic identification.* An anonymous fingerprinting scheme with the automatic identification is first proposed in [6], and is improved in [7]. However, these schemes have semi-anonymity in the sense that the coalition of the merchant and the registration center can identify the buyer of a content only from communication record of the purchase. On the other hand, in [8], the anonymous fingerprinting scheme with the automatic identification based on group signature schemes is proposed and provides the perfect anonymity as in [3–5]. The major advantage of the scheme [8] is that a buyer registers only once for all purchase. However, the time complexity for a merchant and a buyer at each purchase is considerably large. This is a great disadvantage because many contents are purchased usually.

In this paper, we propose an efficient anonymous fingerprinting scheme with automatic identification which overcomes the disadvantages of the previous anonymous fingerprinting schemes with automatic identification [6–8]. That is, the perfect anonymity is provided and the time complexity for a merchant and a buyer at each purchase is small in the proposed scheme. From the discussion in [9], even if a merchant also plays the role of a registration center, the proposed scheme can provide the perfect anonymity. However, the degree of anonymity depends on the number of the buyers registered at a registration center. It is preferable that a registration center is separated from a merchant and is shared with several merchants. The proposed scheme uses a digital coin technique [10] for efficiency. The previous digital coin is based on a random value generated by the buyer and only the random value is embedded in the purchased content as the secret information. In the previous coin-based anonymous fingerprinting schemes, to identify the original buyer of the content from the embedded random value, the merchant has to cooperate with the registration center who is committed the random value together with the identifier from the buyer. In the proposed scheme, the involved digital coin is extended to contain not only a random value generated by the buyer but also the identifier of the buyer. The merchant cannot obtain the embedded identifier, but can check the correctness of the embedded identifier. In this way, the identifier of the buyer is embedded correctly in the purchased content retaining the anonymity of the buyer. As long as the buyer keeps the purchased content secret from others, the anonymity of the buyer is kept as the general privacy protection schemes. However, if the buyer redistributes the purchased content and the merchant confiscates the content, the merchant can identify the buyer by himself/herself from the identifier of the buyer embedded in the content. The buyer has to register at the registration center for each purchase as in the previous coin-based scheme [4, 5]. On the other hand, the total amount of computation of the proposed scheme at each purchase is less than that of the group signature-based scheme [8]. This is a great advantage because many contents are purchased usually.

The rest of this paper is organized as follows. The model of proposed scheme is shown in Section 2. The detail of protocols of the proposed scheme is described in Section 3. In Section 4, the security and the complexity of the proposed scheme are evaluated.

2 MODEL

In this section, the model of the anonymous fingerprinting scheme with automatic identification is shown. Participants in the proposed scheme are a merchant M, a buyer B, a registration center RC, and an arbiter A (see Figure 1). An arbiter represents an arbitrary honest party who a merchant should convince the result of an identification. There are several merchants, buyers, and registration centers. It is assumed that each buyer B can already digitally sign under the buyer's identifier ID_B. That is, a buyer has the unique identifier ID_B and a key pair of a signing key sk_B and a verification key vk_B, and ID_B and vk_B have been published. It is also assumed that each registration center RC has the unique identifier ID_{RC}.

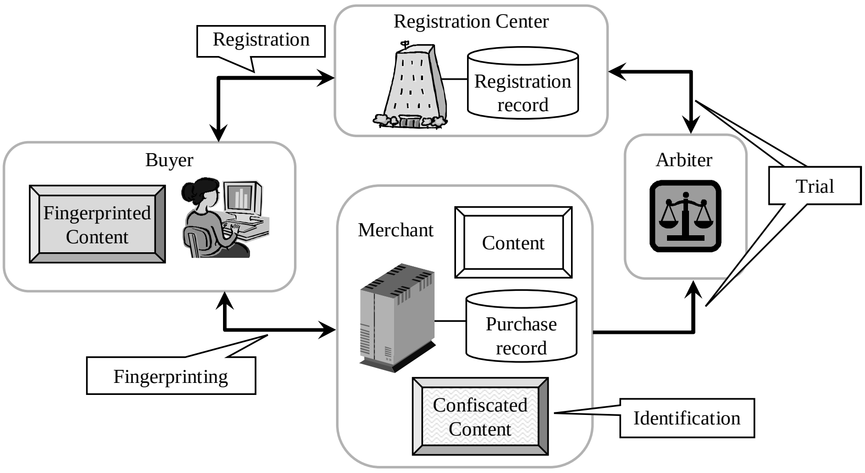


Figure 1: The model of the anonymous fingerprinting scheme with automatic identification.

Definition 1 (Components of the proposed system).
In the proposed scheme, there are four protocols and one algorithm: Preparation, Registration, Fingerprinting, and Trial protocols, and Identification algorithm.

- **Preparation:** This protocol is carried out by registration centers. Registration centers agree on and publish parameters which are necessary for the following protocols.
- **Registration:** This protocol is carried out by a buyer and a registration center at every purchase. The buyer generates a one-time account number and a key pair of an anonymous signing key and an anonymous verification key. The account number and the key pair are used for purchasing content. The buyer registers the account number and an encrypted form of the anonymous verification key together with the buyer's signature to the registration center. The registration center stores them as a registration record. The registration center issues a registration certificate of the account number to the buyer.
- **Fingerprinting:** This protocol is carried out by a merchant and an anonymous buyer at every purchase. The merchant inputs the public key of the registration center the buyer registered at and secretly inputs the original version of content. The buyer inputs a registration certificate. The common input is a *text* which describes the contract referring to this purchase. The output for the merchant is called a purchase record. The output for the buyer is the fingerprinted content.
- **Identification:** This algorithm is carried out by a merchant when the merchant confiscates a redistributed content. The merchant inputs the confiscated content, the original version of this content, and all purchase records for this content. The outputs for the merchant are the identifier of the original buyer of the content and some proofs for the verification of the validity of the identification.
- **Trial:** This protocol is carried out by the merchant, the arbiter, and the registration center. The merchant inputs data outputted in identification protocol. The arbiter obtains one of the outputs, *buyer_guilty* which denotes that the arbiter confirms the buyer redistributed the contents, *merchant_guilty* which denotes that the merchant misbehaved, or *center_guilty* which denotes that the registration center misbehaved.

It is noteworthy that Identification is not a protocol but an algorithm. This means that a merchant can identify the original buyer of the confiscated content in Identification without a help of any registration center, while all previous anonymous fingerprinting schemes except [6–8] need a help of a registration center in Identification.

In the following, the security requirements for the anonymous fingerprinting scheme are shown. The proposed scheme satisfies these requirements.

Definition 2 (Integrity).

- **Security for the merchant:** When an honest merchant confiscates an illegally redistributed content, the merchant can identify one participant in a coalition, which redistributes the content, and convince any arbiter that this identification is correct as long as the size of the coalition is a polynomial order on the security parameter. That is, the merchant obtains information which is sufficient for Trial as an output of Identification, and then any arbiter obtains either *buyer_guilty* or *center_guilty* as an output in Trial.
- **Security for the buyer:** Unless the buyer redistributes content illegally or helps illegal redistribution, any arbiter does not obtain the output *buyer_guilty* in Trial.
- **Security for the registration center:** Unless the registration center helps illegal redistribution, any arbiter dose not obtain the output *center_guilty* in Trial.

Definition 3 (Unlinkability).
Purchases of honest buyers cannot be linked even by a collusion of all merchants and registration centers. That is, a merchant cannot know whether buyers of two purchases are same or not.

The notations used in this paper are summarized in Table 1.

Table 1: Notations.

ID_B	The identifier of a buyer B
ID_{RC}	The identifier of a registration center RC
sk_B	A secret signing key of the buyer ID_B
vk_B	A public verification key corresponding to sk_B
x_{RC}	A secret signing key of the registration center ID_{RC}
h_{RC}	A public verification key corresponding to x_{RC}

3 PROPOSED SCHEME

3.1 Design concepts

The proposed scheme is based on the coin-based anonymous fingerprinting scheme in [4]. In the scheme in [4], a buyer registers a random value generated by him/her at the registration center together with the identifier of the buyer, and obtains a coin. The coin is based on the random value but no one can obtain the value from the coin. The buyer sends the coin to the merchant and obtains the content in which the random value is embedded. To identify the original buyer from a confiscated content, the merchant extracts the embedded random value and sends the value to the registration center. The registration center identifies the original buyer from the value and registration records.

To enable the merchant to identify the original buyer without cooperation of the registration center (i.e., without the registration records), the identifier of a buyer is embedded in the purchased content. To achieve this idea, the coin is issued based on not only the random value registered by the buyer but also the identifier of the buyer by using the restrictive blind signature scheme [11]. The restrictiveness of the blind signature scheme prevents the buyer from obtaining the coin based on another buyer's identifier. Here, the restrictiveness means that the buyer can only obtain a signature of which message is transformed with some restriction from a message the signer knows. The signature and the message the signer knows correspond to the coin and the identifier of the buyer, respectively.

3.2 Protocols

In this section, the protocols and the algorithm of the proposed scheme are shown. The techniques of the restrictive blind signature scheme [11] and the Schnorr signature scheme [12] are used in these protocols. "$||$" denotes the concatenation of data. $a \in_R B$ means "a is chosen from B randomly." For a prime p, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ and $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

Preparation:

- Registration centers agree on and publish the following parameters.
  - Two primes p, q with $q|(p-1)$.
  - Six generators $g, g_1, g_2, g_3, g_4, g_5$ of a group G_q which is a subgroup of order q of the multiplicative group $\mathbb{Z}_p^*$.
  - Hash function $Hash$.
- Each registration center generates a key pair of a signing key $x_{RC} \in_R \mathbb{Z}_q^*$ and a verification key $h_{RC} = g^{x_{RC}} \bmod p$, is issued a certificate of h_{RC} by a certification authority and publishes the certificate.

Registration:

1. The buyer B generates a one-time account number h_1, a key pair of an anonymous signing key k and an anonymous verification key pk_{text}. The buyer registers h_1 and an encrypted form of pk_{text} to the registration center RC. The details of this procedure is as follows (see also Figure 2).

   i. The buyer chooses $i \in_R \mathbb{Z}_q^*$ so that $g_1^i g_2^{ID_B||ID_{RC}} g_3 \bmod p \neq 1$ holds. The buyer computes a one-time account number $h_1 = g_1^i \bmod p$ and a public key for ElGamal encryption $h_4 = g_4^i \bmod p$, where i plays the role of the corresponding secret key.

   ii. The buyer chooses an anonymous signing key $k \in_R \mathbb{Z}_q^*$ and computes the corresponding public key $pk_{text} = g_5^k \bmod p$. The buyer encrypts pk_{text} by ElGamal encryption so that $enc = (d_1, d_2) = (h_4^y pk_{text} \bmod p, g_4^y \bmod p)$, where $y \in_R \mathbb{Z}_q^*$.

   iii. The buyer signs on (h_1, h_4, enc) with sk_B. This signature is denoted by SIG_{coin}.

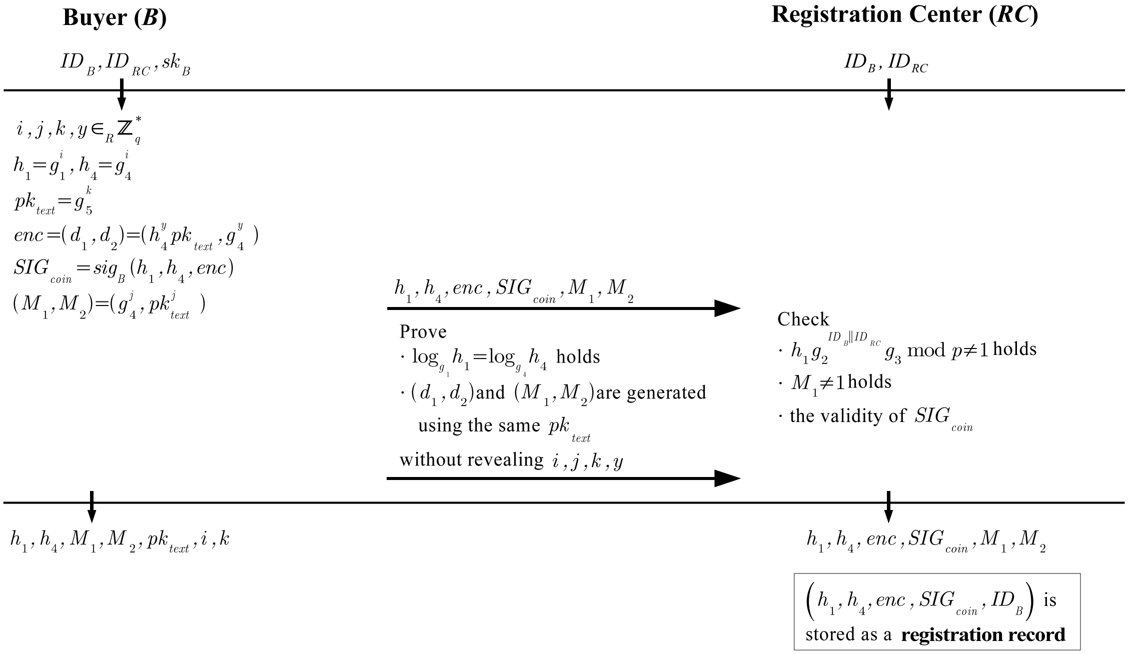
   iv. The buyer computes a pair $(M_1, M_2) = (g_4^j \bmod p, pk_{text}^j \bmod p)$, where $j \in_R \mathbb{Z}_q^*$ and $M_1 \neq 1$. This pair is an additional encoding of pk_{text}.

   v. The buyer sends (h_1, h_4, enc), SIG_{coin}, and (M_1, M_2) to the registration center.

   vi. The registration center verifies that $h_1 g_2^{ID_B||ID_{RC}} g_3 \bmod p \neq 1$ and $M_1 \neq 1$ are hold, and verifies the validity of SIG_{coin}. If any of verifications fails, the registration center refuses this registration.

   vii. The buyer proves to the registration center that $\log_{g_1} h_1 = \log_{g_4} h_4$ holds and both $enc = (d_1, d_2)$ and (M_1, M_2) are encryption forms of pk_{text} without revealing i, j, k and y. This is done in the same way as [4].

   viii. The registration center stores $(h_1, h_4, enc, SIG_{coin}, ID_B)$ as a *registration record.*



Buyer (*B*)
Registration Center (*RC*)
ID_B, ID_{RC}, sk_B
ID_B, ID_{RC}
$i, j, k, y \in_R \mathbb{Z}_q^*$
$h_1 = g_1^i, h_4 = g_4^i$
$pk_{text} = g_5^k$
$enc = (d_1, d_2) = (h_4^y pk_{text}, g_4^y)$
$SIG_{coin} = sig_B(h_1, h_4, enc)$
$(M_1, M_2) = (g_4^j, pk_{text}^j)$
$h_1, h_4, enc, SIG_{coin}, M_1, M_2$
Prove
· $\log_{g_1} h_1 = \log_{g_4} h_4$ holds
· (d_1, d_2) and (M_1, M_2) are generated using the same pk_{text}
without revealing i, j, k, y
Check
· $h_1 g_2^{ID_B||ID_{RC}} g_3 \bmod p \neq 1$ holds
· $M_1 \neq 1$ holds
· the validity of SIG_{coin}
$h_1, h_4, M_1, M_2, pk_{text}, i, k$
$h_1, h_4, enc, SIG_{coin}, M_1, M_2$
$(h_1, h_4, enc, SIG_{coin}, ID_B)$ is stored as a **registration record**

Figure 2: Registering the buyer at the registration center.

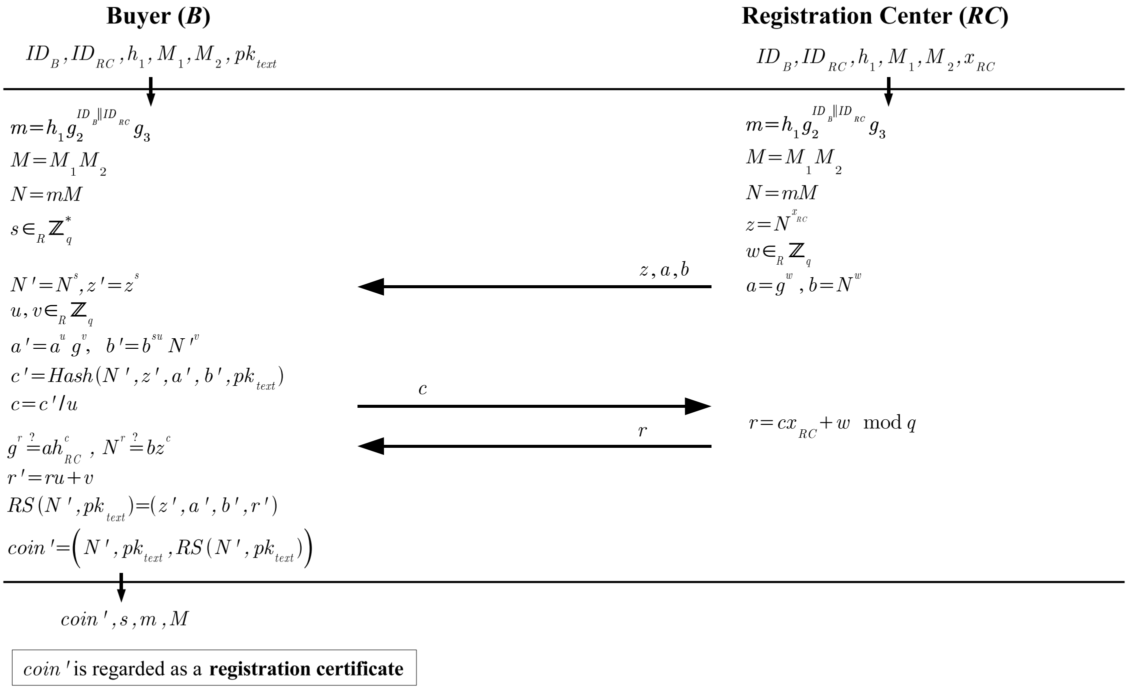
2. The registration center RC issues a registration certificate of the account number, the identifiers of the buyer and registration center, and the pair (M_1, M_2) to the buyer. The details of this procedure is as follows (see also Figure 3).

   i. Let $m = h_1 {g_2}^{ID_B || ID_{RC}} g_3 \bmod p$, $M = M_1 M_2$ and $N = mM$. The registration center computes $z = N^{x_{RC}} \bmod p$. The registration center generates $w \in_R \mathbb{Z}_q$ and computes $a = g^w \bmod p$ and $b = N^w \bmod p$. Then the registration center sends (z, a, b) to the buyer.

   ii. The buyer generates $s \in_R \mathbb{Z}_q^*$, and computes $N' = N^s \bmod p$ and $z' = z^s \bmod p$. The buyer also generates $u, v \in_R \mathbb{Z}_q$, and computes $a' = a^u g^v \bmod p$ and $b' = b^{su} N'^v \bmod p$. Then the buyer computes $c' = Hash(N', z', a', b, pk_{text})$, and sends $c = c'/u \bmod q$ to the registration center.

   iii. The registration center sends $r = cx_{RC} + w \bmod q$ to the buyer.

   iv. The buyer accepts if and only if $g^r = ah_{RC}^c \bmod p$ and $N^r = bz^c \bmod p$ hold. If this verification passes, the buyer computes $r' = ru + v \bmod q$ and obtains a restrictive blind signature $RS(N', pk_{text}) = (z', a', b', r')$ on N' and pk_{text}. $coin' = (N', pk_{text}, RS(N', pk_{text}))$ is regarded as a *registration certificate* of the buyer. From the blindness of the restrictive blind signature scheme [10], the registration center cannot know neither s nor $coin'$.



Buyer (*B*)
$ID_B, ID_{RC}, h_1, M_1, M_2, pk_{text}$
Registration Center (*RC*)
$ID_B, ID_{RC}, h_1, M_1, M_2, x_{RC}$
$m = h_1 g_2^{ID_B || ID_{RC}} g_3$
$M = M_1 M_2$
$N = mM$
$s \in_R \mathbb{Z}_q^*$
$m = h_1 g_2^{ID_B || ID_{RC}} g_3$
$M = M_1 M_2$
$N = mM$
$z = N^{x_{RC}}$
$w \in_R \mathbb{Z}_q$
$a = g^w, b = N^w$
z, a, b
$N' = N^s, z' = z^s$
$u, v \in_R \mathbb{Z}_q$
$a' = a^u g^v,\ b' = b^{su} N'^v$
$c' = Hash(N', z', a', b', pk_{text})$
$c = c'/u$
c
r
$r = cx_{RC} + w \bmod q$
$g^r \overset{?}{=} ah_{RC}^c,\ N^r \overset{?}{=} bz^c$
$r' = ru + v$
$RS(N', pk_{text}) = (z', a', b', r')$
$coin' = (N', pk_{text}, RS(N', pk_{text}))$
$coin', s, m, M$
$coin'$ is regarded as a **registration certificate**

Figure 3: Issuing a registration certificate.

Fingerprinting:

This protocol is depicted in Figure 4.

1. The buyer selects an unused coin $coin' = (N', pk_{text}, RS(N', pk_{text}))$.
2. The buyer computes $m' = m^s \bmod p$, $M' = M^s \bmod p$ and $s' = sj \bmod p$.

3. The buyer makes a Schnorr signature $(\tilde{c}, \tilde{r})$ on *text* with the anonymous signing key k so that $\tilde{c} = Hash(g_5^{\tilde{w}} \bmod p, pk_{text}, text), \tilde{r} = \tilde{w} - k\tilde{c}$,where $\tilde{w} \in_R \mathbb{Z}_q^*$. This signature is denoted by SIG_{text}.
4. The buyer sends $coin', m', M', s'$ and SIG_{text} to the merchant.
5. The merchant verifies the validity of $coin'$ and SIG_{text}.
    - The merchant computes $c' = Hash(N', z', a', b', pk_{text})$ and confirms that $g^{r'} = a'h_{RC}^{c'} \bmod p$ and $N'^{r'} = b'z'^{c'} \bmod p$ hold.
    - The merchant verifies that SIG_{text} is a signature on *text* with pk_{text}.
    - The merchant verifies that $N' = m'M', N' \neq 1, m' \neq 1$ and $M' = g_4^{s'} pk_{text}^{s'}$ hold.
6. The buyer proves to the merchant in zero-knowledge that the buyer knows a representation of m' with respect to (g_1, g_2, g_3) and of pk_{text} with respect to g_5. This is done in the same way as in [4].
7. The merchant stores $(coin', m', M', s', text, SIG_{text})$ as a *purchase record* of the content.
8. The buyer selects $emb = (is, (ID_B||ID_{RC})s, s)$ such that $m' = g_1^{is} g_2^{(ID_B||ID_{RC})s} g_3^s \bmod p$ holds, as the fingerprint to be embedded in the content.
9. The merchant embeds *emb* in the content using the embedding protocol in [5] by cooperating with the buyer. In this protocol, the merchant can verify that *emb* is embedded but cannot know *emb*.

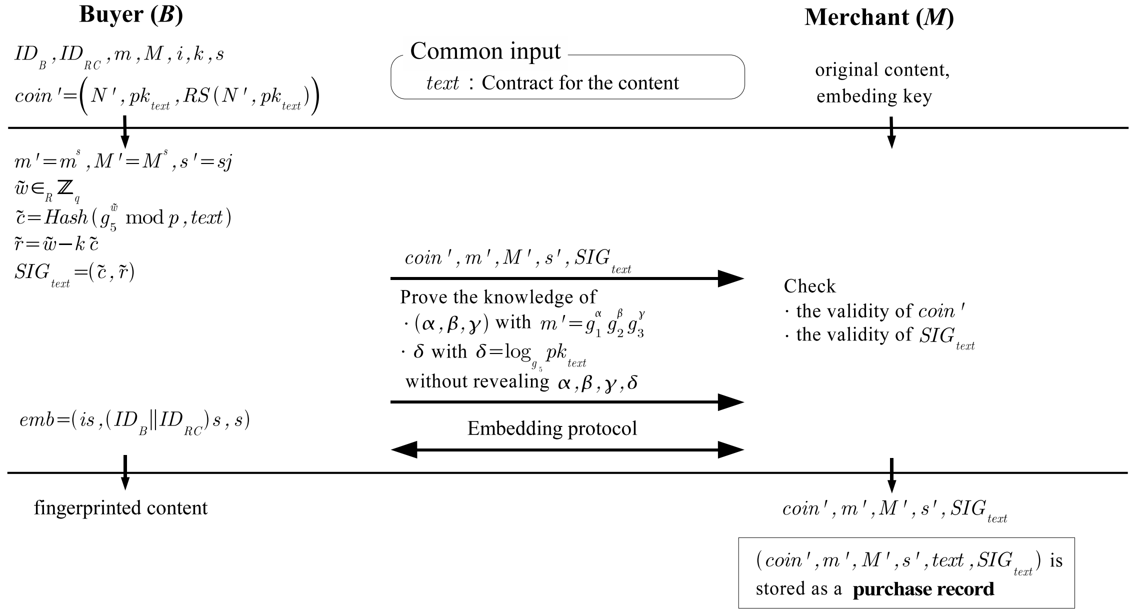

Buyer (*B*)
Merchant (*M*)
$ID_B, ID_{RC}, m, M, i, k, s$
$coin' = (N', pk_{text}, RS(N', pk_{text}))$
Common input
text : Contract for the content
original content,
embeding key
$m' = m^s, M' = M^s, s' = sj$
$\tilde{w} \in_R \mathbb{Z}_q$
$\tilde{c} = Hash(g_5^{\tilde{w}} \bmod p, text)$
$\tilde{r} = \tilde{w} - k\tilde{c}$
$SIG_{text} = (\tilde{c}, \tilde{r})$
$coin', m', M', s', SIG_{text}$
Prove the knowledge of
· (α, β, γ) with $m' = g_1^{\alpha} g_2^{\beta} g_3^{\gamma}$
· δ with $\delta = \log_{g_5} pk_{text}$
without revealing $\alpha, \beta, \gamma, \delta$
Check
· the validity of *coin'*
· the validity of SIG_{text}
$emb = (is, (ID_B \| ID_{RC})s, s)$
Embedding protocol
fingerprinted content
$coin', m', M', s', SIG_{text}$
$(coin', m', M', s', text, SIG_{text})$ is
stored as a **purchase record**

Figure 4: Fingerprinting protocol.

Identification:

1. The merchant extracts $emb = (e_1, e_2, e_3)$ from the confiscated content.
2. The merchant obtains $\hat{i}$ and $ID_{\hat{B}}||ID_{\hat{RC}}$ by computing $\hat{i} = e_1/e_3 \bmod q$ and $ID_{\hat{B}}||ID_{\hat{RC}} = e_2/e_3 \bmod q$, respectively.
3. The merchant computes $\hat{m}' = g_1^{e_1} g_2^{e_2} g_3^{e_3} \bmod p$, and seeks a purchase record $(\hat{coin}', \hat{m}', \hat{M}', \hat{s}', \hat{text}, SIG_{\hat{text}})$ which contains $\hat{m}'$ from purchase records of the content.

Trial:

1. Let $\hat{s} = e_3$. The merchant sends $proof = (ID_{\hat{B}}, ID_{\hat{RC}}, \hat{i}, \hat{s}, \hat{s}', \hat{coin}', \hat{text}, SIG_{\hat{text}})$ to an arbiter. If it is clear from $\hat{text}$ that the redistribution is legal, then the arbiter refuses this trial.
2. The arbiter computes $\hat{h}_1 = g_1^{\hat{i}}$ and sends $\hat{h}_1$ and $ID_{\hat{B}}$ to the registration center $\hat{RC}$ for requesting to submit the signature SIG_{coin} and the ciphertext $enc = (d_1, d_2)$ with respect to $\hat{h}_1$ and $ID_{\hat{B}}$. If the registration center refuses the request, then the arbiter decides that the registration center $\hat{RC}$ is guilty, i.e., the arbiter obtains *center_guilty*.
3. The registration center seeks a registration record which includes $\hat{h}_1$ and $ID_{\hat{B}}$, and sends SIG_{coin} and enc included in the record to the arbiter.
4. The arbiter computes $\hat{h}_4 = g_4^{\hat{i}}$ and verifies that SIG_{coin} is a signature on $(\hat{h}_1, \hat{h}_4, enc)$ with respect to $vk_{\hat{B}}$. If this verification passes, then it is confirmed that $\hat{i}$ is generated by the buyer $\hat{B}$ and the original buyer of the content is the buyer $\hat{B}$. If this verification fails, then the arbiter decides that the registration center $\hat{RC}$ is guilty, i.e., the arbiter obtains *center_guilty*.
5. The arbiter computes $pk_{text} = d_1/d_2^{\hat{i}}$ and verifies that $\hat{pk}_{text} = pk_{text}$ holds where $\hat{pk}_{text}$ is included in $\hat{coin}'$. The arbiter also verifies that $\hat{N}' = g_1^{\hat{i}\hat{s}} g_2^{(ID_{\hat{B}}||ID_{\hat{RC}})\hat{s}} g_3^{\hat{s}} g_4^{\hat{s}'} pk_{text}^{\hat{s}'}$ holds and the validity of $\hat{coin}'$ and $SIG_{\hat{text}}$ where $\hat{N}'$ is included in $\hat{coin}'$. If these verifications pass, then it is confirmed that the buyer $\hat{B}$ has issued $\hat{coin}'$ and has spent $\hat{coin}'$ in the purchase described in $\hat{text}$. If these verifications fail, then the arbiter decides that the merchant is guilty, i.e., the arbiter obtains *merchant_guilty*.
6. If all the above verification passes, then the arbiter decides that the buyer $\hat{B}$ is guilty, i.e., the arbiter obtains *buyer_guilty*.

4 EVALUATION

4.1 Security

The security of the proposed scheme is proved on the following assumptions.

- The Discrete Log assumption [11].
- The Diffie-Hellman assumption [11].
- The involved cryptographic schemes including the embedding protocol in [5] are secure.

First, a lemma is shown. This lemma can be derived from Corollary 8 of [10].

Lemma 1 *On the Discrete Log assumption, there is no polynomial-time algorithm which, on a randomly chosen input generators* $(g_1, g_2, \ldots, g_k)$ *of* G_q *and* $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}_q^k$*, outputs* $(a'_1, a'_2, \ldots, a'_k) \in \mathbb{Z}_q^k$ *such that* $\prod_{i=1}^k g_i^{a_i} = \prod_{i=1}^k g_i^{a'_i}$ *holds and* $a'_l \neq a_l$ *for at least one of* $l \in \{1, 2, \ldots, k\}$*.*

This lemma means that no one can obtain another representation of $\prod_{i=1}^k g_i^{a_i}$ with respect to $(g_1, g_2, \ldots, g_k)$. We will prove that the security requirements given in Definitions 2 and 3 are satisfied by the proposed scheme.

Security for the merchant: To show that the requirement is satisfied, we will show that the merchant can identify the original buyer from a confiscated content. On the assumption that the restrictive blind signature scheme [10] is secure, the buyer B can obtain only such $coin' = (N', pk_{text}, RS(N', pk_{text}))$ that $N' = (h_1 {g_2}^{ID_B||ID_{RC}} g_3 M_1 M_2)^s$ holds, where h_1, M_1 and

M_2 are registered at the registration center RC by the buyer B and s is generated by the buyer B.

From Lemma 1 and the assumption that the embedding protocol [5] is secure, the buyer can obtain only a content in which (e_1, e_2, e_3) is embedded where $m' = g_1^{e_1} g_2^{e_2} g_3^{e_3}$, $coin' = (m'M', pk_{text}, RS(m'M', pk_{text}))$ and $(e_1, e_2, e_3) = (is, (ID_B||ID_{RC})s, s)$ hold. Therefore, the merchant can obtain $(is, (ID_B||ID_{RC})s, s)$ from a confiscated content and can identify the original buyer B.

Security for the buyer: The security for the buyer of the proposed scheme can be proven similar way to the scheme in [5]. Therefore, only the outline of the proof is shown.

As long as the buyer $\hat{B}$ does not redistribute the purchased content and keeps the private information secret, the merchant cannot know $\hat{i}$, and cannot generate $proof = (ID_{\hat{B}}, ID_{\hat{RC}}, \hat{i}, \hat{s}, \hat{s}', \hat{coin}', \hat{text}, SIG_{\hat{text}})$. By colluding with the registration center, the merchant can generate another proof $proof' = (ID_{\hat{B}}, ID_{\hat{RC}}, \tilde{i}, \hat{s}, \hat{s}', \hat{coin}', \hat{text}, SIG_{\hat{text}})$ where $\tilde{i}$ is chosen by the merchant and does not equal $\hat{i}$. However, no registration record includes $\tilde{h}_1 = g_1^{\tilde{i}}$ and the corresponding signature $SIG_{\tilde{coin}}$ because the buyer $\hat{B}$ does not register $\tilde{h}_1$. Therefore, in this case, the merchant cannot convince the arbiter that the honest buyer $\hat{B}$ is guilty.

If the buyer $\hat{B}$ redistributes the purchased content, then the merchant can generate any proof $proof' = (ID_{\hat{B}}, ID_{\hat{RC}}, \tilde{i}, \hat{s}, \hat{s}', \tilde{coin}', \tilde{text}, SIG_{\tilde{text}})$ with $\tilde{i} = \hat{i}$ for any text $\tilde{text}$ by colluding with the registration center. However, for $\tilde{pk}_{text}$ which is included in $\tilde{coin}'$, the equation $\tilde{pk}_{text} = pk_{text}$ does not hold because the merchant does not know the anonymous signing key k. Therefore, as long as the redistribution does not conflict with $text$, the merchant cannot convince the arbiter that the honest buyer $\hat{B}$ is guilty.

Security for the registration center: As mentioned in the security for the merchant, $\hat{i}$ obtained from a confiscated content is the random value $\hat{i}$ which the buyer $\hat{B}$ has generated and registered at the registration center $\hat{RC}$. Therefore, if the registration center follows protocols, the arbiter never decides the registration center is guilty.

Unlinkability: The digital coin involved in the proposed scheme is extended from the digital coin [10] so that the identifiers of the buyer and the registration center, i.e., $ID_B||ID_{RC}$, are used for issuing the coin. Even if the registration center knows N and $ID_B||ID_{RC}$ such that $N = h_1 {g_2}^{ID_B||ID_{RC}} g_3 M$, the signature $RS(N', pk_{text})$ is unlinkable on the assumption that the restrictive blind signature scheme is secure. Therefore, $coin'$ is unlinkable as same as the digital coin [10]. That is, a merchant cannot know whether buyers of two purchases are same or not even if the merchant colludes with the registration center.

4.2 Complexity

In this section, the time complexity of the proposed scheme is given, and is compared with that of the group signature-based anonymous fingerprinting scheme [8]. In [8], it is mentioned that a group signature scheme such as [13] in which the key setup of the revocation manager can execute after the registration of group members can be used for the fingerprinting scheme. In this paper, it is assumed that the group signature-based anonymous fingerprinting scheme [8] involves the group signature scheme [13]. We employ the general measure of the time complexity, that is, the number of modular exponentiations because the modular exponentiation requires greater computational effort than other operations.

The number of modular exponentiations at each protocol and algorithm is summarized in Table 2. In this table, q and q_R denote the security parameters of the proposed scheme and the group signature-based scheme, respectively. The recommended values of q and q_R are

$\log_2 q = 160$ [14] and $\log_2 q_R = 1100$ [13], respectively. This evaluation is not tight in the sense that the actual numbers of modular exponentiations in the group signature-based scheme are larger than those shown in Table 2. The numbers in the proposed scheme are actual.

Table 2: The number of modular exponentiations.

		The proposed scheme				The group signature-based scheme [8] with [13]			
		RC	B	M	A	RC	B	M	A
Preparation		1	–	–	–	1	–	–	–
Registration		25	34	–	–	11	16	–	–
Fingerprinting	Embedding [5]	–	$6\log_2 q + 10$ $= 970$	13	–	–	$2\log_2 q_R + 4$ $= 2204$	5	–
	Other part	–	7	14	–	–	34	32	–
Identification		–	–	3	–	–	–	1	–
Trial		–	–	–	13	–	–	2	4

$\log_2 q = 160$, $\log_2 q_R = 1100$

In the proposed scheme, Registration and Fingerprinting are executed for each purchase. On the other hand, in the group signature-based scheme, Registration is executed only once for all purchase and Fingerprinting is executed for each purchase. The time complexity for the registration center in the proposed scheme is larger than that in the group signature-based scheme. However, in the proposed scheme, the total time complexity for the buyer at each purchase, i.e., the time complexity of Registration and Fingerprinting, is about 45% of the time complexity of Fingerprinting in the group signature-based scheme. For the same environment as in [15] where generating a signature using the group signature scheme takes the signer about 4 seconds, Fingerprinting of the group signature-based scheme is estimated to take the buyer about 270 seconds since the computation of the buyer in Fingerprinting except Embedding of the group signature-based scheme corresponds to generating a signature using the group signature scheme. Then, the computation of the buyer in Fingerprinting of the proposed scheme is reduced to about 120 seconds. For the time complexity required for the merchant at each purchase, the proposed scheme is more efficient than the group signature-based scheme, too. That is, the proposed scheme is more efficient for the buyer and the merchant.

The most of the computation in Fingerprinting is executed for the embedding protocol. The same embedding protocol is involved in the proposed scheme and the group signature-based scheme. In the embedding protocol, the buyer commits the embedded information to the merchant, and proves the knowledge of the embedded information to the merchant in zero-knowledge. The computation for the embedding protocol is according to the size of the embedded information. The size of the embedded information in the proposed scheme is smaller than that in the group signature-based scheme. Therefore, the buyer can execute the embedding protocol more efficiently in the proposed scheme.

The time complexity of Identification for the merchant and that of Trial for the arbiter in the proposed scheme are larger than those in the group signature-based scheme. However, Identification and Trial are not executed frequently, i.e., those are executed only when the merchant confiscates a copy of the content. This can be regarded as a minor disadvantage.

5 CONCLUSION

In this paper, an anonymous fingerprinting scheme with automatic identification is proposed. The security and the time complexity of the proposed scheme are evaluated. The proposed scheme is the first coin-based scheme which has the feature of the automatic identification. The previous anonymous fingerprinting scheme with automatic identification is based on a group signature scheme. By using a digital coin, the time complexity of the buyer and the merchant at each purchase is reduced from that of the previous group signature-based scheme.

We would like to evaluate the time complexity of the proposed scheme experimentally in the real environment to show the degree of the reduction. To make the proposed scheme more efficiently, the scheme should be improved so that less information is embedded in the purchased content, and the efficiency of the embedding scheme should be improved. These are the future work of this study.

6 REFERENCES

[1] G.R. Blakley, C. Meadows, and G.B. Purdy, "Fingerprinting Long Forgiving Message," CRYPTO'85, LNCS 218, pp.180–189, Springer-Verlag, 1986.

[2] B. Pfitzmann and M. Schunter, "Asymmetric Fingerprinting," EUROCRYPT'96, LNCS 1070, pp.84–95, Springer-Verlag, 1996.

[3] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," IBM Reserch Report, RZ2881, (#90829), IBM Reserch Division, 1996.

[4] B. Pfitzmann and A. Sadeghi, "Anonymous fingerprinting with Direct Non-Repudiation," ASIACRYPT 2000, LNCS 1976, pp.401–414, Springer-Verlag, 2000.

[5] B. Pfitzmann and A. Sadeghi, "Coin-Based Anonymous Fingerprinting," EUROCRYPT'99, LNCS 1592, pp.150–164, Springer-Verlag, 1999.

[6] J. Domingo-Ferrer, "Anonymous fingerprinting of Electronic Information with Automatic Identification of Redistributors," Electronics Letters, vol.34, no.13, pp.1303–1304, IEE, 1998.

[7] C. Chung, S. Choi, Y. Choi, and D. Won, "Efficient Anonymous Fingerprinting of Electronic Information with Improved Automatic Identification of Redistributors," ICISC 2000, LNCS 2015, pp.221–234, Springer-Verlag, 2001.

[8] J. Camenisch, "Efficient Anonymous Fingerprinting with Group Signatures," ASIACRYPT 2000, LNCS 1976, pp.415–428, Springer-Verlag, 2000.

[9] A. Sadeghi, "How to Break a Semi-anonymous Fingerprinting Scheme," Information Hiding 2001, LNCS 2137, pp.384–394, Springer-Verlag, 2001.

[10] S. Brands, "An Efficient Off-line Electronic Cash System Based On The Representation Problem," Certurn voor Wiskunde en Informatica, Computer Science/Department of Algorithmics and Architecture, Report CS-R9323, 1993.

[11] S. Brands, "Untraceable Off-line Cash in Wallet with Observers," CRYPTO'93, LNCS 773, pp.302–318, Springer-Verlag, 1994.

[12] C.P. Schnorr, "Efficient Signature Generation by Smart Card," Journal of Cryptology, vol.4, no.3, pp.161–174, Springer-Verlag, 1991.

[13] J. Camenisch and M. Michels, "Separability and Efficiency for Generic Group Signature Schemes," CRYPTO'99, LNCS 1666, pp.413–430, Springer-Verlag, 1999.

[14] Information-technology Promotion Agency, Japan, CRYPTREC Report 2002, 2003.

[15] T. Kato, K. Okada, and T. Yoshida , "Development of Anonymous Authentication System for Personal Data Protection," (in Japanese) CSS 2003, pp.569–574, Information Processing Society of Japan, 2003.