PAPER *Special Section on Cryptography and Information Security*

# A Traitor Traceable Conference System with Dynamic Sender

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

**SUMMARY** This paper addresses the problem of designing an unconditionally secure conference system that fulfills the requirements of both *traceability* and *dynamic sender*. In a so-called conference system, a common key is shared among all authorized users, and messages are encrypted using the shared key. It is known that a straightforward implementation of such a system may present a number of security weaknesses. Our particular concern lies in the possibility that unauthorized users may be able to acquire the shared key by illegal means, say from one or more authorized but dishonest users (called *traitors*). An unauthorized user who has successfully obtained the shared key can now decrypt scrambled messages without leaving any evidence on who the traitors were. To solve this problem, in this paper we propose a conference system that admits dynamic sender traceability. The new solution can detect traitors, even if the sender of a message is dynamically determined after a shared key is distributed to authorized users. We also prove that this scheme is unconditionally secure.

***key words:*** *traitor traceable scheme, authentication scheme, dynamic sender, unconditional security*

## 1. Introduction

### 1.1 Background

We address a new type of conference systems which can be proved to be unconditionally secure. In a generic conference system, if an authorized user wishes to send a message in a confidential way to other authorized users within the group, a common conference key must be shared in advance. The shared key will thenceforth enable the sender to encrypt the message using a symmetric key encryption algorithm. The resultant ciphertext will then be broadcast to other authorized users who can decrypt the message with ease by the use of the shared key. This simple setting, however, may give rise to a serious problem: what if an authorized user exposes, incidentally or deliberately, the secret-key, resulting in the key being passed over to an unauthorized user? We will not be able to specify then, which one of the authorized users' shoulder the key has slipped away from by just looking at the already-exposed key. This is due to the fact that the exposed key, or the shared key has been shared among all the authorized users and hence the copies of the key in the users' hands are all indistinguishable.

One answer to the above problem is to use a traitor tracing scheme which has a property called *traceability.* The concept of traceability was originally introduced by Chor, Fiat and Naor [2] in 1994, and has been studied intensively in the literatures [1], [6]–[8], [14], [15]. To understand traceability, suppose there are $n$ users $T, U_1, U_2, \ldots, U_{n-1}$, where $T$ is the designated sender, and all others $U_1, U_2, \ldots, U_{n-1}$ are receivers. The sender $T$ has a secret encryption key $e_T$ and receivers $U_1, U_2, \ldots, U_{n-1}$ possess in a secure way the matching decryption keys $e_1, e_2, \ldots, e_{n-1}$, respectively. In order to send a source state (or a message) $s$ to the receivers, $T$ must first encrypt $s$ by the use of $e_T$, then broadcast the resultant ciphertext $e_T(s)$, and finally, each receiver $U_i$ $(1 \leq i \leq n-1)$ recovers $s$ from the ciphertext using the secret-key $e_i$. If by any chance a receiver exposes the decryption key to an unauthorized user (i.e. an outsider), the sender may identify the traitorous receiver to whom the decryption key can be traced. This in fact, is the main property that underlies the idea of traceability and is exertive in real-time settings. If we say that the source state is at the earliest or at a "fresh" state of information, then at the time an unauthorized user has obtained it from the traitor, the information will no longer be "fresh."

Though these traceability schemes may seem appropriate for tracing traitors in conference systems, in fact, most existing schemes are not. Namely, these schemes are mostly designed for broadcasting for one designated transmitter and many subscribers, and it is difficult to determine dynamically, who the sender of a message is. Note that in generic conference systems, the sender is dynamically determined only after setting up the system. In *public-key traitor tracing* [1], [6], [15], any entity can encrypt a source state and this method alone can satisfy the property of a dynamic sender. In fact, all of the related schemes known to date can satisfy the property of dynamic sender. However, these

Manuscript received March 23, 2001.
Manuscript revised August 2, 2001.
Final manuscript received September 20, 2001.

[†] The authors are with the 3rd Department, Institute of Industrial Science, The University of Tokyo, 153-8505 Tokyo, Japan.

[††] The author is with the Department of Software and Information Systems, University of North Carolina, Charlotte, USA.

[*] The author is supported by a Research Fellowship from Japan Society for the Promotion of Science (JSPS).

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

schemes only offer computational security, which is dependent on certain unproven assumptions. There has never existed a traceability scheme that allows a sender to be dynamic.

### 1.2 Our Results

In this paper, we construct a conference system with an additional property other than traceability; that is to allow a sender to be *dynamic*. In the proposed scheme, the sender will be dynamically determined after distributing each user's secret information. Furthermore, our scheme is unconditionally secure. Hence, this is the first unconditionally secure traceability scheme with dynamic sender. We will show further that the memory-size required of each authorized user in our scheme will be significantly smaller than that required in the following trivial construction: prepare $n$ independent traceability schemes so that each authorized user plays a role of the sender in at least one of the $n$ schemes.

Also, we show a modified version of the proposed traceable encryption scheme that fulfills authenticity as well. From the properties of the proposed traceable encryption scheme, an authentication scheme for the proposed encryption scheme needs to meet the property of dynamic sender, multireceiver and unconditional security. In addition to that property, secrecy for a transmitted message will be also required. Here, we need to note that in many authentication schemes, adversaries can extract messages to be authenticated from the authenticator even if the message is encrypted by an encryption scheme. Therefore, it will not be possible to simply apply the commonly used authentication schemes to our proposed traceable encryption scheme. Generally, unconditionally secure authentication codes [4], [13] are used for point-to-point authentication. As an extension to these schemes, *multireceiver authentication codes* [3], [5], [9]–[11] have been extensively studied in the literature. In these schemes, multiple receivers verify broadcasted messages. And in our paper, we construct an appropriate authentication scheme for our proposed traceable encryption scheme by modifying an existing multireceiver authentication code.

The remaining part of this paper is organized in the following manner: in Sect. 2, we address a model of traceable encryption schemes with dynamic sender. The concept of $(n, \omega, \epsilon)$-*traceable encryption scheme with dynamic sender* ($(n, \omega, \epsilon)$-TESDS) is introduced followed by discussion of details. We also construct $(n, \omega, \epsilon)$-TESDS by using symmetric polynomials with two variables over finite fields. In Sect. 3, we show a modified version of $(n, \omega, \epsilon)$-TESDS which fulfills the property of authenticity. Finally, in Sect. 4, we close the paper with some concluding remarks.

## 2. Traceable Encryption Scheme with Dynamic Sender

### 2.1 The Model

We consider the following model for secure conference systems: there is a trusted authority, in short TA, a set of $n$ authorized users denoted by $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$, and a broadcast channel. In the set-up phase, the TA distributes a piece of secret information $k_i$ to each authorized user $U_i$. Authorized user $U_i$ can now encrypt the message with his secret information $k_i$, and is broadcasted to other authorized users. It is then, decrypted by each authorized user $U_j$ and finally, the message with his own secret information $k_j$ is recovered. Now, let $M$ be a finite set of possible messages, and assume that there is a probability distribution on $M$. Each authorized user can now choose a message according to this probability distribution. Let $K$ and $C$ be finite sets of possible secret information and ciphertexts, respectively.

Next, we discuss the security of the traitor traceable encryption scheme with dynamic sender.

**Definition 1:** A scheme in the model described above is called an $(n, \omega, \epsilon)$-*traceable encryption scheme with dynamic sender* ($(n, \omega, \epsilon)$-TESDS for short) if the following conditions are satisfied:

(1) No unauthorized user can obtain any information regarding the message from the ciphertext without using an authenticated user's secret information given by TA.

(2) For every coalition of at most $\omega$ authorized but dishonest users (traitors), the following holds: suppose that the secret information of the colluders has been used to construct a pirate key. If the pirate key can decrypt any ciphertext in the system, then one of the coalition members is identified as a traitor with a probability greater than $\epsilon$, where $\epsilon$ is a security parameter. Namely, there exists an algorithm $\mathcal{A}$ such that: if $W$ is a set of possible colluders, where $|W| \leq \omega$, and $k_p$ is a pirate key constructed by $W$ so that $k_p$ can decrypt any ciphertext in the system, then

$$\Pr(\mathcal{A}(k_p) = U_i(\in W)) > \epsilon,$$

where the probability is taken over all possible $k_p$, the coin tosses of $\mathcal{A}$ if $\mathcal{A}$ is probabilistic.

For simplicity, we assume that after the key distribution phase, only one user can broadcast at most a single encrypted message (namely, this is a *one-time use* scheme). Note that no other users are allowed to broadcast a message.

As seen in the above model, $(n, \omega, \epsilon)$-TESDS is an unconditionally secure encryption scheme within a group.

## 2.2 Construction of $(n, \omega, \epsilon)$-TESDS

In this subsection, we construct an $(n, \omega, \epsilon)$-TESDS, where $\epsilon = \frac{1}{q}$, by using a polynomial over the finite field $GF(q)$.

1) Key generation and distribution by TA:
Let $GF(q)$ be the finite field with $q$ elements. We assume that for each authorized user $U_i$, his identity $u_i$ is an element in $GF(q)$. We also assume that $M = GF(q)$. TA generates a symmetric polynomial with two variables:
$$f(x,y) = \sum_{i=0}^{\omega}\sum_{j=0}^{\omega} a_{ij}x^i y^j$$
where the coefficients $a_{ij}(= a_{ji}) \in GF(q)$ are uniformly taken at random. After that, the TA securely sends $f(u_i, y)$ to the authorized user $U_i$. The secret information for $U_i$ is $f(u_i, y)$.
2) Encryption:
For a message $m \in M$, an authorized user $U_i$ encrypts it to $c(y) := m + f(u_i, y)$ by his secret information $f(u_i, y)$. Then, the ciphertext is broadcasted to other authorized users.
3) Decryption:
When an authorized user $U_j$ receives a ciphertext $c(y)$ from $U_i$, he decrypts it by using the formula $c(y)|_{y=u_j} - f(u_j, y)|_{y=u_i} = m$.

Note that our construction described above is similar to that of [6] by Kurosawa and Desmedt. We can see that our construction can be considered as an extension to that of Kurosawa-Desmedt scheme, since our scheme admits *dynamic sender*. In other words, after the key distribution phase, any authorized user can each be a potential sender.

Discussion on *traceability* follows. It has been seen that our construction employs traceability as also described in Kurosawa-Desmedt scheme [6]. Here, for simplicity, in our model of Definition 1 we assume that a pirate key $k_p$ so that it can decrypt any ciphertext contains a secret information $k_i$ for some authorized user $U_i$ when it is exposed. Thus, in the above construction, we assume that when a user's secret information is exposed to some unauthorized users, the exposed key contains the form $(u, f(u, y))$, where $u$ is an identity of some authorized user. Obviously, if the exposed key includes the form $f(u_i, u_j)$, we cannot specify which one of $U_i$ or $U_j$ has exposed the secret information. However, in this case, unauthorized users can only decrypt the ciphertext from $U_i$ or $U_j$. But, here in our setting, any authorized user can be a potential sender so this would not matter in the first place. Therefore, the only things we need to consider is the exposed key, which has the ability of decrypting the ciphertext sent by any possible senders.

Furthermore, we need to consider other existing effective attack methods, which is discussed and can be read in [14]. In this paper, we do not intend to pursue the case of all the attack methods, but with the exception of the exposed keys in the form of $(u, f(u, y))$[†].

We show the following result:

**Theorem 1:** The construction described in this subsection results in an $(n, \omega, \frac{1}{q})$-TESDS.

*Proof.* It is clear that unauthorized users cannot obtain any information about the message from the ciphertext without using the secret information given by the TA. Here, we show that if a pirate key generated by them can decrypt any ciphertext in the system, then one of the coalition members is identified with probability of more than $\frac{1}{q}$. Suppose that a coalition of authorized users $\{U_{i_1}, \cdots, U_{i_\omega}\}$ generates a pirate key $k_p$ with probability of more than $\frac{1}{q}$ such that $k_p$ does not include $(u_{i_1}, f(u_{i_1}, y))$, or $(u_{i_2}, f(u_{i_2}, y))$, or $\cdots$, or $(u_{i_\omega}, f(u_{i_\omega}, y))$. Since $k_p$ can decrypt any ciphertext in the system, $k_p$ must contain at least $(x_0, f(x_0, y))$ for some $x_0 \notin \{u_{i_1}, \cdots, u_{i_\omega}\}$. However, this will be impossible, because the maximum degree of $x$ in $f(x, y)$ is $\omega$ and the coalition of authorized users has only $(u_{i_1}, f(u_{i_1}, y)), (u_{i_2}, f(u_{i_2}, y)), \cdots, (u_{i_\omega}, f(u_{i_\omega}, y))$.

The following theorem shows the required memory size for the above scheme.

**Theorem 2:** The required memory size for the proposed $(n, \omega, \frac{1}{q})$-TESDS is as follows:
$$\begin{aligned}|M| &= q, \text{ (size of a message (or a plaintext))}\\ |K| &= q^{\omega+1} \text{ (size of a user's secret information)},\\ |C| &= q^{\omega+1} \text{ (size of a ciphertext)}.\end{aligned}$$

Hence, the above scheme requires each authorized user to store $(\omega + 1)\log q$ bits. The length of a ciphertext is $(\omega + 1)\log q$ bits. In addition, the above scheme requires the TA to store $\frac{(\omega+1)(\omega+2)}{2}\log q$ bits.

## 2.3 Comparing Memory Sizes

In this subsection, we compare the memory sizes required in our construction of $(n, \omega, \epsilon)$-TESDS, where $\epsilon = \frac{1}{q}$, with the trivial construction derived from Kurosawa-Desmedt scheme [6].

With our notations introduced in 2.1, Kurosawa-Desmedt scheme can be described as follows. The

[†] If in a situation where this restriction is not reasonable, then the security of our scheme is unproven as well as the security of Kurosawa-Desmedt scheme [6]. The method for securely constructing variants in Kurosawa-Desmedt scheme is also an open problem (cf. [14]).

**Table 1** The required memory sizes of each user's secret information, in the proposed $(n, \omega, \frac{1}{q})$-TESDS and trivial construction based on [6], assuming that $|q| = 160$ bits and $\omega$ is determined appropriately for each $n$.

| | $n = 100$ | $n = 1,000$ | $n = 10,000$ | $n = 100,000$ |
|---|---|---|---|---|
| | $\omega = 20$ | $\omega = 100$ | $\omega = 500$ | $\omega = 1000$ |
| Our scheme | 0.41Kbyte | 1.97Kbyte | 9.79Kbyte | 19.6Kbyte |
| Trivial construction | 2.34Kbyte | 21.5Kbyte | 205Kbyte | 1970Kbyte |

scheme consists of $n$ participants $S, U_1, U_2, \ldots, U_{n-1}$, where $S$ is a sender and $U_1, U_2, \ldots, U_{n-1}$ are receivers, and the following phases:

1) Key generation and distribution by TA:
Let $GF(q)$ be the finite field with $q$ elements. We assume that for each authorized receiver $U_i$, his identity $u_i$ is an element in $GF(q)$. We also assume that $M = GF(q)$. TA generates a polynomial over $GF(q)$ with one variable:

$$f(x) = \sum_{i=0}^{\omega} a_i x^i$$

where the coefficients $a_i \in GF(q)$ are taken uniformly at random. After that, the TA securely sends $f(x)$ as an encryption key to the authorized sender $S$, and for each receiver $U_i$, $f(u_i)$ is sent to $U_i$ as a decryption key. The secret information for $S$ is $f(x)$ and that of $U_i$ is $f(u_i)$.

2) Encryption:
For a message $m \in M$, the sender $S$ encrypts it to $c(x) := m + f(x)$ by his secret information $f(x)$. Then, the ciphertext is broadcasted to other authorized receivers.

3) Decryption:
When an authorized receiver $U_j$ receives a ciphertext $c(x)$ from $S$, he decrypts it by using the formula $c(x)|_{x=u_j} - f(u_j) = m$.

For a construction of our model of $(n, \omega, \epsilon)$-TESDS in which any user can perform encryption and/or decryption, a trivial construction is to use $n$ independent copies of the above scheme. The trivial construction then requires the following parameters:

**Proposition 1:** The trivial construction derived from Kurosawa-Desmedt scheme for our model of $(n, \omega, \epsilon)$-TESDS requires:

$$\epsilon = 1/q$$
$$|M| = q$$
$$|K| = q^{\omega+n}$$
$$|C| = q^{\omega+1}$$

Hence, in the trivial construction each user stores $(n+\omega) \log_2 q$ bits for his secret information. Comparing our construction with the trivial construction of multiple usage of traitor traceability schemes (with non-dynamic sender) [6], we see that our construction considerably reduces the required memory size for a user's secret information (see Table 1). Also, it should be noted that in the trivial construction, the TA stores $n(n + \omega) \log q$ bits, while our construction presented in 2.2 requires the TA to strore only $\frac{(\omega+1)(\omega+2)}{2} \log q$ bits.

Finally, we note required memory sizes of our construction. It is shown that Kurosawa-Desmedt scheme is optimal in the model of [6] in terms of memory sizes. Also our proposed scheme matches the lower bounds presented in [6]. Therefore, it could be almost said optimal in terms of memory sizes. However, since our model is slightly different from that in [6], the optimality is not strictly shown by the authors yet. Detailed analysis on lower bounds of the model is an interesting open problem.

## 3. Authentication Scheme for $(n, \omega, \epsilon)$-TESDS

Generally, a conference system requires not only confidentiality, but also integrity. In this section, we show an authentication scheme for the proposed conference system. More precisely, we propose a modified version of the proposed encryption scheme that fulfills authenticity based on multireceiver authentication codes. Namely, in this version of the scheme as well as in the original proposed scheme, at least one traitor will be detected when a pirate key is confiscated. In addition, receivers of the transmitted message can remain confidential from the original sender of the message. Furthermore, likewise the original proposed scheme, the sender of the message is dynamically determined after distributing each authorized user's secret information by the TA.

In order to construct an authentication scheme for our conference system, *multireceiver authentication codes with dynamic sender* (DMRA) [9], [11] are regarded the most suitable security primitives. In DMRA, after distributing the secret information to all authorized users by the TA, any authorized user will be able to generate the message's authenticator which eventually is verified by all other authorized users.

In the following subsections, we propose an authentication scheme for our conference system based on techniques used in DMRA [9], [11].

### 3.1 Required Properties

As already mentioned above, traceability and dynamic sender, are the two desirable properties in constructing an authentication scheme for a conference system. In addition to these properties, secrecy of a message, that is, *confidentiality* can also be regarded as one of the desirable requisites. Although the existing DMRAs [9], [11] may be regarded as appropriate security primitives for an authentication scheme for a conference system, a straightforward implementation of DMRAs cannot guarantee the confidentiality. Namely, in these existing DMRAs, adversaries can easily obtain the source state to be authenticated if the authenticator is a correct one, assuming that they may have secret information for message verification for the DMRAs. We need to note that the properties of DMRAs in [9], [11] will be sufficient if adversaries does not have secret information for message verification. Thus, in Sect. 3.2, we establish a model of authentication codes, called $(n, \omega, \epsilon)$-ATESDS, that fulfills authenticity and confidentiality, concurrently with traceability, dynamic sender and unconditional security. Then, in Sect. 3.3, we propose a construction method for the model $(n, \omega, \epsilon)$-ATESDS by combining the DMRA with $(n, \omega, \epsilon)$-TESDS. A remarkable property of our proposed scheme is that adversaries cannot obtain any information on the plaintext unless they have a correct decryption key for the proposed $(n, \omega, \epsilon)$-TESDS.

In addition, DMRA in [11] is insecure when used as in [11][†].

## 3.2 The Model

In our model, there is a TA, $n$ users $\mathcal{U} = \{U_1, \cdots, U_n\}$ and a broadcast channel. The channel is subjected to spoofing attack; either a codeword can be inserted into the channel or a transmitted codeword can be substituted with a fraudulent one. The attack is directed towards the channel consisting of a sender and a receiver, $\{U_i, U_j\}$, $U_i$ and $U_j$, respectively. An adversary may either be an unauthorized user, or equal to or less than a coalition of $\omega$ authorized users. We assume that the TA is only active during key distribution phase. The system consists of the following three phases.

**1.Key generation and distribution by TA**
The TA generates and distributes secret information to each authorized user.

**2.Broadcast**
One authorized users encrypts a message by using $(n, \omega, \epsilon)$-TESDS, generates the authenticator of the message, and then broadcasts the messages.

**3.Verification**
After decrypting the message, every authorized user verifies authenticity of the broadcasted message using their secret information.

For simplicity, we assume that after the key distribution phase, only one authorized user can transmit one authenticated message at a time (namely, this is a *one-time use* scheme). An adversary can perform *impersonation* or *substitution* attack by constructing fraudulent codeword. The attack is considered successful if the receiver accepts the codeword. In impersonation attack, an adversary is assumed to not have seen any previous communication, while in substitution attack, the adversary is assumed to have seen at least one transmitted codeword.

An *Authenticated* $(n, \omega, \epsilon)$-*TESDS* ($(n, \omega, \epsilon)$-ATESDS) is an authentication code where every $t$ ($t \leq \omega$) adversaries cannot perform impersonation and/or substitution attack on any of the other authorized user pairs with probability of more than $\epsilon$, and also where no adversary can obtain the plaintext without using user's secret information in $(n, \omega, \epsilon)$-TESDS. When pirated secret information is confiscated, at least one traitor can be detected.

More formally, we define the security of $(n, \omega, \epsilon)$-ATESDS as follows:

**Definition 2:** A scheme described above is called an *authenticated* $(n, \omega, \epsilon)$-*traceable encryption scheme with dynamic sender* ($(n, \omega, \epsilon)$-ATESDS), where $\epsilon$ is a security parameter, if in addition to the conditions for $(n, \omega, \epsilon)$-TESDS (Def. 1) the following conditions are satisfied:

(1) (impersonation) Any coalition of $t$ authorized users ($t \leq \omega$) cannot forge a fraudulent message which a verifier accepts as authentic with probability of more than $\epsilon$.

(2) (substitution) After seeing a pair of valid ciphertext in $(n, \omega, \epsilon)$- TESDS and its authenticator, any coalition of $t$ authenticated users ($t \leq \omega$) cannot forge a fraudulent ciphertext which a verifier accepts as authentic with probability of more than $\epsilon$ (the target ciphertext is not the same as the pair of valid encrypted message and its authenticator ).

In the sequel, let $M$ and $C$ be a finite set of possible messages (or plaintexts) and possible ciphertexts, respectively, as in Sect. 2. Also, let $K'$ be the set of all possible secret information of an authorized user in $(n, \omega, \frac{1}{q})$-ATESDS, and $A$ the set of all possible authenticated messages in $(n, \omega, \epsilon)$-ATESDS, where an authenticated message is a pair of ciphertext and an authenticator for the ciphertext. Then, the above two conditions in Definition 2 are described as follows [9], [11]:

(1) (impersonation): For any set of colluders $W$, where $|W| \leq \omega$, and any pair of users $U_i$ and $U_j$ with $U_i, U_j \notin W$,

$$\max_{k_W} \max_{\alpha} \Pr(U_j \text{ accepts } \alpha \text{ as authentic by } U_i | k_W) \leq \epsilon,$$

[†] Security analysis on this scheme and its fixation will appear in our future paper.

where $\alpha$ runs over $A$, $k_W$ is taken over all possible secret information shared by $W$.

(2) (substitution): Formally, in the substitution attack, there are two cases:

(2-1) (message substitution): For any set of colluders $W$, where $|W| \leq \omega$, and any pair of users $U_i$ and $U_j$ with $U_i, U_j \notin W$,

$$\max_{k_W}\max_{\alpha}\max_{\alpha'} \Pr(U_j \text{ accepts } \alpha' \text{ as authentic by } U_i | k_W, \alpha) \leq \epsilon,$$

where $\alpha$ is taken over all valid authenticated messages generated by $U_i$, $\alpha'$ runs over $A$ such that $\alpha' \neq \alpha$, $k_W$ is taken over all possible secret information shared by $W$.

(2-2) (entity substitution): For any set of colluders $W$, where $|W| \leq \omega$, and any 3-tuple of users $U_i$,$U_{i'}$ $(i \neq i')$ and $U_j$ with $U_i, U_{i'}, U_j \notin W$,

$$\max_{k_W}\max_{\alpha}\max_{\alpha'} \Pr(U_j \text{ accepts } \alpha' \text{ as authentic by } U_{i'} | k_W, \alpha) \leq \epsilon,$$

where $\alpha$ is taken over all valid authenticated messages generated by $U_i$, $\alpha'$ runs over $A$, $k_W$ is taken over all possible secret information shared by $W$.

### 3.3 Construction of $(n, \omega, \epsilon)$-ATESDS

In this subsection, we show a construction of $(n, \omega, \epsilon)$-ATESDS, where $\epsilon = \frac{1}{q}$, by using polynomials over the finite field $GF(q)$.

In order to propose $(n, \omega, \frac{1}{q})$-ATESDS, we make use of the construction method of $(n, \omega, \frac{1}{q})$-TESDS presented in 2.2.

1) Key generation and distribution by TA:
Let $GF(q)$ be the finite field with $q$ elements. We assume that each authorized user $U_i$ has already obtained his secret information for $(n, \omega, \frac{1}{q})$-TESDS. The TA generates $2(\omega + 1)$ symmetric polynomials with two variables:

$$g_{l,k}(x, y) = \sum_{i=0}^{\omega+1}\sum_{j=0}^{\omega+1} a_{ij}^{(l,k)} x^i y^j \quad (l = 0, \cdots, \omega, \ k = 1, 2)$$

where the coefficients $a_{ij}^{(l,k)} (= a_{ji}^{(l,k)}) \in GF(q)$ are taken uniformly at random. The TA securely sends $g_{l,k}(u_i, y)$ $(l = 0, \cdots, \omega, \ k = 1, 2)$ to $U_i$. The secret information of $U_i$ for $(n, \omega, \frac{1}{q})$-ATESDS is the secret information in $(n, \omega, \frac{1}{q})$-TESDS and $g_{l,k}(u_i, y)$ $(l = 0, \cdots, \omega, \ k = 1, 2)$.

2) Broadcast:
For a message $m \in M$, $U_i$ first encrypts it to $c(y)$ by $(n, \omega, \frac{1}{q})$-TESDS. Letting $c(y)$ be $\sum_{i=0}^{\omega} c_i y^i$, $U_i$ generates the authenticator $a_l(y) := g^{(l,1)}(u_i, y) + c_l g^{(l,2)}(u_i, y)$ $(l = 0, \cdots, \omega)$. Afterwards, he broadcasts $c(y)$ and $a_l(y)$ $(l = 0, \cdots, \omega)$.

3) Verification:
On receiving $c(y)$ and $a_l(y)$ $(l = 0, \cdots, \omega)$ from $U_i$, $U_j$ first decrypts $c(y)$ with the secret information in the $(n, \omega, \frac{1}{q})$- TESDS. Then, $U_j$ accepts $c(y)$ and $a_l(y)$ $(l = 0, \cdots, \omega)$ as authentic and is also from $U_i$ if, $a_l(y)|_{y=u_j} = g^{(l,1)}(u_j, y)|_{y=u_i} + c_l g^{(l,2)}(u_j, y)|_{y=u_i}$ for all $l$ $(l = 0, \cdots, \omega)$.

In the above construction, we can see how remarkable that is to use symmetric functions for generating each user's secret information, similarly to how symmetric functions are used in the DMRAs in [9], [11]. This facts shows the property of a dynamic sender.

Next, we show the following result:

**Theorem 3:** The above scheme is an $(n, \omega, \frac{1}{q})$-ATESDS. Therefore, the probability of being a successful attack in impersonation or substitution is at most $\frac{1}{q}$, and adversaries can obtain no information of $m$ if they do not have an authorized user's secret information for $(n, \omega, \frac{1}{q})$- TESDS.

*Proof.* See Appendix.

The following theorem shows the required memory size for the above scheme.

**Theorem 4:** The required memory size for the proposed $(n, \omega, \frac{1}{q})$- ATESDS is as follows:

$$|K'| = q^{2\omega^2+7\omega+4}$$

(size of a user's secret information),

$$|A| = q^{\omega^2+4\omega+2}$$

(size of an authenticated message).

Hence, the above scheme requires each authorized user to store $(2\omega^2 + 7\omega + 4)\log_2 q$ bits. The length of an authenticated message (a pair of ciphertext and its authenticator) is $(\omega^2 + 4\omega + 2)\log_2 q$ bits. In addition, the proposed $(n, \omega, \frac{1}{q})$-ATESDS requires the TA to store $\frac{(2\omega+7)(\omega+1)(\omega+2)}{2} (= \omega^3 + \frac{13}{2}\omega^2 + \frac{25}{2}\omega + 7)\log_2 q$ bits.

## 4. Conclusion

In this paper, we studied a traitor traceable conference system with dynamic sender. In our scheme, after distributing each authorized user's secret information by a trusted authority, any authorized user can encrypt and authenticate a message and broadcast it to other authorized users. The broadcast message can be decrypted and verified by any authorized users in the system. Our scheme embodies traceability in that it detects at least one traitor upon confiscation of a forged key with a probability great than $\epsilon = \frac{1}{q}$, where $\epsilon$ is a security parameter. Furthermore, our system is unconditionally secure with respect to a dynamic sender.

### References

[1] D. Boneh and M. Franklin, "An efficient public key traitor tracing scheme," Proc. CRYPTO'99, LNCS 1592, pp.338–353, Springer-Verlag, 1999.

[2] B. Chor, A. Fiat, and M. Naor, "Tracing traitors," Proc. CRYPTO'94, LNCS 839, pp.257–270, Springer-Verlag, 1994.

[3] 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.

[4] E.N. Gilbert, F.J. MacWilliams, and N.J.A. Sloane, "Codes which detect deception," Bell System Technical Journal, vol.53, pp.405–425, 1974.

[5] T. Johansson, "Further results on asymmetric authentication schemes," Information and Computation, vol.151, pp.100–133, 1999.

[6] K. Kurosawa and Y. Desmedt, "Optimum traitor tracing and asymmetric schemes," Proc. Eurocrypt'98, LNCS 1403, pp.145–157, Springer-Verlag, 1998.

[7] B. Pfitzmann, "Trials of traced traitors," Proc. Information Hiding'96, LNCS 1172, pp.49–64, Springer-Verlag, 1996.

[8] B. Pfitzmann and M. Waidner, "Asymmetric fingerprinting for larger collusions," Proc. ACM-CCS'97, pp.145–157, 1997.

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

[10] R. Safavi-Naini and H. Wang, "Broadcast authentication in group communication," Proc. Asiacrypt'99, LNCS1716, pp.399–411, Springer-Verlag, 1999.

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

[12] R. Safavi-Naini and Y. Wang, "Sequential traitor tracing," Proc. CRYPTO 2000, LNCS 1880, pp.316–332, Springer-Verlag, 2000.

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

[14] D. Stinson and R. Wei, "Key preassigned traceability schemes for broadcast encryption," Proc. SAC'98, LNCS 1556, pp.144–156, Springer-Verlag, 1998.

[15] Y. Watanabe, G. Hanaoka, and H. Imai, "Efficient asymmetric public-key traitor tracing without trusted agents," Proc. Cryptographer's Track at RSA Conference 2001, LNCS 2020, pp.392–407, Springer-Verlag, 2001.

## Appendix: Proof of Theorem 3

First, we show that the proposed $(n, \omega, \frac{1}{q})$-ATESDS provides authenticity. For the $c(y)$, each of $c_l$ $(l = 0, \cdots, \omega)$ is authenticated as follows. Assume that after seeing a signed message $c(y), a_l(y)$ $(l = 0, \cdots, \omega)$ published by $U_{i_0}$, a coalition of authorized $U_1, \cdots, U_\omega$ generate $c(y), a'_l(y)$ $(l = 0, \cdots, \omega)$, such that the user $U_{i_2}$ will accept it as a valid signed message of the user $U_{i_1}$, i.e. $a'_l(y)|_{y=u_{i_2}} = g^{(l,1)}(u_{i_2}, y)|_{y=u_{i_1}} + c_l g^{(l,2)}(u_{i_2}, y)|_{y=u_{i_0}}$ $(l = 0, \cdots, \omega)$. Let

$$g^{(l,k)}(x, y) = \mathbf{x}\ A^{(l,k)}\ {}^t\mathbf{y} \quad (l = 0, \cdots, \omega,\ k = 1, 2),$$

where

$$\mathbf{x} := (1, x, x^2, \cdots, x^{\omega+1}),$$
$$\mathbf{y} := (1, y, y^2, \cdots, y^{\omega+1}),$$

and $A^{(l,k)}$ $(l = 0, \cdots, \omega,\ k = 1, 2)$ are $(\omega + 2) \times (\omega + 2)$ symmetric matrices over $GF(q)$. Then, the colluders have $(\omega + 2) \times (\omega + 1)$ matrices $D^{(l)}$ $(l = 0, \cdots, \omega)$, where

$$D^{(l)} := (A^{(l,1)} + c_l A^{(l,2)})U,$$

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

From Lemma 2.1 in [9], there exist $q$ different matrices $X$ such that

$$D^{(l)} = XU$$

for each of $D^{(l)}$. This implies that there are $q$ different values for $A^{(l,1)} + c_l A^{(l,2)}$.

In order for the colluders to succeed the attack, they need to find a $a'_l(y)$ $0 \le l \le \omega$ such that

$$a'_l(u_{i_2}) = \mathbf{u}_{i_1}\ (A^{(l,1)} + c_l A^{(l,2)})\ {}^t\mathbf{u}_{i_2}$$

where

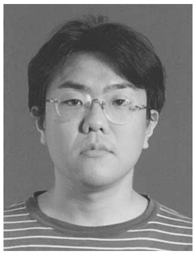
$$\mathbf{u}_{i_1} := (1, u_{i_1}, {u_{i_1}}^2, \cdots, {u_{i_1}}^{\omega+1}),$$
$$\mathbf{u}_{i_2} := (1, u_{i_2}, {u_{i_2}}^2, \cdots, {u_{i_2}}^{\omega+1}).$$

Letting $d_l$ be

$$d_l := \mathbf{u}_{i_1}\ (A^{(l,1)} + c_l A^{(l,2)})\ {}^t\mathbf{u}_{i_2},$$

$q$ different matrices for $A^{(l,1)} + c_l A^{(l,2)}$ result in $q$ different values for $d_l$. This indicates that the probability of a success to find $a'_l(y)$, such that $a'_l(u_{i_2}) = d_l$, does not exceed $\frac{1}{q}$, i.e. the probability of a successful substitution is at most $\frac{1}{q}$. Similarly, we can prove also that the probability of a successful impersonation is at most $\frac{1}{q}$.

We further show that any unauthorized users cannot obtain any information of the plaintext from an authenticator unless they have a user's secret information in $(n, \omega, \frac{1}{q})$-TESDS. Suppose that advasaries want to obtain information on the plaintext $m$ from the authenticator $a_l(y)$ $(l = 0, \cdots, \omega)$. Even if they have the additional secret information for $(n, \omega, \frac{1}{q})$-ATESDS for authentication, the only information they can obtain will be of the ciphertext $c(y)$. Therefore, the adversaries cannot obtain any information of the plaintext without the use of user's secret information in $(n, \omega, \frac{1}{q})$-TESDS.



**Goichiro Hanaoka** is currently a Ph.D. student in the Information and Communication Engineering Department at the University of Tokyo, Tokyo, Japan. He has received his bachelors and masters degrees in Electronic engineering and Information and communication engineering from the University of Tokyo in 1997 and 1999, 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. He is a Research Fellow of Japan Society for the Promotion of Science (JSPS).

**Junji Shikata** received the B.S. and M.S. degrees from Kyoto University, Japan, in 1994 and 1997 respectively, and the Ph.D. degree from Osaka University, Japan, in 2000. Currently, he is a postdoctoral fellow in the Institute of Industrial Science, the University of Tokyo, Japan.

**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. His research interests include cryptography, network security, and secure electronic commerce. 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, Japan, in 1966, 1968 and 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. He received Excellent Book Awards from IEICE in 1976 and 1991. He also received the Best Paper Award (Yonezawa Memorial Award) from IEICE in 1992, the Distinguished Services Award from the Association for Telecommunication Promotion in 1994, the Telecom System Technology Prize from the Telecommunication Advancement Foundation and Achievement Award from IEICE in 1995. In 1998 he was awarded Golden Jubilee Paper Award by the IEEE Information Theory Society. He was elected an IEEE Fellow for his contributions to the theory of coded modulation and two-dimensional codes in 1992. He chaired several committees of scientific societies such as the IEICE Professional Group on Information Theory. He served as the editor of several scientific journals of IEICE, IEEE etc. He chaired a lot of international conferences such as 1993 IEEE International Theory Workshop and 1996 International Symposium on Information Theory and Its Applications (ISITA'96). Dr. Imai has been on the board of IEICE, the IEEE Information Theory Society, Japan Society of Security Management (JSSM) and the Society of Information Theory and Its Applications (SITA). At present he serves as President of the IEICE Engineering Sciences Society.