Unconditionally Secure Anonymous Encryption and Group Authentication*

Goichiro Hanaoka[1], Junji Shikata[2], Yumiko Hanaoka[3], and Hideki Imai[1]

[1] Information & Systems, Institute of Industrial Science, University of Tokyo
4-6-1 Komaba, Meguro-ku, Tokyo 153-8508, Japan.
hanaoka@imailab.iis.u-tokyo.ac.jp, imai@iis.u-tokyo.ac.jp
[2] Graduate School of Environment and Information Sciences,
Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan.
shikata@mlab.jks.ynu.ac.jp
[3] Security Systems Laboratory, Multimedia Laboratories, NTT DoCoMo, Inc.
3-5 Hikarino-oka, Yokosuka 239-8536, Japan.
claudia@mml.yrp.nttdocomo.co.jp

Abstract. Anonymous channels or similar techniques that can achieve sender's anonymity play important roles in many applications. However, they will be meaningless if cryptographic primitives containing his identity is carelessly used during the transmission. The main contribution of this paper is to study the security primitives for the above problem. In this paper, we first define *unconditionally secure asymmetric encryption scheme* (USAE), which is an encryption scheme with unconditional security and is impossible for a receiver to deduce the identity of a sender from the encrypted message. We also investigate tight lower bounds on required memory sizes from an information theoretic viewpoint and show an optimal construction based on polynomials. We also show a construction based on combinatorial theory, a non-malleable scheme and a multi-receiver scheme. Then, we define and formalize *group authentication code* (GA-code), which is an unconditionally secure authentication code with anonymity like group signatures. In this scheme, any authenticated user will be able to generate and send an authenticated message while the receiver can verify the legitimacy of the message that it has been sent from a legitimate user but at the same time retains his anonymity. For GA-code, we show two concrete constructions.

1 Introduction

In many applications, there is a need to allow user or the author of the message to be able to transmit message without revealing his/her identity, e.g. electronic voting. A most commonly used cryptographic technique that is used to build an actual implementation of these characters, is called *anonymous channels* [9, 10,

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

1]. However, if not carefully designed, i.e. when a sender uses encryption and authentication methods requiring the sender's identity for decryption or message verification, these systems can be easily compromised, thus corrupting results or violating senders' privacy. For example, if Diffie-Hellman key exchange (with certificates) [13] or (conventional) digital signatures are used, the receiver will be able to easily obtain information regarding the sender's identity, and also may leave the message contents along with the identity of the sender open to perusal. In computationally secure setting, this problem can be solved straightforwardly by using (conventional) public-key encryption e.g. [24, 17] and group signatures [11, 8] shielding the sender's identity. 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. However, this presumption no longer assures the security of computationally secure schemes as the progress in computers as well as further refinement of various algorithms in near future make it computationally able to solve the larger size number-theoretic problems. Unfortunately, in unconditionally secure environment, in which no computational difficulty is assumed, there is yet no straightforward answer to this; all of the current existing schemes use mutual information between sender and receiver, and this mutual information is utilized as a shared communication key between them. This implies that the receiver has to know certain information regarding the sender in prior to selecting a shared secret, and this means, loss of anonymity. (This also implies that *unconditionally secure* public-key encryption scheme is essentially non-existing, since in the model of public-key cryptosystems, a sender and a receiver do not share mutual information between them.) As the increasing computational power approaches where security policy can no longer assume on the difficulty of computationally hard problems, it must shift its focus on assuring the solvency of unconditionally secure schemes that provides long-term security. Similar problem arises in authentication as well. In conventional authentication schemes, the identity of the sender is required for verifying integrity of a transmitted message. In order to protect the sender's privacy in a computationally secure setting, group signatures [11, 8] was proposed and since then, group signatures has been greatly studied in the literatures. However, in unconditional setting, there has never existed an authentication scheme that assures anonymity of the sender like that seen in the group signature schemes. For the importance of preparing for the eventual need of long-term security, unconditionally secure setting must be considered a *sine qua non* for a security policy. The main contribution of this paper is to study models, bounds and constructions of novel security primitives on the above problem with no computational assumption. In this paper, we first define *unconditionally secure asymmetric encryption scheme* (USAE), which is an encryption scheme with unconditional security in which a receiver cannot obtain any information of the identity of a sender from the encrypted message. We also investigate tight lower bounds on required memory sizes from information theory and also show concrete constructions of USAE schemes based on polynomials and cover free family [15]. USAE based on polynomials is optimal due to that it matches the lower bounds. We further show another construction from combinatorial theory, a non-malleable scheme and a multi-receiver scheme. We then, define and formalize *group authentication code*, which is an unconditionally secure authentication code with anonymity like group signatures. In this proposed scheme, any authenticated user will be able to generate an authenticated message and sends it to the receiver. The receiver is then able to verify the authenticity of the received message while maintaining the privacy of the user. Moreover, neither a recipient nor a group authority can obtain any meaningful information of the user who had generated the authenticated message, i.e. no one can link any message to the author who cast it. However, by cooperating with group authority, such as in the case of disputes, the receiver is able to obtain the sender's identity.

1.1 Related works

Unconditionally secure key distribution schemes For confidentiality without computational assumptions, unconditionally secure key distribution schemes are often utilized as suitable security primitives. Blom [5] made the first attempt to construct an unconditionally secure key distribution scheme using MDS linear codes, and his idea was later generalized by Matsumoto and Imai [22], *key predistribution schemes* (KPS), who also proposed a simpler version of KPS, *linear scheme*. Blundo, De Santis, Herzberg, Kutten, Vaccaro and Yung [6] proposed a concrete construction of KPS for conference key distribution and investigated lower bounds on required memory size for users and showed that their scheme, as well as Blom's original scheme and Matsumoto-Imai's scheme, all matched the lower bounds. Blundo, Mattos and Stinson [7], as well as Kurosawa, Yoshida, Desmedt and Burmester [21] showed other interesting bounds on required memory sizes. In [29], in depth survey of various constructions of KPS and corresponding properties has been investigated. KPS may seem to be the best building blocks for unconditionally secure communication systems, however, they are not suitable for certain applications e.g. electronic voting systems, that must ensure user's anonymity; the identity of a sender is required for a recipient to generate the communication key. In all of the existing KPS hitherto, a sender and a receiver's secret information must be used to generate the communication key, and therefore, all of the currently existing schemes does not meet the security requirement for a system with anonymity. As far as we know, there has never existed an unconditionally secure key distribution scheme without a requirement of sender's identity.

Unconditionally secure authentication schemes and group signatures For a secure authentication without computational assumptions, unconditionally secure authentication codes (A-codes) [18, 27] may be considered which has been intensively studied in the literatures. An overall structure of A-codes is as follows. In the first stage of A-codes, a trusted authority generates secret information for each of sender and receiver. Then, the sender generates an authenticated message by using his given secret information and transmits it to the receiver. Finally, the receiver verifies the validity of the authenticated message with his secret information. Here, no adversary succeed impersonation nor substitution attack even if the adversary has unlimited computational power. There has also been many attempts to modify A-codes with the aim of enhancing the codes with desirable properties other than anonymity, such as asymmetricity [28] and multireceiver-authenticity [12]. However, in none of these attempted modifications, receivers were able to identify the sender of the message. Thus, there were no existing A-codes and their variants that were applicable concerning the protection of the sender's identity, i.e. no anonymity. Though there are some unconditionally secure digital signature schemes [19, 20, 26] that do exist, these schemes yet too, do not provide anonymity. However, in computationally secure settings, anonymity can be achieved by using *group signatures* [11, 8]. For a group signature, a user is able to prove that he is a legitimate user of the group by using his secret information given by a group authority, and in the case of a dispute, the group authority can identify the user from a published signature signed by the user. Group signature is therefore a suitable authenticating scheme that can be used especially in case where the privacy of the user has to be maintained. However, all the existing group signature schemes are based on computational assumptions and will be broken if certain computationally hard problems, e.g. discrete logarithm or factoring, are solved.

1.2 Our results

We start this paper by defining *unconditionally secure asymmetric encryption scheme* (USAE) with formal definitions. USAE is an encryption scheme with unconditional security in which a receiver cannot gain any information of a particular user from an encrypted message. We investigate from information theory, the lower bounds for the required memory sizes of a ciphertext, a sender and a receiver's secrets. Further, we propose concrete constructions of USAE based on polynomials and also constructions based on cover free families. Polynomial based construction is optimal due to that it matches the lower bounds which in turn implies that the lower bounds are all tight. One important fact to mention, it is remarkable that these bounds that we show are considerably different from those in Shannon's model for conventional unconditionally secure symmetric encryption. Comparison between polynomial-based and cover free family-based schemes are also made. In addition, we study an extension of USAE, that with non-malleability. More precisely, a formal definition of non-malleability, a concrete non-malleable scheme and a security proof are investigated. Furthermore, another extension of USAE, for multiple-receiver setting, is shown. We continue by defining *group authentication code* (GA-code) with formal definitions. GA-code is an unconditionally secure authentication code with anonymity like group signatures. In GA-codes, any user in a group can generate an authenticated message and verify it as long as it has been sent from a legitimate user in a group. Moreover, a receiver is not able to obtain any meaningful information of a particular user who had generated the authenticated message. However, in the case of disputes, a receiver is able to obtain the sender's identity by cooperating with a group authority. It is important to note here that group authority or the receiver by itself will be insufficient in obtaining to obtain any information regarding the user i.e. they must cooperate. We then show two concrete constructions of GA-code with formal security proofs. One construction is based on polynomials and the other on cover free families and A-codes. Organization of this paper is as follows: In section 2, we study the model, bounds and constructions for USAE. Polynomial based USAE construction is optimal due to that it matches the lower bounds. This in turn implies that the lower bounds are all tight. We also show other efficient and secure implementations of USAE. In section 3, we show model and concrete construction for GA-code with formal security proof.

2 Unconditionally secure asymmetric encryption

In this section, model, security definition, lower bounds and concrete constructions of USAE are shown. One of our constructions is optimal in terms of required memory sizes for a ciphertext, an encryption key and a decryption key. It should be noted that the definition that we use for "asymmetric encryption" in this paper is not equivalent to the meaning of "public-key encryption" in a general sense. Here, in USAE, "asymmetric" is used as a pair of encryption and decryption keys that are asymmetric, where an encryption key is not public.

2.1 Model

Since no computational difficulty is assumed in USAE, it is impossible for a sender to secretly transmit a message using only the public information. This means that in order to construct a USAE, a different assumption (rather than computational assumptions) will be required, e.g. existence of a noisy channel, that of a quantum channel, bounds of memory or threshold of the number of malicious users. For simplicity, we introduce the *trusted initializer model* [23], in which we assume a trusted initializer who honestly distributes each user's secret in the initial phase and deletes his memory after the distribution of the secrets. We should note that the trusted initializer can be removed by using multi-party computation [4] if the number of malicious users is less than a third of the total number of users and there exists a private channel between each pair of users.

In the model of USAE, there are $n + 2$ participants, a set of n senders $\{S_1, \cdots, S_n\}$, a receiver R and a trusted initializer TI. TI generates encryption keys $e_1, \cdots, e_n$ for $S_1, \cdots, S_n$, respectively, and a decryption key d for R. After distributing these keys, TI deletes his memory. In order to send a plaintext m to R with confidentiality, $s \in \{S_1, \cdots, S_n\}$ encrypts m by using e_i and transmits a ciphertext c to R. R decrypts c by using d and recovers m.

2.2 Definition

Here, we formally define the security of USAE. It should be noted that, in addition to confidentiality, anonymity of a sender is required for USAE. Let

$\mathcal{S}$, $\mathcal{E}_i$ $(i = 1, \cdots, n)$, $\mathcal{D}$, $\mathcal{M}$ and $\mathcal{C}$ denote the random variables induced by s, e_i $(i = 1, \cdots, n)$, d, m and c, respectively. For a random variable $\mathcal{X}$, $H(\mathcal{X})$ denotes the entropy of $\mathcal{X}$. For $\mathcal{X}$, let $X := \{x | \Pr(\mathcal{X} = x) > 0\}$. $|X|$ denotes the cardinality of X. We assume that at most k $(0 \leq k \leq n-1)$ authorized senders are malicious. Then, the security of USAE is formally defined as follows:

Definition 1 We say that $(\mathcal{E}_1, \cdots, \mathcal{E}_n, \mathcal{D}, \mathcal{M}, \mathcal{C})$ is a (k, n)-*one-time USAE* if

1. R can correctly decrypt m from c, that is, $H(\mathcal{M}|\mathcal{C}, \mathcal{D}) = 0$.
2. Any set of k malicious senders has no information on m from c. Namely, for any set of k malicious senders $\{S_{i_1}, \cdots, S_{i_k}\} \subset \{S_1, \cdots, S_n\}$ such that $s \notin \{S_{i_1}, \cdots, S_{i_k}\}$, $H(\mathcal{M}|\mathcal{C}, \mathcal{E}_{i_1}, \cdots, \mathcal{E}_{i_k}) = H(\mathcal{M})$.
3. R obtains no information on the identity of s from c. Namely, $H(\mathcal{S}|\mathcal{C}) = H(\mathcal{S})$.
4. Additionally, we assume that a ciphertext c is uniquely determined from a plaintext m and an encryption key e_i, i.e. $H(\mathcal{C}|\mathcal{M}, \mathcal{E}_i) = 0 \quad$ for any i.

2.3 Lower bounds

In this subsection, lower bounds on required memory sizes for a ciphertext, an encryption key and a decryption key in USAE are shown. These bounds are all tight since we also show a construction which matches them (see section 2.4, for details). Note that proofs of Theorem 1, 3 and Lemma 1 are omitted, and will apear in the full version of this paper. We begin by showing a lower bound on the required memory size for a ciphertext.

Theorem 1 *In a (k, n)-one-time USAE, $H(\mathcal{C}) \geq H(\mathcal{M}) + H(\mathcal{S})$.*

Theorem 1 implies that the required memory size for a ciphertext is always larger than that for a plaintext by at least $H(\mathcal{S})$ bits. Next is a lemma that shows the relationship between the required memory size for an encryption key e_i and for a ciphertext c in USAE.

Lemma 1 *In a (k, n)-one-time USAE, $H(\mathcal{E}_i) \geq H(\mathcal{C}), \quad$ for any i.*

Lemma 1 implies that the memory size requirement for an encryption key in USAE is equal or greater than that for a ciphertext. This is also closely related to the famous Shannon's result [25]. That is, in unconditionally secure symmetric encryption, it is a well-known fact that the required memory size for an encryption key is equal or greater than that for a plaintext, assuming that a ciphertext is uniquely determined from a plaintext and an encryption key. Now, a lower bound on the required memory size for an encryption key is shown.

Theorem 2 *In a (k, n)-one-time USAE, $H(\mathcal{E}_i) \geq H(\mathcal{M}) + H(\mathcal{S}), \quad$ for any i.*

Proof. From Lemma 1 and Theorem 1, we have $H(\mathcal{E}_i) \geq H(\mathcal{M}) + H(\mathcal{S})$ for any i. □

Theorem 2 implies that the required memory size for an encryption key is always larger than that for a plaintext by at least $H(\mathcal{S})$ bits. Finally, we show a lower bound on the required memory size for a decryption key.

Theorem 3 *In a (k,n)-one-time USAE, $H(\mathcal{D}) \geq (k+1)H(\mathcal{M})$ if the equality in Lemma 1 is satisfied for any i.*

Theorem 3 implies that the required memory size for a decryption key is $(k+1)$ times larger than that for a plaintext.

2.4 Constructions

Now, we show two concrete constructions of USAE. One of the constructions is based on polynomials over finite fields, and the other one on cover free family [15]. The polynomial based construction is optimal in terms of required memory sizes for a ciphertext, an encryption key and a decryption key. For the cover free family construction, security parameters can be flexibly determined.

In this subsection, we assume that the distribution of the sender is uniform, that is, $\Pr(\mathcal{S} = S_i) = \frac{1}{n}$ for any i $(1 \leq i \leq n)$.

Optimal construction from polynomials. Here, we show an optimal (k,n)-one-time USAE which meets all our bounds. This means that the lower bounds in the previous subsection are all tight.

Definition 2 A (k,n)-one-time USAE is *optimal* if one has equalities in Theorem 1, 2 and 3.

Optimal (k,n)-one-time USAE based on polynomials

1. Setting up: Let $|M| = q$, where q is a prime power and $q \geq n$. TI chooses a uniformly random polynomial $f(x) = \sum_{i=0}^{k} a_i x^i$ over $GF(q)$. TI also chooses distinct numbers b_i $(1 \leq i \leq n)$ from a set $B \subseteq GF(q)$ uniformly at random, where $|B| = n$. B may be public to all players. Next, TI gives $f(x)$ to R as his decryption key, and also gives $\{b_1, f(b_1)\}, \{b_2, f(b_2)\}, \cdots, \{b_n, f(b_n)\}$ to $S_1, S_2, \cdots, S_n$ as encryption keys, respectively. TI deletes his memory after distributing the keys.

2. Encryption: Sender S_i encrypts m by $c = \{b_i, c'\}$, where $c' := f(b_i) + m$.

3. Decryption: Receiver R decrypts c by $f(x)$ as follows: $m = c' - f(x)|_{x=b_i}$.

Theorem 4 *The above scheme is an optimal (k,n)-one-time USAE.*

Proof. In the above scheme, $H(\mathcal{C}) = H(\mathcal{M}) + \log_2 n$, $H(\mathcal{E}_i) = H(\mathcal{M}) + \log_2 n$ $(1 \leq i \leq n)$ and $H(\mathcal{D}) = (k+1)H(\mathcal{M})$. It is clear that the above scheme satisfies the first condition of Def. 1. Suppose that colluders $S_{i_1}, \cdots, S_{i_k}$, such that $S_i \notin \{S_{i_1}, \cdots, S_{i_k}\}$, can obtain certain information on m from c. This implies that the colluders has certain information on $f(b_i)$. However, this is impossible because $\deg f(x) = k$ and the colluders knows only the k points of $f(x)$. Hence, the above scheme satisfies the second condition of Def. 1. Finally, since, for a ciphertext $c = \{b, c'\}$ such that $b \in B$ and $c' = f(b) + m$, any of $S_1, \cdots, S_n$ can be a possible sender of the ciphertext from R's point of view, and therefore, R can determine who the sender of the ciphertext is with probability at most $1/n$. Hence, the above scheme satisfies the third condition of Def. 1 as well. □

Construction from cover free family. Here, we show a construction of USAE based on cover free family [15] which allows a more flexible parameter setting than the polynomial based one. Namely, in cover free family based construction, it is possible to choose parameters n and $|M|$ with $|M| < n$, while, in polynomial based construction, these two parameters must always be determined to be $|M| \geq n$.

Definition 3 Let $L := \{\ell_1, \ell_2, \cdots, \ell_t\}$ and $F = \{F_1, \cdots, F_n\}$ be a family of subsets of L. We call (L, F) an (n, t, k) *cover free family* (CFF) if $F_0 \not\subset F_1 \cup \cdots \cup F_k$ for all $F_0, F_1, \cdots, F_k \in F$, where $F_i \neq F_j$ if $i \neq j$.

A trivial CFF is the family consisting of single element subsets, in which case $n = t$. It should also be noted that there exist nontrivial constructions of CFF with $n > t$. Construction of CFFs is intensively studied in various areas of mathematics such as finite geometry, design theory, and probability theory. Concrete methods for generating CFF are given in [16].

(k, n)-one-time USAE based on (n, t, k)-CFF

1. Setting up: TI first generates an (n, t, k)-CFF such that each of ℓ_i $(1 \leq i \leq t)$ is an element of $GF(q)$, where $\mathcal{M} = GF(q)$. TI also chooses distinct numbers r_i $(1 \leq i \leq n)$ from $\{1, 2, \cdots, n\}$ uniformly at random. An algorithm that generates F_i $(1 \leq i \leq n)$ from i and L may be public to all players. Next, TI gives L to R as his decryption key. TI also gives $\{r_i, \ell^{(i)}\}$ $(1 \leq i \leq n)$ to S_i $(1 \leq i \leq n)$, respectively, as encryption keys, where $\ell^{(i)} := \sum_{\ell \in F_{r_i}} \ell$. After distributing the keys, TI deletes his memory.

2. Encryption: Sender S_i encrypts m by $c = \{r_i, c'\}$, where $c' = m + \ell^{(i)}$.

3. Decryption: Receiver R generates F_{r_i} from L and r_i. Then, R computes m as $m = c' - \sum_{\ell \in F_{r_i}} \ell$.

Theorem 5 *The above scheme is a (k, n)-one-time USAE.*

Proof. It is obvious that the above scheme satisfies all of conditions in Def. 1. □

The required memory sizes for the above construction is formally addressed as follows:

Theorem 6 *The required memory sizes in the above construction are given as follows:*

$$H(\mathcal{C}) = \log_2 nq, \;\; H(\mathcal{E}_i) = \log_2 nq \quad \textit{for any } i \;\; (1 \leq i \leq n), \;\; H(\mathcal{D}) = t \log_2 q.$$

It should be noted that the cover free family based construction matches the lower bounds on the required memory sizes for a ciphertext and an encryption key.

Comparison. Here, comparison between polynomial and cover free family based constructions is explored. Given the fact described above, our polynomial construction is optimal in terms of required memory sizes. Therefore, polynomial based construction is theoretically superior to the cover free family based construction storage wise. However, polynomial based construction can only be implemented when $|M| \geq n$ although, in most practical situations, this restriction may be ignored. On the other hand, for the cover free family based construction, it allows even for $|M| < n$ when there exist an appropriate cover free family. We now show an example of system parameter settings in the case when this restriction do, applies. For the following situation, the cover free family based construction will be more suitable than polynomial based construction in terms of required memory sizes.

Example. Assume that the message space is $\{yes, no\}$ and we need a $(127, 128)$-one-time USAE. For the polynomial based construction, a finite field $GF(q)$ with $q \geq 128$ is required. Consequently, the size of a ciphertext will be at least 14 bits. A receiver and a sender must then store at least 896 bits and 14 bits, respectively. For the cover free family based construction, $(128, 128, 127)$-CFF (trivial CFF) over $GF(2)$, the size of a ciphertext will be 8 bits at the least, and a receiver and a sender store at least 128 bits and 8 bits, respectively. For the described situation, we can see a significant advantage of the cover free family based construction over the polynomial based construction.

In summary, different constructions are advantageous for different perspectives, so, one construction may do better than another under certain circumstances. However, the polynomial based construction is generally most suitable for typical security parameter settings in USAE. And for the case when $|M| < n$, the cover free family based construction betters.

Memory sizes requirement can be reduced further for the above example if we utilize nontrivial CFF instead. However, in a nontrivial CFF, the number of malicious senders cannot be set to a considerably larger number than the total number of the senders. This fact is due to the following proposition:

Proposition 1 ([16]) *In a nontrivial (n, t, k)-CFF with $n > t$, $\frac{k(k-1)}{2} \leq n$.*

2.5 Extensions

Non-malleable scheme. Here, we consider *non-malleability* [14] of the proposed USAE. Frankly, non-malleability means an adversary's inability: given a challenge ciphertext c, to generate a different ciphertext $\hat{c}$ such that the plaintexts $m, \hat{m}$ underlying these two ciphertexts are meaningfully related. For computational encryption schemes, formal definitions of non-malleability are given in [2, 3]. Here, we give a definition of non-malleability for USAE.

Definition 4 Let $\hat{c}(\neq c)$ be another ciphertext which could have been generated by s instead of c in USAE, and $\hat{m}(\neq m)$ be a plaintext underlying $\hat{c}$. Let $\hat{\mathcal{C}}$ and $\hat{\mathcal{M}}$ denote random variables induced by $\hat{c}$ and $\hat{m}$, respectively. A USAE is *perfectly non-malleable* if the following equation holds:

$$H(\hat{\mathcal{M}}|\mathcal{C}, \hat{\mathcal{C}}, \mathcal{M}, \mathcal{E}_{i_1}, \cdots, \mathcal{E}_{i_k}) = H(\hat{\mathcal{M}}|\mathcal{C}, \mathcal{M}), \tag{1}$$

for any set of k malicious senders $\{S_{i_1}, \cdots, S_{i_k}\} \subset \{S_1, \cdots, S_n\}$ such that $s \notin \{S_{i_1}, \cdots, S_{i_k}\}$.

The above definition is reasonable since Eq. 1 implies that even if an adversary knows a pair of $\{c, m\}$, there is no other ciphertext which can give further information except the information that its underlying plaintext is not identical to m. In other words, no adversary can generate a ciphertext whose plaintext is meaningfully related to m when Eq. 1 holds.

A USAE which satisfies perfect non-malleability is constructed as follows:

Non-malleable (k, n)-one-time USAE based on polynomials

1. Setting up: Let $|M| = q$, where q is a prime power and $q \geq n$. TI chooses a uniformly random polynomials $f_i(x) = \sum_{j=0}^{k} a_{ij}x^j$ $(i = 1, 2)$ over $GF(q)$. TI also chooses distinct numbers b_i $(1 \leq i \leq n)$ from a set $B \subseteq GF(q)$ uniformly at random, where $|B| = n$, such that $f_2(b_i) \neq 0$ for any i $(1 \leq i \leq n)$. B may be public to all players. Next, TI gives $f_1(x)$ and $f_2(x)$ to R as his decryption key, and also gives $\{b_1, f_1(b_1), f_2(b_1)\}, \{b_2, f_1(b_2), f_2(b_2)\}, \cdots, \{b_n, f_1(b_n), f_2(b_n)\}$ to $S_1, S_2, \cdots, S_n$ as encryption keys, respectively. TI deletes his memory after distributing the keys.

2. Encryption: Sender S_i encrypts m by $c = \{b_i, c'\}$, where $c' := f_1(b_i) + mf_2(b_i)$.

3. Decryption: Receiver R decrypts c by $f_1(x)$ and $f_2(x)$ as follows: $m = (c' - f_1(x)|_{x=b_i})/f_2(x)|_{x=b_i}$.

Theorem 7 *The above scheme is a perfectly non-malleable (k, n)-one-time USAE.*

Proof. Similarly to the proof of Theorem 4, it can be proved that the above scheme is a (k, n)-one-time USAE. Now, we show that the above scheme satisfies the equality of Eq. 1. It is obvious that

$$H(\hat{\mathcal{M}}|\mathcal{C}, \mathcal{M}) = -\sum_{m \in M} \sum_{\hat{m} \in M \setminus \{m\}} \Pr(\mathcal{M} = m) \Pr(\hat{\mathcal{M}} = \hat{m}|\mathcal{M} = m) \cdot \log_2 \Pr(\mathcal{M} = m) \Pr(\hat{\mathcal{M}} = \hat{m}|\mathcal{M} = m). \quad (2)$$

Next, we show that $H(\hat{\mathcal{M}}|\mathcal{C}, \hat{\mathcal{C}}, \mathcal{M}, \mathcal{E}_{i_1}, \cdots, \mathcal{E}_{i_k})$ is equivalent to that in Eq. 2. Since both $\deg f_1(x)$ and $\deg f_2(x)$ are k, no information on $f_1(x)$ and $f_2(x)$ cannot be obtained even if $e_1, \cdots, e_k$ are used. Then, a set of all possible values for $(f_1(x), f_2(x))$ becomes $\Gamma := \{(\gamma_1, \gamma_2)|c' = \gamma_1 + m\gamma_2,\ \gamma_2 \neq 0\}$. Consequently, for given $\hat{c}(= \{b_i, \hat{c}'\})$, a set of all possible plaintext $\hat{m}$ underlying $\hat{c}$ is $M' := \{m'|m' = (\hat{c}' - \gamma_1)/\gamma_2,\ \forall(\gamma_1, \gamma_2) \in \Gamma\}$. From Lemma 2 and 3, we have $M' = M\setminus\{m\}$ and a mapping $\tau : \Gamma \to M'$, such that $\tau(\gamma_1, \gamma 2) = (\hat{c}' - \gamma_1)/\gamma_2$, is bijective. Hence, we have

$$\begin{aligned}
&H(\hat{\mathcal{M}}|\mathcal{C}, \hat{\mathcal{C}}, \mathcal{M}, \mathcal{E}_{i_1}, \cdots, \mathcal{E}_{i_k}) \\
&= -\sum_{m \in M} \sum_{(\gamma_1, \gamma_2) \in \Gamma} \Pr(\mathcal{M} = m) \Pr(\hat{\mathcal{M}} = \tau(\gamma_1, \gamma_2)|\mathcal{M} = m) \\
&\qquad\qquad \cdot \log_2 \Pr(\mathcal{M} = m) \Pr(\hat{\mathcal{M}} = \tau(\gamma_1, \gamma_2)|\mathcal{M} = m) \\
&= -\sum_{m \in M} \sum_{\hat{m} \in M \setminus \{m\}} \Pr(\mathcal{M} = m) \Pr(\hat{\mathcal{M}} = \hat{m}|\mathcal{M} = m) \\
&\qquad\qquad \cdot \log_2 \Pr(\mathcal{M} = m) \Pr(\hat{\mathcal{M}} = \hat{m}|\mathcal{M} = m). \quad (3)
\end{aligned}$$

From Eq. 2 and 3, Eq. 1 holds. □

Lemma 2 *For a given ciphertext* $c(=\{b_i, c'\}) \in C$ *and its corresponding plaintext* $m \in M$*, let* $\Gamma := \{(\gamma_1, \gamma_2) | c = \gamma_1 + m\gamma_2,\ \gamma_2 \neq 0\}$*. Then, for any* $\hat{c}(= \{b_i, \hat{c}'\}) \in C$*, such that* $\hat{c}' \neq c'$*,* $(\hat{c}' - \gamma_1)/\gamma_2 \neq m$ *if* $(\gamma_1, \gamma_2) \in \Gamma$*.*

Proof. Suppose that there exist $(\gamma_1, \gamma_2) \in \Gamma$, such that $(\hat{c}' - \gamma_1)/\gamma_2 = m$. Then, $\hat{c}' = \gamma_1 + m\gamma_2 = c'$. Since $\hat{c}' \neq c'$, this is a contradiction. □

Lemma 3 *For a given ciphertext* $c(=\{b_i, c'\}) \in C$ *and its corresponding plaintext* $m \in M$*, let* $\Gamma := \{(\gamma_1, \gamma_2) | c = \gamma_1 + m\gamma_2,\ \gamma_2 \neq 0\}$*. Then, for any* $\hat{c}(= \{b_i, \hat{c}'\}) \in C$*, such that* $\hat{c}' \neq c'$*,* $(\hat{c}' - \gamma_{11})/\gamma_{12} \neq (\hat{c}' - \gamma_{21})/\gamma_{22}$ *if* $(\gamma_{11}, \gamma_{12}) \neq (\gamma_{21}, \gamma_{22})$ *and* $(\gamma_{11}, \gamma_{12}), (\gamma_{21}, \gamma_{22}) \in \Gamma$*.*

Proof. Suppose that there exist $(\gamma_{11}, \gamma_{12}), (\gamma_{21}, \gamma_{22}) \in \Gamma$, such that $(\hat{c}' - \gamma_{11})/\gamma_{12} = (\hat{c}' - \gamma_{21})/\gamma_{22}$. Letting $\hat{m} := (\hat{c}' - \gamma_{11})/\gamma_{12} (= (\hat{c}' - \gamma_{21})/\gamma_{22})$, we have $\hat{c}' = \gamma_{11} + \hat{m}\gamma_{12} = \gamma_{21} + \hat{m}\gamma_{22}$. Hence,

$$(\gamma_{11} - \gamma_{21}) = -\hat{m}(\gamma_{12} - \gamma_{22}). \tag{4}$$

Also, since $c' = \gamma_{11} + m\gamma_{12} = \gamma_{21} + m\gamma_{22}$, it is clear that

$$(\gamma_{11} - \gamma_{21}) = -m(\gamma_{12} - \gamma_{22}). \tag{5}$$

From Eq. 4 and 5, it is obvious that $(\gamma_{11} - \gamma_{21}) = (\gamma_{12} - \gamma_{22}) = 0$ or $m' = m$. When $(\gamma_{11} - \gamma_{21}) = (\gamma_{12} - \gamma_{22}) = 0$, we get $(\gamma_{11}, \gamma_{12}) = (\gamma_{21}, \gamma_{22})$. This is a contradiction. On the other hand, when $m' = m$, this is also a contradition due to Lemma 2. □

Multiple-receiver scheme. The model of USAE described in section 2.1 is built for a single receiver. That is, there exists only one receiver for the entire model. From this, we can extend the model to be a multiple receiver model and show an efficient implementation of it. More detailed discussion will be provided in the full version of this paper.

3 Group authentication code

In this section, we show a model, security definition and a concrete construction of GA-code, which is an unconditionally secure authentication code with anonymity like group signatures. With the combination of USAE and GA-code, a secure communication system, which assures confidentiality, authenticity and user's anonymity can be constructed without any computational assumptions.

3.1 Model

Similar to what we saw in the model of USAE, we introduce the *trusted initializer model* for GA-code as well. In GA-code model, there are $n + 3$ participants, a set of n senders $\{S_1, \cdots, S_n\}$, a receiver R, a group authority G and a trusted initializer, TI. TI generates secret information $u_1, \cdots, u_n$ for $S_1, \cdots, S_n$, respectively, and secret information v for R. TI also generates secret information w for G. After distributing these keys, TI deletes his memory. In order to send a plaintext m to R with authenticity, $s \in \{S_1, \cdots, S_n\}$ generates an authenticated message α from m by using u_i and transmits α to R. R verifies the validity of α by using m and v. In a situation where R wants to reveal the identity of the sender, R can obtain it by cooperating with G only if G approves R's request.

3.2 Definition

Here, we formally define the security of GA-code. In GA-code, a sender is able to prove that he is a legitimate member of a group, $\{S_1, \cdots, S_n\}$. In addition, by cooperating with G, R can obtain the identity of the sender fairly simply. However, each of R and G alone, cannot reveal the sender's identity.

An adversary can perform *impersonation* or *substitution* by constructing a fraudulent codeword. The attack is considered successful if the receiver accepts the codeword. In impersonation, an adversary is assumed to not have seen any communication occurred priorly, while in substitution, the adversary have seen at least one transmitted codeword. Both impersonation and substitution can be performed by either senders and outsiders, where none of TI, G, R, $S_1, \cdots, S_n$ is included in the collusion of the outsiders. Also, senders' attack is considered to be successful if a fraudulent codeword is accepted by the receiver and no fraudulent message is traced back to the malicious sender who wrote the message by the receiver and a group authority. Outsiders' attack is considered successful if the receiver accepts the fraudulent codeword. Note that, mixed collusion attack delivered together by senders and outsiders is referred to an attack made only by senders.

Let $\mathcal{S}, \mathcal{U}_i$ $(i = 1, \cdots, n)$, $\mathcal{V}$, $\mathcal{W}$, $\mathcal{M}$ and $\mathcal{A}$ denote the random variables induced by s, u_i $(i = 1, \cdots, n)$, v, w, m and α, respectively. For $\mathcal{X}$, let $X := \{x | \Pr(\mathcal{X} = x) > 0\}$. $|X|$ denotes the cardinality of X.

We assume that at most k $(0 \le k \le n-1)$ authorized senders are malicious. Then, the security of GA-code is formally defined as follows:

Definition 5 We say that $(\mathcal{U}_1, \cdots, \mathcal{U}_n, \mathcal{V}, \mathcal{W}, \mathcal{M}, \mathcal{A})$ is a (p, k, n)-*one-time group authentication code* (GA-code) if

1. Any set of k malicious senders can perform impersonation with probability at most p. Namely, for any set of k malicious senders $\{S_{i_1}, \cdots, S_{i_k}\} \subset S$,

$$\max_{u_{i_1}, \cdots, u_{i_k}} \max_{\alpha} \Pr(R \text{ accepts } \alpha \wedge \text{none of } \{S_{i_1}, \cdots, S_{i_k}\}$$
$$\text{is detected as the sender of } \alpha | u_{i_1}, \cdots, u_{i_k}) \le p.$$

2. Any outsiders can perform impersonation with probability at most p, i.e. $\max_\alpha \Pr(R \text{ accepts } \alpha) \le p$.

3. Any set of k malicious senders can perform substitution with probability at most p. Namely, letting $\mathcal{S} = S_{i_0}$, for any set of k malicious senders $S_{i_1}, \cdots, S_{i_k}$ such that $S_{i_0} \notin \{S_{i_1}, \cdots, S_{i_k}\}$,

$$\max_{u_{i_1},\cdots,u_{i_k}} \max_{\alpha'} \max_{\alpha,\alpha\neq\alpha'} \Pr(R \text{ accepts } \alpha \wedge \text{none of } \{S_{i_1}, \cdots, S_{i_k}\} \text{ is detected as the sender of } \alpha | u_{i_1}, \cdots, u_{i_k}, \alpha') \leq p,$$

where α' is taken over the set of valid authenticated messages which can be generated by S_{i_0}.

4. Any set of outsiders can perform substitution with probability at most p, i.e. letting α' be an authenticated message which is generated by an honest user, $\max_{\alpha'} \max_{\alpha,\alpha\neq\alpha'} \Pr(R \text{ accepts } \alpha|\alpha') \leq p$.

5. R obtains no information on the identity of s from α, namely, $\Pr(\mathcal{S} = S_i|\alpha, v) = \Pr(\mathcal{S} = S_i)$ for any α and i $(1 \leq i \leq n)$.

6. G obtains no information on the identity of s from α, namely, $\Pr(\mathcal{S} = S_i|\alpha, w) = \Pr(\mathcal{S} = S_i)$ for any α and i $(1 \leq i \leq n)$.

7. Cooperating with G, R can reveal the identity of the sender of the authenticated message α with probability more than $\Pr(\mathcal{S} = S_{i_0})$, where S_{i_0} is the sender of α.

3.3 Constructions

In this subsection, we show a couple of constructions of GA-codes; one is based on polynomials and the other is based on cover free families.

Construction from polynomials. Based on polynomials, a GA-code can be constructed as follows:

GA-code based on polynomials

1. Setting up: Let $M = GF(q)\backslash\{0\}$, where q is a prime power and $q \geq n$. TI chooses a uniformly random polynomials $f(x)$ and $g(x)$ over $GF(q)$ such that $\deg f(x) \leq k+1$ and $\deg g(x) \leq k+1$. TI also chooses distinct numbers b_i $(1 \leq i \leq n)$ from $B \subseteq GF(q)$ uniformly at random, where $|B| = n$ such that $f(b_i) \neq f(b_j)$ for any i, j with $1 \leq i, j \leq n,\ i \neq j$. Next, TI gives $f(x)$ and $g(x)$ to R as v, and also gives $\{b_1, f(b_1), g(b_1)\}, \{b_2, f(b_2), g(b_2)\}, \cdots, \{b_n, f(b_n), g(b_n)\}$ to $S_1, S_2, \cdots, S_n$ as $u_1, u_2, \cdots, u_n$, respectively. TI also generates a mapping $\pi : GF(q) \to S$ such that $\pi(f(b_i)) = S_i$ and gives it to G as w. TI deletes his memory after distributing the keys.

2. Message generation: Sender S_i generates an authenticated message α for m as $\alpha = \{m, b_i, h\}$, where $h := f(b_i)m + g(b_i)$.

3. Verification: Receiver R accepts α as valid if h is identical to $f(x)|_{x=b_i}m + g(x)|_{x=b_i}$.

4. Tracing: When R wants to reveal the identity of the sender, R first sends a request to G. If R's request is approved by G, R transmits $f(b_i)$ to G via a secure channel. Then, G reveals the sender's identity by $S_i = \pi(t)$ and transmits this result back to R.

The security of the above scheme is addressed as follows:

Lemma 4 *In the GA-code based on polynomials, colluders, which include at most k of $\{S_1, S_2, \cdots, S_n\}$, can perform impersonation with probability at most $\frac{1}{q}$. (See conditions 1 and 2 of Def. 5.)*

Proof. For succeeding impersonation by collusion of senders $\{S_{i_1}, \cdots, S_{i_k}\}$, adversaries need to produce a fraudulent message $\{b, m', h'\}$ such that $h' = f(b)m' + g(b)$ and $b \notin \{b_{i_1}, \cdots, b_{i_k}\}$. Since the malicious senders have only k points of $g(x)$, it is therefore, impossible to obtain any information on $g(b)$, and accordingly, they also have no information on h'. Therefore, the probability of succeeding the attack will be at most $1/q$. In similar manner to this, we can also prove that the probability of succeeding outsiders' impersonation is at most $1/q$. □

Lemma 5 *In the GA-code based on polynomials, colluders, which include at most k of $\{S_1, S_2, \cdots, S_n\} \backslash \{S_{i_0}\}$, can perform substitution with probability at most $\frac{1}{q-k}$, where S_{i_0} is the honest sender who sends a valid authenticated message α' to R. (See conditions 3 and 4 of Def. 5.)*

Proof. For succeeding substitution by senders $\{S_{i_1}, \cdots, S_{i_k}\}$, adversaries need to produce a fraudulent message $\{b, m', h'\}$ such that $h' = f(b)m' + g(b)$, $b \notin \{b_{i_1}, \cdots, b_{i_k}\}$ and $\{b, m', h'\} \neq \alpha (= \{b_{i_0}, m, h\})$, where α is an authenticated message generated by S_{i_0}. For the fraudulent message $\{b, m', h'\}$, we consider the following cases: 1) $b = b_{i_0}$ and $m' \neq m$, 2) $b \neq b_{i_0}$ and $m' = m$, 3) $b \neq b_{i_0}$ and $m' \neq m$. For case 1) $b = b_{i_0}$ and $m' \neq m$, we have $h' = f(b)(m' - m) + h$. Since the adversaries only have $f(b_{i_1}), \cdots, f(b_{i_k})$, and $\deg f(x) = k+1$, the only information the adversaries have is $f(b) \notin \{f(b_{i_1}), \cdots, f(b_{i_k})\}$. Consequently, there are $q - k$ possible values for $f(b)$. Hence, from $h' = f(b)(m' - m) + h$, there also exist $q - k$ different values for h' for any $\{b_{i_0}, m, m', h\}$. This implies that the probability for succeeding substitution does not exceed $1/(q - k)$. For case 2) $b \neq b_{i_0}$ and $m' = m$, we have $\deg(f(x)m' + g(x)) = k + 1$ and the adversaries have only $f(b_{i_0})m'+g(b_{i_0})$ and $f(b_{i_1})m'+g(b_{i_1}), \cdots, f(b_{i_k})m'+g(b_{i_k})$. Hence, the adversaries have no information on $h = f(b)m' + g(b)$, consequently, the probability for succeeding substitution also does not exceed $1/q$. For case 3) $b \neq b_{i_0}$ and $m' \neq m$, we have $\deg g(x) = k + 1$ and the adversaries only have $f(b_{i_0})m + g(b_{i_0})$ and $g(b_{i_1}), \cdots, g(b_{i_k})$. This means, the adversaries have no information on $g(b)$. Also, this implies that they do not have any information on h' because $h' = f(b)m' + g(b)$, consequently, the probability for succeeding substitution also does not exceed $1/q$. Similarly, we can also prove that the probability of succeeding outsiders' substitution will be at most $1/q$. □

Together, any adversaries can succeed their impersonation or substitution with probability at most $1/(q - k)$.

Lemma 6 *R or G can determine who had generated the authenticated message α with probablitiy at most $\Pr(\mathcal{S} = S_{i_0})$. Additionally, cooperating with G, R can reveal the identity of the sender of the authenticated message α with probability 1, if α is valid. (See conditions 5, 6 and 7 of Def. 5.)*

Proof. Regarding the sender's anonymity, it is clear that R has no information on the identity of the sender since R does not know the mapping π. Hence, R can only determine the probability of the generator of the authenticated message α to be at most $\Pr(\mathcal{S} = S_{i_0})$. On the other hand, though G knows π, G too, has no information regarding the identity of the sender since G does not know $g(b_{i_0})$. The probability of G determining who the generator of α is, is at most $\Pr(\mathcal{S} = S_{i_0})$. However, by cooperating with G, R can identify the sender with probability 1 if α is valid. □

Theorem 8 *The above scheme is a* $(\frac{1}{q-k}, k, n)$*-one-time GA-code.*

Proof. From Lemmas 4, 5 and 6, it is obvious that the above theorem is true. □

In the security definition of GA-code, it is assumed that G does not join any colluders who try to perform impersonation or substitution. We should note that the probability of succeeding substitution can be increased when G joins a collusion attack. Since G knows $f(b_i)$ which is assigned to S_i, for example, he can substitute a valid authenticated message $\alpha := \{m, b_i, f(b_i)m + g(b_i)\}$ with a forged message $\alpha' := \{m+1, b_i, f(b_i)(m+1) + g(b_i)\}$ which will be accepted by R. If such an attack is to be avoided, we can fix the above scheme with a slight modification as follows: TI uniformly at random chooses two mappings $\pi_1 : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$ and $\pi_2 : \{1, 2, \cdots, n\} \to S$ such that $\pi_2(\pi_1(b_i)) = S_i$ instead of π. Then, $\{f(x), g(x), \pi_1\}$ and π_2 are given to R and G as v and w, respectively.

The required memory sizes for the above construction is formally addressed as follows:

Theorem 9 *The required memory sizes in the above scheme are given as follows:*

$$H(\mathcal{A}) = \log_2 nq(q-1),\ H(\mathcal{U}_i) = \log_2 nq^2 \quad \textit{for any } i\ (1 \le i \le n),$$
$$H(\mathcal{V}) = 2(k+2)\log_2 q,\ H(\mathcal{W}) = \sum_{i=0}^{n-1} \log_2 (q-i).$$

Construction from cover free family. Another construction of GA-code is based on CFF. An advantage to use the CFF based GA-code is recalling USAE, it does not always require $|M| + 1 \ge n$ while the requirement is an absolute for the polynomial based GA-code.

In order to construct a GA-code from CFF, we also introduce "classical" A-codes [18, 27] which include only one sender and one receiver. In such A-codes, there are 3 participants, a sender $\tilde{S}$, a receiver $\tilde{R}$ and a trusted initializer $\tilde{\text{TI}}$. $\tilde{\text{TI}}$ generates secret information $\tilde{u}$ and $\tilde{v}$ for $\tilde{R}$ and $\tilde{S}$, respectively, such that $\tilde{u} = \tilde{v}$. In order to send a plaintext $\tilde{m}$ to $\tilde{R}$, $\tilde{S}$ generates his authenticated message $\tilde{\alpha}$ from $\tilde{m}$ by using $\tilde{u}$ and transmits $\tilde{\alpha}$ to $\tilde{R}$. $\tilde{R}$ verifies the validity of $\tilde{\alpha}$ by using $\tilde{m}$ and $\tilde{v}$. We note that $\tilde{S}$ or $\tilde{R}$ may generate $\tilde{u}$ and $\tilde{v}$ in order to remove $\tilde{\text{TI}}$.

Definition 6 Let $\tilde{\mathcal{U}}, (\tilde{\mathcal{V}},)\tilde{\mathcal{M}}$ and $\tilde{\mathcal{A}}$ denote the random variables induced by $\tilde{u}, (\tilde{v},)\tilde{m}$ and $\tilde{\alpha}$, respectively. We say that $(\tilde{\mathcal{U}}, (\tilde{\mathcal{V}},)\tilde{\mathcal{M}}, \tilde{\mathcal{A}})$ is a *p-authentication code* (A-code) if

1. Any outsiders (which do not include $\tilde{S}$, $\tilde{R}$ or $\tilde{\text{T}}$I) can perform impersonation with probability at most p. Namely, $\max_{\tilde{\alpha}} \Pr(\tilde{R} \text{ accepts } \tilde{\alpha}) \le p$.
2. Any set of outsiders can perform substitution with probability at most p. Namely, letting $\tilde{\alpha'}$ be an authenticated message which is generated by $\tilde{S}$, $\max_{\tilde{\alpha'}} \max_{\tilde{\alpha},\ \tilde{\alpha} \ne \tilde{\alpha'}} \Pr(\tilde{R} \text{ accepts } \tilde{\alpha} | \tilde{\alpha'}) \le p$.

Construction methods of A-codes are given in, for example, [18, 27]. In the followings, for simplicity, let $f : \tilde{M} \times \tilde{U} \to \tilde{A}$ denote a mapping such that $f(\tilde{m}, \tilde{u}) = \tilde{\alpha}$. Additionally, notations for CFF is the same as that in Def. 3.

GA-code based on cover free families

1. Setting up: Let $M := \tilde{M}$. TI first generates an (n, t, k)-CFF such that each of ℓ_i $(1 \le i \le t)$ is an element of $\tilde{U}$. TI also chooses distinct numbers r_i $(1 \le i \le n)$ from $\{1, 2, \cdots, n\}$ uniformly at random. An algorithm that generates F_i $(1 \le i \le n)$ from i and L may be public to all players. TI further uniformly at random chooses two mappings $\pi_1 : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$ and $\pi_2 : \{1, 2, \cdots, n\} \to S$ such that $\pi_2(\pi_1(r_i)) = S_i$ for $1 \le i \le n$. Next, TI gives $\{L, \pi_1\}$ to R as v. TI also gives $\{r_i, F_{r_i}\}$ $(1 \le i \le n)$ to S_i $(1 \le i \le n)$, respectively, as u_i. In addition, π_2 is given to G as w. After distributing the keys, TI deletes his memory.
2. Message generation: Sender S_i generates an authenticated message α for m as $\alpha := \{r_i, {\alpha'}_1^{(r_i)}, {\alpha'}_2^{(r_i)}, \cdots, {\alpha'}_{|F_{r_i}|}^{(r_i)}\}$, where ${\alpha'}_j^{(r_i)} := f(m, \ell_j^{(r_i)})$ $(1 \le j \le |F_{r_i}|)$, assuming that $F_{r_i} = \{\ell_1^{(r_i)}, \ell_2^{(r_i)}, \cdots, \ell_{|F_{r_i}|}^{(r_i)}\}$.
3. Verification: Receiver R first generates F_{r_i} from L and r_i. Then, R accepts α as valid if ${\alpha'}_j^{(r_i)}$ is identical to $f(m, \ell_j^{(r_i)})$ for all j $(1 \le j \le |F_{r_i}|)$.
4. Tracing: When R wants to reveal the identity of the sender, R first sends a request to G. If R's request is approved by G, R calculates $t = \pi_1(r_i)$ and transmits it to G. Then, G reveals the sender's identity by $S_i = \pi_2(t)$ and transmits this result back to R via a secure channel.

Theorem 10 *The above scheme is a (p, k, n)-one-time GA-code.*

The proof of the theorem is straightforward.

The required memory sizes for the above construction is formally addressed as follows:

Theorem 11 *The required memory sizes in the above scheme are given as follows:*

$$H(\mathcal{A}) = \log_2 n + |F| H(\tilde{\mathcal{A}}),\ H(\mathcal{U}_i) = \log_2 n + |F| H(\tilde{\mathcal{U}}) \quad \text{for any } i\ (1 \le i \le n),$$
$$H(\mathcal{V}) = tH(\tilde{\mathcal{U}}) + \sum_{i=0}^{n-1} \log_2 (i+1),\ H(\mathcal{W}) = \sum_{i=0}^{n-1} \log_2 (i+1),$$

assuming that all $|F_{r_i}|$ $(1 \le i \le n)$ are of the same size $|F|$.

As mentioned so far, we see that the above scheme does not always require $|M|+1 \geq n$ while the polynomial based GA-code can be utilized only when $|M|+1 \geq n$. In addition, it should be noticed that the size of α can be reduced if each of ${\alpha'}_1^{(r_i)}, {\alpha'}_2^{(r_i)}, \cdots, {\alpha'}_{|F_{r_i}|}^{(r_i)}$ contains the same m.

3.4 Remarks

In the previous subsection, we showed GA-codes in a single-receiver model. A multiple-receiver extension that was made similarly to MUSAE for GA-code was omitted here, but will appear later in the full version. Tight bounds for the required memory sizes in GA-code is important in analyzing optimality, and is also an interesting open problem to be thought out.

By the combination of USAE and GA-code, a secure communication system with confidentiality, authenticity and sender's anonymity was constructed. It should be noticed that the security of this system was proven without any computational assumptions and assures long-term security.

References

1. M. Abe, "Universally verifiable mix-net with verification work independent of the number of mix-servers," Proc. of EUROCRYPT'98, LNCS 1403, Springer-Verlag, pp.437-447, 1998.
2. M. Bellare, A. Desai, E. Jokipii and P. Rogaway, "A concrete security treatment of symmetric encryption," Proc. of 38th IEEE Symposium on Foundations of Computer Science (FOCS), pp.394-403, 1997.
3. M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, "Relations among notions of security for public-key encryption schemes," Proc. of CRYPTO'98, LNCS 1462, Springer-Verlag, pp.26-45, 1998.
4. M. Ben-Or, S. Goldwasser and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," Proc. of 20th ACM Symposium on the Theory of Computing (STOC), pp.1-10, 1988.
5. R. Blom, "Non-public key distribution," Proc. of CRYPTO'82, Plenum Press, pp.231-236, 1983.
6. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly secure key distribution for dynamic conferences," Proc. of CRYPTO'92, LNCS 740, Springer-Verlag, pp.471-486, 1993.
7. C. Blundo, L. A. Frota Mattos and D.R. Stinson, "Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution," Proc. of CRYPTO'96, LNCS 1109, Springer-Verlag, pp.387-400, 1996.
8. J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," Proc. of CRYPTO'97, LNCS 1294, Springer-Verlag, pp.410-424, 1997.
9. D. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms," Communication of the ACM, 24, pp.84-88, 1981.
10. D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," Journal of Cryptology, 1, 1, pp.65-75, 1987.
11. D. Chaum and E. van Heyst, "Group signatures," Proc. of EUROCRYPT'91, LNCS 547, Springer-Verlag, pp.257-265, 1991.

12. Y. Desmedt, Y. Frankel and M. Yung, "Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback," Proc. of IEEE Infocom'92, pp.2045-2054, 1992.
13. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. on Inform. Theory, IT-22, pp. 644-654, 1976.
14. D. Dolev, C. Dwork and M. Naor, "Non-malleable cryptography," Proc. of 23rd ACM Symposium on the Theory of Computing (STOC), pp.542-552, 1991.
15. P. Erdös, P. Frankl and Z. Furedi, "Families of finite sets in which no sets is covered by the union of two others," Journal of Combin. Theory Ser. A 33, pp.158-166, 1982.
16. P. Erdös, P. Frankl and Z. Furedi, "Families of finite sets in which no sets is covered by the union of r others," Israel Journal of Math., 51, pp.79-89, 1985.
17. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. on Inform. Theory, IT-31, 4, pp.469-472, 1985.
18. E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, "Codes which detect deception," Bell System Technical Journal, 53, pp.405-425, 1974.
19. G. Hanaoka, J. Shikata, Y. Zheng and H. Imai, "Unconditionally secure digital signature schemes admitting transferability," Proc. of ASIACRYPT 2000, LNCS 1976, Springer-Verlag, pp.130-142, 2000.
20. 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. of PKC 2002, LNCS 2274, Springer-Verlag, pp.64-79, 2002.
21. K. Kurosawa, T. Yoshida, Y. Desmedt and M. Burmester, "Some bounds and a construction for secure broadcast encryption," Proc. of ASIACRYPT'98, LNCS 1514, Springer-Verlag, pp.420-433, 1998.
22. T. Matsumoto and H. Imai, "On the KEY PREDISTRIBUTION SYSTEM: a practical solution to the key distribution problem," Proc. of CRYPTO'87, LNCS 293, Springer-Verlag, pp.185-193, 1987.
23. R. Rivest, "Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer," unpublished manuscript.
24. R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," Communication of the ACM, 21, 2, pp.120-126, 1978.
25. C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, pp.656-715, 1949.
26. J. Shikata, G. Hanaoka, Y. Zheng and H. Imai, "Security notions for unconditionally secure signature schemes," Proc. of EUROCRYPT 2002, LNCS2332, Springer-Verlag, pp.434-449, 2002.
27. G. J. Simmons, "Authentication theory/coding theory," Proc. of CRYPTO'84, LNCS 196, Springer-Verlag, pp.411-431, 1984.
28. G. J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes," Proc. of EUROCRYPT'87, Springer-Verlag, pp.151-165, 1987.
29. D. R. Stinson, "On some methods for unconditionally secure key distribution and broadcast encryption," Designs, Codes and Cryptography, 12, pp.215-243, 1997.