コンピュータセキュリティ　18−35
(2002. 7. 19)

署名者の匿名性を有するディジタル署名方式

桑門　秀典†　　田中　初一†

† 神戸大学工学部　〒657-8501 兵庫県神戸市灘区六甲台町 1-1
E-mail: †{kuwakado,tanaka}@eedept.kobe-u.ac.jp

あらまし　あるグループ内の一人のユーザが文書に署名したことを検証者は確認できるが，検証者はその署名者を特定できないようなディジタル署名方式 (ring 署名方式) が Rivest, Shamir, Tauman により提案された．ring 署名方式は，内部告発者が自分の身元を明かすことなく，報道関係者に文書の信頼性を保証することに利用できる．この論文では，あるグループ内の k 人のユーザが署名できるように拡張した ring 署名方式の二つの実現方法を提案する．提案方式 1 は，ランダム自己帰着問題の零知識証明に基づいている．提案方式 2 は，有限体上の多項式を利用して実現されている．これら提案方式の構成法は，Rivest, Shamir, Tauman の ring 署名方式の構成法とは異なる．また，いずれの方式においても，署名者の匿名性は，署名者の身元を特定しようとする者の計算能力に関係なく，無条件に保証される．
キーワード　ディジタル署名，ring 署名，匿名性，ランダム自己帰着問題，多項式

Digital Signature Schemes with Anonymous Signers

Hidenori KUWAKADO† and Hatsukazu TANAKA†

† Faculty of Engineering, Kobe University　1-1 Rokkodai Nada Kobe Hyogo, 657-8501 Japan
E-mail: †{kuwakado,tanaka}@eedept.kobe-u.ac.jp

Abstract　Rivest, Shamir, and Tauman have proposed a ring signature scheme such that a verifier can make sure that someone in a group signs a message, but cannot decide the identification of the signer. The application of the ring signature is whistle-blowing. Without revealing the identification of the signer, the third party can check the validity of the message. In this paper, we propose the generalized version of the ring signature scheme, which makes it possible for k members to sign a message without revealing their identification to the verifier. We show two implementations of such a signature scheme; one is based on zero-knowledge proof of random self-reducible problems, and the other is based on the polynomial over a finite field. Similar to the ring signature scheme, the anonymity of signers in our schemes is unconditional. Namely, the identification of the signers is impossible even if unlimited computational resources are available. The construction of our schemes is different from that of the ring signature; our schemes do not make the ring of signatures.
Key words　digital signature, ring signature, anonymous signer, random self-reducible problem, polynomial

1 Introduction

Rivest, Shamir, and Tauman [8] have formalized the notion of ring signature schemes. A ring signature is considered as one of group signature schemes. The ring signature has the following properties.

(1) A verifier can make sure that someone in a group signs a message, but cannot decide who signs. This anonymity of the signer is unconditional; even if the verifier has unlimited computational resources, the verifier cannot identify the signer.

(2) There is no manager of the group. There is no procedures for setting the group, and distributing the special information.

(3) When the signer signs the message, the signer does not require the cooperation of the other members in the group. It is sufficient that the signer knows the verifying keys of the other members.

The application of the ring signature is whistle-blowing. When a whistle blower sends a document to a journalist, the whistle blower does not want to reveal the identity to the journalist. If the whistle blower does not reveal the identity, then the journalist may not believe the content of the document. In order to solve this problem, the whistle blower chooses members who are plausible for writing the document, and signs the document using the ring signature scheme. Due

to the ring signature, the journalist finds that the document came from a reliable person, but cannot identify who in the group is the whistle blower.

As stated in [8], schemes similar to the ring signature have been proposed. However, these schemes are less efficient or have different objectives. On the other hand, the ring signature is efficient. It consists of individual signature schemes, a collision-resistant hash function, and a symmetric cipher.

Precisely speaking, the ring signature enables the verifier to make sure that at least one member in the group signs the message. In this paper we generalize the ring signature. Namely, our schemes enable the verifier to make sure that at least k members in the group sign the message. However, it seems difficult to generalize the ring signature to such a scheme. Therefore, we show two implementations of such a scheme whose the constructions are different from the ring signature.

The word "ring" is suitable for the signature scheme proposed by Rivest, Shamir, and Tauman because the chain of signatures actually forms the ring. However, it is not suitable for our schemes because the chain of signatures does not form the ring. Hence, we call a signature scheme with the signer's anonymity an *anonymous signature scheme.*

This paper is organized as follows. In Sect. 2, we state some definitions, and summarize the previous works. In Sect. 3, we propose an anonymous signature scheme based on the random self-reducible problem. This anonymous signature scheme is applicable to practical signature schemes such as the Fiat-Shamir scheme [3] and DSS [4]. We prove the anonymity of signers in the same manner as zero-knowledge proof. As an example, we describe the anonymous signature scheme based on the Fiat-Shamir scheme. In Sect. 4, we propose another anonymous signature scheme which is based on the polynomial. The class of signature schemes which this anonymous signature is applicable to is same as that of the ring signature, and is wider than that of our former scheme. In Sect. 5, we concludes this paper.

2 Preliminaries

2.1 Definitions

We call a set of possible signers a *group*, denoted by $\mathcal{G}$. In this paper, we denote by U_i a member (a possible signer) in $\mathcal{G}$. We call members who actually sign a message *signers*, and members excluding the signers *non-signers*. Let $\mathcal{S}$ and $\bar{\mathcal{S}}$ denote the set of signers and the set of non-signers, respectively. Here, the following relationship holds.

$$\mathcal{G} = \mathcal{S} \cup \bar{\mathcal{S}}, \quad \mathcal{S} \cap \bar{\mathcal{S}} = \emptyset$$

We often denote the member in $\mathcal{G}$ by the index i instead of U_i. In such a case, $\mathcal{G} = \{0, 1, 2, \ldots, n-1\}$.

A (k, n) anonymous signature scheme is a signature scheme such that, for a group $\mathcal{G}$ with n possible signers, the third party can verify that at least k members (signers) sign the message, but cannot find who are signer. The anonymity of the signers is unconditional. Namely, even if the third party has unlimited computational resources, the third party cannot decide the identification of the signers with probability larger than k/n. From this definition, the ring signature scheme is considered as a $(1, n)$ anonymous signature scheme.

Similar to the ring signature scheme, the anonymous signature scheme is setup-free. In order to generate a signature, all the signers needs is knowledge of non-signers' verifying keys. The verification must satisfy the soundness and the completeness of usual signature schemes except for the anonymity of the signers.

2.2 Random Self-Reducible Problem and Signature Scheme

It is known that random self-reducible problems are closely related with cryptographic protocols. Tompa and Wall [10] have shown the random self-reducible problem has perfect zero-knowledge proof. Okamoto and Ohta [6] [5] have shown identification protocols and signature schemes based on the random self-reducible problem. This section provides a summary on the random self-reducible problem stated in the above papers.

The random self-reducible problem is defined as follows. Let $\mathcal{N}$ be a countably infinite set. For any $N \in \mathcal{N}$, let $|N|$ denote the length of a representation of N. Let U, V be finite sets, and $R \subseteq U \times V$ be a relation. The domain of R and the image of x are denoted by

$$\mathrm{dom}R = \{u \in U | (u, v) \subseteq R \text{ for } \exists v \in V\},$$
$$R(u) = \{v | (u, v) \in R\},$$

respectively. Here, R is the following relation.

$$\{((N, u), v | N \in \mathcal{N} \text{ and } (u, v) \in R)\}$$

The relation R is said to be random self-reducible if and only if the following three properties are satisfied.

R1: There is an $|N|^{O(1)}$ time algorithm $A_1(N, u, r)$ that, given any inputs $N \in \mathcal{N}$ and $u \in \mathrm{dom}R$ and $r \in \{0,1\}^w$, outputs $u' \in \mathrm{dom}R$. If r is random, uniform, and independent, then u' is uniformly distributed over $\mathrm{dom}R$.
R2: There is an $|N|^{O(1)}$ time algorithm $A_2(N, u, \bar{r}, v')$ that, given $N, u, \bar{r}$ and any $v' \in R(u')$, outputs some $v \in R(u)$. Here, $\bar{r}$ is the finite prefix of r used in computing $u' = A_1(N, u, r)$.
R3: There is an $|N|^{O(1)}$ time algorithm $A_3(N, u, r, v)$ that, given N, u, r and any $v \in R(u)$, outputs some $v' \in R(u')$. If the bits of r are random, uniform, and independent, then v' is uniformly distributed over $R(u')$.

For example, the quadratic residue problem is one of random self-reducible problems. That is, the relation R is $u \equiv v^2 \pmod{N}$. Algorithms A_1, A_2, A_3 are given as follows:

$$\begin{cases} A_1(N, u, r) = ur^2 \bmod N \\ A_2(N, u, r, v') = v'/r \bmod N \\ A_3(N, u, r, v) = vr \bmod N. \end{cases}$$

In addition, the relation R must satisfy the following two properties to have perfect zero-knowledge proof.

R4: There is a probabilistic $|N|^{O(1)}$ expected time algorithm $A_4(N,u,v)$ that, given N,u,v, outputs `true` if $(u,v) \in R$, otherwise outputs `false`.
R5: There is a probabilistic $|N|^{O(1)}$ expected time algorithm $A_5(N)$ that, on input N, outputs a pair of $(u,v) \in R$ at random, where u uniformly distributed over dom$R$ and v uniformly distributed over $R(u)$.

We note that the above definition state nothing about the complexity for computing v from (N,u). In order to apply the random self-reducible problem to a signature scheme, we assume that it is infeasible. Then a signature scheme is constructed as follows [5]. The verifying key are the singing key are $\{N,u\}$ and v, respectively, where $(u,v) \in R$. The signer uniformly chooses r_i $(i = 0,1,\ldots,t-1)$ at random. The signer computes $u'_i = A_1(N,u,r_i)$. For a message m and u'_i, the signer obtains the following binary vector.

$$(b_0,b_1,\ldots,b_{t-1}) = f(m,u'_0,u'_1,\ldots,u'_{t-1}),$$

where f is a public one-way hash function. The signer defines

$$w_i = \begin{cases} r_i & \text{if } b_i = 0 \\ A_3(N,u,r_i,v) & \text{if } b_i = 1. \end{cases}$$

The signature of m is $\{u'_0,u'_1,\ldots,u'_{t-1},w_0,w_1,\ldots,w_{t-1}\}$. A verifier accepts m if the following equations hold for all i.

$$\begin{cases} A_1(N,u,w_i) = u'_i & \text{if } b_i = 0 \\ A_4(N,u'_i,w_i) = \texttt{true} & \text{if } b_i = 1. \end{cases}$$

3 (k,n) Anonymous Signature Scheme Based on the Random Self-Reducible Problem

We propose a (k,n) anonymous signature scheme based on the random self-reducible problem. The anonymity of the proposed scheme is similar to the idea of the witness indistinguishable protocol by Feige and Shamir [2].

3.1 Protocol

Suppose that all members in $\mathcal{G}$ use signature schemes based on a same random self-reducible problem R. Let u_i and v_i denote the verifying key and the singing key of a member U_i, respectively. Here, $(u_i,v_i) \in R$ for $i = 0,1,\ldots,n-1$.

The k signers uniformly choose nt bit strings $r_{i,j}$ $(i = 0,1,\ldots,n-1, j = 0,1,\ldots t-1)$ at random. The signers define a matrix

$$\widehat{u} = \begin{pmatrix} \widehat{u}_{0,0} & \widehat{u}_{0,1} & \ldots & \widehat{u}_{0,t-1} \\ \widehat{u}_{1,0} & \widehat{u}_{1,1} & \ldots & \widehat{u}_{1,t-1} \\ \vdots & \vdots & & \vdots \\ \widehat{u}_{n-1,0} & \widehat{u}_{n-1,1} & \ldots & \widehat{u}_{n-1,t-1} \end{pmatrix}$$

in which the element $\widehat{u}_{i,j}$ is computed as

$$\widehat{u}_{i,j} = A_1(N,u_i,r_{i,j}).$$

The signers define t random permutations π_j on $\{0,1,\ldots,n-1\}$. Using π_j, the signers permute n elements of the j-th column of $\widehat{u}$. The resulting matrix u' is denoted by

$$u' = \begin{pmatrix} u'_{0,0} & u'_{0,1} & \ldots & u'_{0,t-1} \\ u'_{1,0} & u'_{1,1} & \ldots & u'_{1,t-1} \\ \vdots & \vdots & & \vdots \\ u'_{n-1,0} & u'_{n-1,1} & \ldots & u'_{n-1,t-1} \end{pmatrix}.$$

Here, the relationship between $\widehat{u}$ and u' is

$$u'_{\pi(i),j} = \widehat{u}_{i,j}$$

for $i = 0,1,\ldots,n-1, j = 0,1,\ldots,t-1$. Using a public one-way hash function f, the signers obtain a binary vector $\mathbf{b}$, that is,

$$\begin{aligned} \mathbf{b} &= (b_0,b_1,\ldots,b_{t-1}) \\ &= f(m,u'). \end{aligned} \tag{1}$$

The signers define a matrix w as

$$w = \begin{pmatrix} w_{0,0} & w_{0,1} & \ldots & w_{0,t-1} \\ w_{1,0} & w_{1,1} & \ldots & w_{1,t-1} \\ \vdots & \vdots & & \vdots \\ w_{n-1,0} & w_{n-1,1} & \ldots & w_{n-1,t-1} \end{pmatrix},$$

where the element is computed as

$$w_{\pi_j(i),j} = \begin{cases} r_{i,j} & \text{if } b_j = 0 \text{ and } \forall i \\ A_3(N,u_i,r_{i,j},v_i) & \text{if } b_j = 1 \text{ and } i \in \mathcal{S} \\ \perp & \text{if } b_j = 1 \text{ and } i \in \bar{\mathcal{S}} \end{cases} \tag{2}$$

for $i = 0,1,\ldots,n-1, j = 0,1,\ldots,t-1$. As a result, the signature σ_m of m is given as

$$\sigma_m = [\mathcal{G},u',\{\tau_j | b_j = 0, j = 0,1,\ldots,t-1\},w], \tag{3}$$

where τ_j is the inverse permutation of π_j. Notice that π_j is random, but not one-way.

A verifier first computes the binary vector $\mathbf{b}$ by Eq. (1). For $\ell = 0,1,\ldots,n-1, j = 0,1,\ldots,t-1$, the verifier check that

$$\begin{cases} A_1(N,u_{\tau_j(\ell)},w_{\tau_j(\ell),j}) = u'_{\ell,j} & \text{if } b_j = 0 \\ A_4(N,u_{\ell,j},w_{\ell,j}) = \texttt{true} & \text{if } b_j = 1 \text{ and } w_{\ell,j} \neq \perp \end{cases} \tag{4}$$

Moreover, when $b_j = 1$, the verifier checks that the number of $w_{\ell,j} \neq \perp$ is k. If all tests are passed, then the verifier accepts m as a valid message.

3.2 Security

Forgery: The difficulty of forgery mainly depends on the infeasibility of computing v from (N,u). Except for the formal difference in the hash function, if the underlying individual signature scheme stated in Sect. 2.2 is broken, then the proposed scheme is broken. Conversely, if the proposed scheme is broken, then the underlying individual signature scheme is broken.

Anonymity: Firstly, each of elements of u' is uniformly distributed over dom$R$ because of the definition R1. Hence, the distribution of the elements does not depend on signers.

Secondly, let us consider the distribution of elements in the j-th column of w for j such as $b_j = 0$. From Eq. (2), $w_{\pi_j(i),j}$

is uniformly distributed over dom$R$ because $r_{i,j}$ is chosen in such a way. Namely, the distribution of elements in the j-th column is uniform on dom$R$ regardless of signers.

Thirdly, we examine the case of for j such as $b_j = 1$. Since row elements of the j-th column are permuted, the row index does not give information about signers. For simplicity, suppose that $0, 1, 2 \in \mathcal{S}$. Let us recall that the element $\widehat{u}_{i,j}$ is computed as follows:

$$\widehat{u}_{i,j} = A_1(N, u_i, r_{i,j}).$$

From the definition R1, $\widehat{u}_{0,j}$ is uniformly distributed over dom$R$ by varying $r_{i,j}$. Since $\widehat{u}_{1,j}, \widehat{u}_{2,j} \in$ dom$R$, there are $r_{0,j}^{(1)}$ and $r_{0,j}^{(2)}$ such that

$$\widehat{u}_{1,j} = A_1(N, u_0, r_{0,j}^{(1)}), \quad \widehat{u}_{2,j} = A_1(N, u_0, r_{0,j}^{(2)}).$$

From the distribution of $\widehat{u}_{0,j}$, the number of such $r_{0,j}^{(1)}$ is equal to that of such $r_{0,j}^{(2)}$. This means that the value of $\widehat{u}_{i,j}$ does not leak information about signers. Therefore, in the case of for j such as $b_j = 1$ and $i \in \mathcal{S}$, the distribution of elements in the j-th column does not depend on signers.

Finally, in the case of for j such as $b_j = 1$ and $i \in \bar{\mathcal{S}}$, it is trivial that the distribution does not depend on signers.

Summarizing the above discussion, we have the following theorem.

[Theorem 1] The signature scheme described in Sect. 3.1 is a (k, n) anonymous signature scheme.

3.3 Performance

We estimate the amount of computation and the size of signature in the scheme described in Sect. 3.1. We denote by $C(A)$ the amount of computation for an algorithm A. The average amount of computations is given by

$$ntC(A_1) + ntC(\pi_j) + C(f) + kC(A_3) + \frac{nt}{2}C(A_1) + \frac{kt}{2}C(A_4),$$

where the first four terms are for signing and the remainders are for verification. We ignore the computation for generating $r_{i,j}$.

From Eq. (3), the size of a signature is given by

$$nt|\bar{u}| + \frac{t}{2}|\tau_j| + \frac{t}{2}n|r_{i,j}| + \frac{t}{2}k|\bar{v}|,$$

where $|\bar{u}|$ is the size of an element in dom$R$, the second term is for the permutations, and $|\bar{v}|$ is the size of an element in the range of R. We ignore the sizes of $\mathcal{G}$ and $\perp$.

3.4 Example

As a typical example of the scheme described in 3.1, we show a $(1, 2)$ anonymous signature scheme based on the quadratic residue problem, that is, based on the the Fiat-Shamir scheme [3] [7].

3.4.1 Protocol

Suppose that two members U_0, U_1 use the Fiat-Shamir scheme. Let n be the common modulus is N, and u_i, v_i be the verifying key and the signing key of U_i where $u_i = v_i^2 \bmod N$, respectively.

Signing: Suppose that U_0 is a signer. First, U_0 chooses $r_{i,j}$ $(i = 0, 1, j = 0, 1, \ldots, t-1)$ at random from Z_N. U_0 defines a matrix

$$\widehat{u} = \begin{pmatrix} \widehat{u}_{0,0} & \widehat{u}_{0,1} & \cdots & \widehat{u}_{0,t-1} \\ \widehat{u}_{1,0} & \widehat{u}_{1,1} & \cdots & \widehat{u}_{1,t-1} \end{pmatrix}$$

where the element $\widehat{u}_{i,j}$ is computed as

$$\widehat{u}_{i,j} = u_i r_{i,j}^2 \bmod N.$$

U_0 defines t random permutations π_j on $\{0, 1\}$. Using π_j, U_0 permutes two elements of the j-th column of $\widehat{u}$. The resulting matrix u' is denoted by

$$u' = \begin{pmatrix} u'_{0,0} & u'_{0,1} & \cdots & u'_{0,t-1} \\ u'_{1,0} & u'_{1,1} & \cdots & u'_{1,t-1} \end{pmatrix}.$$

Here, the relationship between $\widehat{u}$ and u' is

$$u'_{\pi(i),j} = \widehat{u}_{i,j}$$

for $i = 0, 1, j = 0, 1, \ldots, t-1$. Using a public one-way hash function f, U_0 obtains a binary vector $\mathbf{b}$ from a message m and u', that is,

$$\begin{aligned} \mathbf{b} &= (b_0, b_1, \ldots, b_{t-1}) \\ &= f(m, u'). \end{aligned} \tag{5}$$

U_0 defines a matrix w as

$$w = \begin{pmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,t-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,t-1} \end{pmatrix},$$

where the element is computed as

$$w_{\pi_j(i),j} = \begin{cases} r_{i,j} & \text{if } b_j = 0 \text{ and } i = 0, 1 \\ v_0 r_{0,j} & \text{if } b_j = 1 \text{ and } i = 0 \\ \perp & \text{if } b_j = 1 \text{ and } i = 1 \end{cases}$$

for $i = 0, 1, j = 0, 1, \ldots, t-1$. As a result, the signature σ_m of m is defined as

$$\sigma_m = [U_0, U_1, u', \{\tau_j | \forall j \text{ such that } b_j = 0\}, w], \tag{6}$$

where τ_j is the inverse permutation of π_j.

Verification: A verifier obtains the binary vector $\mathbf{b}$ by Eq. (5). For $\ell = 0, 1, j = 0, 1, \ldots, t-1$, the verifier checks that

$$\begin{cases} u'_{\ell,j} = u_{\tau_j(\ell)} w_{\pi_j(\ell),j} & \text{if } b_j = 0 \\ u'_{\ell,j} = w_{\ell,j}^2 \bmod N & \text{if } b_j = 1 \text{ and } w_{\ell,j} \neq \perp \end{cases} \tag{7}$$

Moreover, when $b_j = 1$, the verifier checks that one of two elements in the j-th column is $\perp$. If all tests are passed, then the verifier accepts m as a valid message.

3.4.2 Security

Since we have already proved the anonymity of the signer in Sect. 3.2, we discuss the difficulty of the forgery. We prove the following theorem on the security against forgery.

[Theorem 2] The $(1, 2)$ anonymous signature scheme described in Sect. 3.4.1 is as secure as the Fiat-Shamir signature scheme.

We first focus on the difference of the one-way hash functions. While the input of the one-way hash function in Sect. 3.4.1 is a scalar and a matrix, the input of the one-way hash function of the Fiat-Shamir scheme is a scalar and a vector (or a sequence of scalars). When the one-way hash function in Sect. 3.4.1 is used in the the Fiat-Shamir scheme, the unused elements are considered as zero. Hence, the formal difference on the one-way hash functions is not critical.

Suppose that an adversary succeeds in forging a signature of the proposed scheme, denoted by

$$\sigma_m = [u', \{\tau_j | \forall j \text{ such that } b_j = 0\}, w].$$

Then the following tuple is considered as the signature of the Fiat-Shamir signature scheme by U_0.

$$\sigma_m^{(0)} = [u'_{\ell,j}, w_{\ell,j} | \ell = \tau_j(0) \text{ if } b_j = 0, w_{\ell,j} \neq \perp \text{ if } b_j = 1].$$

Similarly, the following tuple is considered as one by U_1.

$$\sigma_m^{(1)} = [u'_{\ell,j}, w_{\ell,j} | \ell = \tau_j(1) \text{ if } b_j = 0, w_{\ell,j} \neq \perp \text{ if } b_j = 1].$$

Conversely, suppose that the adversary succeeds in forging a signature of the Fiat-Shamir signature scheme, for example, for U_0. The adversary computes $\widehat{u}_{1,j} = u_1 r_{1,j}^2 \bmod N$ for randomly chosen $r_{1,j}$, and decides t permutations π_j adequately, Then, the adversary can obtain the signature such as Eq. (6).

3.5 Modification

As seen in Eq. (4), the method for verifying the validity of a message directly consists of algorithms of the random self-reducible problem. However, there are signature schemes in which the verifying method is more complicate; for example, Schnorr's scheme [9], DSS [4], and ElGamal's scheme [1]. In this section, we show a $(1,2)$ anonymous signature scheme based on Schnorr's scheme. It is easy to generalize this scheme to a (k,n) anonymous signature scheme. The idea described here is applicable to DSS and ElGamal's scheme.

As parameters of Schnorr's scheme, let p, q, g denote a large prime, a prime satisfying $q|p-1$, and a generator of a multiplicative group with order q in GF(p), respectively. Let y_i, s_i be the verifying key and the signing key of a member i where $y_i = g^{-s_i}$, respectively

Suppose that U_0 is a signer. U_0 computes a signature (e_0, v_0) of a message m by Schnorr's scheme, that is,

$$e_0 = f(g^{r_0} \bmod p, m), \quad v_0 = r_0 + s_0 e_0 \bmod q,$$

where f is a public one-way hash function and r_0 is a random value in Z_q. After choosing r_1 from Z_q at random, U_0 computes e_1 as

$$e_1 = f(g^{r_1} \bmod p, m).$$

U_0 defines u_0, u_1 as

$$u_0 = g^{v_0} \bmod p, \quad u_1 = g^{r_1}/y_1^{e_1} \bmod p.$$

Considering that the relation R is $u = g^v \bmod p$, U_0 generates a signature σ_m by the method described in Sect. 3.1. Hence, the signature of m is

$$\Sigma_m = [U_0, U_1, e_0, e_1, u_0, u_1, \sigma_m].$$

A verifier first checks that, for $i = 0, 1$,

$$e_i = f(u_i y^{e_i} \bmod p, m).$$

If they hold, then the verifier checks σ_m by the method described in Sect. 3.1. If all tests are passed, then the verifier accepts m as a valid message.

4 (k,n) Anonymous Signature Scheme Based on the Polynomial

In this section, we propose another implementation of a (k,n) anonymous signature scheme. Differing from the scheme proposed in Sect. 3.1, the scheme described here does not require any special properties of underlying signature schemes. This property is also satisfied by the ring signature which is a $(1,n)$ anonymous signature scheme. Accordingly, our scheme is same as the ring signature in terms of the scope of underlying signature schemes.

Similar to the ring signature, let us assume the followings to simplify a protocol.

- The underlying signature scheme is based on trap-door permutations to generate and verify signatures. That is, it is easy to compute $y_i = g_i(x_i)$ for given x_i, but it is hard to compute $x_i = g_i^{-1}(y_i)$ for given y_i without the trap-door information (the signing key). We assume that if x_i is uniformly chosen from the domain at random, then the y_i is also done over the range and vice versa.
- The domain (range) of g_i is same. The method for this requirement has been shown in [8]. Without loss of generality, the domain is a finite field GF(q); if the domain is $\{0,1\}^\ell$, then it can be considered as GF(2^ℓ).

4.1 Protocol

Signing: Suppose that k members in $\mathcal{G}$ sign a message m. The k signers computes $f(m)$ where f is using a public collision-resistant hash function such that the range is same as that of g_i. The signers picks random r_i for $i \in \bar{\mathcal{S}}$ where $\bar{\mathcal{S}}$ is the set of non-signers. Then the signers computes $y_i = g_i(r_i)$. Using the Lagrange formula, the signers obtains the $(n-k)$-degree polynomial $p(x)$ which goes through points $(0, f(m))$, (i, y_i) for $i \in \bar{\mathcal{S}}$. Notice that $p(x)$ is unique because the number of non-signers is $n-k$. The signers uses their trap-door information in order to invert g_i on $p(i)$ to obtain r_i, that is,

$$r_i = g_i^{-1}(p(i)) \text{ for } i \in \mathcal{S}.$$

Notice that $(i, p(i))$ is the point on the curve $y = p(x)$ over the finite field. As a result, the signature of m is given as

$$\sigma_m = [\mathcal{G}, p(x), \{r_i | i \in \mathcal{G}\}].$$

Verification: A verifier checks that $f(m) = p(0)$. The verifier computes $y_i = p(i)$ for $i \in \mathcal{G}$. Then the verifier checks that $y_i = g_i(r_i)$ for $i \in \mathcal{G}$. If all tests are passed, then the verifier accepts m as a valid message.

4.2 Security

Forgery: The difficulty of forgery mainly depends on the infeasibility of computing g_i^{-1}. Let us assume that it is infeasible and the distribution of y_i is uniformly distributed over the range at random. The probability that an adversary who is not included in $mathcal M$ succeeds in forging a signature is equal to the probability that n points are located on a curve $p(x)$ with degree $n-k$. Hence, it is $1/q^k$.

Anonymity: Since y_i $(i \in \bar{\mathcal{S}})$ is uniformly distributed over the range, $p(x)$ is uniformly chosen from the set of $(n-k)$-degree polynomials. It follows that $p(x)$ does not leak information about signers. In addition, $p(i)$ $(i \in \mathcal{S})$ is uniformly distributed over the range. Hence, r_i $(i \in \mathcal{S})$ is uniformly distributed over the domain. Accordingly, the distribution of a signature does not depend on signers.

[Theorem 3] The signature scheme described in Sect. 4.1 is a (k,n) anonymous signature scheme.

5 Conclusions

In this paper, we have proposed two implementations of a (k,n) anonymous signature scheme; one is based on the zero-knowledge proof of the random self-reducible problem, and the other is based on the $(n-k)$-degree polynomial over a finite field. Although the principle of our schemes is different from that of the ring signature, our schemes achieve the unconditional anonymity of signers as well as the ring signature.

References

[1] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. IT-31, no. 4, pp. 469–472, 1985.

[2] U. Feige and A. Shamir, "Witness indistinguishable and witness hiding protocols," Proceedings of The 22nd Annual ACM Symposium on Theory and Computing, pp. 416–426, 1990.

[3] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," Advances in Cryptology - CRYPTO'86, Lecture Notes in Computer Science, vol. 263, pp. 186–194, 1986.

[4] National Institute of Standards and Technology, "Digital signature standard (DSS)," Federal Information Processing Standards Publication 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf, 2000.

[5] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," Advances in Cryptology - CRYPTO'92, Lecture Notes in Computer Science, vol. 740, pp. 31–53, 1993.

[6] T. Okamoto and K. Ohta, "Divertible zero knowledge interactive proofs and commutative random self-reducibility," Advances in Cryptology - EUROCRYPT'89, Lecture Notes in Computer Science, vol. 434, pp. 134–149, 1990.

[7] D. Pointcheval and J. Stern, "Security proofs for signature schemes," Advances in Cryptology - EUROCRYPT'96, Lecture Notes in Computer Science, vol. 1070, pp. 387–398, 1996.

[8] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, pp. 552–565, 2001.

[9] C. P. Schnorr, "Efficient signature generation by smart cards," Journal of Cryptology, vol. 4, pp. 161–174, 1991.

[10] M. Tompa and H. Woll, "Random self-reducibility and zero knowledge interactive proofs of possession of information," Proceedings of The 28th Symposium on Foundations of Computer Science, pp. 472–482, 1987.