A Construction of Multi-receiver Authentication Codes with Dynamic Sender from Linear Codes *

Shangdi Chen† Lizhen Chang‡

College of Science, Civil Aviation University of China, Tianjin, 300300;
Shanxi Technology And Business University, Taiyuan, 030006, P.R.China

Abstract Multi-receiver authentication codes with dynamic sender (DMRA-codes) are extensions of traditional group communication system in which any member of a group can broadcast an authenticated message such that all other group members can individually verify its authenticity, and some malicious participants of group can not successfully impersonate the potential sender, or substitute a transmitted message. In this paper, a construction of DMRA-code will be given using linear code and its unconditional security is also guaranteed.
Keywords Multi-receiver; Authentication code; Dynamic; Linear code
Mathematics Subject Classification 2000: 05B25, 94A62

1 Introduction

With the development of information technology, traditional point-to-point message authentication systems have been extensively studied in the literature. In this paper, we consider authentication for group communication. As we all known, many schemes have been proposed by several researchers to provide authentication to secure group communication. Y.Desmedt and

*The Project-sponsored by the National Natural Science Foundation of China(61179026), the Fundamental Research Funds of the Central Universities of China(3122014K015).
†Corresponding author. E-mail: 11csd@163.com; sdchen@cauc.edu.cn
‡Corresponding author. E-mail: clzscj.123@163.com; 362969673@qq.com

R.Safavi-Naini developed a series of authentication schemes in [1-2] which consider a single transmitter who is fixed before hand. Safavi-Naini and Wang extended the schemes in [3-4] and they relaxed the restriction that the sender is fixed before hand and introduced a dynamic sender concept in which any one of the users can become the sender. In [5], they dropped the restriction of a single dynamic sender and developed a scheme for the situation with t senders. In [6-7], Aparna and Amberker constructed some secure authentication codes with dynamic senders, which promoted the growth of group communication in further. In this paper, a new construction of multi-receiver authentication code with dynamic sender (DMRA-code) will be proposed, the parameters and maximum probabilities of success in various attacks are also computed.

In this paper, let $GF(q)$ be the finite field with q elements, where q is a power of a prime. We use $GF(q)^k$ to denote the k-dimensional row vector space over $GF(q)$. The set of all non-zero elements of $GF(q)^k$ is denoted as $GF(q)^{k^*}$.

The rest of the paper is organized as follows. In section 2 we describe the models of multi-receiver authentication codes with dynamic senders (DMRA-code). In section 3 we give the calculating formulas of the probability of attacks which are from a group of receivers who have access to part of the key information. We present, in section 4, a new construction of DMRA-code and the bounds. Finally, we conclude the paper.

2 The Models of DMRA-code

In this section, we study MRA-codes with dynamic senders. We consider the scenario where there is a group of k users $U = \{U_1, U_2, \cdots, U_k\}$ and a KDC who only runs the keys distribution of participants. In this model, because every user can be a sender as well as a receiver to other users, so the keys of each user have also dual functions which can not only encode but also decode messages. Let $C_i = (S, E_i, M_i; f_i, g_{ij})$ $(j \neq i)$ be authentication codes of user U_i and U_j, where $\{i, j\} \subset \{1, 2, \cdots, k\}$, $f_i : S \times E_i \longrightarrow M_i$ be authentication algorithm of user U_i, $g_{ij} : S \times E_i \longrightarrow M_j$ be verification algorithm of U_i. For authenticating a message, every user should comply with protocols:

(1)Key Distribution: The KDC randomly chooses a encoding rule $e \epsilon E$ and applies some key distribution algorithms to generate a key e_i for each user U_i, then secretly sends e_i to U_i. In addition, KDC also generates k distinct values a_i which are public knowledge as identity information for user U_i, $(i = 1, 2, \cdots, k)$;

(2)Broadcast: If a user U_i wants to send a source state s to others, U_i computes $m_i = f_i(s, e_i)$ and sends (s, m_i) to others with his identity information a_i;

(3)Verification: A user U_j $(j \neq i)$ uses his verification algorithm g_{ji} to accept or reject the received codeword. That is, he checks the authenticity by verifying whether $m_i = g_{ji}(s, e_j)$ or not. If the equality holds, the message is authentic and is accepted. Otherwise, the message is rejected.

We assume that the system follows the Kerckhoff's principle which except the actual used keys of each user, the other information of the whole system is public. This includes the uniform probability distribution of the source states and the keys of users.

3 The calculation formulas

In the whole system, we assume $U = \{U_1, U_2, \cdots, U_k\}$ $(k \geq 3)$ are a group of users, S is the source state space, E_i is the encoding rules set of user U_i and M_i is the message space of user U_i, $(1 \leq i \leq k)$.

To assess the security, we consider the probabilities of success in various attacks. Attackers could be outsiders who do not have access to any key information, or insiders who have part of key information. We only need to consider the latter group as it is at least as powerful as the former. We consider the system to protect against the coalition of groups of up to a maximum size of users, and study impersonation and substitution attacks.

Let L be a subset of $\{1, 2, \cdots, k\}$ with $|L| = w-1$ $(w \leq k-1)$. Without loss of generality, let $L = \{1, 2, \cdots, w-1\}$, denote $U_L = \{U_1, U_2, \cdots, U_{w-1}\}$ and $E_L = E_1 \times E_2 \times \cdots \times E_{w-1}$.

In the impersonation attack, U_L collude and try to launch an attack against a pair of users U_i and U_j, by generating a message such that U_j accepts it as authentic and as being sent from U_i. It can be expressed as

$$P_I(i,j) = \max_{e_L \in E_L, \{i,j\} \not\subset L} \left\{ \frac{\max\limits_{m \in M_i} |\{e_j \in E_j \mid e_j \subseteq m, p(e_L, e_j) \neq 0\}|}{|\{e_j \in E_j \mid p(e_L, e_j) \neq 0\}|} \right\}.$$

P_I is the best probability of all such attacks and is defined by $P_I = \max\limits_{\{i,j\}} P_I(i,j)$, where $L \cup \{i,j\}$ runs through all the $w+1$-subsets of $\{1, 2, \cdots, k\}$.

In the substitution attack, after seeing a valid message m broadcasted by U_i, the collaborators U_L construct a new message m' $(m' \neq m)$ such that

U_j will accept m' as being sent from U_i. We denote the success probability in this case by

$$P_S(i,j) = \max_{e_L \in E_L, \{i,j\} \not\subset L} \max_{e_i \in E_i} \max_{e_i \subseteq m} \left\{ \frac{\max_{m \neq m' \in M_i} |\{e_j \in E_j | e_j \subseteq m, e_j \subseteq m', p(e_L, e_j) \neq 0\}|}{|\{e_j \in E_j | e_j \subseteq m, p(e_L, e_j) \neq 0\}|} \right\},$$

and the best probability of all such attacks by $P_S = \max_{\{i,j\}} P_S(i,j)$, where $L \cup \{i,j\}$ runs through all the $w+1$-subsets of $\{1,2,\cdots,k\}$.

Notes: (1) $p(e_L, e_j) \neq 0$ implies that any source state s encoded by e_L can be authenticated by e_j. (2) $e_j \subseteq m$ implies that m can be verified to be authentic by e_j.

4 Construction and the Bounds

Safavi-Naini and Wang [3-4] gave two constructions of DMRA-code based symmetric polynomials, they also showed that the latter one is optimal and has the minimum number of keys set E_i for each user U_i and the shortest length of the authenticated message M_i. So far, there is no other optimal construction. In this section, a new construction of DMRA-code will be proposed based linear codes and that the construction would result in new optimal system.

Let the set of source states be $S = GF(q) \backslash \{-1\}$; the set of i-th user's encoding rules $E_i = \{e_i | e_i \in GF(q)^k \times GF(q)^{k^*}\}$; the set of the authenticated message $M_i = \{m_i | m_i \in C\} \subseteq GF(q)^n$, where $C = [n,k]$ is a linear code over $GF(q)$. A $k \times n$ matrix G over $GF(q)$ is called a generator matrix of C if its row vectors generate the linear subspace C and G is publicly known.

Define the encoding map of each user U_i $(i = 1,2,\cdots,k)$ as

$$f_i : S \times E_i \longrightarrow M_i, f_i(s, e_i) = (\delta_i + s\gamma_i)G \quad (1 \leq i \leq k),$$

where $e_i = (\delta_i, \gamma_i) \in E_i$.

The decoding map of each user U_i with another user U_j as

$$g_{ij} : S \times E_i \longrightarrow M_j, g_{ij}(s, e_i) = [(\delta_i + s\gamma_i) + (1+s)(a_j - a_i)]G,$$

where $a_i, a_j \in GF(q)^k$ and $i \neq j$.

This code works as follows:

1.***Key distribution phase***

(1)The KDC randomly chooses an (u, v) of $C \times C^*$ and assumes $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n)$. Then he calculates (α_1, β_1) satisfying $\alpha_1 G = u$, $\beta_1 G = v$, that is $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^k$;

(2)The KDC randomly selects k distinct elements $b_1, b_2, \cdots, b_k$ of $GF(q)^{k^*}$ and computes $\delta_i = \alpha_1 + b_i$, $\gamma_i = \beta_1 + b_i$ such that $\gamma_i \neq 0$, $i = 1, 2, \cdots, k$. Then he privately transmits $e_i = (\delta_i, \gamma_i)$ to user U_i for each $1 \leq i \leq k$, which consists of the secret key of U_i;

(3)KDC also randomly chooses $b_0 \in GF(q)^{k^*}$ and calculates values $a_i = b_0 + b_i$ which is public knowledge and is used as identity information for user U_i, $(i = 1, 2, \cdots, k)$.

2.***Broadcast phase*** For $1 \leq i \leq k$, assume user U_i wants to construct an authenticated message for a source state $s \in S$. U_i computes $m_i = f_i(s, e_i) = (\delta_i + s\gamma_i)G$ and sends (s, a_i, m_i) to all the other users.

3. ***Verification phase*** The user U_j $(j \neq i)$ can verify the authenticity of the message in the following way. U_j accepts (s, a_i, m_i) as authentic being sent from U_i if $g_{ji}(s, e_j) = [(\delta_j + s\gamma_j) + (1 + s)(a_i - a_j)]G = m_i$, otherwise, he rejects it.

For the sake of simplicity, we assume that after the key distribution phase, each user can only send at most a single authenticated message.

Next, we will show that the above construction is a well defined DMRA-code.

Lemma 4.1 Let $C_i = (S, E_i, M_i; f_i)$, then $C_i (1 \leq i \leq k)$ is an A-code.

Proof. For any $s \in S$, $e_i \in E_i$, we assume that $e_i = (\delta_i, \gamma_i)$, then $f_i(s, e_i) = (\delta_i + s\gamma_i)G = m_i \in M_i$; Conversely, for any $m_i \in M_i$, choose $e_i = (\delta_i, \gamma_i) \in E_i$, let $f_i(s, e_i) = (\delta_i + s\gamma_i)G = m_i$, then $\delta_i G = m_i - s\gamma_i G$. Because m_i is a codeword, so $m_i - s\gamma_i G$ is also a codeword. Thus there must exist a $\delta_i \in GF(q)^k$ satisfying f_i. It means that f_i is a surjection.

If $s' \in S$ is another source state satisfying $m_i = f_i(s', e_i)$, then $(\delta_i + s'\gamma_i)G = (\delta_i + s\gamma_i)G$, thus $(s - s')\gamma_i G = 0$. As $\gamma_i \neq 0$, $\gamma_i G \neq 0$ and $s = s'$. That is, s is the uniquely source state determined by e_i and m_i. So $C_i (1 \leq i \leq k)$ is an A-code.

Lemma 4.2 For any valid message $m = (s, a_i, m_i)$ from user U_i, U_j $(j \neq i)$ will accept it.

Proof. For any valid message $m = (s, a_i, m_i)$ from user U_i, there must exist $e_i = (\delta_i, \gamma_i) \in E_i$, such that $m_i = (\delta_i + s\gamma_i)G$. According to the given protocol, we can get $\delta_i = \alpha_1 + b_i$, $\gamma_i = \beta_1 + b_i$ and $a_i = b_0 + b_i$, $1 \leq i \leq k$, where $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^k$ and $(b_0, b_i) \in GF(q)^{k^*} \times GF(q)^{k^*}$. Thus

$$\begin{aligned} m_i &= [(\alpha_1 + b_i) + s(\beta_1 + b_i)]G \\ &= [(\alpha_1 + s\beta_1) + (1+s)b_i]G \\ &= [(\alpha_1 + b_j) + s(\beta_1 + b_j) + (1+s)(b_i - b_j)]G \\ &= [\delta_j + s\gamma_j + (1+s)((a_i - b_0) - (a_j - b_0))]G \\ &= [\delta_j + s\gamma_j + (1+s)(a_i - a_j)]G, \end{aligned}$$

where $e_j = (\delta_j, \gamma_j) \in E_j$ is the key of user U_j. It means that message $m = (s, a_i, m_i)$ could be verified by user U_j. So U_j will accept it.

From Lemma 4.1 to Lemma 4.2, we can see this construction is well defined. Next, we will compute the parameters and the maximum probability of success in various attacks.

Theorem 4.1 The parameters of constructed authentication code with dynamic sender are: $|S| = q - 1; |E_i| = q^k(q^k - 1); |M_i| = |C| = q^k$.

Proof. The result is straightforward.

Lemma 4.3 For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\} \in E_L$, where $(\delta_l, \gamma_l) \in GF(q)^k \times GF(q)^{k^*}, (l = 1, 2, \cdots, w-1)$, let the number of e_j which is incidence with e_L be a. Then $a = q^k - (w+1)$.

Proof. For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\}$, according to the given protocol, we can get $\delta_l = \alpha_1 + b_l$, $\gamma_l = \beta_1 + b_l$, $(l = 1, 2, \cdots, w-1)$ for a common and fixed $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^k$. That is, (δ_l, γ_l) is only determined by b_l of $GF(q)^{k^*}$. Let $e_j = (\delta_j, \gamma_j)$, then e_j is incidence with e_L if and only if $\delta_j = \alpha_1 + b_j$, $\gamma_j = \beta_1 + b_j$. As $b_j \in GF(q)^{k^*}$, $b_j \neq -\beta_1$ and $b_j \neq b_l$, $(l = 1, 2, \cdots, w-1)$, the number of b_j is $q^k - (w+1)$. It means that the number of e_j which is incidence with e_L is $q^k - (w+1)$. So $a = q^k - (w+1)$.

Lemma 4.4 For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\} \in E_L$, where $(\delta_l, \gamma_l) \in GF(q)^k \times GF(q)^{k^*}, (l = 1, 2, \cdots, w-1)$, $m \in M_i$, where m is generated by collaborators U_L who want to send it to U_j with the identity information of U_i. Let the number of e_j $(j \neq i)$ which is incidence with e_L contained in m be c. Then $c = 1$.

Proof. Let $e_j = (\delta_j, \gamma_j)$, $m = (s, a_i, m_i')$ generated by collaborators U_L. For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\}$, similarly, we can get $\delta_l = \alpha_1 + b_l$, $\gamma_l = \beta_1 + b_l$, $(l = 1, 2, \cdots, w-1)$ for a common and fixed $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^k$. If e_j is incidence with e_L, then

$$\delta_j = \alpha_1 + b_j, \quad \gamma_j = \beta_1 + b_j,$$

for some $b_j \in GF(q)^{k^*}$.

Again, $e_j \subseteq m$, then

$$[(\delta_j + s\gamma_j) + (1+s)(a_i - a_j)]G = m'_i.$$

By combining the above equations, we can get

$$\begin{aligned} & [(\alpha_1 + b_j) + s(\beta_1 + b_j) + (1+s)(a_i - a_j)]G \\ = & [(1+s)b_j + (\alpha_1 + s\beta_1) + (1+s)(a_i - a_j)]G = m'_i. \end{aligned}$$

As m'_i is a codeword, there must uniquely exist a $\xi \in GF(q)^k$ satisfying that

$$(1+s)b_j + (\alpha_1 + s\beta_1) + (1+s)(a_i - a_j) = \xi,$$

thus

$$(1+s)b_j = \xi - (\alpha_1 + s\beta_1) - (1+s)(a_i - a_j).$$

Because (a_i, a_j), (α_1, β_1) and (s, ξ) are fixed and $s \neq -1$, so b_j is only determined by them. That is, the number of e_j which is incidence with e_L contained in m is only one. Then $c = 1$.

Lemma 4.5 For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\} \in E_L$, where $(\delta_l, \gamma_l) \in GF(q)^k \times GF(q)^{k^*}, (l = 1, 2, \cdots, w-1)$, $m \in M_i$, where m is sent by user U_i who want to broadcast it to other users. Let the number of e_j which is incidence with e_L contained in m be d. Then $d = q^k - (w+2)$.

Proof. Let $e_j = (\delta_j, \gamma_j)$, $m = (s, a_i, m_i)$ sent by user U_i. For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\}$, from Lemma 4.3, we can get $\delta_l = \alpha_1 + b_l$, $\gamma_l = \beta_1 + b_l$, $(l = 1, 2, \cdots, w-1)$ for a common and fixed $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^k$. That is, (δ_l, γ_l) is only determined by b_l of $GF(q)^{k^*}$. If e_j is incidence with e_L, then

$$\delta_j = \alpha_1 + b_j, \quad \gamma_j = \beta_1 + b_j,$$

for some $b_j \in GF(q)^{k^*}$.

Again, we have known that $e_j \subseteq m$ and m is encoded by e_i, the key of user U_i, which means that e_j is incidence with e_i. Let $e_i = (\delta_i, \gamma_i)$, similarly, we can see that $\delta_i = \alpha_1 + b_i$, $\gamma_i = \beta_1 + b_i$.

By combining the above conclusions, it is easily to get $b_j \neq -\beta_1$, $b_j \neq b_i$ and $b_j \neq b_l$, $(l = 1, 2, \cdots, w-1)$. Also, $b_j \in GF(q)^{k^*}$, then the number of b_j satisfying the above requirements is $q^k - (w+2)$. That is, $d = q^k - (w+2)$.

Lemma 4.6 For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\} \in E_L$, where $(\delta_l, \gamma_l) \in GF(q)^k \times GF(q)^{k^*}, (l = 1, 2, \cdots, w-1)$, $m \in M_i$, $m' \in M_i$ $(m' \neq m)$, where m is sent by user U_i and m' is generated by collaborators U_L who want to send it to user U_j with the identity information of U_i. Let the number of e_j which is incidence with e_L contained both in m and m' be f. Then $f = 1$.

Proof. Let $e_j = (\delta_j, \gamma_j)$, $m = (s, a_i, m_i)$ and $m' = (s', a_i, m_i')$ $(s \neq s')$. For any fixed $e_L = \{(\delta_1, \gamma_1), (\delta_2, \gamma_2), \cdots, (\delta_{w-1}, \gamma_{w-1})\}$, similarly, we can get $\delta_l = \alpha_1 + b_l$, $\gamma_l = \beta_1 + b_l$, $(l = 1, 2, \cdots, w-1)$ for a common and fixed $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^k$. It means that (δ_l, γ_l) is only determined by $b_l \in GF(q)^{k^*}$. If e_j is incidence with e_L, then

$$\delta_j = \alpha_1 + b_j, \quad \gamma_j = \beta_1 + b_j,$$

for some $b_j \in GF(q)^{k^*}$. Again, $e_j \subseteq m$ and $e_j \subseteq m'$, then from the given protocol, we can see that

$$[(\delta_j + s\gamma_j) + (1+s)(a_i - a_j)]G = m_i$$

and

$$[(\delta_j + s'\gamma_j) + (1+s')(a_i - a_j)]G = m_i'.$$

By combining all the above conclusions, we can get

$$[(\alpha_1 + b_j) + s(\beta_1 + b_j) + (1+s)(a_i - a_j)]G = m_i$$

and

$$[(\alpha_1 + b_j) + s'(\beta_1 + b_j) + (1+s')(a_i - a_j)]G = m_i'.$$

Because both m_i and m_i' are codewords, so there must exist two fixed values (σ_1, σ_2) satisfying that

$$\alpha_1 + b_j + s(\beta_1 + b_j) + (1+s)(a_i - a_j) = \sigma_1$$

and

$$\alpha_1 + b_j + s'(\beta_1 + b_j) + (1+s')(a_i - a_j) = \sigma_2,$$

where $(\sigma_1, \sigma_2) \in GF(q)^k \times GF(q)^k$. Hence, $(s - s')(\beta_1 + b_j + a_i - a_j) = \sigma_1 - \sigma_2$. As $s \neq s'$, $\beta_1 + b_j + a_i - a_j = (s - s')^{-1}(\sigma_1 - \sigma_2)$. Also, a_i, a_j and β_1 are fixed, so b_j is only defined. That is, the number of e_j satisfying all the above requirements is only one. Then $f = 1$.

Theorem 4.2 In this authentication code with dynamic sender, if the encoding rules of users are chosen according to a uniform probability distribution, then the largest probabilities of success for different types of deceptions are $P_I = \frac{1}{q^k-(w+1)}$, and $P_S = \frac{1}{q^k-(w+2)}$.

Proof. (1) From Theorem 4.3 and Lemma 4.4, we know that the largest probability of $w-1$ malicious users' successful impersonation attack is

$$P_I(i,j) = \max_{e_L\in E_L,\{i,j\}\not\subset L}\left\{\frac{\max_{m\in M_i}|\{e_j\in E_j|e_j\subseteq m,p(e_L,e_j)\neq 0\}|}{|\{e_j\in E_j|p(e_L,e_j)\neq 0\}|}\right\} = \frac{c}{a} = \frac{1}{q^k-(w+1)}.$$

(2) From Lemma 4.5 and Lemma 4.6, we know that the largest probability of $w-1$ malicious users' successful substitution attack is

$$P_S(i,j) = \max_{e_L\in E_L,\{i,j\}\not\subset L}\max_{e_i\in E_i}\max_{e_i\subseteq m}\left\{\frac{\max_{m\neq m'\in M_i}|\{e_j\in E_j|e_j\subseteq m,e_j\subseteq m',p(e_L,e_j)\neq 0\}|}{|\{e_j\in E_j|e_j\subseteq m,p(e_L,e_j)\neq 0\}|}\right\}, = \frac{f}{d} = \frac{1}{q^k-(w+2)}.$$

Obviously, both $P_I(i,j)$ and $P_S(i,j)$ are constants, so $P_I = P_I(i,j) = \frac{1}{q^k-(w+1)}$ and $P_S = P_S(i,j) = \frac{1}{q^k-(w+2)}$.

Compared with the construction of R.Safavi-Naini and H.Wang[4], we see that in this model the size of each user's key is $|E_i| = q^k(q^k-1) > q^{2w}$ for all $1 \leq i \leq k$, and the size of codewords is $|M_i| = |C| = q^k > q^w|S|$. At the same time, it is easily to see that $P_I < \frac{1}{q}$ and $P_S < \frac{1}{q}$. That is, the beat chances of success in the corresponding attacks are more reduced than [4].

5 Conclusion

Multi-receiver Authentication codes with dynamic sender (DMRA-code) are interesting and important cryptographic primitive in secure group communication. In this paper, we mainly gave a new construction of DMRA-code using linear code and derived related bounds. In addition, according to the above results, we can see that it is more optimal than the result of [4]. Also, there are many applications for such system, such as group communication of conference system, airline travel, network security etc., where members of a group want to broadcast messages such that every other group members can verify the authenticity of the received messages. Of course, they are interesting open problems, which need us to do further research.

References

[1] Y.Desmedt, Y.Frankle and M.Yung. Multi-receiver / Multi-sender network security: efficient authenticated multicast / feedback.IEEE Infocom'92, 1992, pp.2045-2054.

[2] R.Safavi-Naini and H.Wang, Bounds and Constructions for Multireceiver Authentication Codes, Lecture Notes in Computer Science, Vol.(1514/1998), 1998, pp.242-256.

[3] R.Safavi-Naini and H.Wang, New Results on Multireceiver Authentication codes, In Advances in Cryptology-Eurocrypt'98,LNCS,1438(1998), pp.527-541.

[4] R.Safavi-Naini and H.Wang, Multi-receiver authentication codes: Models, Bounds, Constructions and Extensions, Information and Computation, 151, 1999, pp.148-172.

[5] R.Safavi-Naini and H.Wang, Broadcast Authentication for Group Communication, Theoretical Computer Science, 269(1-2), 2001, pp.1-21.

[6] R.Aparna and B.B.Amberker, Multi-Sender Multi-Receiver Authentication For Dynamic Secure Group Communication, IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.10, 2007, pp.310-315.

[7] R.Aparna and B.B.Amberker, Authenticated Secure Group Communication using Broadcast Encryption Key Computation, Fifth International Conference on Information Technology: New Generations, 2008, pp.348-353.