Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 602539, 10 pages
http://dx.doi.org/10.1155/2013/602539

Research Article

A New Construction of Multisender Authentication Codes from Pseudosymplectic Geometry over Finite Fields

Xiuli Wang

College of Science, Civil Aviation University of China, Tianjin 300300, China

Correspondence should be addressed to Xiuli Wang; xlwang@cauc.edu.cn

Received 7 December 2012; Accepted 20 February 2013

Academic Editor: Song Cen

Multisender authentication codes allow a group of senders to construct an authenticated message for one receiver such that the receiver can verify authenticity of the received message. In this paper, we construct one multisender authentication code from pseudosymplectic geometry over finite fields. The parameters and the probabilities of deceptions of this code are also computed.

1. Introduction

Multisender authentication code was firstly constructed by Gilbert et al. in [1] in 1974. Multisender authentication system refers to a group of senders that cooperatively send a message to the receiver, and then the receiver should be able to ascertain that the message is authentic. About this case, many scholars had also much researches and had made great contributions to multisender authentication codes [2–6].

In the actual computer network communications, multisender authentication codes include sequential model and simultaneous model. Sequential model is that each sender uses its own encoding message to the receiver, and 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, and then the synthesizer forms an authenticated message and verifies whether the message is legal or not. In this paper, we will adopt the second model.

In a simultaneous model, there are four participants: a group of senders $P = \{P_1, P_2, \ldots, P_n\}$, the keys distribution center, he is responsible for the key distribution to senders and receiver, including solving the disputes between them, a receiver R, a synthesizer, he only runs the trusted synthesis algorithm. The code works as follows: each sender and receiver has their own cartesian authentication code, respectively. Let $(S, E_i, T_i; f_i)$ $(i = 1, 2, \ldots, n)$ be the senders' cartesian authentication code, $(S, E_R, T; g)$ be the receiver's cartesian authentication code, $h : T_1 \times T_2 \times \cdots \times T_n \to T$ the synthesis algorithm. $\pi_i : E \to E_i$ is a subkey generation algorithm, where E is the key set of the key distribution center. When authenticating a message, the senders and the receiver should comply with the protocol. The key distribution center randomly selects an encoding rule $e \in E$ and sends $e_i = \pi_i(e)$ to the ith sender P_i $(i = 1, 2, \ldots, n)$ secretly, and then he calculates e_R by e according to an effective algorithm and secretly sends e_R to the receiver R; if the senders would like to send a source state s to the receiver R, P_i computes $t_i = f_i(s, e_i)$ $(i = 1, 2, \ldots, n)$ and sends $m_i = (s, t_i)$ $(i = 1, 2, \ldots, n)$ to the synthesizer through an open channel; the synthesizer receives the message $m_i = (s, t_i)$ $(i = 1, 2, \ldots, n)$ and calculates $t = h(t_1, t_2, \ldots, t_n)$ by the synthesis algorithm h and then sends message $m = (s, t)$ to the receiver R, 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 key distribution center is credible, though he know the senders' and receiver's encoding rules, he will not participate in any communication activities. When transmitters and receiver are disputing, the key distribution center settles it. At the same time, we assume that the system follows Kerckhoff's principle in which except for the actual used keys, the other information of the whole system is public.

In a multisender authentication system, we assume that the whole senders are cooperating 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. In the whole system, we assume that $\{P_1, P_2, \dots, P_n\}$ are senders, R is a receiver, E_i is the encoding rules set of the sender P_i, and E_R is the decoding rules set of receiver R. If the source state space S and the key space E_R of receiver R are according to a uniform distribution, then the probability distribution of message space M and tag space T is determined by the probability distribution of S and E_R. Consider $L = \{i_1, i_2, \dots, i_l\} \subset \{1, 2, \dots, n\}$, $l < n$, $P_L = \{p_1, p_2, \dots, p_l\}$, and $E_L = \{E_{p_1}, E_{p_2}, \dots, E_{p_l}\}$. Now, let us consider the attacks from malicious groups of senders. Here, there still are two kinds of attacks.

(i) *The Opponent's Impersonation Attack*. P_L sends a message m to receiver. P_L is successful if the receiver accepts it as legitimate message. Denote $P_I(L)$ as the largest probability of some opponent's successful impersonation attack, and it can be expressed as

$$P_I(L) = \max_{e_L \in E_L} \max_{m \in M} P\left(m \text{ is accepted by } \frac{R}{e_L}\right). \tag{1}$$

(ii) *The Opponent's Substitution Attack*. It is the largest probability of some opponent's successful substitution attack, and it can be expressed as

$$P_S(L) = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P\left(m' \text{ is accepted by } \frac{R}{m, e_L}\right). \tag{2}$$

In this paper, we give a construction about multisender authentication code from pseudosymplectic geometry over finite fields.

2. Pseudosymplectic Geometry

Let F_q be the finite field with q elements, where q is a power of 2, $n = 2\nu + \delta$, and $\delta = 1, 2$. Let

$$K = \begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \qquad S_1 = \begin{pmatrix} K & \\ & 1 \end{pmatrix}, \qquad S_2 = \begin{pmatrix} K & & \\ & 0 & 1 \\ & 1 & 1 \end{pmatrix}, \tag{3}$$

and S_δ is a $(2\nu + \delta) \times (2\nu + \delta)$ nonalternate symmetric matrix.

The pseudosymplectic group of degree $(2\nu + \delta)$ over F_q is defined to be the set of matrices $Ps_{2\nu+\delta}(F_q) = \{T \mid TS_\delta {}^tT = S_\delta\}$ denoted by $Ps_{2\nu+\delta}(F_q)$.

Let $F_q^{(2\nu+\delta)}$ be the $(2\nu + \delta)$-dimensional row vector space over F_q. $Ps_{2\nu+\delta}(F_q)$ has an action on $F_q^{(2\nu+\delta)}$ defined as follows:

$$\begin{gathered} F_q^{(2\nu+\delta)} \times Ps_{2\nu+\delta}(F_q) \longrightarrow F_q^{(2\nu+\delta)}, \\ ((x_1, x_2, \dots, x_{2\nu+\delta}), T) \longrightarrow (x_1, x_2, \dots, x_{2\nu+\delta}) T. \end{gathered} \tag{4}$$

The vector space $F_q^{(2\nu+\delta)}$ together with this group action is called the pseudosymplectic space over the finite field F_q of characteristic 2.

Let P be an m-dimensional subspace of $F_q^{(2\nu+\delta)}$; then, $PS_\delta {}^tP$ is cogredient to one of the following three normal forms:

$$\begin{gathered} M(m, 2s, s) = \begin{pmatrix} 0 & I^{(s)} & \\ I^{(s)} & 0 & \\ & & 0^{(m-2s)} \end{pmatrix}, \\ M(m, 2s+1, s) = \begin{pmatrix} 0 & I^{(s)} & & \\ I^{(s)} & 0 & & \\ & & 1 & \\ & & & 0^{(m-2s-1)} \end{pmatrix}, \\ M(m, 2s+2, s) = \begin{pmatrix} 0 & I^{(s)} & & & \\ I^{(s)} & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 1 & \\ & & & & 0^{(m-2s-2)} \end{pmatrix}, \end{gathered} \tag{5}$$

for some s such that $0 \le s \le [m/2]$. We say that P is a subspace of type $(m, 2s + \tau, s, \epsilon)$, where $\tau = 0, 1$, or 2 and $\epsilon = 0$ or 1, if

(i) $PS_\delta {}^tP$ is cogredient to $M(m, 2s + \tau, s)$;

(ii) $e_{2\nu+1} \notin P$ or $e_{2\nu+1} \in P$ according to $\epsilon = 0$ or $\epsilon = 1$, respectively.

Let P be an m-dimensional subspace of $F_q^{(2\nu+\delta)}$. Denote by $P^\perp$ the set of vectors which are orthogonal to every vector of P; that is,

$$P^\perp = \left\{ y \in F_q^{(2\nu+\delta)} \mid yS_\delta {}^tx = 0 \ \forall x \in P \right\}. \tag{6}$$

Obviously, $P^\perp$ is a $(2\nu + \delta - m)$-dimensional subspace of $F_q^{(2\nu+\delta)}$.

More properties of pseudosymplectic geometry over finite fields can be found in [7].

In [2], Desmedt et al. gave two constructions for MRA-codes based on polynomials and finite geometries, respectively. There are other constructions of multisender authentication codes which are given in [3–6]. The construction of authentication codes is of combinational design in its nature. We know that the geometry of classical groups over finite fields, including symplectic geometry, pseudosymplectic geometry, unitary geometry, and orthogonal geometry, can provide a better combination of structure and can be easy to count. In this paper, we construct one multisender authentication code from pseudosymplectic geometry over finite fields. The parameters and the probabilities of deceptions of this code are also computed. We realize the generalization and application of the similar idea and method of article [8] from symplectic geometry to pseudosymplectic geometry over finite fields.

3. Construction

Let $\mathbb{F}_q$ be a finite field with q elements and e_i $(1 \leq i \leq 2\nu+2)$ the row vector in $\mathbb{F}_q^{(2\nu+2)}$ whose ith coordinate is 1 and all other coordinates are 0. Assume that $2 < n+1 < r < \nu$. Let $U = \langle e_1, e_2, \ldots, e_n \rangle$; that is, U is an n-dimensional subspace of $\mathbb{F}_q^{(2\nu+2)}$ generated by $e_1, e_2, \ldots, e_n$, and then $U^{\perp} = \langle e_1, \ldots, e_\nu, e_{\nu+n+1}, \ldots, e_{2\nu+2} \rangle$. Consider $W_i = \langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n \rangle$, $1 \leq i \leq n$; then, $W_i^{\perp} = \langle e_1, \ldots, e_\nu, e_{\nu+i}, e_{\nu+n+1}, \ldots, e_{2\nu+2} \rangle$. The set of source states $S = \{s \mid s$ is a subspace of type $(2r-n+1, 2(r-n), r-n, 1)$ and $U \subset s \subset U^{\perp}\}$; the set of ith sender's encoding rules $E_{P_i} = \{e_{P_i} \mid e_{P_i}$ is a subspace of type $(n+1, 0, 0, 0)$ and $U \subset e_{P_i}, e_{P_i} \perp W_i\}$, $1 \leq i \leq n$; the set of receiver's decoding rules $E_R = \{e_R \mid e_R$ is a subspace of type $(2n, 2n, n, 0)$ and $U \subset e_R\}$; the set of ith sender's tags $T_i = \{t_i \mid t_i$ is a subspace of type $(2r-n+2, 2(r-n+1), r-n+1, 1)$ and $U \subset t_i \subset W_i^{\perp}, t_i \not\subset U^{\perp}\}$; the set of receiver's tags $T = \{t \mid t$ is a subspace of type $(2r+1, 2r, r, 1)$ and $U \subset t\}$.

Define the encoding map $f_i : S \times E_{P_i} \to T_i$, $f_i(s, e_{P_i}) = s + e_{P_i}$, $1 \leq i \leq n$.

The decoding map $f : S \times E_R \to T$, $f(s, e_R) = s + e_R$.

The synthesizing map $h : T_1 \times T_2 \times \cdots \times T_n \to T$, $h(t_1, t_2, \ldots, t_n) = A(t_1 + t_2 + \cdots + t_n)$, where A is a nonsingular matrix and $A(t_1 + t_2 + \cdots + t_n)$ is a subspace of type $(2r+1, 2r, r, 1)$.

The code works as follows.

(1) *Key Distribution*. The key distribution center randomly chooses an $e_R \in E_R$ and selects a $(2n, n)$ subspace e such that $U \subset e$, and it selects $e_{P_i} \in E_{P_i}$ so that $e_{P_1} + e_{P_2} + \cdots + e_{P_n} = e$, and A is a nonsingular matrix satisfying $e_R = \langle e, A \rangle$. The key distribution center randomly secretly sends e_R, e_{P_i} to the receiver and the senders, respectively, and sends A to the synthesizer.

(2) *Broadcast*. If the senders want to send a source state $s \in S$ to the receiver R, the sender P_i calculates $t_i = f_i(s, e_{P_i}) = s + e_{P_i}$ then sends t_i $(1 \leq i \leq n)$ to the synthesizer.

(3) *Synthesis*. After the synthesizer receives $t_1, t_2, \ldots, t_n$, he calculates $h = (t_1, t_2, \ldots, t_n) = A(t_1 + t_2 + \cdots + t_n)$ and then sends $m = (s, t)$ to the receiver R.

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

Let

$$U = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix} \end{array}; \tag{7}$$

then,

$$U^{\perp} = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(\nu-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix} \end{array},$$

$$W_i^{\perp} = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(\nu-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix} \end{array}. \tag{8}$$

Lemma 1. *Let $C_i = (S, E_{P_i}, T_i; f_i)$; the code is a cartesian authentication code, $1 \leq i \leq n$.*

Proof. For any $e_{p_i} \in E_{P_i}$, $s \in S$. Because e_{p_i} is a subspace of type $(n+1, 0, 0, 0)$ and $U \subset e_{p_i} \subset U^{\perp}$, we can assume that

$$e_{p_i}=\begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & R_8 & R_9 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix}\end{array}. \tag{9}$$

Obviously, $e_{p_i}\cap U^{\perp}=U$. Let $s\in S$; since $U\subset s\subset U^{\perp}$, s has the form as follows:

$$s=\begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & B_2 & 0 & B_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \tag{10}$$

where B_2, B_4 is a subspace of type $(2(r-n), 2(r-n), r-n, 0)$ in the pseudosymplectic space $F_q^{(2\nu+2)}$. Let $t_i=s+e_{p_i}$; then,

$$t_i=\begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & B_2 & 0 & 0 & 0 & 0 & B_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & R_8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix}\end{array},$$

$$t_iS_2\,{}^tt_i\sim\begin{pmatrix} I^{(r-n)} & 0 & 0 & 0 \\ 0 & I^{(r-n)} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{11}$$

Obviously, $t_i\not\subset U^{\perp}$. So, t_i is a subspace of type $(2r-n+2, 2(r-n+1), r-n+1, 1)$ satisfying $U\subset t_i\subset W_i^{\perp}$; that is, $t_i\in T_i$.

Furthermore, we know that $t_i\cap U^{\perp}=(s+e_{p_i})\cap U^{\perp}=s+(e_{p_i}\cap U^{\perp})=s+U=s$.

Conversely, for any $t_i\in T_i$, let $s=t_i\cap U^{\perp}$, $L\subset t_i$, satisfying $t_i=s\oplus L$. Obviously, $U\subset s\subset U^{\perp}$. For $U\subset t_i\subset W_i^{\perp}$, let

$$t_i=\begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & B_2 & 0 & 0 & 0 & 0 & B_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & R_8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix}\end{array}. \tag{12}$$

Obviously,

$$t_i\cap U^{\perp}=\begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & C_2 & 0 & 0 & 0 & 0 & C_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix}\end{array}. \tag{13}$$

For t_i being a subspace of type $(2r-n+2, 2(r-n+1), r-n+1, 1)$, then $t_i\cap U^{\perp}$ is a subspace of type $(2r-n+1, 2(r-n), r-n, 1)$; that is, $s\in S$. Choose

$$L=\begin{pmatrix} 0 & 0 & B_2 & 0 & 0 & 1 & 0 & B_4 & 0 & 0 \end{pmatrix}. \tag{14}$$

Let $e_{P_i}=U+L$; then, $e_{P_i}\in E_{P_i}$, and $s\oplus L=s\oplus e_{P_i}$. Therefore, f_i is a surjection. For any $t_i\in T_i$, $e_{P_i}\in E_{P_i}$, if there exist $s\in S$ so that $t_i=s+e_{P_i}$; then, $s\in t_i\cap U^{\perp}$. However, $\dim s=2r-n+1=\dim(t_i\cap U^{\perp})$, and so $s=t_i\cap U^{\perp}$; that is, s is determined by t_i and e_{P_i}. □

Lemma 2. *Let $C = (S, E_R, T; g)$; the code is a cartesian authentication code.*

Proof. (1) For any $s \in S$, $e_R \in E_R$. From the definition of s and e_R, we assume that

$$s = \begin{pmatrix} U \\ Q \\ e_{2\nu+1} \end{pmatrix} \begin{matrix} n \\ 2(r-n) \\ 1 \end{matrix},$$

$$\begin{pmatrix} U \\ Q \\ e_{2\nu+1} \end{pmatrix} S_2 {}^t\begin{pmatrix} U \\ Q \\ e_{2\nu+1} \end{pmatrix} = \begin{pmatrix} 0^{(n)} & 0 & 0 & 0 \\ 0 & 0 & I^{(r-n)} & 0 \\ 0 & I^{(r-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (15)$$

$$e_R = \begin{pmatrix} U \\ V \end{pmatrix} \begin{matrix} n \\ n \end{matrix},$$

$$\begin{pmatrix} U \\ V \end{pmatrix} S_2 {}^t\begin{pmatrix} U \\ V \end{pmatrix} S_2 {}^t\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} \\ I^{(n)} & 0 \end{pmatrix}.$$

Obviously, for any $v \in V$ and $v \neq 0$, $v \notin s$; therefore,

$$t = s + e_R = \begin{pmatrix} U \\ V \\ Q \\ e_{2\nu+1} \end{pmatrix}, \quad (16)$$

$$\begin{pmatrix} U \\ V \\ Q \\ e_{2\nu+1} \end{pmatrix} S_2 {}^t\begin{pmatrix} U \\ V \\ Q \\ e_{2\nu+1} \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} & 0 & 0 & 0 \\ I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-n)} & 0 \\ 0 & 0 & I^{(r-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (17)$$

From the above mentioned, t is a subspace of type $(2r+1, 2r, r, 1)$ and $U \subset t$; that is, $t \in T$.

(2) For $t \in T$, t is a subspace of type $(2r+1, 2r, r, 1)$ and $U \subset t$; so, there is a subspace $V \subset t$, satisfying

$$\begin{pmatrix} U \\ V \end{pmatrix} S_2 {}^t\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} \\ I^{(n)} & 0 \end{pmatrix}. \quad (18)$$

Then, we can assume that

$$t = \begin{pmatrix} U \\ V \\ Q \\ e_{2\nu+1} \end{pmatrix} \quad (19)$$

satisfying

$$\begin{pmatrix} U \\ V \\ Q \\ e_{2\nu+1} \end{pmatrix} S_2 {}^t\begin{pmatrix} U \\ V \\ Q \\ e_{2\nu+1} \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} & 0 & 0 & 0 \\ I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-n)} & 0 \\ 0 & 0 & I^{(r-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (20)$$

Let

$$s = \begin{pmatrix} U \\ Q \\ e_{2\nu+1} \end{pmatrix}, \quad (21)$$

for s is a subspace of type $(2r-n+1, 2(r-n), r-n, 1)$ and $U \subset s \subset U^{\perp}$; that is, $s \in S$ is a source state. For any $v \in V$ and $v \neq 0$, $v \notin s$ is obvious; that is, $V \cap U^{\perp} = \{0\}$. Therefore, $t \cap U^{\perp} = \left(\begin{smallmatrix} U \\ Q \\ e_{2\nu+1} \end{smallmatrix}\right) = s$. Let $e_R = \left(\begin{smallmatrix} U \\ V \end{smallmatrix}\right)$; then, e_R is receiver's decoding rule satisfying $t = s + e_R$.

If s' is another source state contained in t, then $U \subset s' \subset U^{\perp}$. Therefore, $s' \subset t \cap U^{\perp} = s$, while $\dim s' = \dim s$, and so $s' = s$; that is, s is the uniquely source state contained in t.

From Lemmas 1 and 2, we know that such construction of multisender authentication codes is reasonable, and there are n senders in this system. Next, we compute the parameters of this code and the maximum probability of success in impersonation attack and substitution attack by group of senders. □

Lemma 3. *Some parameters of this code are*

$$|S| = N(2(r-n), 2(r-n), r-n, 0; 2\nu+2);$$
$$|E_{P_i}| = q^{\nu-n+1} \quad (1 \le i \le n). \quad (22)$$

Proof. Since $U \subset s \subset U^{\perp}$, s has the following form:

$$s = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & B_2 & 0 & B_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad (23)$$

where B_2, B_4 is a subspace of type $(2(r-n), 2(r-n), r-n, 0)$ in the pseudosymplectic space $F_q^{(2\nu+2)}$. So, $|S| = N(2(r-n), 2(r-n), r-n, 0; 2\nu+2)$.

For any $e_{P_i} \in E_{P_i}$, we can assume that e_{P_i} has the following form:

$$e_{P_i} = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & 1 & 0 & R_8 & R_9 & R_{10} \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{matrix} \end{array}. \quad (24)$$

Since e_{p_i} is a subspace of type $(n+1,0,0,0)$, so $R_3 = 0$ and $R_{10} = 0$, R_8, R_9 arbitrarily. Therefore, $|E_{P_i}| = q^{\nu-n+1}$. □

Lemma 4. *(1) For any $t_i \in T_i$, the number of t_i containing e_{P_i} is $q^{r-n+1} (1 \le i \le n)$;*

(2) The number of the ith sender's tag is $|T_i| = q^{\nu-r} N(2(r-n), 2(r-n), r-n, 0; 2\nu+2)$ $(1 \le i \le n)$.

Proof. (1) Considering the transitivity properties of the same subspaces under the pseudosymplectic groups, we may take t_i as follows:

$$t_i = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(r-n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & r-n & \nu-r & l & i-l-1 & 1 & n-i & r-n & \nu-r & 1 & 1 \end{matrix} \end{array}. \quad (25)$$

twocolumngrid If $e_{P_i} \subset t_i$, then we assume that

$$e_{P_i} = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & R_7 & 0 & R_9 & 0 & R_{11} & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & r-n & \nu-r & l & i-l-1 & 1 & n-i & r-n & \nu-r & 1 & 1 \end{matrix} \end{array}; \quad (26)$$

from $e_{P_i} \perp W_i$, we know that $R_7 = 1$, where R_9, R_{11} arbitrarily, and therefore the number of t_i containing e_{P_i} is q^{r-n+1} $(1 \le i \le n)$.

(2) We know that every t_i contains only one source state $t_i \cap U^{\perp}$ and the number of t_i containing e_{P_i}. Therefore, we have $|t_i| = |S||E_{P_i}|/q^{r-n+1} = |S| q^{\nu-n+1}/q^{r-n+1} = q^{\nu-r} N(2(r-n), 2(r-n), r-n, 0; 2\nu+2)$. □

Lemma 5. *(1) The number of the receiver's decoding rules is $|E_R| = q^{n(\nu-n+1)}$.*

(2) For any $t \in T$, the number of e_R which contained t is $q^{n(r-n+1)} (1 \le i \le n)$.

(3) The number of the receiver's tag is $|T| = q^{n(\nu-r)} N(2(r-n), 2(r-n), r-n, 0; 2\nu+2)$.

Proof. (1) Let $e_R \in E_R$; e_R has the following form:

$$e_R = \begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & I^{(n)} & R_4 & R_5 & R_6 \end{pmatrix} \\ \begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 \end{matrix} \end{array}. \quad (27)$$

For e_R being a subspace of type $(2n, 2n, n, 0)$, so R_2 and $R_6 = 0$; R_4, R_5 arbitrarily. Therefore, $|E_R| = q^{n(\nu-n+1)}$.

(2) Considering the transitivity properties of the same subspaces under the pseudosymplectic groups, we may choose t as follows:

$$t = \begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{matrix} n & r-n & \nu-r & n & r-n & \nu-r & 1 & 1 \end{matrix} \end{array}. \quad (28)$$

If $e_R \subset t$, then

$$e_R = \begin{array}{c}\begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & R_5 & 0 & R_7 & 0 \end{pmatrix} \\ \begin{matrix} n & r-n & \nu-r & n & r-n & \nu-r & 1 & 1 \end{matrix}\end{array}, \tag{29}$$

where R_5 and R_7 arbitrarily. Therefore, the number of e_R which contained t is $q^{n(r-n+1)}$.

(3) Similar to Lemma 4(2), $|T| = |S||E_R|/q^{r-n+1} = |S|q^{n(\nu-n+1)}/q^{r-n+1} = q^{n(\nu-r)}N(2(r-n), 2(r-n), r-n, 0; 2\nu+2)$.

Without loss of generality, we assume that $L = \{i_1, i_2, \ldots, i_l\} \subset \{1, 2, \ldots, n\}$, $l < n$, $P_L = \{p_1, p_2, \ldots, p_l\}$, and $E_L = \{E_{p_1}, E_{p_2}, \ldots, E_{p_l}\}$. Now, let us consider the attacks on R from malicious groups of senders. □

Lemma 6. *For any $e_L = \{E_{p_1}, E_{p_2}, \ldots, E_{p_l}\} \in E_L$, the number of e_R containing e_L is $q^{(\nu-n+1)(n-l)}$.*

Proof. For any $e_L = \{E_{p_1}, E_{p_2}, \ldots, E_{p_l}\} \in E_L$, we assume e_L to be as follows:

$$e_L = \begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(l)} & 0 & R_6 & R_7 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{matrix}\end{array}. \tag{30}$$

If $e_R \supset e_L$, then e_R has the following form:

$$e_R = \begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(l)} & 0 & R_6 & R_7 & 0 \\ 0 & 0 & 0 & 0 & I^{(n-l)} & R_6' & R_7' & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{matrix}\end{array}, \tag{31}$$

where R_6', R_7' arbitrarily. Therefore, the number of e_R containing e_L is $q^{(\nu-n+1)(n-l)}$. □

Lemma 7. *For any $t \in T$ and $e_L = \{E_{p_1}, E_{p_2}, \ldots, E_{p_l}\} \in E_L$, the number of e_R which contained in t and containing e_L is $q^{(r-n+1)(n-l)}$.*

Proof. For any $t \in T$, we assume t to be as follows:

$$t = \begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(r-n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & r-n & \nu-r & l & n-l & r-n & \nu-r & 1 & 1 \end{matrix}\end{array}. \tag{32}$$

If $e_L \subset t$, then e_L has the following form:

$$e_L = \begin{array}{c}\begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(l)} & 0 & R_7 & 0 & R_9 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & r-n & \nu-r & l & n-l & r-n & \nu-r & 1 & 1 \end{matrix}\end{array}. \tag{33}$$

Since $e_L \subset e_R \subset t$, then we assume e_R to be as follows:

$$e_R = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(l)} & 0 & R_7 & 0 & R_9 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(n-l)} & H_7 & 0 & H_9 & 0 \end{pmatrix} \\ \begin{matrix} l & n-l & r-n & \nu-r & l & n-l & r-n & \nu-r & 1 & 1 \end{matrix} \end{array}, \tag{34}$$

where H_7 and H_9 arbitrarily. Therefore, the number of $e_R$which contained in t and containing e_L is $q^{(r-n+1)(n-l)}$. □

Lemma 8. *Assume that t_1 and t_2 are two distinct tags ($t_1, t_2 \in T$) decoded by receiver's key e_R, and s_1 and s_2 contained in t_1 and t_2 are two source states, respectively. Let $s_0 = s_1 \cap s_2$, $\dim s_0 = k$; then, $n \le k \le 2r - n$, and the number of e_R which contained in $t_1 \cap t_2$ and containing e_L is $q^{(k-r)(n-1)}$.*

Proof. Since $t_1 = s_1 + e_R, t_2 = s_2 + e_R$, and $t_1 \ne t_2$, then $s_1 \ne s_2$. For any $s \in S, U \in s$, obviously $n \le k \le 2r - n$. Assume that s_i' is the complementary subspace of s_0 in the s_i; then, $s_i = s_0 + s_i'$ $(i = 1, 2)$. From $t_i = s_i + e_R = s_0 + s_i' + e_R$ and $s_i = t_i \cap U^{\perp}$, we know that $s_0 = (t_1 \cap U^{\perp}) \cap (t_2 \cap U^{\perp}) = t_1 \cap t_2 \cap U^{\perp} = s_1 \cap t_2 = s_2 \cap t_1$, and $t_1 \cap t_2 = (s_1 + e_R) \cap t_2 = (s_0 + s_1' + e_R) \cap t_2 = ((s_0 + e_R) + s_1') \cap t_2$, since $s_0 + e_R \subseteq t_2$; then, $t_1 \cap t_2 = (s_0 + e_R) + (s_1' \cap t_2)$, while $s_1' \cap t_2 \subseteq s_1 \cap t_2 = s_0$, and so we have $t_1 \cap t_2 = s_0 + e_R$.

From the definition of t, we may take t_i, $i = 1, 2$, as follows:

$$t_i = \begin{array}{cc} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_{i_7} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} l \\ n-l \\ r-n \\ l \\ n-l \\ r-n \\ 1 \end{matrix} \\ \begin{matrix} l & n-l & r-n & \nu-r & l & n-l & r-n & \nu-r & 1 & 1 \end{matrix} & \end{array}. \tag{35}$$

Let

$$t_1 \cap t_2 = \begin{array}{cc} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} l \\ n-l \\ r-n \\ l \\ n-l \\ r-n \\ 1 \end{matrix} \\ \begin{matrix} l & n-l & r-n & \nu-r & l & n-l & r-n & \nu-r & 1 & 1 \end{matrix} & \end{array}. \tag{36}$$

From the above mentioned, we know that $t_1 \cap t_2 = s_0 + e_R$, and then $\dim (t_1 \cap t_2) = k + 2n - n = k + n$; therefore,

$$\dim \begin{pmatrix} 0 & P_7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = k + n - (2n + r - n) = k - r. \tag{37}$$

For any $e_L, e_R \subset t_1 \cap t_2$, we can assume that

$$
e_L = \begin{array}{cc}
\begin{pmatrix}
I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & I^{(l)} & 0 & R_7 & 0 & R_9 & 0
\end{pmatrix} & \begin{matrix} l \\ n-l \\ l \end{matrix} \\
\begin{matrix} l & n-l & r-n & \nu-r & l & n-l & r-n & \nu-r & 1 & 1 \end{matrix} &
\end{array},
$$

$$
e_R = \begin{array}{cc}
\begin{pmatrix}
I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & I^{(l)} & 0 & R_7 & 0 & R_9 & 0 \\
0 & 0 & 0 & 0 & 0 & I^{(n-l)} & H_7 & 0 & H_9 & 0
\end{pmatrix} & \begin{matrix} l \\ n-l \\ l \\ n-l \end{matrix} \\
\begin{matrix} l & n-l & r-n & \nu-r & l & n-l & r-n & \nu-r & 1 & 1 \end{matrix} &
\end{array}, \tag{38}
$$

where every row of

$$\begin{pmatrix} 0 & H_7 & 0 & H_9 & 0 \end{pmatrix} \tag{39}$$

is the linear combination of the base of

$$\begin{pmatrix} 0 & P_7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{40}$$

Therefore, the number of $e_R \subset t_1 \cap t_2$ and containing e_L is $q^{(k-r)(n-l)}$. □

Theorem 9. *In the constructed multisender authentication codes, the largest probabilities of success for impersonation attack and substitution attack from P_L on a receiver R are*

$$P_I(L) = \frac{1}{q^{(\nu-r)(n-l)}}, \qquad P_S(L) = \frac{1}{q^{2(n-l)}}, \tag{41}$$

respectively.

Proof. Impersonation Attack. P_L, after receiving his secret keys, encodes a message and sends it to receiver. P_L is successful if the receiver accepts it as legitimate message. So,

$$
\begin{aligned}
P_I(L) &= \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{\left|\left\{e_R \in E_R \mid e_L \subset e_R \text{ and } e_R \subset t\right\}\right|}{\left|\left\{e_R \in E_R \mid e_L \subset e_R\right\}\right|} \right\} \\
&= \frac{q^{(n-l)(r-n+1)}}{q^{(n-l)(\nu-n+1)}} = \frac{1}{q^{(\nu-r)(n-l)}}.
\end{aligned} \tag{42}
$$

Substitution Attack. P_L replaces t with another message t', after it observes a legitimate message t. P_L is successful if the receiver accepts it as legitimate message. So,

$$
\begin{aligned}
P_S(L) &= \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} \left\{ \frac{\left|\left\{e_R \in E_R \mid e_R \subset t, t' \text{ and } e_L \subset e_R\right\}\right|}{\left|\left\{e_R \in E_R \mid e_R \subset t \text{ and } e_L \subset e_R\right\}\right|} \right\} \\
&= \max_{n \le k \le 2r-n} \frac{q^{(n-l)(k-r)}}{q^{(n-l)(r-n+1)}} \\
&= \max_{n \le k \le 2r-n} \frac{1}{q^{(2r-n+1-k)(n-l)}} \\
&= \frac{1}{q^{(n-l)}}.
\end{aligned} \tag{43}
$$

□

Acknowledgments

This work is supported by the NSF of China (61179026) and Fundamental Research of the Central Universities of China Civil Aviation University of Science special (ZXH2012k003).

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] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/multi-sender network security: efficient authenticated multi-cast/feedback," in *Proceedings of the the 11th Annual Conference of the IEEE Computer and Communications Societies (Infocom '92)*, pp. 2045–2054, May 1992.

[3] K. Martin and R. Safavi-Naini, "Multi-sender authentication schemes with unconditional security," in *Information and Communications Security*, vol. 1334 of *Lecture Notes in Computer Science*, pp. 130–143, Springer, Berlin, Germany, 1997.

[4] W. Ma and X. Wang, "Several new constructions of multi-trasmitters authentication codes," *Acta Electronica Sinica*, vol. 28, no. 4, pp. 117–119, 2000.

[5] 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 (Eurcrypt '87), vol. 304 of *Lecture Notes in Computer Science*, pp. 151–165, 1987.

[6] C. Shangdi and C. Lizhen, "Two constructions of multi-sender authentication codes with arbitration based linear codes," *WSEAS Transactions on Mathematics*, vol. 11, no. 12, 2012.

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

[8] C. Shangdi and Z. Dawei, "Two constructions of multireceiver authentication codes from symplectic geometry over finite fields," *Ars Combinatoria*, vol. 99, pp. 193–203, 2011.