Research Article

A Construction of Multisender Authentication Codes with Sequential Model from Symplectic Geometry over Finite Fields

Shangdi Chen[1] and Chunli Yang[2]

[1] *College of Science, Civil Aviation University of China, Tianjin 300300, China*
[2] *Information Security Center, Beijing University of Posts and Telecommunications, P.O. Box 126, Beijing 100876, China*

Correspondence should be addressed to Shangdi Chen; sdchen@cauc.edu.cn

Multisender 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 multisender authentication codes with sequential model from symplectic geometry over finite fields, and the parameters and the maximum probabilities of deceptions are also calculated.

1. Introduction

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 that the information is integrated. Digital signature and authentication codes are two important means of authenticating the information and provide good service in the network. In practical, digital signature is computationally secure assuming that the computing power of adversary is limited and a mathematical problem is intractable and complex. However, authentication codes are generally safe (unconditional secure) and relatively simple. In the 1940s, C. E. Shannon first put forward the concept of perfect secrecy authentication system using the information theory. In the 1980s, information theory method had been applied to the problem of authentication by G. J. Simmons; then authentication codes became the foundation for constructing unconditionally secure authentication system. In 1974, Gilbert et al. constructed the first authentication code [1], which is a landmark in the development of authentication theory. During the same period, Simmons independently studied the authentication theory and established three participants and four participants certification models [2]. The famous mathematician Wan Zhexian constructed an authentication code without arbitration from the subspace of the classical

geometry [3]. In the case of transmitter and receiver being not honest, Ma et al. constructed a series of authentication codes with arbitration [4–9]. Xing et al. constructed authentication codes using algebraic curve and nonlinear functions, respectively [10, 11]. Safavi-Naini and Wang gave some results on multireceiver authentication codes [12]. Chen et al. made great contributions on multisender authentication codes from polynomials and matrices [13–19].

With the rapid development of information science, the traditional one-to-one authentication codes have been unable to meet the requirements of network communication, thus making the study of multiuser authentication codes particularly important. Multiuser authentication code is a generalization of traditional two-user authentication code. It can be divided into two cases: one is a sender and many receivers authentication codes; the other one is many senders and a receiver authentication codes. We call the former as multireceiver authentication codes and the latter as multisender authentication codes. Safavi-Naini R gave some results on multireceiver authentication codes using the subspace of the classical geometry, while there are only some multisender authentication codes using polynomials and matrices to construct. We present the first construction multisender authentication code using the subspace of the classical geometry, specifically symplectic geometry.

The main contribution of our paper is constructing a multi-sender authentication code using symplectic geometry.

Furthermore, we calculate the corresponding parameters and the maximum probabilities of deceptions.

The paper is organised as follows. Section 2 gives the models of multisender authentication codes. In Section 3, we provide the calculation formulas on probability of success in attacks by malicious groups of senders. In Section 4, we give some definitions and properties on geometry of symplectic groups over finite fields. In Section 5, a construction of multisender authentication codes with sequential model from symplectic geometry over finite fields is given; then the parameters and the maximum probabilities of deceptions are also calculated. We give a comparison with the other construction of multisender authentication [19] in Section 6.

2. Models of Multisender Authentication Codes

We review the concepts of authentication codes which can be extracted from [20].

Definition 1 (see [20]). A systematic Cartesian authentication code C is a 4-tuple $(S, E, T; f)$, where S is the set of source states, E is the set of keys, T is the set of authenticators, and $f : S \times E \to T$ is the authentication mapping. The message space $M = S \times T$ is the set of all possible messages.

In the actual computer network communications, multisender authentication codes include sequential models and simultaneous models. Sequential models are that each sender uses his own encoding rules to encode a source state orderly, and the last sender sends the encoded message to the receiver; then the receiver receives the message and verifies whether the message is legal or not. Simultaneous models are that all senders use their own encoding rules to encode a source state simultaneously; 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 the following we will give out the working principles of two modes of multisender authentication codes and the protocols that the participants should follow.

Definition 2 (see [17]). In sequential model, there are three participants: a group of senders $U = \{U_1, U_2, \ldots, U_n\}$; a Key Distribution Center (KDC), for the distribution keys to senders and receiver; a receiver who receives the authenticated message and verifies the message true or not. The code works as follows: each sender and receiver has their own Cartesian authentication code, respectively. It is used to generate part of the message and verify authenticity of the received message. Sender's authentication codes are called branch authentication codes, and receiver's authentication code is called channel authentication code. Let $(S_i, E_i, T_i; f_i)$, $i = 1, 2, \ldots, n$, be the ith sender's Cartesian authentication codes, and let $T_{i-1} \subset S_i$, $1 \le i \le n$, $(S, E, T; f)$ be the receiver's Cartesian authentication code, and let $S = S_1$, $T = T_i, \pi_i : E \to E_i$ be a subkey generation algorithm. For authenticating

a message, the senders and the receiver should comply with protocols:

  (1) KDC randomly selects an $e \in E$ and secretly sends it to the receiver R and sends $e_i = \pi_i(e)$ to the ith sender $U_i, i = 1, 2, \ldots, n$;

  (2) if the senders would like to send a source state s to the receiver R, U_1 calculates $t_1 = f_1(s, e_1)$ and then sends t_1 to U_2 through an open channel; U_2 receives t_1 and calculates $t_2 = f_2(t_1, e_2)$ and then sends t_2 to U_3 through an open channel. In general, U_i receives t_{i-1} and calculates $t_i = f_i(t_{i-1}, e_i)$ and then sends t_i to U_{i+1} through an open channel, $1 < i < n$. U_n receives t_{n-1} and calculates $t_n = f_n(t_{n-1}, e_n)$ and then sends $m = (s, t_n)$ through an open channel to the receiver R;

  (3) when the receiver receives the message $m = (s, t_n)$, he checks the authenticity by verifying whether $t_n = f(s, e)$ or not. If the equality holds, the message is regarded as authentic and is accepted. Otherwise, the message is rejected.

Definition 3 (see [17]). In simultaneous model of a multisender authentication code, there are four participants: a group of senders $U = \{U_1, U_2, \ldots, U_n\}$; a Key Distribution Center (KDC), for the distribution keys to senders and receiver; a synthesizer C who only runs the trusted synthesis algorithm; a receiver who receives the authenticated message and verifies the message true or not. The code works as follows: each sender and receiver has their own Cartesian authentication code, respectively. It is used to generate part of the message and verify the received message. Sender's authentication codes are called branch authentication codes, and receiver's authentication code is called channel authentication code. Let $(S_i, E_i, T_i; f_i)$, $i = 1, 2, \ldots, n$, be the sender's Cartesian authentication codes, let $(S, E, T; f)$ be the receiver's Cartesian authentication code, let $g : T_1 \times T_2 \times \cdots \times T_n \to T$ be the synthesis algorithm, and let $\pi_i : E \to E_i$ be a subkey generation algorithm. For authenticating a message, the senders and the receiver should comply with protocols:

  (1) KDC randomly selects a encoding rule $e \in E$ and secretly sends it to the receiver R and sends $e_i = \pi_i(e)$ to the ith sender $U_i, i = 1, 2, \ldots, n$;

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

  (3) the synthesizer C receives the messages $m_i = (s, t_i)$, $i = 1, 2, \ldots, n$, and calculates $t = g(t_1, t_2, \ldots, t_n)$ using the synthesis algorithm g; then sends message $m = (s, t)$ to the receiver R;

  (4) when the receiver receives the message $m = (s, t)$, he checks the authenticity by verifying whether $t = f(s, e)$ or not. If the equality holds, the message is regarded as authentic and is accepted. Otherwise, the message is rejected.

3. Probabilities of Deceptions

We assume that the arbitrator (KDC) and the synthesizer (C) are credible; though they know the senders' and receiver's encoding rules, they do not participate in any communication activities. When transmitter and receiver are disputing, the arbitrator settles it. At the same time, assume that the system follows Kerckhoff's principle which the other information of the whole system is public except the actual used keys. Assume that the source state space S and the receiver's decoding rules space E_R are according to a uniform probability distribution; then the probability distribution of message space M and tag space T is determined by the probability distribution of S and E_R. In a multisender authentication system, assume that the whole senders cooperate to form a valid message; that is, all senders as a whole and receiver are reliable. But there are some malicious senders which they together cheat the receiver; the part of senders and receiver are not credible; they can take impersonation attack and substitution attack.

Assume that $U_1, U_2, \ldots, U_n$ are senders, R is a receiver, and E_i is the encoding rules of U_i, $1 \leq i \leq n$. E_R is the decoding rules of receiver R. $L = \{i_1, i_2, \ldots, i_l\} \subset \{1, 2, \ldots, n\}$, $l < n$, $U_L = \{U_{i_1}, U_{i_2}, \ldots, U_{i_l}\}$, $E_L = \{E_{i_1}, E_{i_2}, \ldots, E_{i_l}\}$.

Impersonation Attack. U_L, after receiving their secret keys, sends a message m to receiver. U_L is successful if the receiver accepts it as legitimate message. Denote $P_I[L]$ as the maximum probability of success of the impersonation attack. It can be expressed as

$$P_I[L] = \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accepted by } R \mid e_L). \quad (1)$$

Substitution Attack. U_L, after observing a legitimate message, substitutes it with another message m'. U_L is successful if m' is accepted by receiver as authentic. Denote $P_S[L]$ as the maximum probability of success of the substitution attack. It can be expressed as

$$P_S[L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(m' \text{ is accepted by } R \mid m, e_L). \quad (2)$$

4. Symplectic Geometry

In this section, we give some definitions and properties on geometry of symplectic groups over finite fields, which can be extracted from [20].

Let $\mathbb{F}_q$ be a finite field with q elements, $n = 2\nu$ and define the $2\nu \times 2\nu$ alternate matrix

$$K = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}. \quad (3)$$

The symplectic group of degree 2ν over $\mathbb{F}_q$, denoted by $Sp_{2\nu}(\mathbb{F}_q)$, is defined to be the set of matrices

$$Sp_{2\nu}(\mathbb{F}_q) = \{T \mid TK^tT = K\}, \quad (4)$$

with matrix multiplication as its group operation. Let $\mathbb{F}_q^{(2\nu)}$ be the 2ν-dimensional row vector space over $\mathbb{F}_q$. $Sp_{2\nu}(\mathbb{F}_q)$ has an action on $\mathbb{F}_q^{(2\nu)}$ defined as follows:

$$\mathbb{F}_q^{(2\nu)} \times Sp_{2\nu}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^{(2\nu)},$$
$$((x_1, x_2, \ldots, x_{2\nu}), T) \longrightarrow (x_1, x_2, \ldots, x_{2\nu}) T. \quad (5)$$

The vector space $\mathbb{F}_q^{(2\nu)}$ together with this action of $Sp_{2\nu}(\mathbb{F}_q)$ is called the symplectic space over $\mathbb{F}_q$.

Let P be an m-dimensional subspace of $\mathbb{F}_q^{(2\nu)}$. We use the same latter P to denote a matrix representation of P; that is, P is an $m \times 2\nu$ matrix of rank m such that its rows form a basis of P. The PK^tP is alternate. Assume that it is of rank $2s$; then P is called a subspace of type (m, s). It is known that subspaces of type (m, s) exist in $\mathbb{F}_q^{(2\nu)}$ if and only if

$$2s \leq m \leq \nu - s. \quad (6)$$

It is also known that subspaces of the same type form an orbit under $Sp_{2\nu}(\mathbb{F}_q)$. Denote by $N(m, s; 2\nu)$ the number of subspaces of type (m, s) in $\mathbb{F}_q^{(2\nu)}$.

Denote by $P^\perp$ the set of vectors which are orthogonal to every vector of P; that is,

$$P^\perp = \{y \in \mathbb{F}_q^{(2\nu)} \mid yK^tx = 0 \text{ for all } x \in P\}. \quad (7)$$

Obviously, $P^\perp$ is a $(2\nu - m)$-dimensional subspace of $\mathbb{F}_q^{(2\nu)}$.

Readers can refer to [15] for notations and terminology, which are not explained, on symplectic geometry of classical groups over finite fields.

5. Construction

Let $\mathbb{F}_q$ be a finite field with q elements. Assume that $1 < n < r < \nu$. $U = \langle e_1, e_2, \ldots, e_n \rangle$; then $U^\perp = \langle e_1, \ldots, e_\nu, e_{\nu+n+1}, \ldots, e_{2\nu} \rangle$. Let $W_i = \langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n \rangle$; then $W_i^\perp = \langle e_1, \ldots, e_\nu, e_{\nu+i}, e_{\nu+n+1}, \ldots, e_{2\nu} \rangle$. The set of source states $S = \{s \mid s \text{ is a subspace of type } (2r - n, r - n) \text{ and } U \subset s \subset U^\perp\}$; the set of ith sender's encoding rules $E_i = \{e_i \mid e_i \text{ is a subspace of type } (n+1, 1), U \subset e_i \text{ and } e_i \perp W_i\}$, $1 \leq i \leq n$; the set of receiver's decoding rules $E_R = \{e_R \mid e_R \text{ is a subspace of type } (2n, n) \text{ and } U \subset e_R\}$; the set of tags $T_i = \{t_i \mid t_i \text{ is a subspace of type } (2r - n + i, r - n + i) \text{ and } U \subset t_i\}$, $1 \leq i \leq n$.

Define the encoding maps:

$$f_1 : S \times E_1 \longrightarrow T_1, \qquad f_1(s, e_1) = s + e_1,$$
$$f_i : T_{i-1} \times E_i \longrightarrow T_i, \quad f_i(t_{i-1}, e_i) = t_{i-1} + e_i, \quad 2 \leq i \leq n. \quad (8)$$

Define the decoding map:

$$f : S \times E_R \longrightarrow T_n, \qquad f(s, e_R) = s + e_R. \quad (9)$$

This code works as follows.

(1) *Key Distribution.* First, the KDC does a list L of senders; assume that $L = \{1, 2, \ldots, n\}$. Then, the KDC randomly chooses a subspace $e_R \in E_R$ and privately sends e_R to the receiver R. Last, the KDC randomly chooses a subspace $e_i \in E_i$ and $e_i \subset e_R$, then privately sends e_i to the ith sender, $1 \leq i \leq n$.

(2) *Broadcast.* For a source state $s \in S$, the sender U_1 calculates $t_1 = s + e_1$ and sends (s, t_1) to U_2. The sender U_2 calculates $t_2 = t_1 + e_2$ and sends (s, t_2) to U_3. Finally, the sender U_n calculates $t_n = t_{n-1} + e_n$ and sends $m = (s, t_n)$ to the receiver R.

(3) *Verification.* Since the receiver R holds the decoding rule e_R, R accepts m as authentic if $t_n = s + e_R$. Otherwise, it is rejected by R.

Lemma 4. *Let $C = (S, E_R, T_n; f)$, $C_1 = (S, E_1, T_1; f_1)$, $C_i = (T_{i-1}, E_i, T_i; f_i)$ $(2 \leq i \leq n)$; then C, C_1, C_i are all Cartesian authentication codes.*

Proof. First, we show that C is a Cartesian authentication code.

(1) For $s \in S, e_R \in E_R$. Let

$$s = \begin{pmatrix} U \\ Q \end{pmatrix} \begin{matrix} n \\ 2(r-n) \end{matrix},$$
$$e_R = \begin{pmatrix} U \\ V \end{pmatrix} \begin{matrix} n \\ n. \end{matrix} \tag{10}$$

From the definition of s and e_R, we can assume that

$$\begin{pmatrix} U \\ Q \end{pmatrix} K \; {}^t\begin{pmatrix} U \\ Q \end{pmatrix} = \begin{pmatrix} 0^{(n)} & 0 & 0 \\ 0 & 0 & I^{(r-n)} \\ 0 & -I^{(r-n)} & 0 \end{pmatrix},$$
$$\begin{pmatrix} U \\ V \end{pmatrix} K \; {}^t\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} \\ -I^{(n)} & 0 \end{pmatrix}. \tag{11}$$

Obviously, we have $v \notin s$ for any $v \in V$ and $v \neq 0$. Therefore,

$$t_n = s + e_R = \begin{pmatrix} U \\ V \\ Q \end{pmatrix},$$
$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} K \; {}^t\begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} & 0 & 0 \\ -I^{(n)} & 0 & * & * \\ 0 & * & 0 & I^{(r-n)} \\ 0 & * & -I^{(r-n)} & 0 \end{pmatrix}. \tag{12}$$

From above, t_n is a subspace of type $(2r, r)$ and $U \subset t_n$; that is, $t_n \in T_n$.

(2) For $t_n \in T_n$, t_n is a subspace of type $(2r, r)$ containing U. So there is subspace $V \subset t_n$, satisfying

$$\begin{pmatrix} U \\ V \end{pmatrix} K \; {}^t\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} \\ -I^{(n)} & 0 \end{pmatrix}. \tag{13}$$

Then, we can assume that $t_n = \begin{pmatrix} U \\ V \\ Q \end{pmatrix}$, satisfying

$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} K \; {}^t\begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} & 0 & 0 \\ -I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-n)} \\ 0 & 0 & -I^{(r-n)} & 0 \end{pmatrix}. \tag{14}$$

Let $s = \begin{pmatrix} U \\ Q \end{pmatrix}$; then s is a subspace of type $(2r-n, r-n)$ and $U \subset s \subset U^\perp$; that is, $s \in S$ is a source state. For any $v \in V$ and $v \neq 0$, we have $v \notin s$ and $V \cap U^\perp = \{0\}$. Therefore, $t_n \cap U^\perp = \begin{pmatrix} U \\ Q \end{pmatrix} = s$. Let $e_R = \begin{pmatrix} U \\ V \end{pmatrix}$; then e_R is a transmitter's encoding rule satisfying $t_n = s + e_R$.

If s' is another source state contained in t_n, then $U \subset s' \subset U^\perp$. Therefore, $s' \subset t_n \cap U^\perp = s$, while $\dim s' = \dim s$, so $s' = s$. That is, s is the uniquely source state contained in t_n.

Similarly, we can show that C_1 and C_i $(2 \leq i \leq n)$ are also Cartesian authentication code. $\qquad\square$

From Lemma 4, we know that such construction of multisender authentication codes is reasonable. Next we compute the parameters of this code.

Lemma 5. *The number of the source states is $|S| = N(2(r-n), r-n; 2(\nu-n))$.*

Proof. For any $s \in S$, since $U \subset s \subset U^\perp$, s has the form

$$s = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & P_2 & 0 & P_4 \end{pmatrix} \begin{matrix} n \\ 2(r-n) \end{matrix} \tag{15}$$
$$\begin{matrix} n & \nu-n & n & \nu-n, \end{matrix}$$

where (P_2, P_4) is a subspace of type $(2(r-n), r-n)$ in the symplectic space $F_q^{2(\nu-n)}$. Therefore, the number of the source states is $|S| = N(2(r-n), r-n; 2(\nu-n))$. $\qquad\square$

Lemma 6. *The number of the ith sender's encoding rules is $|E_i| = q^{2(\nu-n)}$.*

Proof. For any $e_i \in E_i$, e_i is a subspace of type $(n+1, 1)$ containing U and e_i is orthogonal to W_i. So we can assume that $e_i = {}^t(e_1, \ldots, e_n, u)$, where $u = (x_1 \; x_2 \; \cdots \; x_{2\nu})$. Obviously, $x_1 = \cdots = x_n = x_{\nu+1} = \cdots = x_{\nu+i-1} = x_{\nu+i+1} = \cdots = x_{\nu+n} = 0$, $x_{\nu+i} = 1$, and $x_{n+1}, \ldots, x_\nu, x_{\nu+n+1}, \ldots, x_{2\nu}$ arbitrarily. Therefore, $|E_i| = q^{2(\nu-n)}$. $\qquad\square$

Lemma 7. *The number of the receiver's decoding rules is $|E_R| = q^{2n(\nu-n)}$.*

Proof. For any $e_R \in E_R$, since e_R is a subspace of type $(2n, n)$ containing U, e_R has the form

$$e_R = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & Q_2 & I^{(n)} & Q_4 \end{pmatrix} \begin{matrix} n \\ n \end{matrix} \tag{16}$$
$$\begin{matrix} n & \nu-n & n & \nu-n, \end{matrix}$$

where Q_2, Q_4 are arbitrary matrices. Therefore, $|E_R| = q^{2n(\nu-n)}$. $\qquad\square$

Lemma 8. *(1) The number of decoding rules e_R contained in t_n is $q^{2n(r-n)}$;*

(2) the number of the tags is $|T_n| = q^{2n(v-r)}N(2(r-n), r-n; 2(v-n))$.

Proof. (1) For any $t_n \in T_n$, t_n is a subspace of type $(2r, r)$ and $U \subset t_n$. We assume that t_n has the form

$$t_n = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-n)} & 0 \\ n & r-n & v-r & n & r-n & v-r. \end{pmatrix} \begin{matrix} n \\ r-n \\ n \\ r-n \end{matrix} \tag{17}$$

If $e_R \subset t_n$, then we can assume that

$$e_R = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(n)} & R_5 & 0 \\ n & r-n & v-r & n & r-n & v-r, \end{pmatrix} \begin{matrix} n \\ n \end{matrix} \tag{18}$$

where R_2, R_5 are arbitrary matrices. Therefore, the number of e_R contained in t_n is $q^{2n(r-n)}$.

(2) We know that a tag contains only one source state and the number of decoding rules e_R contained in t_n is $q^{2n(r-n)}$. Therefore, we have $|T_n| = |S||E_R|/q^{2n(r-n)} = q^{2n(v-r)}N(2(r-n), r-n; 2(v-n))$. □

Theorem 9. *The parameters of the above constructed multi-sender authentication code are*

$$|S| = N(2(r-n), r-n; 2(v-n));$$
$$|E_i| = q^{2(v-n)};$$
$$|E_R| = q^{2n(v-n)};$$
$$|T_n| = q^{2n(v-r)}N(2(r-n), r-n; 2(v-n)). \tag{19}$$

Without loss of generality, we can assume that $U_L = \{U_1, U_2, \ldots, U_l\}$, $E_L = \{E_1 \times \cdots \times E_l\}$, where $l < n$.

Lemma 10. *For any $e_L = (e_1, e_2, \ldots, e_l) \in E_L$, the number of e_R containing e_L is $q^{2(n-l)(v-n)}$.*

Proof. For any $e_L = (e_1, e_2, \ldots, e_l) \in E_L$, we can assume that

$$e_L = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & P_3 & I^{(l)} & 0 & P_6 \\ l & n-l & v-n & l & n-l & v-n. \end{pmatrix} \begin{matrix} l \\ n-l \\ l \end{matrix} \tag{20}$$

If $e_L \subset e_R$, then e_R has the form

$$e_R = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & P_3 & I^{(l)} & 0 & P_6 \\ 0 & 0 & P_3' & 0 & I^{(n-l)} & P_6' \\ l & n-l & v-n & l & n-l & v-n, \end{pmatrix} \begin{matrix} l \\ n-l \\ l \\ n-l \end{matrix} \tag{21}$$

where P_3', P_6' are arbitrary matrices. Therefore, the number of e_R containing e_L is $q^{2(n-l)(v-n)}$. □

Lemma 11. *For any $t_n \in T_n$ and $e_L = (e_1, e_2, \ldots, e_l) \in E_L$, the number of e_R contained in t_n and containing e_L is $q^{2(n-l)(r-n)}$.*

Proof. For any $t_n \in T_n$, t_n is a subspace of type $(2r, r)$ and $U \subset t_n$. We assume that t_n has the form

$$t_n = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-n)} & 0 \\ n & r-n & v-r & n & r-n & v-r. \end{pmatrix} \begin{matrix} n \\ r-n \\ n \\ r-n \end{matrix} \tag{22}$$

If $e_L \subset t_n$, assume that e_L has the form

$$e_L = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & R_7 & 0 \\ l & n-l & r-n & v-r & l & n-l & r-n & v-r. \end{pmatrix} \begin{matrix} l \\ n-l \\ l \end{matrix} \tag{23}$$

If $e_R \subset t_n$ and $e_L \subset e_R$, then

$$e_R = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & R_7 & 0 \\ 0 & 0 & R_3' & 0 & 0 & I^{(n-l)} & R_7' & 0 \\ l & n-l & r-n & v-r & l & n-l & r-n & v-r, \end{pmatrix} \begin{matrix} l \\ n-l \\ l \\ n-l \end{matrix} \tag{24}$$

where R_3', R_7' are arbitrary matrices. Therefore, the number of e_R contained in t_n and containing e_L is $q^{2(n-l)(r-n)}$. □

Lemma 12. *Assume that $t_n \in T_n$ and $t_n' \in T_n$ are two distinct tags which are decoded by receiver's decoding rule e_R. s_1 and s_2 contained in t_n and t_n', respectively. Let $s_0 = s_1 \cap s_2$, dim $s_0 = k$; then $n \le k \le 2r - n - 1$; the number of e_R contained in $t_n \cap t_n'$ and containing e_L is $q^{(n-l)(k-n)}$.*

Proof. Since $t_n = s_1 + e_R$, $t_n' = s_2 + e_R$ and $t_n \ne t_n'$, then $s_1 \ne s_2$. And for any $s \in S$, $U \subset s$, therefore, $n \le k \le 2r - n - 1$. Assume that s_i' is the complementary subspace of s_0 in the s_i; then $s_i = s_0 + s_i'$ $(i = 1, 2)$. Because of $t_n = s_1 + e_R = s_0 + s_1' + e_R$, $t_n' = s_2 + e_R = s_0 + s_2' + e_R$ and $s_1 = t_n \cap U^\perp$, $s_2 = t_n' \cap U^\perp$, we know $s_0 = (t_n \cap U^\perp) \cap (t_n' \cap U^\perp) = t_n \cap t_n' \cap U^\perp = s_1 \cap t_n' = s_2 \cap t_n$, and $t_n \cap t_n' = (s_1 + e_R) \cap t_n' = (s_0 + s_1' + e_R) \cap t_n' = ((s_0 + e_R) + s_1') \cap t_n'$. Since $s_0 + e_R \subseteq t_n'$, then $t_n \cap t_n' = (s_0 + e_R) + (s_1' \cap t_n')$, while $s_1' \cap t_n' \subseteq s_1 \cap t_n' = s_0$, so $t_n \cap t_n' = s_0 + e_R$.

From the definition of the t_n and t_n', we assume that

$$
t_n = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & P_{22} & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & 0 & P_{44} \end{pmatrix} \begin{matrix} n \\ r-n \\ n \\ r-n \end{matrix}
$$
$$
\quad\quad n \quad v-n \quad n \quad v-n,
$$

(25)

$$
t_n' = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & P_{22}' & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & 0 & P_{44}' \end{pmatrix} \begin{matrix} n \\ r-n \\ n \\ r-n \end{matrix}
$$
$$
\quad\quad n \quad v-n \quad n \quad v-n.
$$

Let

$$
t_n \cap t_n' = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & P_2 & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & 0 & P_4 \end{pmatrix} \begin{matrix} n \\ r-n \\ n \\ r-n \end{matrix}
$$
$$
\quad\quad n \quad v-n \quad n \quad v-n.
$$

(26)

And from above we know that $t_n \cap t_n' = s_0 + e_R$; then dim $(t_n \cap t_n') = k + n$; therefore,

$$
\dim \begin{pmatrix} 0 & P_2 & 0 & 0 \\ 0 & 0 & 0 & P_4 \end{pmatrix} = k - n.
$$

(27)

For any $e_L \subset t_n \cap t_n'$, we assume that

$$
e_L = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 \end{pmatrix} \begin{matrix} l \\ n-l \\ l \end{matrix}
$$
$$
\quad l \quad n-l \quad v-n \quad l \quad n-l \quad v-n.
$$

(28)

If $e_R \subset t_n \cap t_n'$ and $e_L \subset e_R$, then e_R has the form

$$
e_R = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 \\ 0 & 0 & R_3' & 0 & I^{(n-l)} & R_6' \end{pmatrix} \begin{matrix} l \\ n-l \\ l \\ n-l \end{matrix}
$$
$$
\quad l \quad n-l \quad v-n \quad l \quad n-l \quad v-n.
$$

(29)

So, every row of $(0 \quad R_3' \quad 0 \quad R_6')$ is the linear combination of $\begin{pmatrix} 0 & P_2 & 0 & 0 \\ 0 & 0 & 0 & P_4 \end{pmatrix}$. Therefore, the number of e_R contained in $t_n \cap t_n'$ and containing e_L is $q^{(n-l)(k-n)}$. □

Theorem 13. *In the constructed multi-sender authentication codes, the maximum probabilities of success for impersonation attack and substitution attack from U_L on the receiver R are*

$$
P_I(L) = \frac{1}{q^{2(n-l)(v-r)}}, \qquad P_S(L) = \frac{1}{q^{(n-l)}}.
$$

(30)

Proof. (1) *Impersonation Attack.* U_L, after receiving their secret keys, sends a message m to R. U_L is successful if the receiver accepts it as authentic. Therefore,

$$
\begin{aligned}
P_I(L) &= \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{|\{e_R \in E_R \mid e_L \subset e_R, e_R \subset t\}|}{|\{e_R \in E_R \mid e_L \subset e_R\}|} \right\} \\
&= \frac{q^{2(n-l)(r-n)}}{q^{2(n-l)(v-n)}} \\
&= \frac{1}{q^{2(n-l)(v-r)}}.
\end{aligned}
$$

(31)

(2) *Substitution Attack.* R_L, after observing a message m that is transmitted by the sender, replaces m with another message m'. R_L is successful if m' is accepted by R as authentic. Therefore,

$$
\begin{aligned}
&P_S(L) \\
&= \max_{e_L \in E_L} \max_{m \in M} \max_{m \ne m' \in M} \left\{ \frac{|\{e_R \in E_R \mid e_L \subset e_R, e_R \subset t, e_R \subset t'\}|}{|\{e_R \in E_R \mid e_L \subset e_R, e_R \subset t\}|} \right\} \\
&= \max_{n \le k \le 2r-n-1} \frac{q^{(n-l)(k-n)}}{q^{2(n-l)(r-n)}} \\
&= \frac{1}{q^{(n-l)}}.
\end{aligned}
$$

(32)

□

6. The Advantage of the Constructed Authentication Code

The security of an authentication code could be measured by the maximum probabilities of deceptions. The smaller the probability of successful attack, the higher the security of the authentication codes. Now let us compare the security of our constructed authentication code with the known one [19].

The constructed authentication code in [19] is also a multisender authentication code from symplectic geometry over finite fields, but which is in simultaneous model. If we choose the parameters n, n', r, and v with $1 < n < n' < r < v$, $n > (r/2)$, and $n' - n > v - r$, from Table 1 we see that the maximum probabilities of deceptions of our construction are smaller than the construction in [19]. Therefore, compared with the construction in [19], our construction is more efficient.

TABLE 1: $(n > r/2, n' - n > \nu - r)$.

Constructions	[19]	Size relation	Ours
The number of senders	n	=	n
The number of attackers	$l, 1 \le l < n$	=	$l, 1 \le l < n$
The parameters of codes			
$\quad|S|$	$N(2(r-n), r-n; 2(\nu-n))$	=	$N(2(r-n), r-n; 2(\nu-n))$
$\quad|E_i|$	$q^{2(\nu-n)}$	=	$q^{2(\nu-n)}$
$\quad|E_R|$	$q^{2n'(\nu-n')}$	>	$q^{2n(\nu-n)}$
$\quad|T|$	$N(2(r-n), r-n; 2(\nu-n))q^{2n'(\nu-r-n'+n)}$	<	$N(2(r-n), r-n; 2(\nu-n))q^{2n(\nu-r)}$
The probabilities of deceptions			
$\quad P_I(L)$	$\dfrac{1}{q^{2(n'-l)(\nu+n-n'-r)-(n'-n)(n-l)}}$	>	$\dfrac{1}{q^{2(n-l)(\nu-r)}}$
$\quad P_S(L)$	$\dfrac{1}{q^{(n'-l)(2n-2n'+1)+(n'-n)(n-l)}}$	>	$\dfrac{1}{q^{n-l}}$

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

References

[1] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, "Codes which detect deception," *The Bell System Technical Journal*, vol. 53, pp. 405–424, 1974.

[2] G. J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes," in *Proceedings of the 6th Annual International Conference on Theory and Application of Cryptographic Techniques (Eurocrypt '87)*, vol. 304, pp. 151–165, 1988.

[3] Z. X. Wan, "Construction of cartesian authentication codes from unitary geometry," *Designs, Codes and Cryptography*, vol. 2, no. 4, pp. 333–356, 1992.

[4] W. P. Ma and X. M. Wang, "A construction of authentication codes with arbitration based on symplectic spaces," *Chinese Journal of Computers*, vol. 22, no. 9, pp. 949–952, 1999.

[5] G. You, S. Xinhua, and W. Hongli, "Construction of authentication codes with arbitration from symplectic geometry over finite fields," *Acta Scientiarum Naturalium Universitatis Nankaiensis*, vol. 41, no. 6, pp. 72–77, 2008.

[6] S. Chen and D. Zhao, "New construction of authentication codes with arbitration from pseudo-symplectic geometry over finite fields," *Ars Combinatoria*, vol. 97, pp. 453–465, 2010.

[7] S. Chen and D. Zhao, "Two constructions of optimal Cartesian authentication codes from unitary geometry over finite fields," *Acta Mathematicae Applicatae Sinica*, vol. 29, no. 4, pp. 829–836, 2013.

[8] S. Chen and D. Zhao, "Construction of multi-receiver multi-fold authentication codes from singular symplectic geometry over finite fields," *Algebra Colloquium*, vol. 20, no. 4, pp. 701–710, 2013.

[9] L. Ruihu and L. Zunxian, "Construction of A^2-codes from symplectic geometry," *Journal of Shanxi Normal University*, vol. 26, no. 4, pp. 10–15, 1998.

[10] C. Xing, H. Wang, and K.-Y. Lam, "Constructions of authentication codes from algebraic curves over finite fields," *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 886–892, 2000.

[11] C. Carlet, C. Ding, and H. Niederreiter, "Authentication schemes from highly nonlinear functions," *Designs, Codes and Cryptography*, vol. 40, no. 1, pp. 71–79, 2006.

[12] R. Safavi-Naini and H. Wang, "Multireceiver authentication codes: models, bounds, constructions, and extensions," *Information and Computation*, vol. 151, no. 1-2, pp. 148–172, 1999.

[13] S. Chen and D. Zhao, "Construction of multi-receiver multi-fold authentication codes from singular symplectic geometry over finite fields," *Algebra Colloquium*, vol. 20, no. 4, pp. 701–710, 2013.

[14] S. Chen and D. Zhao, "Two constructions of multireceiver authentication codes from symplectic geometry over finite fields," *Ars Combinatoria*, vol. 99, pp. 193–203, 2011.

[15] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/multi-sender network security: efficient authenticated multicast/feedback," in *Proceedings of the the 11th Annual Conference of the IEEE Computer and Communications Societies*, vol. 3, pp. 2045–2054, May 1992.

[16] Q. Yingchun and Z. Tong, "Multiple authentication Code with multi-transmitter and its constructions," *Journal of Zhongzhou University*, vol. 20, no. 1, pp. 118–120, 2003.

[17] M. Wen-Ping and W. Xin-Mei, "Several new constructions on multitransmitters authentication codes," *Acta Electronica Sinica*, vol. 28, no. 4, pp. 117–119, 2000.

[18] D. Qingling and L. Shuwang, "Bounds and construction for multi-sender authentication code," *Computer Engineering and Applications*, vol. 10, pp. 9–10, 2004.

[19] S. Chen and C. Yang, "A new construction of multisender authentication codes from symplectic geometry over finite fields," *Ars Combinatoria*, vol. 106, pp. 353–366, 2012.

[20] Z. Wan, *Geometry of Classical Groups over Finite Fields*, Science Press, Beijing, China, 2nd edition, 2002.