PAPER *Special Section on Cryptography and Information Security*

Efficient Unconditionally Secure Digital Signatures*

Goichiro HANAOKA[†a)], **Junji SHIKATA**[††], ***Nonmembers***, **Yuliang ZHENG**[†††], ***Member***,
and* Hideki IMAI**[†], ***Fellow

SUMMARY Digital signatures whose security does not rely on any unproven computational assumption have recently received considerable attention. While these unconditionally secure digital signatures provide a foundation for long term integrity and non-repudiation of data, currently known schemes generally require a far greater amount of memory space for the storage of secret and public keys than a traditional digital signature. The focus of this paper is on methods for reducing memory requirements of unconditionally secure digital signatures. A major contribution of this paper is to propose two novel unconditionally secure digital signature schemes, one called a symmetric construction and other an asymmetric construction, which require a significantly smaller amount of memory. As a specific example, with a typical parameter setting the required memory size for a user is reduced to be approximately $\frac{1}{10}$ of that in a previously known scheme. Another contribution of the paper is to show an attack on a multireceiver authentication code which was proposed by Safavi-Naini and Wang. A simple method to fix the problem of the multireceiver authentication code is also proposed.

key words: *digital signature, unconditional security*

1. Introduction

Digital signatures represent one of the most widely used security technologies for ensuring unforgeability and non-repudiation of digital data. While some data only require the assurance of integrity for a relatively short period of time, say up to two years, there are many cases where it is necessary for signed documents to be regarded as legally valid for a much longer period of time. Some of the examples of data that require long-term integrity include court records, long-term leases and contracts.

Most digital signatures are created and verified using cryptography based on number-theoretic problems. These schemes and the infrastructure within which they operate are restricted in scope that they rely for their security on the assumed computational difficulty of computing certain number-theoretic problems, such as factoring large composites or solving discrete logarithms in large finite fields; RSA [21], Fiat-Shamir [9], ESIGN [18] are examples of ones that are based on the difficulty of factoring, and ElGamal [8], Schnorr [25], DSA [7] are ones based on the difficulty of solving discrete logarithms. However, this presumption no longer assures the security of current digital signatures as the progress in computers as well as further refinement of various algorithms make it computationally possible to solve the larger size number-theoretic problems in the future.

In August 1999, a team of cryptography researchers from around the world completed the factorization of an 512-bit RSA composite with the use of the Number Field Sieve method [3]. With the rapid advancement in the speed of computers, one can safely predict that factoring even larger composites may become feasible at some point of time in future. We also note that innovative factoring algorithms may emerge, dramatically changing the landscape of public key cryptosystems whose security hinges on the presumed hardness of certain number theoretic problems. In yet another significant development, the past few years have witnessed significant progress in quantum computers. These computers, if built, will have the capacity to improve profoundly known algorithms for factoring and solving discrete logarithms [1], [27], whereby challenging the long term security of all digital signature schemes based on number-theoretic problems.

The above discussions show clearly that there is a need to devise digital signature schemes that provide assurance of long term integrity. A possible solution to this problem is digital signature schemes whose security does not rely on any unproven assumption. The present authors have recently proposed the first unconditionally secure digital signature schemes (with transferability) [13], [26]. An interesting and very useful property of these signature schemes is that they admit transferability, allowing the recipient of a signature to transfer it to another recipient without fearing that the security of

Manuscript received March 20, 2003.
Manuscript revised June 26, 2003.
Final manuscript received August 8, 2003.

[†] The authors are with the 3rd Department, Institute of Industrial Science, The University of Tokyo, Tokyo, 153-8505 Japan. The first author is supported by a Research Fellowship from Japan Society for the Promotion of Science (JSPS).

[††] The author is with the Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama-shi, 240-8501 Japan.

[†††] The author is with Department of Software and Information Systems, UNC Charlotte, 9201, University City Blvd, Charlotte, NC 28223, USA.

a) E-mail: hanaoka@imailab.iis.u-tokyo.ac.jp

[*] A preliminary version of this paper was presented at Fifth International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2002) [14].

the signature might be compromised. However, these signature schemes do have a disadvantage, namely the size of a user's secret information is very large. This disadvantage may pose a serious problem in practice, especially when a user's secret information need to be stored in such devices as smart cards.

A major contribution of this work is to propose two novel unconditionally secure digital signature schemes that require significantly less amount of memory for each user's secret information. As an example, consider an organization that has 100,000 users. With the new signature schemes, the required memory size for each user is reduced to approximately $\frac{1}{10}$ of that required by previously known schemes. Another contribution of this paper is to present an attack on a multireceiver authentication code proposed by Safavi-Naini and Wang, which is followed by a method to fix that problem. Safavi-Naini and Wang's multireceiver authentication code is related to one of our new unconditionally secure digital signature schemes. More specifically, one of our approaches succeeds in reducing the required memory size for a user's secret information by unifying secret data for both signing and verification.

1.1 Related Work

Authentication Codes. There have been attempts to modify unconditionally secure authentication codes [10], [28] with the aim of enhancing the codes with added security properties. An obvious approach is to transform an unconditionally secure authentication code into an unconditionally secure digital signature. To achieve this, however, one faces two insurmountable technical hurdles. The first hurdle lies in authentication codes, especially the conventional Cartesian ones, which do not provide the function of non-repudiation, simply because a receiver can easily forge a sender's message and vice versa. The second hurdle is that the receiver is always designated, which means that a signature cannot be verified by another party without having the shared key.

An extension to authentication codes is called, *authentication codes with arbitration* or A^2-codes [12], [15]–[17], [29], [30]. These codes involve a trusted third party called an arbiter. The arbiter help resolve disputes at times when a receiver forges a sender's message or the sender claims that the message has been forged by the receiver. A^2-codes have been further improved to have a less trustworthy arbiter as one of the requirements. These improved codes are called, A^3-codes [2], [5], [11], [12], [31], [32]. A property common to both codes is that the receiver of an authenticated message has to be designated. Therefore, in a signature system where the receiver is not designated, both A^2-codes and A^3-codes cannot be used as digital signatures.

Another extension made to authentication codes, *multireceiver authentication codes* (MRA) [6], [12], [22], have been extensively studied in the literature. In a MRA scheme, a broadcast message can be verified by any one of the receivers. Earlier MRA schemes required the sender himself to be designated. In order to ease the requirement of the designated sender, several variations of *MRA with dynamic sender* or DMRA have been proposed [22]–[24]. Among these schemes, we especially looked into Safavi-Naini and Wang's DMRA [22], [24] which we thought has an interesting construction. In their scheme, a user's secret information for generating authenticated messages and that for verifying them is the same. Which means that, their scheme requires significantly less amount of memory size compared to other DMRAs. Further, in one of our new schemes, with this application, the required memory size for a user's secret information of our schemes can be reduced as well.

It is important to note that these schemes make sense only in the case of broadcasting. If MRA or DMRA is used for point-to-point authentication, then the sender can easily generate a fraudulent message, which is accepted by the receiver and not by other participants. The situation is made complex due to a reason that the same fraudulent message may had been generated by the receiver himself. A further problem associated to this situation is that, MRA nor DMRA provide transferability. In particular, if an authenticated message is transferred from one verifier to another, the second verifier can forge a message that appears to be perfectly valid and may naturally transfer it to the next verifier. For these reasons, neither MRA nor DMRA satisfies the non-repudiation requirement of digital signature.

Unconditionally Secure Signatures. Chaum and Roijakkers [4] originally made the attempt to construct an unconditionally secure signature scheme using cryptographic protocols. However, their basic scheme was impractical, as it only signed a single bit message. Furthermore, their level of security of a signature decreased as the signature moved from one verifier to another. In practice, it is important for a signature scheme to have *transferability*, i.e., its security is not compromised when a signature is transferred among users. By applying A^3-codes, Johansson [12] proposed an improved version of Chaum-Roijakkers scheme, but Johansson did not address transferability of signature scheme.

Pfitzmann and Waidner proposed another version of unconditionally secure signature schemes [19], [20]. However, their unconditional security was limited for signers. Recently, the present authors proposed an unconditionally secure digital signature which addresses all known required properties including transferability [13]. However, that signature scheme (the HSZI-AC00 scheme, for short) requires a large amount of memory, which could be a problem in certain applications, e.g. smart card based systems.

1.2 Main Results

In this paper, we first present an attack on Safavi-Naini and Wang's DMRA [24]. More specifically, in their scheme, by observing a valid signature of an honest signer, a coalition of adversaries can make an impersonation attack with non-negligible probability. We also show a simple method to fix that problem.

Next, we show two novel unconditionally secure digital signature schemes that admit transferability. Both these schemes significantly reduce the required memory size for a user's secret information. In the first one, *symmetric construction*, the required memory size for a user's secret information is significantly reduced by unifying secret information for signing and that for verification. However, the required memory size for a signature is slightly increased compared to the HSZI-AC00 scheme. The basic idea behind unifying secret information for signing and verification in the symmetric construction is partially based on the idea from the fixed version of Safavi-Naini and Wang's DMRA. In the second construction, *asymmetric construction*, the required memory size is reduced without increasing the required memory size for a signature. More precisely, this scheme is optimal in terms of the required memory size for a signature as well as in the HSZI-AC00 scheme. As an example for 100,000 users with appropriate security parameter settings, the required memory size for a user is reduced to $\frac{1}{10}$ of that required in the previous method.

The organization of the remaining part of this paper is as follows: In Sect. 2, we give a brief review of Safavi-Naini and Wang's multireceiver authentication code, and demonstrate an attack on it. We also show a method to fix the problem. In Sect. 3, new unconditionally secure digital signature schemes are presented. Lastly, Sect. 4 presents a comparison between the proposed schemes with the previous method.

2. Analysis of Safavi-Naini and Wang's DMRA

In general, DMRA is an authentication code where any entity in a system can generate and verify an authenticated message. In this section, we give a brief review of Safavi-Naini and Wang's multireceiver authentication codes with dynamic senders (the SW-DMRA, for short) [22], [24]. As already mentioned, in this scheme, secret information for generating an authenticated message and that for verifying is the same. Primarily due to this property, the required memory size for a user's secret information in the SW-DMRA could be decreased to be significantly smaller to that of other DMRAs. However, the SW-DMRA is insecure when used as in [24]. In this section, we also demonstrate an attack on the SW-DMRA, and present a method to fix that problem. This attack is easy to perform and indeed, very effective. In this attack, by observing a valid authenticated message, colluders can forge any user's valid authenticated message with probability 1.

2.1 Basic Idea of Safavi-Naini and Wang's DMRA

A fundamental idea for the SW-DMRA in unifying secret information for generating and verifying an authenticated message is as follows. We assume that there are n users $\mathcal{U} = \{U_1, \cdots, U_n\}$ and a trusted authority (TA) who generates and distributes secret information for each user. First, TA generates a random symmetric function $f(x, y)$ and distributes $f_i(x) := f(x, U_i)$ for each user U_i $(i = 1, \cdots, n)$. U_i can prove that he is U_i by broadcasting $f_i(x)$ to other users. U_j accepts the broadcasted message if $f_i(U_j) = f_j(U_i)$.

2.2 Implementation of Safavi-Naini and Wang's DMRA

In this subsection, the construction of the SW-DMRA is shown in more detail. This scheme was originally presented in [22] and was then improved and simplified in [24]. Here, we show the improved version. The model of DMRA follows [24].

Let F_q be the finite field with q elements and $\mathcal{S}$ the set of source states. We assume $\mathcal{S} = F_q$ and that each user's identity U_i is represented as distinct number on F_q, and ω is the maximum number of colluders in the system. The construction of the SW-DMRA is as follows.

Safavi-Naini and Wang's DMRA [24]

1. **Key distribution:** The TA chooses uniformly at random two symmetric polynomials $F_0(x, y)$ and $F_1(x, y)$ over F_q with two variables x and y of degree less than $\omega + 1$[†]. For each U_i $(i = 1, \cdots, n)$, the TA privately sends a pair of polynomials $\langle F_0(x, U_i), F_1(x, U_i)\rangle$ to U_i. This constitutes the secret information of U_i.
2. **Broadcast:** If U_i wants to authenticate a source state $s \in F_q$, U_i calculates the polynomial $a_i(x) := F_0(x, U_i) + sF_1(x, U_i)$ and broadcasts $(s, a_i(x))$ with his identity to other users.
3. **Verification:** U_j can verify the authenticity of $(s, a_i(x))$ by first calculating the polynomial

[†] It is important to note that the meaning of the parameter ω in this paper is different from that of w used in [24]. The authors of [24] describe "no $w - 1$ subset of users can perform impersonation and/or substitution attack on any other pair of users" ([24], page 161, Def. 5.1) and "Then TA randomly chooses two symmetric polynomials of degree less than w with coefficients in $GF(q)$" ([24], page 163). Thus, we can see that ω in this paper is equivalent to $w - 1$ in [24]. We also note that our definition of ω is in line with relevant papers by other researchers, including [6], [12].

$b_j(x) := F_0(x, U_j) + sF_1(x, U_j)$ and then accepting $(s, a_i(x))$ as authentic and being sent from U_i if $b_j(U_i) = a_i(U_j)$.

2.3 Performance

As shown in above, in this scheme, U_i's secret information $\langle F_0(x, U_i), F_1(x, U_i) \rangle$ is utilized for both generating and verifying authenticated message. Namely, for each user, the whole distributed secret information is used whether he is a sender or a recipient. Hence, the required memory size for a user's secret information can be reduced to significantly small value. More precisely, this scheme is optimal in terms of the required memory size for a user's secret information due to lower bound on it [24]. In addition, this scheme is also optimal in terms of the required memory size for an authenticated message [24]. For the details, see Theorem 5.2 in [24].

Although the authors of [24] claimed that the probability of succeeding for a collusion of up to ω users in performing all known attacks is at most $\frac{1}{q}$, however, the above scheme is insecure. The details regarding the security of this scheme is shown in [24]. In the next subsection, we demonstrate an attack on the above DMRA.

Here, we further point out the transferability of DMRAs. Generally in DMRAs as already mentioned, messages are transmitted over a broadcast channel, and in this particular situation, transferability is not required. However, for a digital signature (for point-to-point communication), transferability is a property that cannot be neglected. That is, a signature system must allow users to pass signatures among users without compromising the integrity of them. Generally speaking, DMRAs (and MRAs) do not fulfill this requirement. As an example to this, we show the vulnerability of the above DMRA where it allows users to pass authenticated messages among users without a broadcast channel.

Suppose that, U_{i_0} generates $(s, a_{i_0}(x))$ and sends it to U_{i_1}. Then, an adversary can modify the authenticated message as $(s, a'_{i_0}(x))$, such that $a'_{i_0}(U_{i_1}) = a_{i_0}(U_{i_1})$ and $a'_{i_0}(U_{i_2}) \neq a_{i_0}(U_{i_2})$ for a certain user U_{i_2}. On receiving $(s, a'_{i_0}(x))$, U_{i_1} accepts it as valid since $a'_{i_0}(U_{i_1}) = b_{i_1}(U_{i_0})$. However, when U_{i_1} further transfers $(s, a'_{i_0}(x))$ to U_{i_2}, U_{i_2} does not accept it since $a'_{i_0}(U_{i_2}) \neq b_{i_2}(U_{i_0})$, and U_{i_1} will be suspected to have forged it. We call this type of attack *transfer with a trap* following to [13]. For this reason, DMRA (and MRA) cannot be used as a digital signature.

In the remaining part of this section, we show an attack on the SW-DMRA, and also present a method to fix that problem. This attack is easy to perform and indeed, very effective. In this attack, by observing a valid authenticated message, ω colluders can forge any user's valid authenticated message with probability 1.

2.4 Attack on Safavi-Naini and Wang's DMRA

In this subsection, we assume that an adversary can interrupt a valid authenticated message which can also be used in an attack, and prove that in such situation, SW-DMRA is not secure. Notice that SW-DMRA did assume the above attack model to begin with, and we showed that it has failed to prove its security.

Let $\mathcal{W} = \{U_1, \cdots, U_\omega\}$ be the set of the colluders. These colluders can forge any user's authenticated message as described. When $U_0 (\notin \mathcal{W})$ transmits a valid authenticated message $(s, a_0(x))$, the colluders interrupt it and use it for forgery of another user's authenticated message. On observing $(s, a_0(x))$, the colluders generate authenticated messages $(s, a_1(x)), (s, a_2(x)), \cdots, (s, a_\omega(x))$. Letting

$$F_l(x, y) := (1, x, x^2, \cdots, x^\omega) A_l \begin{pmatrix} 1 \\ y \\ y^2 \\ \vdots \\ y^\omega \end{pmatrix}, \ l = 0, 1,$$

where A_l $(l = 0, 1)$ are $(\omega + 1) \times (\omega + 1)$ symmetric matrices over F_q, the colluders now have a matrix D, where

$$D := (A_0 + sA_1) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ U_0 & U_1 & \cdots & U_\omega \\ {U_0}^2 & {U_1}^2 & \cdots & {U_\omega}^2 \\ \vdots & \vdots & \cdots & \vdots \\ {U_0}^\omega & {U_1}^\omega & \cdots & {U_\omega}^\omega \end{pmatrix}.$$

Then, by using D, $A_0 + sA_1$ can be easily obtained as follows:

$$A_0 + sA_1 = D \begin{pmatrix} 1 & 1 & \cdots & 1 \\ U_0 & U_1 & \cdots & U_\omega \\ {U_0}^2 & {U_1}^2 & \cdots & {U_\omega}^2 \\ \vdots & \vdots & \cdots & \vdots \\ {U_0}^\omega & {U_1}^\omega & \cdots & {U_\omega}^\omega \end{pmatrix}^{-1}.$$

If the colluders $\mathcal{W}$ want to forge an authenticated message of a user U_j, where $U_j \notin \mathcal{W} \cup \{U_0\}$, $\mathcal{W}$ calculate

$$a'_j(x) = (1, U_j, U_j^2, \cdots, U_j^\omega)(A_0 + sA_1),$$

and broadcast $(s, a'_j(x))$ as an authenticated message of U_j for the source state s. Since $(s, a'_j(x))$ is exactly equal to U_j's valid authentication message for source state s, the colluders succeed in impersonation (or entity substitution) for U_j (with probability 1).

2.5 Method to Fix the Problem

An essential problem in the SW-DMRA is that $A_0 + sA_1$ can be calculated by using both ω colluders' secret information and an authenticated message generated by an honest user. In order to avoid calculating $A_0 + sA_1$, the rank of $A_0 + sA_1$ must be equal to or larger than $\omega + 1$. This implies that the degree of x and y in $F_0(x, y)$ and $F_1(x, y)$ must be at least $\omega + 1$. Letting the degree of x and y in $F_0(x, y)$ and $F_1(x, y)$ be at least $\omega + 1$, the colluders cannot succeed in the above attack with non-negligible probability. (See also the footnote that appeared earlier in this paper regarding the small but subtle difference between the definition of ω in this paper and that of w in [24].) It should be noted that both the required memory size for a user's secret information and that for an authenticated message are increased by this modification. The authors of [24] claimed that their original scheme is optimal in terms of memory sizes for a user's secret information and an authenticated message, however, the fixed version is not. Optimal construction of DMRA in terms of memory sizes for both a user's secret information and an authenticated message is an interesting open problem. We further point out that schemes in [23] and [13] are optimal only for memory sizes for an authenticated message.

3. Two Novel Methods for Constructing Efficient and Unconditionally Secure Digital Signatures

In this section, we show two constructions of unconditionally secure digital signature schemes, which are called *symmetric construction* and *asymmetric construction*, respectively. In these schemes, though the flexibility of parameter settings is partially lost, the required memory sizes are reduced considerably compared to the previous method. More precisely, in our proposed schemes, the number of signatures users can generate is determined to be only one, while in HSZI-AC00 scheme [13], it can be pre-determined flexibly.

3.1 Model

In this subsection, a model of unconditionally secure signature schemes is shown. This model basically follows as in [13] with a restriction of the number of signatures that users can generate.

We assume that there is a trusted authority, denoted by TA, and n users $\mathcal{U} = \{U_1, U_2, \cdots, U_n\}$. For each user $U_i \in \mathcal{U}$ $(1 \leqq i \leqq n)$, for convenience we use the same symbol U_i to denote the identity of the user. The TA produces secret information on behalf of a user. Once being given the secret information, a user can generate and/or verify signatures by using his own secret information, respectively. A more formal definition is given below:

Definition 1: A scheme Π is a *One-Time Identity-based Signature Scheme for Unconditional Security in a Group (One-Time ISSUSG)* if it is constructed as follows:

1. **Notation:** Π consists of (TA, $\mathcal{U}$, $\mathcal{M}, \mathcal{E}, \mathcal{A}$, **Sig**, **Ver**), where
    - TA is a trusted authority,
    - $\mathcal{U}$ is a finite set of users (to be precise, users' unique names),
    - $\mathcal{M}$ is a finite set of possible messages,
    - $\mathcal{E}$ is a finite set of possible users' secret information,
    - $\mathcal{A}$ is a finite set of possible signatures,
    - $\mathbf{Sig} : \mathcal{E} \times \mathcal{M} \longrightarrow \mathcal{A}$ is a signing-algorithm,
    - $\mathbf{Ver} : \mathcal{M} \times \mathcal{A} \times \mathcal{E} \times \mathcal{U} \longrightarrow \{accept, reject\}$ is a verification-algorithm.
2. **Key Pair Generation and Distribution by TA:** For each user $U_i \in \mathcal{U}$, the TA chooses a secret information $e_i \in \mathcal{E}$, and transmits e_i to U_i via a secure channel. After delivering these secret information, the TA may erase e_i from his memory. And each user keeps his secret information secret.
3. **Signature Generation:** For a message $m \in \mathcal{M}$, a user U_i generates a signature $\alpha = \mathbf{Sig}(e_i, m) \in \mathcal{A}$ by using the secret information in conjunction with the signing-algorithm. The pair (m, α) is regarded as a signed message of U_i. After (m, α) is sent by U_i, no user is allowed to generate another signature. Namely, in this scheme only one signature is allowed to be generated, but any user can potentially become a signer.
4. **Signature Verification:** On receiving (m, α) from U_i, a user U_j checks whether α is valid by using his secret information e_j. More precisely, U_j accepts (m, α) as a valid, signed message from U_i if $\mathbf{Ver}(m, \alpha, e_j, U_i) = accept$.

The main difference between the above definition and the previous one in [13] is that the above model does not allow flexible pre-determination of the number of signatures per user. Hence, this model is called *One-Time* ISSUSG.

For a more formalized discussion for the security of a signature scheme in our model, we define the probability of success of various types of attacks. We consider three broad types of attacks: *impersonation*, *substitution* and *transfer with a trap*. In impersonation, adversaries try to forge a user's signature without seeing the user's valid signature. Note that the adversaries are allowed to observe another user's signature. In substitution, adversaries try to forge a user's signature for a message after seeing the user's valid signature for another message. In transfer with a trap, adversaries try to modify a valid signature to be accepted only by specific verifiers. Description of these attacks are given in [13].

To formally define the probabilities of success in the above three attacks, some notations must be introduced in ahead. Let $\mathcal{W} := \{W \subset \mathcal{U} | \ |W| \leqq \omega\}$, where ω is maximum number of colluders among users.

Each element of $\mathcal{W}$ represents a group of possibly colluding users. Let $e_W = \{e_{k_1}, \cdots, e_{k_j}\}$, where $W = \{U_{k_1}, \cdots, U_{k_j}\}$ $(j \leqq \omega)$, be the set of secret information for a $W \in \mathcal{W}$.

Definition 2: The success probabilities of impersonation, substitution and transfer with a trap attacks, denoted by P_I, P_S and P_T respectively, are formally defined as follows:

1) Success probability of impersonation: for $W \in \mathcal{W}$ and $U_i, U_j \in \mathcal{U}$ with $U_i, U_j \notin W$, we define $P_I(U_i, U_j, W)$ as

$$\begin{aligned} &P_I(U_i, U_j, W) \\ &\quad := \max_{e_W} \max_{1 \leqq k \leqq n, k \neq i} \max_{(m,\alpha)} \max_{(m',\alpha')} \Pr(U_j \text{ accepts} \\ &\qquad\qquad (m', \alpha') \text{ as valid from } U_i | e_W, (m, \alpha)), \end{aligned}$$

where (m, α) is a valid signed message generated by a user U_k $(1 \leqq k \leqq n,\ k \neq i)$ for a message m, and (m, α) runs over $\mathcal{M} \times \mathcal{A}$. Then, P_I is given as $P_I := \max_{\{U_i, U_j, W\}} \Pr(U_i, U_j, W)$, where $W \in \mathcal{W}$ and $U_i, U_j \in \mathcal{U}$ with $U_i, U_j \notin W$.

2) Success probability of substitution: for $W \in \mathcal{W}$ and $U_i, U_j \in \mathcal{U}$ with $U_i, U_j \notin W$, we define $P_S(U_i, U_j, W)$ as

$$\begin{aligned} &P_S(U_i, U_j, W) \\ &\quad := \max_{e_W} \max_{(m,\alpha)} \max_{(m',\alpha')} \Pr(U_j \text{ accepts} \\ &\qquad\qquad (m', \alpha') \text{ as valid from } U_i | e_W, (m, \alpha)), \end{aligned}$$

where (m, α) is a valid signed message generated by U_i for a message m, and (m', α') runs over $\mathcal{M} \times \mathcal{A}$ such that $m' \neq m$. Then, P_S is given as $P_S := \max_{\{U_i, U_j, W\}} \Pr(U_i, U_j, W)$, where $W \in \mathcal{W}$ and $U_i, U_j \in \mathcal{U}$ with $U_i, U_j \notin W$.

3) Success probability of transfer with a trap: for $W \in \mathcal{W}$ and $U_i, U_j \in \mathcal{U}$ with $U_j \notin W$ we define $P_T(U_i, U_j, W)$ as

$$\begin{aligned} &P_T(U_i, U_j, W) \\ &\quad := \max_{e_W} \max_{(m,\alpha)} \max_{(m,\alpha')} \Pr(U_j \text{ accepts} \\ &\qquad\qquad (m, \alpha') \text{ as valid from } U_i | e_W, (m, \alpha)), \end{aligned}$$

where (m, α) is a valid signed message generated by U_i, and α' is taken such that $\alpha \neq \alpha'$. Then, P_T is given as $P_T := \max_{\{U_i, U_j, W\}} \Pr(U_i, U_j, W)$, where $W \in \mathcal{W}$ and $U_i, U_j \in \mathcal{U}$ with $U_j \notin W$.

The concept of (n, ω, p_1, p_2)-*secure* One-Time ISSUSG signature scheme can now be defined, where both p_1 and p_2 are security parameters whose meanings will be made precise in the following definition.

Definition 3: Let Π be a One-Time ISSUSG with n users. Then, Π is (n, ω, p_1, p_2)-*secure* if the following conditions are satisfied: as long as there exist at most ω colluders, the following inequalities hold:

$$\begin{aligned} &\max\{P_I,\ P_S\} \leqq p_1 \\ &P_T \leqq p_2 \end{aligned}$$

where P_I, P_S and P_T are the probabilities of success of impersonation, substitution and transfer with a trap attacks, respectively.

We note that there is an alternative definition of security in which one may use a single security parameter p instead and define the success probability as

$$\max\{P_I,\ P_S,\ P_T\} \leqq p.$$

In practice, however, some applications may attach more weight to impersonation and substitution than against transfer with a trap, while some other applications may put more emphasis on robustness of transfer with a trap. By introducing two separate parameters p_1 and p_2, we have an opportunity to design a signature scheme with fine-tuned level of security.

3.2 Symmetric Construction

In this subsection, we show an implementation in One-Time ISSUSG, called the *symmetric construction*. In this construction, the required memory size for a user's secret information is reduced partially based on the fixed version of the SW-DMRA. Namely, we introduce symmetric functions for unifying the secret information for signing and for verifying. However, it should be noted that it is not trivial to implement, since the SW-DMRA does not fulfill the transferability property. The essential reason behind why the SW-DMRA does not provide transferability is that, for U_i's authenticated message $(s_i, a_i(x))$, any entity can calculate $a_i(U_j)$ and find another function $a'_i(x)$ such that $a'_i(x) \neq a_i(x)$ and $a'_i(U_j) = a_i(U_j)$. This is hard to solve since U_j must be public. We show a solution to this problem in the following.

As before, let $\mathcal{U} := \{U_1, U_2, \cdots, U_n\}$ be the set of n users and TA the trusted authority.

Symmetric construction

1. Key Generation and Distribution by TA:

Let F_{q_0} be the finite field with q_0 elements such that $q_0 \geqq n(\omega + 1)q$, where q is a security parameter of the system. We assume that the size of q_0 is almost the same as $n(\omega + 1)q$. Then, the TA divides F_{q_0} into n disjoint subsets $\mathcal{U}_1, \cdots, \mathcal{U}_n$, such that $|\mathcal{U}_i| = (\omega + 1)q$ for any i, and $\mathcal{U}_i \cap \mathcal{U}_j = \phi$ if $i \neq j$. Here, $\mathcal{U}_i$ $(1 \leqq i \leqq n)$ are made public for all users. For each user U_i $(1 \leqq i \leqq n)$, the TA picks uniformly at random, a number u_i from $\mathcal{U}_i$, respectively, and chooses uniformly at random two symmetric polynomials $F_0(x, y), F_1(x, y)$ over F_{q_0} with two variables x and y of degree at most $\omega+1$. Moreover, we assume a message m is an element in F_{q_0} as well. For each user U_i $(1 \leqq i \leqq n)$, the TA computes his secret information $e_i := \langle F_0(x,u_i), F_1(x,u_i), u_i\rangle$. Then, the TA sends e_i to U_i over a secure channel. Once the secret information has been delivered, there is now no need for the TA to keep the user's secret information.

2. **Signature Generation:** For a message $m \in F_{q_0}$, U_i generates a signature by $\alpha := \langle a_{i,m}(x), u_i\rangle$ using his secret information, where $a_{i,m}(x) := F_0(x,u_i) + mF_1(x,u_i)$. Then, (m,α) is sent by U_i with his identity U_i.
3. **Signature Verification:** On receiving U_i's signature (m,α), user U_j checks whether α is valid or not, by the use of his secret information e_j. Specifically, U_j accepts (m,α) as being a valid message-signature pair from U_i if $(F_0(x,u_j) + mF_1(x,u_j))|_{x=u_i} = a_{i,m}(x)|_{x=u_j}$ and $u_i \in \mathcal{U}_i$.

Theorem 1: The above scheme results in an $(n, \omega, \frac{1}{q_0}, \frac{1}{q})$-secure One-Time ISSUSG scheme.

Proof: Assume that after seeing a signed message (m_{i_0},α) published by U_{i_0}, the colluders $U_1,\cdots,U_\omega$ want to generate (m_{i_1},α'), such that $m_{i_1} = m_{i_0}$ and the user U_{i_2} will accept it as a valid signed message of the user U_{i_1}, i.e. α consists of $\langle a'_{i_1,m_{i_1}}(x), u'_{i_1}\rangle$ such that $a'_{i_1,m_{i_1}}(u_{i_2}) = F_0(u'_{i_1},u_{i_2}) + m_{i_0}F_1(u'_{i_1},u_{i_2})$ and $u'_{i_1} \in \mathcal{U}_{i_1}$. In the followings, we define

$$\mathbf{u'_{i_1}} := (1, u'_{i_1}, \cdots, u'^{\omega+1}_{i_1})$$

$$\mathbf{u_{i_2}} := (1, u_{i_2}, \cdots, u^{\omega+1}_{i_2})$$

$$C := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ u_{i_0} & u_1 & \cdots & u_\omega \\ {u_{i_0}}^2 & {u_1}^2 & \cdots & {u_\omega}^2 \\ \vdots & \vdots & \cdots & \vdots \\ {u_{i_0}}^{\omega+1} & {u_1}^{\omega+1} & \cdots & {u_\omega}^{\omega+1} \end{pmatrix}.$$

Letting

$$F_l(x,y) = (1, x, x^2, \cdots, x^{\omega+1})A_l \begin{pmatrix} 1 \\ y \\ y^2 \\ \vdots \\ y^{\omega+1} \end{pmatrix},\ l = 0,1,$$

where A_l $(l=0,1)$ are $(\omega+2)\times(\omega+2)$ symmetric matrices over F_{q_0}, the colluders have a $(\omega+2)\times(\omega+1)$ matrix D, where

$$D := (A_0 + m_{i_0}A_1)C.$$

From Lemma 2.1 in [22], there exist q_0 different matrices X such that

$$D = XC.$$

This implies that there are q_0 different values for $A_0 + m_{i_0}A_1$. Here, without loss of generality, these q_0 matrices can be expressed as $\{X_0 + \delta X_1 | \delta \in \{0,1,\cdots,q_0-1\}\}$, where X_0 and X_1 are some symmetric matrices such that

$$X_0C = D \quad \text{and} \quad X_1C = 0\ (X_1 \neq 0).$$

In order for the colluders to succeed the attack, they need to find a pair of u'_{i_1} and $a'_{i_1,m_{i_1}}(x)$ such that

$$a'_{i_1,m_{i_1}}(u_{i_2}) = \mathbf{u'_{i_1}}(A_0 + m_{i_0}A_1)\ {}^t\mathbf{u_{i_2}}$$

and $u'_{i_1} \in \mathcal{U}_{i_1}$. Letting d be $\mathbf{u'_{i_1}}(A_0 + m_{i_0}A_1)\ {}^t\mathbf{u_{i_2}}$, q_0 different matrices for $A_0 + m_{i_0}A_1$ result in q_0 different values for d since

$$\mathbf{u'_{i_1}}(X_0 + \delta X_1)\ {}^t\mathbf{u_{i_2}} = x_0 + \delta x_1,$$

where $x_0 := \mathbf{u'_{i_1}}X_0\ {}^t\mathbf{u_{i_2}}$ and $x_1 := \mathbf{u'_{i_1}}X_1\ {}^t\mathbf{u_{i_2}}$. It should be noticed that according to δ, $x_0 + \delta x_1$ takes q_0 different values since $x_1 \neq 0$ due to Lemma 1.

This indicates that the probability of succeeding to find $a'_{i_1,m_{i_1}}(x)$, such that $a'_{i_1,m_{i_1}}(u_{i_2}) = d$, does not exceed $\frac{1}{q_0}$, i.e. $P_I = \frac{1}{q_0}$. Similarly, we can prove $P_S \leqq \frac{1}{q_0}$ and $P_T = \frac{1}{q}$.

Here, we briefly show the proof for $P_T = \frac{1}{q}$. Assume that after seeing a signed message (m_{i_0},α) published by U_{i_0}, the colluders $U_1,\cdots,U_\omega$ want to generate (m_{i_0},α'), such that $\alpha' \neq \alpha$ and the user U_{i_1} will accept it as a valid signed message of the user U_{i_0}. Let α be $\langle a_{i_0,m_{i_0}}(x), u_{i_0}\rangle$ as described in Sect. 3.2. Since $a_{i_0,m_{i_0}}(x)$ is a polynomial with a variable x of degree at most $\omega+1$, $a'_{i_0,m_{i_0}}(x)$ $(a'_{i_0,m_{i_0}}(x) \neq a_{i_0,m_{i_0}}(x))$ has at most $\omega+1$ pairs of $\langle a'_{i_0,m_{i_0}}(c), c\rangle$, such that $c \in F_{q_0}$ and $a'_{i_0,m_{i_0}}(c) = a_{i_0,m_{i_0}}(c)$, where $a'_{i_0,m_{i_0}}(x)$ is a polynomial with a variable x of degree at most $\omega+1$. Hence, the best strategy for succeeding transfer with a trap is as follows: The colluders choose uniformly at random $\omega+1$ distinct numbers $u^{(1)}_{i_1},\cdots,u^{(\omega+1)}_{i_1}$ from $\mathcal{U}_{i_1}$ and generate $a'_{i_0,m_{i_0}}(x)$ $(a'_{i_0,m_{i_0}}(x) \neq a_{i_0,m_{i_0}}(x))$ such that $a'_{i_0,m_{i_0}}(u^{(1)}_{i_1}) = a_{i_0,m_{i_0}}(u^{(1)}_{i_1})$, $a'_{i_0,m_{i_0}}(u^{(2)}_{i_1}) = a_{i_0,m_{i_0}}(u^{(2)}_{i_1})$, $\cdots$, $a'_{i_0,m_{i_0}}(u^{(\omega+1)}_{i_1}) = a_{i_0,m_{i_0}}(u^{(\omega+1)}_{i_1})$. Then, the colluders send $\alpha' = \langle a'_{i_0,m_{i_0}}(x), u_{i_0}\rangle$ to U_{i_1}. The attack is successful if and only if $u_{i_1} \in \{u^{(1)}_{i_1}, u^{(2)}_{i_1}, \cdots, u^{(\omega+1)}_{i_1}\}$. Hence, $P_T = \frac{\omega+1}{(\omega+1)q} = \frac{1}{q}$. □

Lemma 1: Letting $\mathbf{u}_1,\cdots,\mathbf{u}_{\omega+1}$ be $(\omega+2)$-dimensional (row) vectors over F_q. Also, let A be an $(\omega+2)\times(\omega+2)$ symmetric matrix over F_q, such that $\mathbf{u}_iA = 0$ for all i $(1 \leqq i \leqq \omega+1)$ and $A \neq 0$. Then, for any pair of $(\omega+2)$-dimensional vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, such that $(\mathbf{v}_\ell, \mathbf{u}_1, \cdots, \mathbf{u}_{\omega+1})$ $(\ell = 1,2)$ are linearly independent, $\mathbf{v}_1A\,{}^t\mathbf{v}_2 \neq 0$.

Proof. It is clear that $\det A = 0$ and therefore, for any $(\omega+2)$-dimensional (row) vector $\mathbf{v}$, such that $(\mathbf{v}, \mathbf{u}_1, \cdots, \mathbf{u}_{\omega+1})$ are linearly independent, $\mathbf{u}_i \cdot (A\,{}^t\mathbf{v}) =$

0 and $A^t\mathbf{v} \neq 0$ for all i $(1 \leqq i \leqq \omega + 1)$. (We note that if $A^t\mathbf{v} = 0$, A will be determined 0.) Then, assuming $\mathbf{v}_1 \cdot (A^t\mathbf{v}_2) = 0$, $A^t\mathbf{v}_2$ will be 0 or $(\mathbf{v}_1, \mathbf{u}_1, \cdots, \mathbf{u}_{\omega+1})$ will be linearly dependent. This is a contradiction. □

Theorem 2: The required memory size in the above construction is given as follows:

$$|\mathcal{A}| = (\omega + 1)q{q_0}^{\omega+2} \qquad \text{(size of a signature)}$$
$$|\mathcal{E}| = (\omega + 1)q{q_0}^{2\omega+4} \qquad \text{(size of a user's key).}$$

Although in this scheme the required memory size of a signature is slightly increased compared to the HSZI-AC00 scheme [13], that of each user's secret information is significantly reduced. Comparison with the previous method is shown in the following section.

3.3 Asymmetric Construction

In the symmetric construction, though the required memory size of a user's secret information has significantly been reduced, the required memory size of a signature increased compared to the previous method. In this subsection, we show other methods for reducing the required memory size of a user's secret information without increasing the required memory size for a signature. One of the proposed schemes in this subsection is optimal, especially in terms of memory size for a signature. Such schemes are called *asymmetric constructions* since the secret information for signing and that for verification is different. In symmetric construction, on the other hand, the secret information for signing and verification is the same.

As before, let $\mathcal{U} := \{U_1, U_2, \cdots, U_n\}$ be the set of n users and TA the trusted authority.

Asymmetric construction

1. **Key Generation and Distribution by TA:** Let F_q be the finite field with q elements such that $q \geqq n$. The TA picks n elements $v_i = (v_{i,1}, \cdots, v_{i,\omega})$ $(1 \leqq i \leqq n)$ uniformly at random in F_q^ω for users U_i $(1 \leqq i \leqq n)$ respectively, such that $v_{i,1}, \cdots, v_{i,\omega} \in F_q$, and chooses two polynomials uniformly at random, $G_0(x, y_1, \ldots, y_\omega)$ and $G_1(x, y_1, \ldots, y_\omega)$, over F_q with $\omega + 1$ variables $x, y_1, \cdots, y_\omega$, in which the degree of x is at most $\omega + 1$ and that of every y_i is at most 1. Moreover, we assume that each user's identity U_i and a message m are elements of F_q. For each user U_i $(1 \leqq i \leqq n)$, the TA computes U_i's secret information $e_i := \langle G_0(U_i, y_1, \ldots, y_\omega), G_1(U_i, y_1, \ldots, y_\omega), G_0(x, v_i), G_1(x, v_i), v_i\rangle$, where $G_\ell(x, v_i) := G_\ell(x, y_1, \ldots, y_\omega)|_{(y_1,\ldots,y_\omega)=(v_{i,1},\ldots,v_{i,\omega})}$ for $\ell = 0, 1$. The TA then sends e_i to U_i over a secure channel. Once all the keys are delivered, there will be no need for the TA to keep the user's secret information.
2. **Signature Generation:** For a message $m \in F_q$, U_i generates a signature by $\alpha = G_0(U_i, y_1, \ldots, y_\omega) + mG_1(U_i, y_1, \ldots, y_\omega)$ using $G_0(U_i, y_1, \ldots, y_\omega)$ and $G_1(U_i, y_1, \ldots, y_\omega)$. Then, (m, α) is sent by U_i with his identity U_i.
3. **Signature Verification:** On receiving (m, α) from U_i, user U_j checks whether α is valid by the use of his secret information. More specifically, U_j accepts (m, α) as being a valid message-signature pair from U_i if $(G_0(x, v_i) + mG_1(x, v_i))|_{x=U_i} = \alpha|_{(y_1,\ldots,y_\omega)=(v_{j,1},\ldots,v_{j,\omega})}$.

Theorem 3: The above scheme results in an $(n, \omega, (\frac{2}{q} - \frac{1}{q^2}), \frac{1}{q})$-secure One-Time ISSUSG scheme.

Proof of Theorem 3 can be given similarly to Theorem 1. For example, we give an intuitive discussion on the security against impersonation attacks. Without loss of generality, let the set of colluders be $\{U_1, U_2, \cdots, U_\omega\} \in \mathcal{U}$. Assuming that the colluders intend to impersonate a victim sender U_i $(i \notin \{1, \cdots, \omega\})$, any ω colluders cannot obtain $G_\ell(U_i, y_1, \ldots, y_\omega)$ $(\ell = 0, 1)$ since the maximum degrees of x in G_ℓ $(\ell = 0, 1)$ are $\omega + 1$. Then, for generating a forged signed message which will be accepted by a victim receiver U_j $(j \notin \{1, \cdots, \omega\})$, the best strategy will be to forge a signature which can be accepted by the colluders themselves. When using this method, the forged message will be accepted by U_j with probability 1 if $(1, v_{j,1}, \ldots, v_{j,\omega}) \in \{x_1 \cdot (1, v_{1,1}, \ldots, v_{1,\omega}) + \ldots + x_\omega \cdot (1, v_{\omega,1}, \ldots, v_{\omega,\omega})|(x_1, \cdots, x_\omega) \in F_q^\omega\}$ holds. We note that $\Pr((1, v_{j,1}, \ldots, v_{j,\omega}) \in \{x_1 \cdot (1, v_{1,1}, \ldots, v_{1,\omega}) + \ldots + x_\omega \cdot (1, v_{\omega,1}, \ldots, v_{\omega,\omega})|(x_1, \cdots, x_\omega) \in F_q^\omega\}) = 1/q$. In addition, even if the colluders forges a random signed message, the probability of succeeding in the attack is originally $1/q$. Together, with the above strategy, the probability of succeeding in impersonation will be at most $1/q + 1/q - 1/q^2$, where $1/q^2$ is used to eliminate parts that may be over-estimated. Similarly, probabilities of succeeding other attacks can be estimated.

The above scheme can be slightly modified, resulting in another $(n, \omega, \frac{1}{q}, \frac{1}{q})$-secure One-Time ISSUSG scheme.

Theorem 4: In the above construction, the following modification also produces an $(n, \omega, \frac{1}{q}, \frac{1}{q})$-secure One-Time ISSUSG scheme: Instead of choosing randomly, the TA may choose n elements $v_1, \ldots, v_n \in F_q^\omega$, for users' secret information, such that for any $\omega+1$ vectors

$$\begin{aligned} v_{i_1} &= (v_{i_1,1}, \ldots, v_{i_1,\omega}) \\ &\vdots \\ v_{i_{\omega+1}} &= (v_{i_{\omega+1},1}, \ldots, v_{i_{\omega+1},\omega}), \end{aligned}$$

the $\omega+1$ new vectors $(1, v_{i_1,1}, \ldots, v_{i_1,\omega}), \ldots, (1, v_{i_{\omega+1},1}, \ldots, v_{i_{\omega+1},\omega})$ are linearly independent.

Though the proposed $(n, \omega, \frac{1}{q}, \frac{1}{q})$-secure One-Time

Table 1 The required memory sizes of each user's secret information, in the proposed symmetric construction ($(n, \omega, \frac{1}{q_0}, \frac{1}{q})$-secure One-Time ISSUSG), asymmetric construction ($(n, \omega, \frac{1}{q}, \frac{1}{q})$-secure One-Time ISSUSG) and the HSZI-AC00 scheme ($(n, \omega, 1, \frac{1}{q}, \frac{1}{q})$-secure ISSUSG [13]), assuming that $|q| = 160$ bits and ω is determined appropriately for each n.

	$n = 1,000$	$n = 10,000$	$n = 100,000$	$n = 1,000,000$
	$\omega = 500$	$\omega = 2,000$	$\omega = 10,000$	$\omega = 50,000$
Symmetric construction	22Kbyte	91Kbyte	464Kbyte	2,393Kbyte
Asymmetric construction	49Kbyte	196Kbyte	977Kbyte	4,883Kbyte
HSZI-AC00 scheme [13]	69Kbyte	508Kbyte	4,493Kbyte	41,993Kbyte

Table 2 The required memory sizes of a signature, in the proposed symmetric construction ($(n, \omega, \frac{1}{q_0}, \frac{1}{q})$-secure One-Time ISSUSG), asymmetric construction ($(n, \omega, \frac{1}{q}, \frac{1}{q})$-secure One-Time ISSUSG) and the HSZI-AC00 scheme ($(n, \omega, 1, \frac{1}{q}, \frac{1}{q})$-secure ISSUSG [13]), assuming that $|q| = 160$ bits and ω is determined appropriately for each n.

	$n = 1,000$	$n = 10,000$	$n = 100,000$	$n = 1,000,000$
	$\omega = 500$	$\omega = 2,000$	$\omega = 10,000$	$\omega = 50,000$
Symmetric construction	12Kbyte	46Kbyte	233Kbyte	1,197Kbyte
Asymmetric construction	10Kbyte	40Kbyte	196Kbyte	977Kbyte
HSZI-AC00 scheme [13]	10Kbyte	40Kbyte	196Kbyte	977Kbyte

ISSUSG scheme is more secure than the proposed $(n, \omega, \frac{2}{q} - \frac{1}{q^2}, \frac{1}{q})$-secure One-Time ISSUSG scheme in terms of impersonation or substitution, it requires more complicated transactions for generating each user's secret information.

The following theorem states the required memory size of our construction, and its proof is trivial.

Theorem 5: The required memory size in the above constructions is given as follows:

$$|\mathcal{A}| = q^{\omega+1} \qquad \text{(size of a signature)}$$
$$|\mathcal{E}| = q^{5\omega+6} \qquad \text{(size of a user's key).}$$

Corollary 1: The construction proposed in Theorem 4 is optimal in terms of the memory size of a signature.

The proof follows as from [24]. Since the model of One-Time ISSUSG is regarded as a restricted version of that of MRA, lower bounds on required memory sizes for MRA can also be applied to One-Time ISSUSG. The required memory size for the above construction matches the lower bound on a signature presented in Theorem 5.2 in [24].

Comparison of these schemes with the conventional scheme is shown in the following section with more detail.

4. Comparison

In this section, we compare the proposed schemes with the previous method [13]. In the HSZI-AC00 scheme [13], the number of signatures that each user can generate can be pre-determined in a flexible manner. In order to compare the proposed One-Time ISSUSG schemes with the HSZI-AC00 scheme, we set the number of signatures that a user can generate to be one in the previous method. The following proposition shows the required memory sizes for the HSZI-AC00 scheme for this parameter setting.

Proposition 1 ([13]): Letting the number of users be n and the maximum number of colluders ω, then the required memory sizes for the HSZI-AC00 scheme ($(n, \omega, 1, \frac{1}{q}, \frac{1}{q})$-secure ISSUSG [13][†]) are:

$$|\mathcal{A}| = q^{\omega+1} \qquad \text{(size of a signature)}$$
$$|\mathcal{E}| = q^{2n+3\omega+2} \qquad \text{(size of a user's key),}$$

assumie at most 1 signature, the probability of succeeding the impersonation and substitution is at most $\frac{1}{q}$ and that the probability of succeeding transfer with a trap is at most $\frac{1}{q}$.

As shown in Table 1, the required memory size of each user's secret information is significantly reduced in the proposed schemes. In the symmetric construction, though the required memory size of a signature increases, that of each user's secret information is considerably reduced. As an example, for 100,000 users with appropriate security parameter settings, the required memory size for a user's secret information is reduced to 10.3% of that required in the HSZI-AC00 scheme. In the asymmetric construction, the reduction of the required memory size of each user's secret information is less than that in the symmetric construction. However, the required memory of a signature is less than that of

[†] It has now been found that $(n, \omega, \psi, \frac{1}{q}, \frac{1}{q-1})$-secure ISSUSG in [13] is in fact, $(n, \omega, \psi, \frac{1}{q}, \frac{1}{q})$-secure ISSUSG (see the security definition in [13]). Therefore, we have $(n, \omega, 1, \frac{1}{q}, \frac{1}{q-1})$-secure ISSUSG in [13] to be described as $(n, \omega, 1, \frac{1}{q}, \frac{1}{q})$-secure ISSUSG. Details on security of these schemes can be obtained from the present authors.

the symmetric construction. More precisely, the proposed asymmetric construction is optimal in terms of the required memory size of a signature, reminiscent to the HSZI-AC00 scheme. Table 2 shows the required memory sizes for a signature in the proposed schemes and that in the HSZI-AC00 scheme.

Acknowledgemnt

We would like to thank the anonymous reviewers for their helpful comments.

References

[1] D. Boneh and R.J. Lipton, "Quantum cryptanalysis of hidden linear functions," Proc. CRYPTO'95, LNCS 963, pp.424–437, Springer-Verlag, 1995.

[2] E.F. Brickell and D.R. Stinson, "Authentication codes with multiple arbiters," Proc. Eurocrypt'88, LNCS 330, pp.51–55, Springer-Verlag, 1988.

[3] S. Cavallar, B. Dodson, A.K. Lenstra, W.M. Lioen, P.L. Montgomery, B. Murphy, H. te Riele, K. Aardal, J. Gilchrist, G. Guillerm, P.C. Leyland, J. Marchand, F. Morain, A. Muffett, C. Putnam, C. Putnam, and P. Zimmermann, "Factorization of a 512-bit RSA modulus," Proc. Eurocrypt'00, LNCS 1807, pp.1–18, Springer-Verlag, 2000.

[4] D. Chaum and S. Roijakkers, "Unconditionally secure digital signatures," Proc. CRYPTO'90, LNCS 537, pp.206–215, Springer-Verlag, 1990.

[5] Y. Desmedt and M. Yung, "Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attack," Proc. CRYPTO'90, LNCS 537, pp.177–188, Springer-Verlag, 1990.

[6] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/multi-sender network security: Efficient authenticated multicast/feedback," Proc. IEEE Infocom'92, pp.2045–2054, 1992.

[7] National Institute of Standard and Technology (NIST), "Proposed federal information processing standard for digital signature standard (DSS)," Federal Register, vol.56, no.169, pp.42980–42982, 1991.

[8] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol.31, no.4, pp.469–472, 1985.

[9] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," Proc. CRYPTO'86, LNCS 263, pp.186–194, Springer-Verlag, 1986.

[10] E.N. Gilbert, F.J. MacWilliams, and N.J.A. Sloane, "Codes which detect deception," Bell Syst. Tech. J., vol.53, pp.405–425, 1974.

[11] T. Johansson, "Lower bounds on the probability of deception in authentication with arbitration," IEEE Trans. Inf. Theory, vol.40, no.5, pp.1573–1585, 1994.

[12] T. Johansson, "Further results on asymmetric authentication schemes," Inf. Comput., vol.151, pp.100–133, 1999.

[13] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Unconditionally secure digital signature schemes admitting transferability," Proc. Asiacrypt2000, LNCS 1976, pp.130–142, Springer-Verlag, 2000.

[14] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Efficient and unconditionally secure digital signatures and a security analysis of a multireceiver authentication code," Proc. PKC2002, LNCS 2274, pp.64–79, Springer-Verlag, 2002.

[15] K. Kurosawa, "New bound on authentication code with arbitration," Proc. CRYPTO'94, LNCS 839, pp.140–149, Springer-Verlag, 1994.

[16] K. Kurosawa and S. Obana, "Combinatorial bounds for authentication codes with arbitration," Proc. Eurocrypt'95, LNCS 921, pp.289–300, Springer-Verlag, 1995.

[17] S. Obana and K. Kurosawa, "A^2-code = affine resolvable + BIBD," Proc. ICICS'97, LNCS 1334, pp.118–129, Springer-Verlag, 1997.

[18] T. Okamoto, "A fast signature scheme based on congruential polynomial operations," IEEE Trans. Inf. Theory, vol.36, no.1, pp.47–53, 1990.

[19] B. Pfitzmann and M. Waidner, "Fail-stop signatures and their application," Proc. Securicom'91, 9th Worldwide Congress on Computer and Communications Security and Protection, pp.145–160, 1991.

[20] T.P. Pedersen and B. Pfitzmann, "Fail-stop signatures," SIAM J. Comput., vol.26, no.2, pp.291–330, 1997.

[21] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," Commun. ACM, vol.21, no.2, pp.120–126, 1978.

[22] R. Safavi-Naini and H. Wang, "New results on multi-receiver authentication codes," Proc. Eurocrypt'98, LNCS 1403, pp.527–541, 1998.

[23] R. Safavi-Naini and H. Wang, "Broadcast authentication in group communication," Proc. Asiacrypt'99, LNCS 1716, pp.399–411, Springer-Verlag, 1999.

[24] R. Safavi-Naini and H. Wang, "Multireceiver authentication codes: Models, bounds, constructions and extensions," Inf. Comput., vol.151, pp.148–172, 1999.

[25] C. Schnorr, "Efficient signature generation by smart cards," J. Cryptology, vol.4, pp.161–174, 1991.

[26] J. Shikata, G. Hanaoka, Y. Zheng, and H. Imai, "Security notions for unconditionally secure signature schemes," Proc. Eurocrypt2002, LNCS2332, pp.434–449, Springer-Verlag, 2002.

[27] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol.26, no.5, pp.1484–1509, 1997.

[28] G.J. Simmons, "Authentication theory/coding theory," Proc. CRYPTO'84, LNCS 196, pp.411–431, Springer-Verlag, 1984.

[29] G.J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes," Proc. Eurocrypt'87, pp.151–165, Springer-Verlag, 1987.

[30] G.J. Simmons, "A Cartesian construction for unconditionally secure authentication codes that permit arbitration," J. Cryptology, vol.2, pp.77–104, 1990.

[31] R. Taylor, "Near optimal unconditionally secure authentication," Proc. Eurocyrpt'94, LNCS 950, pp.244–253, Springer-Verlag, 1994.

[32] Y. Wang and R. Safavi-Naini, "A^3-codes under collusion attacks," Proc. Asiacrypt'99, LNCS 1716, pp.390–398, Springer-Verlag, 1999.

Goichiro Hanaoka is currently a Research Fellow of Japan Society for the Promotion of Science (JSPS). He received his bachelors degree in Electronic engineering from the University of Tokyo in 1997, and received his masters and Ph.D. degrees in Information and communication engineering from the University of Tokyo in 1999 and 2002, respectively. He was awarded the excellent paper prize from SITA in 2000. His research interests are in the fields of cryptography, electronic payments and network security.

Junji Shikata received the B.S. and M.S. degrees in mathematics from Kyoto University, Japan, in 1994 and 1997, respectively, and the Ph.D. degree in mathematics from Osaka University, Japan, in 2000. From 2000 to 2002 he was a postdoctoral fellow at the Institute of Industrial Science, the University of Tokyo, Japan. Since 2002 he has been with the Graduate School of Environment and Information Sciences, Yokohama National University, Japan. Currently, he is Lecturer of Yokohama National University. His research interests include cryptography, computational number theory and computer science.

Yuliang Zheng received his B.Sc. degree in computer science from Nanjing Institute of Technology, China, in 1982, and the M.E. and Ph.D. degrees, both in electrical and computer engineering, from Yokohama National University, Japan, in 1988 and 1991 respectively. From 1982 to 1984 he was with the Guangzhou Research Institute for Communications, Guangzhou (Canton), China. From 1991 to 2001 he was on the faculty of Australian Defence Force Academy, University of Wollongong and Monash University, all in Australia. Currently he is a Professor of Software and Information Systems, University of North Carolina at Charlotte, USA. He has chaired a number of international conferences and is a co-founder of the PKC international workshop series dedicated to the practice and theory in public key cryptography. Dr. Zheng is widely known as the inventor of the signcryption public key cryptographic algorithm. His research interests include cryptography, network security, and the protection of critical infrastructures. Dr. Zheng is a member of IACR and ACM, and a senior member of IEEE.

Hideki Imai was born in Shimane, Japan on May 31, 1943. He received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, 1971, respectively. From 1971 to 1992 he was on the faculty of Yokohama National University. In 1992 he joined the faculty of the University of Tokyo, where he is currently a Full Professor in the Institute of Industrial Science. His current research interests include information theory, coding theory, cryptography, spread spectrum systems and their applications. From IEICE (the Institute of Electronics, Information and Communication Engineers) he received Best Book Awards in 1976 and 1991, Best Paper Awards in 1992 and 2003, Yonezawa Memorial Paper Award in 1992, Achievement Award in 1995, and Inose Award in 2003. He also received Golden Jubilee Paper Award from the IEEE Information Theory Society in 1998, and official Commendations from the Minster of Public Management, Home Affairs, Posts and Telecommunications in June 2002 and from the Minister of Economy, Trade and Industry in October 2002. He was awarded Honor Doctor Degree by Soonchunhyang University, Korea in 1999 and Docteur Honoris Causa by the University of Toulon Var, France in 2002. He was elected an IEEE Fellow in 1992 and an IEICE Fellow in 2001. He chaired several committees of scientific societies and chaired many international conferences such as IEEE-ITW, IEEE-ISIT, AAECC, PKC, FSE, and WPMC. He served as the leader of research projects supported by JSPS (Japan Society for the Promotion of Science), IPA (Information-technology Promotion Agency, Japan) etc. and as the editor for scientific journals of IEICE, IEEE etc. Dr. Imai was on the board of IEICE (1992–1994, 1996–1999), the IEEE Information Theory Society (IT-SOC, 1993–1998), Japan Society of Security Management (1988–present) and the Society of Information Theory and Its Applications (SITA, 1981–1997). He served as the president of SITA (1997), IEICE Engineering Sciences Society (1998–1999), a vice-president of IEEE IT-SOC (2002–present), and as the chairman of CRYPTREC (Cryptography Techniques Research and Evaluation Committee of Japan) (2000–present).