Regular Paper

Group Signature Scheme with Signature Tracing and Its Application to an Electronic Coupon System

Toru Nakanishi† and Yuji Sugiyama†

A group signature scheme allows a group member to sign messages on the group's behalf in such a way that the signature does not reveal the member's identity. It also has the property of unlinkability, which means that it is infeasible to determine whether two signatures were made by the same member. In the scheme, only a designated trusted third party can identify the member who issued a given signature. However, given a member's identity, this third party cannot trace signatures issued by the member, while the anonymity and unlinkability of unrelated members' signatures are not corrupted. We call the latter type of tracing signature tracing. In this paper, a group signature scheme with signature tracing is proposed. In some application systems, signature tracing is useful for preventing illegal users from accessing a service. As an application of the group signature scheme, we propose an electronic coupon system, where the properties of anonymity and unlinkability are satisfied in normal cases, and, in exceptional cases, the anonymity of payments can be revoked in both directions from the payment to the withdrawal, leading to the customer's identity, and from the withdrawal to the payment.

1. Introduction

The *group signature scheme* is a cryptographic concept introduced by Chaum and van Heijst[1]. It allows a group member to anonymously sign messages on group's behalf. In addition to the anonymity of each signature, a stronger anonymity property, called unlinkability, is also satisfied. Unlinkability means the infeasibility of determining whether two signatures were made by the same signer. However, the anonymity of the signature can be revoked by a trusted third party, called a trustee, in an exceptional case such as a dispute. Camenisch and Stadler[2] proposed the first practical group signature schemes, in the sense that the lengths of a group's public key and signatures do not depend on the size of the group. Group signature schemes have been applied to the various cryptographic systems requiring the anonymous authentication such as electronic cash[3], bidding[4], and voting[5] systems.

Group signature schemes have the property that the trustee can trace a signer's identity (via the view in the signer's membership registration protocol) from a targeted signature, while the other signatures remain anonymous and unlinkable. On the other hand, such schemes do not have the property that, given a targeted member's identity or registration view, the trustee can trace the signatures issued by that member while the other signatures remain anonymous and unlinkable. We call the former type of tracing signer tracing, and the latter signature tracing. If the trustee tries to perform signer tracing on all signatures, he or she can find the signatures made by the targeted member, but, in this case, the anonymity of the unrelated signatures is corrupted. In this paper☆, a group signature scheme with signature tracing is proposed. Note that, since signature tracing violates the unlinkability of the signatures issued by the targeted member, the unlinkability of only the signatures that are not traced is satisfied. In some applications of the group signature scheme, group signature is used to verify that a signer possesses some privilege. For example, in voting, group signature is used to authenticate suffrage. If our group signature scheme with signature tracing is used, it can prevent an illegal voter, such as one who has been disenfranchised, from casting a vote by tracing his group signature. Another type of application requiring signature tracing is the electronic coupon system.

The electronic coupon system was proposed by Okamoto and Ohta[8] as a variant of the electronic cash system. The merit of this system is that a customer withdraws a ticket from the bank and the customer can divide it into

† Department of Communication Network Engineering, Faculty of Engineering, Okayama University

☆ Preliminary versions of the paper appeared in SCIS '99[6] and ISW '99[7].

sub-tickets to pay for items purchased in a shop. However, though this system provides anonymity for each payment, the payments derived from the same ticket are linkable; it is possible to determine whether the payments were made by the same payer. The linked payments enable the other one to trace the payer by other means (that is, by correlating the payments' locality, date, frequency, etc.), as noted by Pfitzmann and Waidner[9]. Furthermore, since this system does not have any method for revoking the anonymity in exceptional cases, it can be attacked by using complete anonymity, for purposes such as the blackmailing and illegal purchases[10),11)].

In an electronic cash system, there are two types of revocation procedure: owner tracing, to identify the person who made a payment, and coin tracing, to link the withdrawal of a coin to the payments of the coin. Owner tracing allows a person who made an illegal purchase to be identified, while coin tracing allows the payments of a coin obtained illegally, such as in a blackmailing attack[12)], to be traced. In such an attack, a customer is blackmailed and is forced to withdraw a coin, so that the blackmailer can pay the coin without being identified. When coin tracing is provided and the attacked customer complains about the withdrawal, payments made with the withdrawn coin can be traced and blocked. Furthermore, coin tracing is also useful for tracing a seller of illegal goods from a detected buyer through the payments made between them, as shown by Davida, et al.[10)].

This paper proposes an electronic coupon system using the proposed group signature scheme, where the properties of anonymity and unlinkability are satisfied in normal cases, and, in exceptional cases, the anonymity of payments can be revoked by owner tracing and coin tracing, called ticket tracing in the coupon system. Note that ticket tracing violates the unlinkability of all payments made with a withdrawn ticket. Since the group signature scheme has signature tracing as well as signer tracing, ticket tracing is possible as well as owner tracing.

This paper is organized as follows: In Section 2, the group signature scheme with signature tracing is defined, the building blocks used in the proposed scheme are introduced, a concrete group signature scheme is presented, and its security is discussed. In Section 3, after the requirements of the electronic coupon system have been reviewed, an electronic coupon system using the group signature scheme with signature tracing is proposed, and its security is discussed. Finally, Section 4 concludes the paper.

2. Group Signature Scheme with Signature Tracing

2.1 Definition

After the schemes of Camenisch and Stadler[2)], some group signature schemes[13)~15)] with no dependency on the group size were proposed, all of them using membership certificates. Since our scheme is also of this type, a definition of the type is given.

Definition 1 A group signature scheme consists of the following procedures:

Setup: Probabilistic algorithms that, on input of security parameter, output the group's public keys and the corresponding secret keys of the group manager and trustee.

Registration: An interactive protocol between the group manager and a user joining the group, where the user outputs a membership certificate and a membership secret.

Signing: A probabilistic algorithm that, on input of a group's public key, a membership certificate, a membership secret and a message, outputs a group signature on the message.

Verification: An algorithm that, on input of a message, a group signature on it, and a group's public key, determines the validity of the group signature on the message with respect to the group's public key.

Signer tracing: An algorithm that, on input of a message, a group signature on it, a group's public key, and a trustee's secret key, outputs the identity of the signer or the view of the registration of the signer. □

Definition 2 A secure group signature scheme satisfies the following properties:

Unforgeability: Only group members can sign messages.

Anonymity and unlinkability: It is neither feasible to decide which member signed a message (Anonymity), nor to decide whether two signatures were made by the same signer (Unlinkability).

No framing: Neither a group member nor the group manager can sign messages on behalf of other members. □

Now, we define signature tracing on the secure group signature scheme as follows:

Definition 3

Signature tracing: An algorithm that, on input of a message, a group signature on it, a view of the registration of a member, a group's public key, and a trustee's secret key, determines whether the group signature is made by the member who conducted the registration. The anonymity and unlinkability of signatures other than that of the traced member must be maintained. □

2.2 Building Blocks

The proposed scheme is extended from the group signature scheme of Camenisch and Stadler[2]. As primitives to prove the knowledge of secret values without leaking any useful information, signatures based on zero-knowledge proofs of knowledge (SPKs) are used in the proposed scheme as well as the original scheme. This subsection defines SPKs. These are converted from zero-knowledge proofs of knowledge (PKs) by the so-called Fiat-Shamir heuristic[16]. That is, the prover determines the challenge by applying a collision-resistant hash-function to the commitment and the signed message and then computes the response as usual. The resulting signature consists of the challenge and the response. Such SPKs can be proven to be secure in the random oracle model[17], given the security of the underlying PKs. Let $SPK_i\{(\alpha, \beta, \ldots) : Predicates\}(m)$ be the signature on message m proving that the signer knows $\alpha, \beta, \ldots$ satisfying the predicates $Predicates$. In this notation, the index i refers to the definition of a particular SPK_i in this subsection, Greek letters denote secret knowledge, and the other letters denote public parameters for both the signer and the verifier. In the proposed scheme as well as the original scheme, which is based on the hardness of the discrete logarithm problem, the relations among the discrete logarithms from cyclic groups are used as predicates to prove. Let $G = \langle g \rangle$ be a cyclic group of order n, which is a subgroup of Z_p^* for a prime $p = 2n + 1$. Let $G' = \langle g' \rangle$ be a cyclic group of order p, which is a subgroup of $Z_{p'}^*$ for a prime $p' = 2p + 1$. The discrete logarithm of $y \in G$ to the base g is $x \in Z_n$ satisfying $y = g^x$. We denote $x = \log_g y$. This is extended to a representation of $y \in G$ to the bases $g_1, g_2, \ldots g_k \in G$ which are $x_1, x_2, \ldots x_k \in Z_n$ satisfying $y = g_1^{x_1} \cdot g_2^{x_2} \cdots g_k^{x_k}$ if such x_i's exist. The double discrete logarithm of $y' \in G'$ to the bases g' and g is $x \in Z_n$ satisfying $y' = g'^{(g^x)}$ if such an x exists. The e-th root of the discrete logarithm of $y \in G$ to the base g is $x \in Z_n$ satisfying $y = g^{(x^e)}$ if such an x exists.

Here, the notations in this paper are shown. The symbol $\|$ denotes the concatenation of two strings. Let $c[i]$ be the i-th rightmost bit of the string c. If A is a set, $a \in_R A$ means that a is chosen at random from A according to the uniform distribution. We assume a collision-resistant hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^k$ ($k \approx 160$).

The first type of SPK is the signature proving the knowledge of representations[2].

Definition 4 An SPK proving the knowledge of representations of $y_1, \ldots, y_w \in G$ to the bases $g_1, \ldots, g_v \in G$ on message m is denoted as

$$SPK_1\left\{(\alpha_1, \ldots, \alpha_u) : \left(y_1 = \prod_{j=1}^{l_1} g_{b_{1j}}^{\alpha_{e_{1j}}}\right) \wedge \cdots \wedge \left(y_w = \prod_{j=1}^{l_w} g_{b_{wj}}^{\alpha_{e_{wj}}}\right)\right\}(m),$$

where constants $l_i \in \{1, \ldots v\}$ indicate the number of bases of y_i, the indices $e_{ij} \in \{1, \ldots, u\}$ refer to the elements $\alpha_1, \ldots, \alpha_u$ and the indices $b_{ij} \in \{1, \ldots, v\}$ refer to the bases $g_1, \ldots, g_v$. □

The signature consists of a $(u + 1)$-tuple $(c, s_1, \ldots, s_u) \in \{0,1\}^k \times (Z_n)^u$ satisfying

$$c = \mathcal{H}\left(m\|y_1\|\cdots\|y_w\|g_1\|\cdots\|g_v \|\{\{e_{ij}, b_{ij}\}_{j=1}^{\ell_i}\}_{i=1}^{w}\|y_1^c \prod_{j=1}^{\ell_1} g_{b_{1j}}^{s_{e_{1j}}}\|\cdots \|y_w^c \prod_{j=1}^{\ell_w} g_{b_{wj}}^{s_{e_{wj}}}\right).$$

This signature is computed as follows: The signer chooses $r_i \in_R Z_n$ for $i = 1, \ldots, u$, computes c as

$$c = \mathcal{H}\left(m\|y_1\|\cdots\|g_v\|\{\{e_{ij}, b_{ij}\}_{j=1}^{\ell_i}\}_{i=1}^{w} \| \prod_{j=1}^{\ell_1} g_{b_{1j}}^{r_{e_{1j}}}\|\cdots\|\prod_{j=1}^{\ell_w} g_{b_{wj}}^{r_{e_{wj}}}\right),$$

and sets $s_i = r_i - c\alpha_i \bmod n$ for $i = 1, \ldots, u$.

For example, $SPK_1\{(\alpha, \beta) : y_1 = g^\alpha \wedge y_2 = h^\beta g^\alpha\}(m)$ is the SPK on m of an entity knowing the discrete logarithm of y_1 to the base g and a representation of y_2 to the bases h and g, where the g-part of this representation equals the discrete logarithm of y_1 to the base g.

The second type is the SPK proving the knowledge of the e-th root of the discrete logarithm of $y \in G$ to the base g on m. The third type is the SPK proving the knowledge of the e-th root of the g-part of a representation of $y \in G$ to the bases h, g on m. If e is small, both can be efficiently constructed[2]. Since the former SPK can be constructed from the latter, the latter and the former are shown in turn. Hereafter, we assume that an element $h \in G$ is available whose discrete logarithm to the base g is unknown.

Definition 5 An SPK of the e-th root of the g-part of a representation of $y \in G$ to the bases h, g on m is denoted as

$$SPK_2\{(\beta, \gamma) : y = h^\beta g^{\gamma^e}\}(m).$$

□

The signature consists of an $(e-1)$-tuple $(v_1, \ldots, v_{e-1}) \in G^{e-1}$ and an SPK:

$$SPK_1\{(\alpha_1, \ldots, \alpha_e, \alpha') : v_1 = h^{\alpha_1} g^{\alpha'} \wedge v_2 = h^{\alpha_2} v_1^{\alpha'} \wedge \cdots \wedge v_{e-1} = h^{\alpha_{e-1}} v_{e-2}^{\alpha'} \wedge y = h^{\alpha_e} v_{e-1}^{\alpha'}\}(m).$$

Definition 6 An SPK of the e-th root of the discrete logarithm of $y \in G$ to the base g on m is denoted as

$$SPK_3\{\delta : y = g^{\delta^e}\}(m).$$

□

The signature consists of two SPKs:

$$SPK_2\{(\alpha_1, \alpha_2) : y = h^{\alpha_1} g^{\alpha_2^e}\}(m), \text{ and } SPK_1\{\alpha_3 : y = g^{\alpha_3}\}(m).$$

The final type of SPK allows the signer to prove that a part of a representation equals the double discrete logarithm. We assume that another element $\tilde{h} \in G$ is available whose discrete logarithm to the base g is unknown.

Definition 7 Let $\ell < k$ be a security parameter. An SPK of the representation of $y \in G$ to the bases h, g and the double discrete logarithm of $y' \in G'$ to the bases g' and $\tilde{h}$ on m, where the h-part of the representation of y to the bases h and g equals the double discrete logarithm of y' to the bases g' and $\tilde{h}$, is denoted as

$$SPK_4\{(\epsilon, \zeta) : y = h^\epsilon g^\zeta \wedge y' = g'^{(\tilde{h}^\zeta)}\}(m).$$

□

It consists of a $(2\ell+1)$-tuple $(c, s_{11}, \ldots, s_{1\ell}, s_{21}, \ldots, s_{2\ell}) \in \{0,1\}^k \times (Z_n)^{2\ell}$ satisfying

$$c = \mathcal{H}(m \| y \| y' \| g \| h \| \tilde{h} \| g' \| t_{11} \| \cdots \| t_{1\ell} \| t_{21} \| \cdots \| t_{2\ell}),$$

where

$$t_{1i} = y^{c[i]} h^{s_{1i}} g^{s_{2i}},$$

$$\text{and } t_{2i} = \begin{cases} g'^{(\tilde{h}^{s_{2i}})} & (c[i] = 0), \\ y'^{(\tilde{h}^{s_{2i}})} & (\text{otherwise}). \end{cases}$$

This signature is computed as follows: The signer chooses $r_{1i}, r_{2i} \in_R Z_n$ to compute $t^*_{1i} = h^{r_{1i}} g^{r_{2i}}, t^*_{2i} = g'^{(\tilde{h}^{r_{2i}})}$ for $i = 1, \ldots, \ell$, sets c as

$$c = \mathcal{H}(m \| y \| y' \| g \| h \| \tilde{h} \| g' \| t^*_{11} \| \cdots \| t^*_{1\ell} \| t^*_{21} \| \cdots \| t^*_{2\ell}),$$

and computes $s_{1i} = r_{1i} - c[i]\epsilon \bmod n$ and $s_{2i} = r_{2i} - c[i]\zeta \bmod n$ for $i = 1, \ldots, \ell$.

This is derived from Stadler's SPK[18], which is an SPK to prove that a discrete logarithm equals a double discrete logarithm. This SPK about the discrete logarithm is straightforwardly extended to the SPK about the representation of Definition 7, by the technique used in SPK_1. Furthermore, another difference between this SPK used in this paper and Stadler's one is the orders of G and G'. The orders of G and G' in this paper are different, and are not prime and prime, respectively, though the orders in Stadler's one are the same prime. This difference does not affect the proof that the underlying PK is a zero-knowledge proof of knowledge.

2.3 Proposed Scheme

In this subsection, we propose a group signature scheme with signature tracing, which is extended from the scheme of Camenisch and Stadler[2].

Let f be a one-way function, let Sig_M be a group manager's signing function in the general digital signature scheme, and let Enc_R be a trustee's encryption function in the public encryption scheme. Informally, the original scheme is as follows: In the registration, a user joining a group sends the group manager $f(x)$ for a membership secret x, and the user obtains a membership certificate $Sig_M(f(x))$. The group signature consists of $Enc_R(f(x))$ and the SPK proving the knowledge of a cer-

tificate on $f(x)$ that the encryption contains. Signer tracing is that the trustee decrypts the encryption.

In our extension, the idea of signature tracing is follows: In the registration, the user additionally sends the manager $Enc_R(g(x))$, where g is another one-way function. The group signature consists of the original one, $h(g(x))$ and the SPK proving the validity, where h is one of the one-way functions and a different function is used for a different group signature. Then, signature tracing is accomplished by decrypting $Enc_R(g(x))$ in a targeted registration to decide whether the $h(g(x))$ part of a group signature is computed from the decrypted $g(x)$.

Now, the proposed scheme is described in detail. Assume that each participant publishes the public key of any digital signature scheme and keeps the corresponding secret key. In all the procedures except signing, the values sent by each participant are signed on the digital signature scheme. The symbol $\tilde{0}$ denotes the empty string.

Setup:

(1) The group manager computes the following:
- An RSA modulus n and two public exponents $e_1, e_2 > 1$
- Two integers $f_1, f_2 > 1$
- A cyclic group $G = \langle g \rangle$ of order n, which is a subgroup of Z_p^* for a prime $p = 2n + 1$
- Elements $h, \tilde{h} \in G$ whose discrete logarithms to base g are unknown
- Another cyclic group $G' = \langle g' \rangle$ of order p, which is a subgroup of $Z_{p'}^*$ for a prime $p' = 2p + 1$

The public key for the manager is $\mathcal{Y}=(n, e_1, e_2, f_1, f_2, G, g, h, \tilde{h}, G', g')$, and the secret key is the factorization of n. Note that e_1, e_2, f_1, and f_2 must satisfy the condition that solving the congruence $f_1 x^{e_1} + f_2 \equiv v^{e_2} \pmod{n}$ is infeasible. The choices for e_1, e_2, f_1, and f_2 are discussed by Camenisch and Stadler[2].

(2) The trustee chooses $\rho \in_R Z_n^*$ to compute $y_R = h^\rho$. The trustee makes y_R public, and keeps ρ secret.

Note that this procedure is the same as that in the original scheme, except the selection of $G', g', \tilde{h}$ and that G is a subgroup of Z_p^*, which is any group of order n in the original.

Registration:

(1) A user joining a group chooses $x \in_R Z_n^*$ to compute $y = x^{e_1} \bmod n$ and $z = g^y$. Then, the user chooses $r_1, r_2 \in_R Z_n^*$ to compute $\tilde{y} = r_1^{e_2}(f_1 y + f_2) \bmod n, C_1 = h^{r_2}\tilde{h}^y$, and $C_2 = y_R^{r_2}$. Furthermore, the user computes the following SPKs:

$$V_1 = SPK_3\{\alpha : z = g^{\alpha^{e_1}}\}(\tilde{0}),$$

$$V_2 = SPK_3\{\beta : g^{\tilde{y}} = (z^{f_1} g^{f_2})^{\beta^{e_2}}\}(\tilde{0}),$$

$$V_3 = SPK_1\{(\gamma, \delta) : C_1 = h^\gamma \tilde{h}^\delta \wedge C_2 = y_R^\gamma \wedge z = g^\delta\}(\tilde{0}).$$

The user sends the manager $(\tilde{y}, z, C_1, C_2, V_1, V_2, V_3)$. The newly added parts from the original scheme are C_1, C_2, and V_3. (C_1, C_2) is the ElGamal encryption[19] of $\tilde{h}^y$. V_3 ensures the validity; that is, (C_1, C_2) is the ElGamal encryption of an element, where the discrete logarithm of the element to the base $\tilde{h}$ equals that of z to the base g.

(2) If V_1, V_2, and V_3 are correct, the manager sends the user $\tilde{v} = \tilde{y}^{1/e_2} \bmod n$.

(3) As well as the original scheme, the user computes $v = \tilde{v}/r_1 \bmod n$ to obtain a membership certificate v for the membership secret x, where $v \equiv (f_1 x^{e_1} + f_2)^{1/e_2} \pmod{n}$.

Signing: When a group member signs a message m, the member first makes the original group signature as follows: The member computes $\tilde{C_1} = h^{\tilde{r_1}} g^y$ and $\tilde{C_2} = y_R^{\tilde{r_1}}$, where $\tilde{r_1} \in_R Z_n^*$, and computes the following SPKs:

$$\tilde{V_1} = SPK_2\{(\alpha, \beta) : \tilde{C_1} = h^\alpha g^{\beta^{e_1}}\}(m),$$

$$\tilde{V_2} = SPK_2\{(\gamma, \delta) : \tilde{C_1}^{f_1} g^{f_2} = h^\gamma g^{\delta^{e_2}}\}(m),$$

$$\tilde{V_3} = SPK_1\{(\epsilon, \zeta) : \tilde{C_1} = h^\epsilon g^\zeta \wedge \tilde{C_2} = y_R^\epsilon\}(m).$$

Furthermore, as the newly added parts, the member chooses $\tilde{r_2} \in_R Z_p^*$ to compute $\tilde{g'} = g'^{\tilde{r_2}}, \tilde{D} = \tilde{g'}^{\tilde{h}^y}$ and the following SPKs:

$$\tilde{V_4} = SPK_4\{(\eta, \theta) : \tilde{C_1} = h^{\eta} g^{\theta} \wedge \tilde{D} = \tilde{g'}^{\tilde{h}^{\theta}}\}(m).$$

The group signature is $(\tilde{C_1}, \tilde{C_2}, \tilde{g'}, \tilde{D}, \tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4})$.

Note that $(\tilde{C_1}, \tilde{C_2})$ is the ElGamal encryption of $z = g^y$. $\tilde{V_4}$ ensures that the discrete logarithm of the encrypted element z to the base g equals the double discrete logarithm of $\tilde{D}$ to the bases $\tilde{g'}$ and $\tilde{h}$.

Verification: The verification of the group signature $(\tilde{C_1}, \tilde{C_2}, \tilde{g'}, \tilde{D}, \tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4})$ is the verification of the SPKs $\tilde{V_1}, \tilde{V_2}, \tilde{V_3}$, and $\tilde{V_4}$.

Signer tracing: This is the same as in the original scheme. The trustee decrypts $(\tilde{C_1}, \tilde{C_2})$ to obtain $z = g^y$. The value leads to the identity of the signer. To show the validity of tracing, the trustee proves that $(\tilde{C_1}, \tilde{C_2})$ is decrypted into z by an SPK. (Refer to the original scheme[2] for details.)

Signature tracing:

(1) From the view of the targeted registration $(\tilde{y}, z, C_1, C_2, V_1, V_2, V_3)$, the group manager sends the trustee (C_1, C_2).

(2) The trustee sends the manager $\hat{h} = C_1 / C_2^{1/\rho}$, which should be $\tilde{h}^y$, and $SPK_1\{\alpha : C_1 = \hat{h} C_2^{\alpha} \wedge h = y_R^{\alpha}\}(\tilde{0})$. This SPK proves that (C_1, C_2) is decrypted into $\hat{h}$.

(3) For the sent $\hat{h}$, the manager (and anyone who received the value) checks whether $\tilde{D} = \tilde{g'}^{\hat{h}}$ holds on a group signature $(\tilde{C_1}, \tilde{C_2}, \tilde{g'}, \tilde{D}, \tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4})$. If it holds, the signature is derived from the targeted registration.

2.4 Security

It is shown that the proposed scheme satisfies the security requirements in Section 2.1. The proposed scheme is based on the infeasibility of comparing discrete logarithms and of computing the double discrete logarithms, the security of the ElGamal encryption, and the security of the original group signature scheme.

Unforgeability: This property is satisfied because of the unforgeability of the original scheme.

Anonymity and unlinkability: Only the newly added parts are discussed here. The added part of the registration is (C_1, C_2, V_3). (C_1, C_2) does not leak information since it is the ElGamal encryption. V_3 also does not leak information, since it is an SPK. Thus, the registration does not affect the anonymity and unlinkability. The added part of the signature is $(\tilde{g'}, \tilde{D}, \tilde{V_4})$. Similarly, the SPK $\tilde{V_4}$ does not leak information. Therefore, the possibly available values are $\tilde{g'}$ and $\tilde{D}$. First, the anonymity is discussed. To identify the signer, the decision $\log_{\tilde{h}}(\log_{\tilde{g'}} \tilde{D}) = \log_g z$ is required. However, it can be proved that this decision is infeasible, as follows:

Assume on the contrary that a probabilistic polynomial time algorithm M decides whether $\log_{\bar{h}}(\log_{\bar{g'}} \bar{D})$ and $\log_g z$ are the same with a non-negligible probability. Then, the following probabilistic polynomial time algorithm $\bar{M}$ with the inputs $\bar{h}_1, \bar{h}_2, \bar{z}_1, \bar{z}_2 \in G$ can be constructed:

First, $\bar{M}$ chooses $\dot{g} \in_R G'$. Next, from it and the input $\bar{z}_1$, $\bar{M}$ computes $\dot{D} = \dot{g}^{\bar{z}_1}$. Finally, $\bar{M}$ runs M with the inputs $\tilde{g'} = \dot{g}$, $\tilde{D} = \dot{D}$, $\tilde{h} = \bar{h}_1$, $g = \bar{h}_2$, and $z = \bar{z}_2$.

Then, since $\log_{\tilde{h}}(\log_{\tilde{g'}} \tilde{D}) = \log_{\bar{h}_1} \bar{z}_1$ and $\log_g z = \log_{\bar{h}_2} \bar{z}_2$, $\bar{M}$ can decide whether $\log_{\bar{h}_1} \bar{z}_1$ and $\log_{\bar{h}_2} \bar{z}_2$ are the same with non-negligible probability. This contradicts the infeasibility of deciding the sameness of discrete logarithms. Thus, the decision of $\log_{\tilde{h}}(\log_{\tilde{g'}} \tilde{D}) = \log_g z$ is also infeasible.

Therefore, the property of anonymity holds.

In the case of the linking of signatures, a decision on the equality of the discrete logarithms is required. Owing to its infeasibility, the property of unlinkability also holds.

No framing: In the original group signature, in order to sign on behalf of another member, that member's secret key x is required. As discussed in the confirmation of the anonymity and unlinkability, the possibly available values are $\tilde{g'}$ and $\tilde{D}$. However, to obtain x from them involves computing a double discrete logarithm. Since this computation is infeasible[2], the condition of no framing holds.

Now, we show the validity of signature tracing in the proposed scheme. First, we observe that the signatures of the member who performed the targeted registration are found by this signature tracing. Owing to the soundness of the SPKs, it is ensured that (C_1, C_2) in the targeted registration is the encryption of

$\tilde{h}^y$. Similarly, the SPK made by the trustee ensures that the decrypted value $\hat{h}$ in Step (2) of signature tracing equals $\tilde{h}^y$. On the other hand, for $(\tilde{g'}, \tilde{D})$ in each group signature, the SPKs in the signature ensures that $\tilde{D} = \tilde{g'}^{\tilde{h}^y}$. Since this function from y to $\tilde{D}$ is a bijection, the verification equation $\tilde{D} = \tilde{g'}^{\hat{h}}$ in Step (3) of signature tracing holds if and only if y in $\hat{h} = \tilde{h}^y$ is the same as y in $\tilde{D} = \tilde{g'}^{\tilde{h}^y}$. This implies that the member who performed the targeted registration is the signer. Thus, the signatures of the member are found by this signature tracing. The anonymity and unlinkability of the other signatures remain, since the encryptions (C_1, C_2) of the other signers are not decrypted.

3. Electronic Coupon System Using a Group Signature Scheme with Signature Tracing

In this section, the group signature scheme proposed in the previous section is applied to an electronic coupon system. In the coupon system, the anonymity and unlinkability are satisfied in normal cases, and, in exceptional cases, the anonymity of payments can be revoked in both directions from the payment to the withdrawal (leading to the customer's identity), and from the withdrawal to the payment.

3.1 Requirements

The participants in an electronic coupon system are customers, shops, a bank, and a trustee. The system consists of setup, withdrawal, payment, deposit, and anonymity revocation protocols.

The requirements for an electronic coupon system are as follows[8),11)]:

Unforgeability: Tickets and transcripts of payments cannot be forged.

Unreusability: The customer who spends a sub-ticket twice or more can be identified.

No swindling: No one except the customer who withdraws a ticket can spend a sub-ticket derived from the ticket. The deposit information can not be forged.

Anonymity: No one except the payer and the trustee can trace the payer from the payment.

Unlinkability: No one except the payer and the trustee can determine whether any pair of payments was made by the same customer.

Anonymity revocation: Anonymity of a transcript of a payment can be revoked only by the trustee and only when necessary, in which case the following revocation procedures should be accomplished:

- **Owner tracing:** To identify the payer of a payment.
- **Ticket tracing:** To link the withdrawal of a ticket to the payments derived from the ticket.

Only the transcript for which a judge's order is given must be de-anonymized.

Divisibility: A ticket is divided into many sub-tickets whose face values are fixed in advance, and the summation of the face values of all sub-tickets is equal to the face value of the original ticket.

Off-line-ness: During payments, the payer communicates only with the shop.

3.2 Proposed System

In the proposed system, a variant of the group signature scheme, called a partially linkable group signature scheme, is used. The linkable group signature scheme[5)] enables a verifier to check whether or not two signatures were made by the same signer without leaking other useful information. The partially linkable group signature scheme enables a verifier to check linking between only signatures agreed by the participants in advance. This idea is introduced by Nakanishi and Fujiwara[20)], and is used independently in a variant of the group signature scheme of Ateniese and Tsudik[21)].

Linkability is introduced by adding $\tilde{f}(x)$ to a group signature, where $\tilde{f}$ is a one-way function and x is a signer's membership secret. Group signatures using the same $\tilde{f}$ become linkable and those using different $\tilde{f}$ become unlinkable. The modification from the scheme in the previous section is as follows: First, in the setup, the participants agree on t which denotes the number of set of linkable signatures, and bases $h'_i \in G'$ $(1 \leq i \leq t)$, whose discrete logarithms to base g' are unknown. The group signature for the i-th set uses $\tilde{h'}_i$ instead of $\tilde{g'}$. Then, when the same $\tilde{h'}_i$ is used for signatures, the signatures are issued by the same signer if $\tilde{D} = \tilde{h'}_i^{\tilde{h}^y}$ of them are the same, and are not issued by the same signer otherwise. On the other hand, when different $\tilde{h'}_i$ and $\tilde{h'}_j$ are used for signatures, they cannot be linked, since the bases of $\tilde{D}$ are different.

Now, we describe an electronic coupon system using the partially linkable group signature

scheme with signature tracing.

Setup: The type of coupon (The face values of the ticket and sub-tickets, the number of sub-tickets, etc.) is agreed by the participants. Then, the group signature scheme is set up. The type is assigned to the public key of the scheme. If different types are used, different public keys are used. Assume that there are t sub-tickets and that each sub-ticket is indexed by i $(1 \leq i \leq t)$.

Withdrawal: The group signature scheme is registered, with a bank playing the role of a group manager and a withdrawing customer playing the role of a user joining a group. As a result, the customer obtains a membership secret x and a membership certificate v for x. The certificate is a ticket that the customer can pay. The bank charges the customer's account the face value of the ticket.

Payment: Assume that each shop owns a unique identifier. Let m be the concatenation of the identifier of the shop obtaining the payment and the time when the payment is made. When the customer pays the i-th sub-ticket, the customer sends the shop the customer's group signature on message m using the base $\tilde{h'}_i$. The shop verifies the validity of the group signature. If the signature is valid, this payment is permitted.

Deposit: The shop sends the bank the group signature as the transcript of the payment. The bank verifies the validity of the signature. Then, the bank checks whether the payment causes the sub-ticket to be overspent by checking whether $(i, \tilde{D})$ in the transcript occurs in the transcripts of all previously deposited payments. If it occurs, the owner tracing protocol follows, since the sub-ticket of the payment is overspent. Otherwise, the face value of the subticket is deposited in the shop's account, and the transcript of the payment is kept in the bank's database.

Anonymity revocation: The anonymity revocation is straightforward. The owner is traced by signer tracing, and the ticket is traced by signature tracing.

3.3 Security

It is discussed that the proposed protocol satisfies the requirements in Section 3.1.

Unforgeability: Because of the unforgeability of the membership certificate and group signature, it is infeasible to forge the ticket and transcript of the payment, respectively.

Unreusability: The linkability of the group signature allows the bank to decide whether two transcripts of payments use the same sub-ticket. The over-spender is identified by owner tracing.

No swindling: Since no one can compute another member's group signature, no one can pay sub-tickets of another customer's ticket.

The deposit information is a transcript of a payment. The transcript is unforgeable, it cannot be replayed owing to the uniqueness of the signed message, and no one can spend another customer's sub-tickets. Therefore, the deposit information cannot be forged.

Anonymity and unlinkability: These properties are satisfied owing to the anonymity and unlinkability of the group signature.

From the description of the protocol, it can be shown straightforwardly that the properties of anonymity revocation, divisibility, and off-line-ness hold.

4. Conclusion

In this paper, a group signature scheme with signature tracing has been proposed, and applied to an electronic coupon system, where the properties of anonymity and unlinkability are satisfied in normal cases, and, in exceptional cases, the anonymity of payments can be revoked by owner and ticket tracing. In the proposed scheme, SPK_4 is less efficient than the other SPKs. An open problem is to propose a group signature scheme with signature tracing where only the efficient SPKs are used. In addition, the security of our scheme is based on the heuristic assumption of the infeasibility of computing (x, v) that satisfies $f_1 x^{e_1} + f_2 \equiv v^{e_2} \pmod{n}$, as in the original scheme[2]. Thus, another open problem is to propose a scheme where the security is proved on the basis of a theoretical clarification of the cryptographic assumptions.

References

1) Chaum, D. and van Heijst, E.: Group Signatures, *Advances in Cryptology—EUROCRYPT '91*, LNCS 547, pp.241–246, Springer-Verlag (1991).

2) Camenisch, J. and Stadler, M.: Efficient Group Signature Schemes for Large Groups, *Advances in Cryptology—CRYPTO '97*, LNCS

1294, pp.410–424, Springer-Verlag (1997).
3) Lysyanskaya, A. and Ramzan, Z.: Group Blind Digital Signatures: A Scalable Solution to Electronic Cash, *2nd Financial Cryptography Conference* (*FC '98*), LNCS 1465, pp.184–197, Springer-Verlag (1998).
4) Chen, L. and Pedersen, T.P.: On the Efficiency of Group Signatures Providing Information-Theoretic Anonymity, *Advances in Cryptology—EUROCRYPT '95*, LNCS 921, pp.39–49, Springer-Verlag (1995).
5) Nakanishi, T., Fujiwara, T. and Watanabe, H.: A Linkable Group Signature and Its Application to Secret Voting, *Trans. IPS Japan*, Vol.40, No.7, pp.3085–3096 (1999).
6) Nakanishi, T., Haruna, N. and Sugiyama, Y.: Electronic Coupon Ticket Protocol with Unlinkable Trascripts of Payments, *Proc. 1999 Symposium on Cryptography and Information Security, W4-3.2*, pp.359–363 (1999).
7) Nakanishi, T., Haruna, N. and Sugiyama, Y.: Unlinkable Electronic Coupon Protocol with Anonymity Control, *Proc. Second International Information Security Workshop* (*ISW '99*), LNCS 1729, pp.37–46, Springer-Verlag (1999).
8) Okamoto, T. and Ohta, K.: One-Time Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E81-A, No.1, pp.2–10 (1998).
9) Pfitzmann, B. and Waidner, M.: How to Break and Repair a "Provably Secure" Untraceable Payment System, *Advances in Cryptology—CRYPTO '91*, LNCS 576, pp.338–350, Springer-Verlag (1992).
10) Davida, G., Frankel, Y., Tsiounis, Y. and Yung, M.: Anonymity Control in E-Cash Systems, *1st Financial Cryptography Conference* (*FC '97*), LNCS 1318, pp.1–16, Springer-Verlag (1997).
11) Fujisaki, E. and Okamoto, T.: Practical Escrow Cash Schemes, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E81-A, No.1, pp.11–19 (1998).
12) von Solms, S. and Naccache, D.: On Blind Signatures and Perfect Crimes, *Computers and Security*, Vol.11, No.6, pp.581–583 (1992).
13) Camenisch, J. and Michels, M.: A Group Signature Scheme Based on an RSA-Variant, *Advances in Cryptology—ASIACRYPT '98*, LNCS 1514, pp.160–174, Springer-Verlag (1998).
14) Camenisch, J. and Michels, M.: Separability and Efficiency for Generic Group Signature Schemes, *Advances in Cryptology—CRYPTO '99*, LNCS 1666, pp.413–430, Springer-Verlag (1999).
15) Ateniese, G., Camenisch, J., Joye, M. and Tsudik, G.: A Practical and Provably Secure Coalition-Resistant Group Signature Scheme, *Advances in Cryptology—CRYPTO 2000*, LNCS 1880, pp.255–270, Springer-Verlag (2000).
16) Fiat, A. and Shamir, A.: How To Prove Yourself: Practical Solutions to Identification and Signature Problems, *Advances in Cryptology—CRYPTO '86*, LNCS 263, pp.186–194, Springer-Verlag (1987).
17) Bellare, M. and Rogaway, P.: Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols, *Proc. First Annual Conference on Computer and Communications Security*, pp.62–73, Association for Computing Machinery (1993).
18) Stadler, M.: Publicly Verifiable Secret Sharing, *Advances in Cryptology—EUROCRYPT '96*, LNCS 1070, pp.190–199, Springer-Verlag (1996).
19) ElGamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *Advances in Cryptology—CRYPTO '84*, LNCS 196, pp.10–18, Springer-Verlag (1985).
20) Nakanishi, T. and Fujiwara, T.: Group Signature for Easy Access Privilege Canceling, *Computer Security Symposium '98* (*CSS '98*), pp.135–140, IPS Japan (1998).
21) Ateniese, G. and Tsudik, G.: Some Open Issues and New Directions in Group Signatures, *3rd Financial Cryptography Conference* (*FC '99*), LNCS 1648, pp.196–211, Springer-Verlag (1999).

(Received November 30, 2000)
(Accepted June 19, 2001)

Toru Nakanishi was born in Kagawa, Japan, on May 22, 1971. He received the M.E. and Ph.D. degrees in information and computer sciences from Osaka University, Toyonaka, Osaka, Japan, in 1995 and 2000, respectively. Since 2000, he has been a research associate in the Department of Communication Network Engineering, Okayama University, Okayama, Japan. His research interests are cryptography and information security. He is a member of IEICE.

Yuji Sugiyama was born in Okayama, Japan, on May 20, 1951. He received the B.E., M.E. and Ph.D. degrees in information and computer sciences from Osaka University, Toyonaka, Osaka, Japan, in 1974, 1976 and 1983, respectively. He joined the faculty of Osaka University in 1977. Since 2000, he has been a professor in the Department of Communication Network Engineering at Okayama University. His current research interests include algebraic specifications and implementation of algebraic languages. He is a member of IEICE.