Two Constructions of Multi-sender Authentication codes with Arbitration based Linear codes

CHEN SHANGDI
College of Science
Civil Aviation University of China
Jinbei Road 2898, 300300, Tianjin
CHINA
11csd@163.com

CHANG LIZHEN
College of Science
Civil Aviation University of China
Jinbei Road 2898, 300300, Tianjin
CHINA
clzscj.123@163.com

Abstract: Multi-sender authentication codes allow a group of senders to construct an authenticated message for a receiver such that the receiver can verify authenticity of the received message. In this paper, we construct two multi-sender authentication codes with arbitration from Linear codes. The parameters and the probabilities of deceptions are also calculated.

Key–Words: Multi-sender, Authentication code, Arbitration, Linear code, Finite field

1 Introduction

In a group communication scenario or communication network, information security consists of confidentiality and authentication. Confidentiality is to prevent the confidential information from decrypting by adversary. The purpose of authentication is to ensure the sender is real and to verify the information is integrated. Digital signature and authentication codes are two important means of authenticating the information. In addition, they can provide good service in the network. However, traditional digital signature has been unable to fully meet the guarantee of information reliability. In many cases, they require individuals to cooperate on the same message sign, the so-called multi signature, then send to the receiver. The receiver receives this message, and verifies its effectiveness. This way is not realistic, and the signature length will multiply with the number of signers. Also, digital signature is computationally secure, in practical, assume that the computing power of adversary is limited and a mathematical problem is intractable and complex. So it is dissatisfied. But authentication codes are able to ensure the reliability of the information, meantime, they are unconditionally safe, relatively simple. Therefore it is necessary to introduce some authentication knowledge. About traditional authentication codes, a lot of researches have been developed. In 1974, Gilbert, Mac Williams and Sloane constructed the first authentication code [1], it is a landmark in the development of authentication theory. During the same period, Simmons studied the authentication theory and established three participants and four participants certification models [2]. Wan Zhexian constructed an authentication code without arbitration from the subspace of the classical geometry [3]. In the case of transmitter and receiver are not honest, Ma Wenping, Wang Xinmei, Gao You, Chen Shangdi, Li Ruihu constructed a series of authentication codes with arbitration [4-7], which promoted the growth of authentication codes in further. However, with the flourish development of communication system, such traditional two users authentication codes are no longer suitable for network requirements, multi-sender and multi-receiver authentication codes come into being. This paper will focus on multi-sender authentication codes. Multi-sender authentication system refers to that a group of senders cooperatively send a message to the receiver, then the receiver should be able to ascertain that the message is authentic. About this case, many scholars had also a lot of researches. Ma Wenping, Desmedt, Du Qingling and Martin et al had made great contributions on multi-sender authentication codes [8-12]. Again, with the expansion of the scope of application, it is very necessary for us to research on multi-transmitters authentication system with arbitration. In this paper, two constructions of multi-sender authentication codes with arbitration using linear codes will be given, the parameters and maximum probabilities of success in various attacks are also computed. Until now, we have not found that someone who ever constructed a multi-sender authentication code using linear code. Therefore, this paper will play an important role for us in expanding our thinking. Meantime, it would enable us to have a new understanding on authentication codes.

In this paper, let $GF(q)$ be the finite field with

q elements, where q is a power of a prime. We use $GF(q)^n$ denote the n-dimensional row vector space over $GF(q)$, and $GF(q)^{k\times n}$ denote the set of all $k \times n$ matrices over $GF(q)$. The sets of all non-zero elements of $GF(q)^n$ and $GF(q)^{k\times n}$ are denoted as $GF(q)^{n*}$ and $GF(q)^{k\times n^*}$, respectively. The transposition of a matrix a is denoted by a^t.

The rest of the paper is organized as follows. In section 2 we describe models of multi-sender authentication codes. In section 3 we give the calculating formulas of the probabilities of success with respect to various attacks. We present, in section 4, two new constructions of multi-sender codes with arbitration. Finally, we conclude the paper.

2 The Models of Multi-sender Authentication Codes with Arbitration

In the actual computer network communications, multi-sender authentication codes with arbitration include sequential model and simultaneous model. Sequential model is that each sender uses its own encoding rules to encode a source state orderly, and the last sender sends the encoded message to the receiver, the receiver receives the message and verifies whether the message is legal or not. Simultaneous model is that all senders use their own encoding rules to encode a source state, and each sender sends the encoded message to the synthesizer respectively, then the synthesizer forms an authenticated message and sends it to the receiver, the receiver receives the message and verifies whether the message is legal or not. In this paper, we will adopt to the second model.

In a simultaneous model, there are four participants: a group of senders $P = \{P_1, P_2, \cdots, P_n\}$, a arbiter, for the distribution keys to senders and receiver, including solving the disputes between them, a receiver R and a synthesizer who only runs the trusted synthesis algorithm. Let $C = (C_1, C_2, \cdots, C_n, C_0; f_i, g)$ be the multi-sender authentication code, the code works as follows: each sender and receiver has their own authentication code, respectively. Let $C_i = (S, E_i, T_i; f_i)(i = 1, 2, \cdots, n)$ be the sender's authentication codes, $C_0 = (S, E_R, T; g)$ be the receiver's authentication code, $h : T_1 \times T_2 \times \cdots \times T_n \longrightarrow T$ be the synthesis algorithm, $\pi_i : E \longrightarrow E_i$ be a sub-key generation algorithm. For authenticating a message, the senders and the receiver should comply with protocols:

(1) The arbiter randomly selects a encoding rule $e\epsilon E$ and sends $e_i = \pi_i(e)$ to the i-th sender $P_i(i = 1, 2, \cdots, n)$ secretly; Then he calculates e_R using e according to a effective algorithm, and secretly sends e_R to the receiver R;

(2) If the senders would like to send a source state s to the receiver R, P_i computes $t_i = f_i(s, e_i)(i = 1, 2, \cdots, n)$ and sends $m_i = (s, t_i)(i = 1, 2, \cdots, n)$ to the synthesizer through an open channel;

(3) The synthesizer receives $(s, (t_1, t_2, \cdots, t_n))$ and calculates $t = h(t_1, t_2, \cdots, t_n)$ using the synthesis algorithm h, then sends message $m = (s, t)$ to the receiver R;

(4) When the receiver R receives the message $m = (s, t)$, he checks the authenticity by verifying whether $t = g(s, e_R)$ or not. If the equality holds, the message is authentic and is accepted. Otherwise, the message is rejected.

We assume that the arbitrator and the synthesizer are credible, though they know the encoding rules of the senders and the receiver, they will not participate in any communication activities. When transmitters and receiver are disputing, the arbitrator settles it. At the same time, we assume that the system follows the Kerckhoff's principle which except the actual used keys, the other information of the whole system is public.

3 The calculation formulas

In the whole system, we assume $P = \{P_1, P_2, \cdots, P_n\}$ are a group of senders, R is the receiver, E_i is the encoding rules set of P_i, $E_P = E_1 \times \cdots \times E_n$ is the encoding rules set of P, E_R is the decoding rules set of receiver R, S is the source state space, T is the tag space and $M = S \times T$ is the message space. Now, let us consider various attacks. Here, there are five kinds of attacks:

(1) The opponent's impersonation attack: the largest probability of an opponent's successful impersonation attack is P_I. Then

$$P_I = \max_{m\in M}\left\{\frac{|\{e_R \in E_R \mid e_R \subset m\}|}{|E_R|}\right\}.$$

(2) The opponent's substitution attack: the largest probability of an opponent's successful substitution attack is P_S. Then

$$P_S = \max_{m\in M}\left\{\frac{\max\limits_{m\neq m'\in M}|\{e_R \in E_R \mid e_R \subset m, e_R \subset m'\}|}{|\{e_R \in E_R \mid e_R \subset m\}|}\right\}.$$

(3) There might $l(1 \le l \le n)$ malicious senders who together cheat the receiver, that is, the part of senders and receiver are not credible, they can take impersonation attack. Let $L = \{i_1, i_2, \cdots, i_l\} \subset$

$\{1, 2, \cdots, n\}$, $(l \leq n)$ and $e_L = \{e_{i_1}, e_{i_2}, \cdots, e_{i_l}\}$. Assume $P_L = \{P_{i_1}, P_{i_2}, \cdots, P_{i_l}\}$, P_L, after receiving their secret keys, send a message m to receiver R, P_L is successful if the receiver accepts it as legitimate message. Denote $P_I(L)$ is the maximum probability of success of the impersonation attack. It can be expressed as

$$P_I(L) = \max_{e_L \in E_L} \max_{e_L \subset e_P} \left\{ \frac{\max_{m \in M} \mid \{e_R \in E_R \mid e_R \subset m, p(e_R, e_P) \neq 0\} \mid}{\mid \{e_R \in E_R \mid p(e_R, e_P) \neq 0\} \mid} \right\}.$$

(4) The receiver's impersonation attack: under the current protocol, the largest probability of the receiver's successful impersonation attack is P_{R_0}.Then

$$P_{R_0} = \max_{e_R \in E_R} \left\{ \frac{\max_{m \in M} \mid \{e_P \in E_P \mid e_P \subset m, p(e_R, e_P) \neq 0\} \mid}{\mid \{e_P \in E_P \mid p(e_R, e_P) \neq 0\} \mid} \right\}.$$

(5) The receiver's substitution attack: under the current protocol, the largest probability of the receiver's successful substitution attack is P_{R_1}. Then

$$P_{R_1} = \max_{e_R \in E_R, m \in M} \left\{ \frac{\max_{m' \in M} \mid \{e_P \in E_P \mid e_P \subset m, m', p(e_R, e_P) \neq 0\} \mid}{\mid \{e_P \in E_P \mid e_P \subset m, p(e_R, e_P) \neq 0\} \mid} \right\}.$$

Notes: (1) $p(e_R, e_P) \neq 0$ implies that any source state s encoded by e_P can be authenticated by e_R. (2) $e_P \subset m$ implies that the message m can be got by e_P encoding some source sate. (3) $e_R \subset m$ implies that m can be verified to be authentic by e_R.

4 Constructions

In [13], some multi-receiver authentication codes have been constructed by using the linear codes. Similarly, two different multi-sender authentication codes with arbitration will be constructed by using linear codes in this paper.

4.1 Construction 1

Let $GF(q)$ be a finite field with q elements. The set of source states $S = GF(q)^*$; the set of i-th transmitter's encoding rules $E_i = \{e_i \mid e_i \in GF(q) \times GF(q)^*\}$; the set of receiver's decoding rules $E_R = \{e_R \mid e_R \in GF(q)^{n \times k} \times GF(q)^{n \times k^*}\}$; the set of i-th transmitter's tags $T_i = \{t_i \mid t_i \in GF(q)\}$; the set of receiver's tags

$$T = \left\{ t = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} \middle| \gamma_i \in C \right\} \subset GF(q)^{n \times n},$$

where γ_i, $1 \leq i \leq n$, is the row vector of t and $C = [n, k]$ is a linear code over $GF(q)$. A $k \times n$ matrix G over $GF(q)$ is called a generator matrix of C, that is, the row vectors of G are formed by a set of base in C.

Define the encoding map of the sender P_i $(i = 1, 2, \cdots, n.)$ as

$$f_i : S \times E_i \longrightarrow T_i, f_i(s, e_i) = u_i + sv_i (1 \leq i \leq n),$$

where $e_i = (u_i, v_i) \in E_i$.

The decoding map of the receiver R as

$$g : S \times E_R \longrightarrow T, g(s, e_R) = (\alpha + s\beta)G,$$

where $e_R = (\alpha, \beta) \in E_R$. And the synthesizing map

$$h : T_1 \times T_2 \times \cdots \times T_n \longrightarrow T,$$

$h(t_1, t_2, \cdots, t_n) = a^t(t_1, t_2, \cdots, t_n)$, where $a \in GF(q)^{n*}$.

This code works as follows:

1. ***Key distribution phase***

(1) The arbiter randomly chooses an $e = (u, v)$ of $C \times C^*$, assumes $u = (u_1, u_2, \cdots, u_n)$ and $v = (v_1, v_2, \cdots, v_n)$ such that u is linear independent with v. Then he calculates $e_i = \pi_i(e) = (u_i, v_i)$ and (α_1, β_1) satisfying $\alpha_1 G = u$, $\beta_1 G = v$. Again $v \neq 0$, so $\beta_1 \neq 0$, then $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k^*}$;

(2) The arbiter also randomly selects an $a = (a_1, a_2, \cdots, a_n) \in GF(q)^{n*}$ and calculates $e_R = (\alpha, \beta)$ such that $\alpha = a^t\alpha_1$, $\beta = a^t\beta_1$;

(3) He secretly sends e_R, e_i to the receiver R and sender $P_i (1 \leq i \leq n)$, respectively, and sends a to the synthesizer.

2. ***Broadcast phase*** If the senders want to send a source state $s \in S$ to the receiver R, P_i calculates $t_i = f_i(s, e_i) = u_i + sv_i$, and sends (s, t_i) to the synthesizer, $(1 \leq i \leq n)$.

3. ***Synthesis phase*** After the synthesizer receivers $(s, (t_1, t_2, \cdots, t_n))$, he calculates $t = h(t_1, t_2, \cdots, t_n) = a^t(t_1, t_2, \cdots, t_n)$, then sends $m = (s, t)$ to the receiver R.

4. ***Verification phase*** When the receiver R receives $m = (s, t)$, he calculates $t' = g(s, e_R) = (\alpha + s\beta)G$. If $t = t'$, he accepts t, otherwise, he rejects it.

Next, we will show that the above construction is a well defined multi-sender authentication code with arbitration.

Lemma 1 *Let $C_i = (S, E_i, T_i; f_i)$, $1 \le i \le n$. Then C_i is an A-code.*

Proof: For any $s \in S$, $e_i \in E_i$, we assume that $e_i = (u_i, v_i)$, then $u_i + sv_i = t_i \in T_i$. Conversely, for any $t_i \in T_i$, choose $e_i = (u_i, v_i)$, let $f_i(s, e_i) = u_i + sv_i = t_i$, then $sv_i = t_i - u_i$, thus $s = {v_i}^{-1}(t_i - u_i)$. If there is a pair of (u_i, v_i), s is only defined. Again, $(u_i, v_i) \in GF(q) \times GF(q)^*$, so the number of (s, e_i) satisfying f_i is $q(q-1)$. That is, f_i is a surjection.

If $s' \in S$ is another source state satisfying $u_i + sv_i = u_i + s'v_i$, then $(s - s')v_i = 0$. As $v_i \neq 0$, $s - s' = 0$, thus $s = s'$. That is, s is the uniquely source state determined by e_i and t_i. So $C_i (1 \le i \le n)$ is an A-code. □

Lemma 2 *Let $C_0 = (S, E_R, T; g)$. Then C_0 is an A-code.*

Proof: For any $s \in S$, $e_R \in E_R$, from the definition of e_R, we assume that $e_R = (\alpha, \beta)$, then

$$g(s, e_R) = (\alpha + s\beta)G = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} \in T;$$

On the other hand, for any $t \in T$, choose $e_R = (\alpha, \beta) \in E_R$, let $g(s, e_R) = (\alpha + s\beta)G = t$, then $\alpha G = t - s\beta G$. Because each row of t is a codeword, so each row of $t - s\beta G$ is a codeword. Thus there must exist a $\alpha \in GF(q)^{n \times k}$ satisfying g. It means that g is a surjection.

If $s' \in S$ is another source state satisfying $t = g(s', e_R)$, then $(\alpha + s\beta)G = (\alpha + s'\beta)G$, thus $(s - s')\beta G = 0$. As $\beta \neq 0$, $\beta G \neq 0, s - s' = 0, s = s'$. That is, s is the uniquely source state determined by e_R and t. So $C_0 = (S, E_R, T; g)$ is an A-code. □

Lemma 3 *For any valid message $m = (s, t)$, it will be accepted by the receiver R.*

Proof: For any valid message $m = (s, t)$, there must exist a pair of $(u, v) \in C \times C^*$ and $a \in GF(q)^{n*}$ such that $t = a^t(u + sv)$. According to the given protocol, we can get $u = \alpha_1 G$ and $v = \beta_1 G$, where $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k*}$. It is easy to see that $t = a^t(u + sv) = a^t(\alpha_1 G + s\beta_1 G) = (a^t\alpha_1 + sa^t\beta_1)G = (\alpha + s\beta)G$, where $e_R = (\alpha, \beta)$ is the key of receiver R. It means that message $m = (s, t)$ could be verified by the receiver, so R will accept it. □

From lemma 1 to lemma 3, we can see this construction is well defined. Next, we will compute the parameters and the maximum probabilities of success in five attacks.

Theorem 4 *The parameters of constructed authentication code with arbitration are: $|S| = q - 1; |E_i| = q(q-1); |T_i| = q; |E_R| = q^{nk}(q^{nk} - 1); |T| = q^{nk}$.*

Proof: The result is straightforward. □

Lemma 5 *For any $m \in M$, let the number of e_R contained in m be b. Then $b = q^{nk} - 1$.*

Proof: Let $m = (s, t) \in M$, $e_R = (\alpha, \beta) \in E_R$. If $e_R \subset m$, then $(\alpha + s\beta)G = t$, $\alpha G = t - s\beta G$. Because s and t are given, for any β, we have known each row of $t - s\beta G$ is a codeword, so there must exist a α satisfying it. That is, α is only determined by β. As $\beta \in GF(q)^{n \times k^*}$, the number of e_R contained in m is $q^{nk} - 1$. Then $b = q^{nk} - 1$. □

Lemma 6 *For any $m = (s, t) \in M$ and $m' = (s', t') \in M$ with $s \neq s'$, let the number of e_R contained both in m and m' be c. Then $c = 1$.*

Proof: Assume $e_R = (\alpha, \beta)$. If $e_R \subset m$ and $e_R \subset m'$, then

$$(\alpha + s\beta)G = t, \ \ (\alpha + s'\beta)G = t'.$$

From the above two equations, we can get that $(s - s')\beta G = t - t'$, $\beta G = (s - s')^{-1}(t - t')$. Because each row of $(s - s')^{-1}(t - t')$ is a fixed codeword, so each row of β is also fixed. Again, we have known α is is only defined by β from Lemma 5, so the number of e_R contained both in m and m' is only one. Then $c = 1$. □

Lemma 7 *For any fixed $e_P = \{(u_i, v_i) \mid (u_i, v_i) \in GF(q) \times GF(q)^*, 1 \le i \le n\}$ containing a given e_L, let the number of e_R which is incidence with e_P be d. Then $d = q^n - 1$.*

Proof: (1). Let us firstly prove a conclusion: assume $a = (a_1, a_2, \cdots, a_n) \in GF(q)^n$ and $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k*}$, if $a^t\alpha_1 = 0$ and $a^t\beta_1 = 0$, then $a = 0$. Indeed, if $a^t\alpha_1 = 0$ and $a^t\beta_1 = 0$, then

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \alpha_1 = 0, \quad \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \beta_1 = 0.$$

Let $\beta_1 = (b_1, b_2, \cdots, b_k)$, then

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \beta_1 = \begin{pmatrix} a_1b_1 & a_1b_2 & \cdots & a_1b_k \\ a_2b_1 & a_2b_2 & \cdots & a_2b_k \\ \vdots & \vdots & & \vdots \\ a_nb_1 & a_nb_2 & \cdots & a_nb_k \end{pmatrix} = 0.$$

Again $\beta_1 \neq 0$, without loss of generality, we assume $b_1 \neq 0$. As $a_i b_1 = 0 (i = 1, 2, \cdots, n)$, $a_i = 0 (i = 1, 2, \cdots, n)$, that is $a = 0$.

(2). For any fixed $e_P = \{(u_i, v_i) \mid (u_i, v_i) \in GF(q) \times GF(q)^*, 1 \leq i \leq n\}$ containing a given e_L, we assume $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n)$, then $u \in C, v \in C^*$. Therefore, there exist a unique $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k*}$ satisfying $\alpha_1 G = u$ and $\beta_1 G = v$. Next, we will consider the number of e_R which is incidence with e_P. Let $e_R = (\alpha, \beta)$, then e_R is incidence with e_P if and only if

$$\alpha = a'^t \alpha_1, \ \ \beta = a'^t \beta_1,$$

for some $a' \in GF(q)^{n*}$. If there are $a', a'' \in GF(q)^{n*}$ satisfying $\alpha = a'^t \alpha_1 = a''^t \alpha_1$ and $\beta = a'^t \beta_1 = a''^t \beta_1$, then $(a'^t - a''^t)\alpha_1 = 0$ and $(a'^t - a''^t)\beta_1 = 0$. As $\beta_1 \neq 0$, according to the above result (1), we can get $a'^t - a''^t = 0$, $a' = a''$. That is, the number of e_R which is incidence with e_P is absolutely decided by a'. As $a' \neq 0$, the number of a' is $q^n - 1$. Then $d = q^n - 1$. □

Lemma 8 *For any fixed $e_P = \{(u_i, v_i) \mid (u_i, v_i) \in GF(q) \times GF(q)^*, 1 \leq i \leq n\}$ containing a given e_L and $m = (s, t)$, let the maximum number of e_R which is incidence with e_P contained in m be e. Then $e = 1$.*

Proof: Let $e_R = (\alpha, \beta)$, for any fixed $e_P = \{(u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n)\}$ containing a given e_L, we assume $u = (u_1, u_2, \cdots, u_n) \in C, v = (v_1, v_2, \cdots, v_n) \in C^*$. Similarly, there must exist a unique $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k*}$ such that $u = \alpha_1 G$ and $v = \beta_1 G$. If e_R is incidence with e_P, then

$$\alpha = a'^t \alpha_1, \ \ \beta = a'^t \beta_1,$$

for some $a' \in GF(q)^{n*}$. It means that the number of e_R which is incidence with e_P is determined by a'. Again, $e_R \subset m$, then

$$(\alpha + s\beta)G = t.$$

By combining the above equations, we can get

$$(\alpha + s\beta)G = (a'^t \alpha_1 + s a'^t \beta_1)G$$

$$= a'^t(\alpha_1 G + s\beta_1 G) = a'^t(u + sv) = t.$$

Because (u, v) and (s, t) have been given, so the number of a' which satisfies the above equation is only one. Thus we can get the number of e_R which is incidence with e_P contained in m is at most one. That is, $e = 1$. □

Lemma 9 *For any fixed $e_R \in E_R$, let the number of e_P which is incidence with e_R be f. Then $f = (q^n - 1)(q - 1)$.*

Proof: Let $e_P = \{(u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n)\}$, we assume that $u = (u_1, u_2, \cdots, u_n)$ and $v = (v_1, v_2, \cdots, v_n)$. Similarly, there exist a pair of (α_1, β_1) satisfying $u = \alpha_1 G$ and $v = \beta_1 G$. For any fixed $e_R = (\alpha, \beta)$, if e_R is incidence with e_P, then

$$\alpha = a'^t \alpha_1, \ \ \beta = a'^t \beta_1,$$

for some $a' \in GF(q)^{n*}$. Because (α, β) has been given, so both a' and (α_1, β_1) satisfying the above equations could be found. Choose a $\lambda \in GF(q)^*$, we can get $\alpha = (\lambda a'^t)(\lambda^{-1}\alpha_1)$ and $\beta = (\lambda a'^t)(\lambda^{-1}\beta_1)$. It means that for any fixed a', the number of λ satisfying the above two equations is $q - 1$. Also, $a' \in GF(q)^{n*}$, the number of a' satisfying them is at most $(q^n - 1)(q - 1)$, then the number of corresponding (α_1, β_1) is $(q^n - 1)(q - 1)$, too. Meantime, we have known that (u, v) is determined by (α_1, β_1). Therefore, the number of (u, v) satisfying the above requirements is $(q^n - 1)(q - 1)$. That is, $f = (q^n - 1)(q - 1)$. □

Lemma 10 *For any fixed $e_R \in E_R$, $m \in M$, let the number of e_P which is incidence with e_R contained in m be g. Then $g = q^n - 1$.*

Proof: Let $e_P = \{(u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n)\}$, then we can get that $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n)$. For any fixed $e_R = (\alpha, \beta)$ and $m = (s, t)$, if e_R is incidence with e_P, then, from the Lemma 9, we can get

$$\alpha G = a'^t u, \ \ \beta G = a'^t v,$$

for some $a' \in GF(q)^{n*}$. Again, $e_P \subseteq m$, then, from the given protocol, we can get

$$t = a^t(u + sv),$$

where a is fixed in the whole theme. Let

$$a^t = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \ \ t = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix},$$

where $\gamma_i (1 \leq i \leq n)$ is the row vector of t. As u is linear independent with v, $t \neq 0$. That is, there is at least a $\gamma_i \neq 0$ satisfying that $\gamma_i = a_i(u + sv)$, then $u + sv = a_i^{-1}\gamma_i$. Let $a_i^{-1}\gamma_i = \delta$. By combining the above conclusions, we can get $(\alpha + s\beta)G =$

$a'^t(u+sv) = a'^t\delta$. Because δ and (α,β) are fixed, so the number of a' satisfying the above equations is at most one. It means that the value of (u,v) is independent with the changer of a'. At the same time, we have known $u+sv=\delta$, $u=\delta-sv$, thus u is only defined by v. As $v \in GF(q)^{n*}$, the number of v is q^n-1, then the number of (u,v) satisfying the above requirements is q^n-1. That is $g=q^n-1$. □

Lemma 11 *For any fixed $e_R=(\alpha,\beta)\in E_R$, and $m=(s,t)$, $m'=(s',t')$ with $s\neq s'$, let the largest number of e_P which is incidence with e_R contained both in m and m' be h. Then $h=1$.*

Proof: Let $e_P=\{(u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n)\}$, then we can get that $u=(u_1,u_2,\cdots,u_n)$, $v=(v_1,v_2,\cdots,v_n)$. For any fixed $e_R=(\alpha,\beta)$, $m=(s,t)$ and $m'=(s',t')$, if e_P is incidence with e_R, then, from the Lemma 9, we can get

$$\alpha G = a'^t u,\ \ \beta G = a'^t v,$$

for some $a'\in GF(q)^{n*}$. Again, $e_P\subseteq m$ and $e_P\subseteq m'$, then, from the given protocol, we can get

$$t=a^t(u+sv),\ \ t'=a^t(u+s'v),$$

where a is fixed in the whole theme. Let

$$a^t=\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix},\ \ t=\begin{pmatrix}\gamma_1\\\gamma_2\\\vdots\\\gamma_n\end{pmatrix},\ \ t'=\begin{pmatrix}\gamma_1'\\\gamma_2'\\\vdots\\\gamma_n'\end{pmatrix}.$$

As u is linear independent with v, $t\neq 0$ and $t'\neq 0$. Similarly, we can get

$$u+sv=\delta,\ \ u+s'v=\delta',$$

where δ and δ' are fixed values, hence

$$v=(s-s')^{-1}(\delta-\delta'),\ \ u=\delta-s(s-s')^{-1}(\delta-\delta').$$

By combining the above conclusions, we can get

$$\alpha G = a'^t u = a'^t[\delta - s(s-s')^{-1}(\delta-\delta')]$$

and

$$\beta G = a'^t v = a'^t[(s-s')^{-1}(\delta-\delta')].$$

Because α,β,s,s',δ and δ' are fixed values, so the number of a' satisfying the above equations is at most one. It means that the value of (u,v) is independent with the changer of a'. At the same time, from the above equation, we have known (u,v) is only fixed. Therefore, the number of (u,v) satisfying the above requirements is at most one. Then $h=1$. □

Theorem 12 *In the above construction 1, if the senders' encoding rules and the receiver's decoding rules are chosen according to a uniform probability distribution, then the largest probabilities of success for different types of deceptions are: $P_I=\frac{1}{q^{nk}}$, $P_S=\frac{1}{q^{nk}-1}$, $P_I(L)=\frac{1}{q^n-1}$, $P_{R_0}=\frac{1}{q-1}$, $P_{R_1}=\frac{1}{q^n-1}$.*

Proof: (1). From Theorem 4 and Lemma 5, we know the number of e_R contained in m is b, $|E_R|=q^{nk}(q^{nk}-1)$. Then the largest probability of an opponent's successful impersonation attack is

$$P_I=\max_{m\in M}\left\{\frac{|\{e_R\in E_R\mid e_R\subset m\}|}{|E_R|}\right\}$$
$$=\frac{b}{|E_R|}=\frac{1}{q^{nk}}.$$

(2). From Lemma 5 and Lemma 6, we know the number of e_R contained in m is b, the number of e_R contained both in m and m' is c. Then the largest probability of an opponent's successful substitution attack is

$$P_S=\max_{m\in M}$$
$$\left\{\frac{\max_{m\neq m'\in M}|\{e_R\in E_R\mid e_R\subset m, e_R\subset m'\}|}{|\{e_R\in E_R\mid e_R\subset m\}|}\right\}$$
$$=\frac{c}{b}=\frac{1}{q^{nk}-1}.$$

(3). From Lemma 7 and Lemma 8, we know that the largest probability of l malicious senders' successful impersonation attack is

$$P_I(L)=\max_{e_L\in E_L}\max_{e_L\subset e_P}$$
$$\left\{\frac{\max_{m\in M}|\{e_R\in E_R\mid e_R\subset m, p(e_R,e_P)\neq 0\}|}{|\{e_R\in E_R\mid p(e_R,e_P)\neq 0\}|}\right\}$$
$$=\frac{e}{d}=\frac{1}{q^n-1}.$$

(4). From Lemma 9 and Lemma 10, we know the number of e_P which is incidence with e_R is f, the number of e_P which is incidence with e_R contained in m is g. Then, under the current protocol, the largest probability of the receiver's successful impersonation attack is

$$P_{R_0}=\max_{e_R\in E_R}$$
$$\left\{\frac{\max_{m\in M}|\{e_P\in E_P\mid e_P\subset m, p(e_R,e_P)\neq 0\}|}{|\{e_P\in E_P\mid p(e_R,e_P)\neq 0\}|}\right\}$$

$$= \frac{g}{f} = \frac{1}{q-1}.$$

(5). From Lemma 10 and Lemma 11, we know the number of e_P which is incidence with e_R contained in m is g, the number of e_P which is incidence with e_R contained both in m and m' is h, Then, under the current protocol, the largest probability of the receiver's successful substitution attack is

$$P_{R_1} = \max_{e_R \in E_R, m \in M}$$

$$\left\{ \frac{\max_{m' \in M} \mid \{e_P \in E_P \mid e_P \subset m, m', p(e_R, e_P) \neq 0\} \mid}{\mid \{e_P \in E_P \mid e_P \subset m, p(e_R, e_P) \neq 0\} \mid} \right\}$$

$$= \frac{h}{g} = \frac{1}{q^n - 1}.$$

□

4.2 Construction 2

Let $GF(q)$ be a finite field with q elements. The set of source states $S = GF(q)^*$; the set of i-th transmitter's encoding rules $E_i = \{e_i \mid e_i \in GF(q) \times GF(q)^*\}$; the set of receiver's decoding rules $E_R = \{e_R \mid e_R \in GF(q)^k \times GF(q)^{k^*}\}$; the set of i-th transmitter's tags $T_i = \{t_i \mid t_i \in GF(q)\}$; the set of receiver's tags $T = C$, 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, that is, the row vectors of G are formed by a set of base in C.

Define the encoding map of the sender P_i $(i = 1, 2, \cdots, n.)$ as

$$f_i : S \times E_i \longrightarrow T_i, f_i(s, e_i) = u_i + sv_i (1 \leq i \leq n),$$

where $e_i = (u_i, v_i) \in E_i$.

The decoding map of the receiver R as

$$g : S \times E_R \longrightarrow T, g(s, e_R) = (\alpha + s\beta)G,$$

where $e_R = (\alpha, \beta) \in E_R$. And the synthesizing map

$$h : T_1 \times T_2 \times \cdots \times T_n \longrightarrow T,$$

$h(t_1, t_2, \cdots, t_n) = (w_1 + sw_2) + (t_1, t_2, \cdots, t_n)$, where $a = (w_1, w_2) \in GF(q)^k \times GF(q)^k$.

This code works as follows:

1. ***Key distribution phase***

(1) The arbiter randomly chooses an $e = (u, v)$ 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 $e_i = \pi_i(e) = (u_i, v_i)$ and (α_1, β_1) satisfying $\alpha_1 G = u$, $\beta_1 G = v$. Again $v \neq 0$, so $\beta_1 \neq 0$, then $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k^*}$;

(2) The arbiter also randomly selects an $a = (w_1, w_2) \in GF(q)^k \times GF(q)^k$ and calculates $e_R = (\alpha, \beta)$ such that $\alpha = w_1 + \alpha_1$, $\beta = w_2 + \beta_1$;

(3) He secretly sends e_R, e_i to the receiver R and sender $P_i (1 \leq i \leq n)$, respectively, and sends a to the synthesizer.

2. ***Broadcast phase*** If the senders want to send a source state $s \in S$ to the receiver R, P_i calculates $t_i = f_i(s, e_i) = u_i + sv_i$, and sends (s, t_i) to the synthesizer, $(1 \leq i \leq n)$.

3. ***Synthesis phase*** After the synthesizer receivers $(s, (t_1, t_2, \cdots, t_n))$, he calculates $t = h(t_1, t_2, \cdots, t_n) = (w_1 + sw_2) + (t_1, t_2, \cdots, t_n)$, then sends $m = (s, t)$ to the receiver R.

4. ***Verification phase*** When the receiver R receives $m = (s, t)$, he calculates $t' = g(s, e_R) = (\alpha + s\beta)G$. If $t = t'$, he accepts t, otherwise, he rejects it.

Next, we will show that the above construction is a well defined multi-sender authentication code with arbitration.

Lemma 13 *Let $C_i = (S, E_i, T_i; f_i)$, $1 \leq i \leq n$. Then C_i is an A-code.*

Proof: The process is similar with the Lemma 1, so we will not repeat them. □

Lemma 14 *Let $C_0 = (S, E_R, T; g)$. Then C_0 is an A-code.*

Proof: For any $s \in S$, $e_R \in E_R$, from the definition of e_R, we assume that $e_R = (\alpha, \beta)$, then $g(s, e_R) = (\alpha + s\beta)G \in C = T$; On the other hand, for any $t \in T$, choose $e_R = (\alpha, \beta) \in E_R$, let $g(s, e_R) = (\alpha + s\beta)G = t$, then $\alpha G = t - s\beta G$. Because t and $s\beta G$ are codewords, so $t - s\beta G$ is also a codeword. Thus there must exist a α satisfying the above equation. That is, g is a surjection.

If $s' \in S$ is another source state satisfying $t = g(s', e_R)$, then $(\alpha + s\beta)G = (\alpha + s'\beta)G$, $(s - s')\beta G = 0$. As $\beta \neq 0$, $\beta G \neq 0$, $s - s' = 0, s = s'$. That is, s is the uniquely source state determined by e_R and t. So $C_0 = (S, E_R, T; g)$ is an A-code. □

Lemma 15 *For any valid message $m = (s, t)$, it will be accepted by the receiver R.*

Proof: For any valid message $m = (s, t)$, there are $(w_1, w_2) \in GF(q)^k \times GF(q)^{k^*}$ and $(u, v) \in C \times C^*$ such that $t = (w_1 + sw_2)G + (u + sv)$. Similarly, from the given protocol, we can get $u = \alpha_1 G$ and $v = \beta_1 G$, where $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k^*}$.

Hence, it is easy to see that $t = (w_1 + sw_2)G + (u + sv) = (w_1 + sw_2)G + (\alpha_1 + s\beta_1)G = [(w_1 + \alpha_1) + s(w_2 + \beta_1)]G = (\alpha + s\beta)G$, where (α, β) is the key of receiver R. That is to say that message $m = (s, t)$ would be verified by the receiver, so R will accept it. □

From lemma 13 to lemma 15, we can know this construction is also well defined. Next, we will compute the parameters and the maximum probabilities of success in various attacks.

Theorem 16 *The parameters of constructed authentication code with arbitration are:* $|S| = q-1; |E_i| = q(q-1); |T_i| = q; |E_R| = q^k(q^k-1); |T| = |C| = q^k$.

Proof: The result is straightforward. □

Lemma 17 *For any* $m \in M$*, let the number of* e_R *contained in* m *be* b'*. Then* $b' = q^k - 1$.

Proof: Let $m = (s, t) \in M$, $e_R = (\alpha, \beta) \in E_R$. If $e_R \subset m$, then $(\alpha + s\beta)G = t$, $\alpha G = t - s\beta G$. Because s and t have been given, for any fixed β, we have known $t - s\beta G$ is a codeword, so there must exist a α satisfying it. That is, α is only determined by β. As $\beta \in GF(q)^{k^*}$, the number of e_R contained in m is $q^k - 1$. Then $b' = q^k - 1$. □

Lemma 18 *For any* $m = (s, t) \in M$ *and* $m' = (s', t') \in M$ *with* $s \neq s'$*, let the number of* e_R *contained both in* m *and* m' *be* c'*. Then* $c' = 1$.

Proof: Assume $e_R = (\alpha, \beta) \in E_R$. If $e_R \subset m$ and $e_R \subset m'$, then

$$(\alpha + s\beta)G = t, \quad (\alpha + s'\beta)G = t'.$$

From the above two equations, we can get that $(s - s')\beta G = t - t'$, $\beta G = (s - s')^{-1}(t - t')$. Because (s, t) and (s', t') have been given, at the same time, we can get $(s - s')^{-1}(t - t')$ is a fixed codeword, so β is also fixed. Again, we have known α is only defined by β from Lemma 17, then the number of e_R contained both in m and m' is only one. That is $c' = 1$. □

Lemma 19 *For any fixed* $e_P = \{(u_i, v_i) \mid (u_i, v_i) \in GF(q) \times GF(q)^*, 1 \leq i \leq n\}$ *containing a given* e_L*, let the number of* e_R *which is incidence with* e_P *be* d'*. Then* $d' = q^k(q^k - 1)$.

Proof: Let $e_R = (\alpha, \beta) \in E_R$, for any fixed $e_P = \{(u_i, v_i) \mid (u_i, v_i) \in GF(q) \times GF(q)^*, 1 \leq i \leq n\}$ containing a given e_L, we assume $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n)$, then $u \in C, v \in C^*$. Therefore, there exist a unique $(\alpha_1, \beta_1) \in GF(q)^k \times GF(q)^{k^*}$ satisfying $\alpha_1 G = u$ and $\beta_1 G = v$. Next, we will consider the number of e_R which is incidence with e_P. If e_R is incidence with e_P, then

$$\alpha = w_1' + \alpha_1, \quad \beta = w_2' + \beta_1,$$

for some $a' = (w_1', w_2') \in GF(q)^k \times GF(q)^k$. Hence, (α, β) is only determined by (w_1', w_2') because of their linear relationship. As $(w_1', w_2') \in GF(q)^k \times GF(q)^k$ and $\beta \neq 0$, the number of (w_1', w_2') is $q^k(q^k - 1)$. Thus the number of e_R which is incidence with e_P is $q^k(q^k - 1)$. That is $d' = q^k(q^k - 1)$. □

Lemma 20 *For any fixed* $e_P = \{(u_i, v_i) \mid (u_i, v_i) \in GF(q) \times GF(q)^*, 1 \leq i \leq n\}$ *containing a given* e_L *and* $m \in M$*, let the maximum number of* e_R *which is incidence with* e_P *contained in* m *be* e'*. Then* $e' = q^k - 1$.

Proof: Let $e_R = (\alpha, \beta) \in E_R$, for any fixed $e_P = \{(u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n)\}$ containing a given e_L and $m = (s, t)$, if e_R is incidence with e_P, according to the Lemma 19, we can get

$$\alpha G = w_1' G + u, \quad \beta G = w_2' G + v,$$

for some $a' = (w_1', w_2') \in GF(q)^k \times GF(q)^k$. It means that the number of e_R which is incidence with e_P is determined by a'. Again, $e_R \subset m$, then

$$(\alpha + s\beta)G = t.$$

By combining the above equations, we can get

$$w_1' G + sw_2' G + u + sv = (w_1' + sw_2')G + u + sv = t,$$

then $(w_1' + sw_2')G = t - (u + sv)$. Because (s, t) and (u, v) have been given, meantime, $t - (u + sv) \in C$ which means that $t - (u + sv)$ is a fixed codeword, so $w_1' + sw_2'$ is also fixed. Let $w_1' + sw_2' = \delta$, where δ is a fixed codeword, then $w_1' = \delta - sw_2'$, thus w_1' is only determined by w_2'. As $w_2' \in GF(q)^k$ and $\beta \neq 0$, the number of w_2' is $q^k - 1$. Then the number of (w_1', w_2') which satisfies the above equation is $q^k - 1$. Hence the number of e_R which is incidence with e_P contained in m is $q^k - 1$, too. So $e' = q^k - 1$. □

Lemma 21 *For any fixed* $e_R \in E_R$*, let the number of* e_P *which is incidence with* e_R *be* f'*. Then* $f' = q^k(q^k - 1)$.

Proof: Let $e_P = \{(u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n)\} \in E_P$, for any fixed $e_R = (\alpha, \beta) \in E_R$, if e_R is incidence with e_P, according to the Lemma 19, we can get that

$$\alpha = w_1' + \alpha_1, \quad \beta = w_2' + \beta_1,$$

for some $(w_1', w_2') \in GF(q)^k \times GF(q)^k$. Then $\alpha_1 = \alpha - w_1', \beta_1 = \beta - w_2'$, thus (α_1, β_1) is only defined by (w_1', w_2'). As $(w_1', w_2') \in GF(q)^k \times GF(q)^k$, the number of (w_1', w_2') which satisfies the above equations is $q^k q^k$. Again, $\beta \neq 0$, hence, the number of (α_1, β_1) is $q^k(q^k - 1)$. At the same time, from the Lemma 19, we have known that (u, v) is only determined by (α_1, β_1), so the number of (u, v) satisfying the above requirements is $q^k(q^k - 1)$. Then $f' = q^k(q^k - 1)$. □

Lemma 22 *For any fixed $e_R \in E_R$, $m \in M$, let the number of e_P which is incidence with e_R contained in m be g'. Then $g' = q^k - 1$.*

Proof: Let $e_P = \{(u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n)\} \in E_P$, assume $u = \{u_1, u_2 \cdots, u_n\}$ and $v = \{v_1, v_2 \cdots, v_n\}$. For any fixed $e_R = (\alpha, \beta)$ and $m = (s, t)$, if e_P is incidence with e_R, according to the lemma 19, we can get

$$\alpha G = w_1' G + u, \ \ \beta G = w_2' G + v,$$

for some $(w_1', w_2') \in GF(q)^k \times GF(q)^k$. Again, $e_P \subset m$, then, from the given protocol, we can get

$$t = (w_1 + sw_2)G + (u + sv),$$

where (w_1, w_2) is fixed in the whole theme. Thus we can get $u + sv = t - (w_1 + sw_2)G$. By combining the above conclusions, we can get

$$(\alpha + s\beta)G = (w_1' + sw_2')G + (u + sv)$$

$$= (w_1' + sw_2')G + t - (w_1 + sw_2)G,$$

then $(w_1' + sw_2')G = (\alpha + s\beta)G + (w_1 + sw_2)G - t$. Because $(\alpha, \beta), (s, t)$ and (w_1, w_2) have been given, so the value of $w_1' + sw_2'$ is fixed. Let $w_1' + sw_2' = \delta'$, where δ' is a fixed value, then $w_1' = \delta' - sw_2'$, thus w_1' is only determined by w_2'. As $w_2' \in GF(q)^k$ and $w_2' \neq \beta$, the number of w_2' is $q^k - 1$, then the number of (w_1', w_2') is $q^k - 1$, too. At the same time, according to the above equation, we have known (u, v) is only defined by (w_1', w_2'), therefore, the number of (u, v) satisfying the above requirements is $q^k - 1$. That is, $g' = q^k - 1$. □

Lemma 23 *For any fixed $e_R = (\alpha, \beta) \in E_R$, $m = (s, t)$ and $m' = (s', t')$ with $s \neq s'$, let the largest number of e_P which is incidence with e_R contained both in m and m' be h'. Then $h' = 1$.*

Proof: Let $e_P = \{(u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n)\} \in E_P$, assume $u = \{u_1, u_2 \cdots, u_n\}$ and $v = \{v_1, v_2 \cdots, v_n\}$. For any fixed $e_R = (\alpha, \beta) \in E_R$, $m = (s, t)$ and $m' = (s', t')$, if e_P is incidence with e_R, similarly, we can get

$$\alpha G = w_1' G + u, \ \ \beta G = w_2' G + v,$$

for some $(w_1', w_2') \in GF(q)^k \times GF(q)^k$. Again, $e_P \subset m$ and $e_P \subset m'$, then, from the given protocol, we get

$$t = (w_1 + sw_2)G + (u + sv)$$

and

$$t' = (w_1 + s'w_2)G + (u + s'v),$$

where (w_1, w_2) is fixed in the whole theme. Thus we get

$$v = (s - s')^{-1}(t - t') - w_2 G$$

and

$$u = t - s(s - s')^{-1}(t - t') - w_1 G.$$

At the same time, by combining the above conclusions, we can get

$$w_2' G = \beta G - v = \beta G - (s - s')^{-1}(t - t') + w_2 G$$

and

$$w_1' G = \alpha G - u = \alpha G - t + s(s - s')^{-1}(t - t') + w_1 G.$$

Because $(\alpha, \beta), (s, t), (s', t')$ and (w_1, w_2) have been given, so the value of (w_1', w_2') could only be fixed. It means that (u, v) satisfying the above requirements is independent with the changer of (w_1', w_2'). Also, according to the above results, we have seen that (u, v) is a fixed value. Thus the number of (u, v) satisfying the above requirements is at most one, so $h' = 1$. □

Theorem 24 *In the above construction 2, if the senders' encoding rules and the receiver's decoding rules are chosen according to a uniform probability distribution, then the largest probabilities of success for different types of attacks are:*

$$P_I = \frac{1}{q^k}, \quad P_S = \frac{1}{q^k - 1}, \quad P_I(L) = \frac{1}{q^k},$$
$$P_{R_0} = \frac{1}{q^k}, \quad P_{R_1} = \frac{1}{q^k - 1}.$$

Proof: (1). From Theorem 16 and Lemma 17, we know the number of e_R contained in m is b', $|E_R| = q^k(q^k - 1)$. Then the largest probability of an opponent's successful impersonation attack is

$$\begin{aligned} P_I &= \max_{m \in M} \left\{ \frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|} \right\} \\ &= \frac{b'}{|E_R|} = \frac{1}{q^k}. \end{aligned}$$

(2). From Lemma 17 and Lemma 18, we know the number of e_R contained in m is b', the number

of e_R contained both in m and m' is c'. Then the largest probability of an opponent's successful substitution attack is

$$\begin{aligned} P_S &= \max_{m\in M}\left\{\frac{\max\limits_{m\neq m'\in M}|\{e_R\in E_R|e_R\subset m,e_R\subset m'\}|}{|\{e_R\in E_R|e_R\subset m\}|}\right\} \\ &= \frac{c'}{b'}=\frac{1}{q^k-1}. \end{aligned}$$

(3). From Lemma 19 and Lemma 20, we know that the largest probability of l malicious senders' successful impersonation attack is

$$\begin{aligned} P_I(L) &= \max_{e_L\in E_L}\max_{e_L\subset e_P} \\ &\quad \left\{\frac{\max\limits_{m\in M}|\{e_R\in E_R|e_R\subset m,p(e_R,e_P)\neq 0\}|}{|\{e_R\in E_R|p(e_R,e_P)\neq 0\}|}\right\} \\ &= \frac{e'}{d'}=\frac{1}{q^k}. \end{aligned}$$

(4). From Lemma 21 and Lemma 22, we know the number of e_P which is incidence with e_R is f', the number of e_P which is incidence with e_R contained in m is g'. Then, under the current protocol, the largest probability of the receiver's successful impersonation attack is

$$\begin{aligned} P_{R_0} &= \max_{e_R\in E_R}\left\{\frac{\max\limits_{m\in M}|\{e_P\in E_P|e_P\subset m,p(e_R,e_P)\neq 0\}|}{|\{e_P\in E_P|p(e_R,e_P)\neq 0\}|}\right\} \\ &= \frac{g'}{f'}=\frac{1}{q^k}. \end{aligned}$$

(5). From Lemma 22 and Lemma 23, we know the number of e_P which is incidence with e_R contained in m is g', the number of e_P which is incidence with e_R contained both in m and m' is h', Then, under the current protocol, the largest probability of the receiver's successful substitution attack is

$$\begin{aligned} P_{R_1} &= \max_{e_R\in E_R,m\in M} \\ &\quad \left\{\frac{\max\limits_{m'\in M}|\{e_P\in E_P|e_P\subset m,m',p(e_R,e_P)\neq 0\}|}{|\{e_P\in E_P|e_P\subset m,p(e_R,e_P)\neq 0\}|}\right\} \\ &= \frac{h'}{g'}=\frac{1}{q^k-1}. \end{aligned}$$

□

5 Conclusion

Multi-sender authentication codes are important cryptography in secure group communication. In this paper, we firstly gave a formal definition of multi-transmitter A-code with arbitration and some calculating formulas. Next, we established a link between linear code and multi-sender A-code with arbitration by giving two constructions that can be used to derive multi-sender authentication codes from linear codes. Finally we calculated the parameters and the maximum probabilities of success in possible attacks. At the same time, we can find that the best chances of success in the corresponding attacks would be greatly reduced when the number n and k are large enough. From the aspect of an opponent's attacks, the first construction is more optimal than the second one.

Acknowledgements: The research was supported by the National Natural Science Foundation of China(61179026), the Fundamental Research Funds of the Central Universities(ZXH2012K003) and the Scientific Research Project of Civil Aviation University of China(2012KYM01).

References:

[1] E. N. Gilbert, F. J. MacWilliamsand, N. J. A. Sloane, codes which detect deception, *Bell System Technical Journal*, Vol. 53, 1974, pp. 405-424.

[2] G. J. Simmons, Message authentication with Arbitration of Transmitter/Receiver Disputes Advances in Cryptoligy-Crypto, *Lecture Notes in Computer Science 304*, Berlin: Springer-verlag, Vol.87, 1988, pp. 151-165.

[3] Wan Zhexian, Construction of Cartesian Authentication Codes from Unitary Geometry, *Designs, Codes and Cryptology*, Vol.2, 1992, pp. 333-356.

[4] Ma Wenping, Wang Xinmei, A Construction of Authentication Codes with Arbitration Based on Symplectic Spaces, *CHINESE J. COMPUTERS*, Vol.22, No.9, 1999, pp. 949-952.

[5] Gao You, Shi Xinhua and Wang Hongli, Construction of Authentication Codes with Arbitration from Symplectic Geometry over Finite Fields, *Acta Scientiarum Naturalium Universitatis Nankaiensis*, Vol.41, 2008, pp. 72-77.

[6] Chen Shangdi and Zhao Dawei, New Construction of Authentication Codes with Arbitration from Pseudo-sympletic Geometry over Finite Fields, *ARS COMBINATORIA*, Vol.97, 2010, pp. 453-465.

[7] Li Ruihu and Li Zunxian, Construction of A^2-codes from Sympletic Geometry, *Journal of Shanxi Normal University (Natural Science)*, Vol. 26, No.4, 1998, pp. 10-15.

[8] Ma Wenping, Wang Xinmei, A Few New Structure Methods of Multi-sender Authentication Codes, *Electronics College Journal*, Vol. 28, No.4, 2000, pp. 117-119.

[9] Y. Desmedt, Y. Frankel and M. Yung, Multer-receiver/Multi-sender network security: efficient authenticated multicast/feedback, *IEEE infocom*, Vol.92, 1992, pp. 2045-2054.

[10] Du Qingling, Lv Shuwang, Bounds and Construction for Multi-sender Authentication code, *Computer Engineering and Applications*, Vol. 40, No.10, 2004, pp. 9-11.

[11] K. M. Martin, R. Safavi-Naini, Multisender authentication systems with unconditional security, *Lecture Notes in Computer Science*, Vol. (1334/1997), 1997, pp. 130-143.

[12] R. Aparna, 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.

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