Designs, Codes and Cryptography, 2, 333–356 (1992)
© 1992 Kluwer Academic Publishers. Manufactured in The Netherlands.

Construction of Cartesian Authentication Codes from Unitary Geometry

ZHE-XIAN WAN
Institute of Systems Science, Academia Sinica, Beijing, China, and
Department of Information Theory, Lund University, Lund, Sweden

Communicated by D. Jungnickel
Received August 28, 1991; Revised April 8, 1992.

Abstract. In the present paper several constructions of Cartesian authentication codes from unitary geometry over finite fields are presented and their size parameters are computed. Assuming that the encoding rules are chosen according to a uniform probability distribution, the probabilities P_I and P_S of a successful impersonation attack and a successful substitution attack, respectively, of these codes are also computed. Moreover, those codes so constructed, for which P_I and P_S are nearly optimal, are also determined.

1. Introduction

Let $\mathcal{S}$, $\mathcal{E}$, and $\mathcal{M}$ be three nonempty finite sets and let f: $\mathcal{S} \times \mathcal{E} \to \mathcal{M}$ be a map, the four tuple $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is called an *authentication code* [4], if

(1) The map $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ is surjective and
(2) For any $m \in \mathcal{M}$ and $e \in \mathcal{E}$ if there is an $s \in \mathcal{S}$ satisfying $f(s, e) = m$, then such an s is uniquely determined by the given m and e.

Suppose that $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is an authentication code, then $\mathcal{S}$, $\mathcal{E}$, and $\mathcal{M}$ are called the set of *source states*, the set of *encoding rules*, and the set of *messages*, respectively and f is called the *encoding map*. Let $s \in \mathcal{S}$, $e \in \mathcal{E}$, and $m \in \mathcal{M}$ be such that $m = f(s, e)$, then we say that the source state s is encoded into the message m under the encoding rule e, and for convenience we say that the message m contains the encoding rule e. The cardinals $|\mathcal{S}|$, $|\mathcal{E}|$, $|\mathcal{M}|$ are called the *size parameters* of the code. Moreover, if the authentication code satisfies the further requirement that given any message m there is a unique source state s such that $m = f(s, e)$ for every encoding rule e contained in m, then the code is called a *Cartesian* authentication code.

Authentication codes are used in communication channels where besides the transmitter and the receiver there is an opponent who may play either the impersonation attack or the substitution attack. By an *impersonation attack* we mean that the opponent sends a message through the channel to the receiver and hopes the receiver will accept it as authentic, i.e., as a message sent by the transmitter. By a *substitution attack* we mean that after the opponent intercepts a message sent by the transmitter to the receiver, he sends another message instead and hopes the receiver will accept it as authentic. To protect against these attacks the transmitter-receiver may use an authentication code which is publicly known and choose a fixed encoding rule e in secret. The set of information which the transmitter would like to be able to transmit to the receiver should be identified with the set of source states of the code. Suppose that the transmitter wants to send a source state s to the receiver. He first encodes s into a message m under the encoding rule, e, i.e., $m = f(s, e)$, and then sends m to the receiver. Once the receiver receives a message m', he first has to judge whether m' is authentic, i.e., whether the encoding rule e is contained in m'. If $e \in m'$, then he regards m' as authentic and decodes m' by e to get a source state s', where $m' = f(s', e)$. If $e \notin m'$ then he regards m' as a false message. The object of the component is to choose a message and send it to the receiver so that the probability of deceiving the receiver, i.e., of causing him to accept as authentic a message not sent by the transmitter is as large as possible. We denote by P_I and P_S, respectively, the largest probabilities that he could deceive the receiver when he plays an impersonation attack and a substitution attack and call them the probabilities of a successful impersonation attack and of a successful substitution attack, respectively.

In [3] some authentication codes based on projective geometry over finite fields were constructed and their size parameters were computed. In the present paper several constructions of authentication codes from unitary geometry over finite fields will be presented and their size parameters will be computed. Moreover, assuming that the encoding rules are chosen according to a uniform probability distribution, the P_I and P_S of these codes will also be computed.

2. The Unitary Geometry

We sketch in the following the main features of the unitary geometry over finite fields which will be used in this paper.

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements, where q is a prime power. $\mathbb{F}_{q^2}$ has an involutive automorphism, i.e., an automorphism of order 2

$$a \mapsto \bar{a} = a^q$$

and the fixed field of this automorphism is $\mathbb{F}_q$.

Let $n \geq 1$. The *unitary group* of degree n over $\mathbb{F}_{q^2}$, denoted by $U_n(\mathbb{F}_{q^2})$ is defined to be the set of matrices

$$U_n(\mathbb{F}_{q^2}) = \{U \in GL_n(\mathbb{F}_{q^2}) \mid U\bar{U}^T = I^{(n)}\}$$

with matrix multiplication as its group operation. Let $V_n(\mathbb{F}_{q^2})$ be the n-dimensional row vector space over $\mathbb{F}_{q^2}$. There is an action of $U_n(\mathbb{F}_{q^2})$ on $V_n(\mathbb{F}_{q^2})$ defined as follows:

$$V_n((\mathbb{F}_{q^2}) \times U_n(\mathbb{F}_{q^2}) \rightarrow V_n(\mathbb{F}_{q^2})$$
$$((x_1, x_2, \ldots, x_n), U) \mapsto (x_1, x_2, \ldots, x_n)U.$$

The vector space $V_n(\mathbb{F}_{q^2})$ with the above action of the group $U_n(\mathbb{F}_{q^2})$ is called the *n-dimensional unitary space* over $\mathbb{F}_{q^2}$.

Let P be an m-dimensional subspace of $V_n(\mathbb{F}_{q^2})$. We use the same letter P to denote a matrix representation of P, i.e., P is an $m \times n$ matrix whose rows form a basis of P. The above defined action of $U_n(\mathbb{F}_{q^2})$ induces an action on the set of subspaces, i.e., the element $U \in U_n(\mathbb{F}_{q^2})$ carries the subspace P into the subspace PU. An $m \times m$ matrix H over $\mathbb{F}_q^2$ is said to be *Hermitian*, if $\bar{H}^T = H$. For an m-dimensional subspace P, the matrix $P\bar{P}^T$ is an $m \times m$ Hermitian matrix, assume that it is of rank r, then r is also called the *rank* of the subspace P and P is called a subspace of *type* (m, r). Subspaces of type $(m, 0)$ are called m-dimensional *totally isotropic* subspaces and subspaces of type (m, m) are called m-dimensional *non-isotropic* subspaces.

It is known that [7] subspaces of type (m, r) exist if and only if

$$2r \le 2m \le n + r$$

and that [8] there exists a subspace of type (m_1, r_1) contained in a subspace of type (m, r) if and only if

$$2r_1 \le 2m_1 \le n + r_1,\ 2r \le 2m \le n + r, \text{ and } 0 \le r - r_1 \le 2(m - m_1).$$

It is well known that [2] subspaces of the same type form a transitive set of subspaces under $U_n(\mathbb{F}_{q^2})$ and that [9] the number of subspaces of type (m, r) in the n-dimensional unitary space $V_n(\mathbb{F}_{q^2})$, denoted by $N(m, r; n)$, is equal to

$$N(m, r; n) = q^{r(n+r-2m)} \frac{\prod_{i=n+r-2m+1}^{n} (q^i - (-1)^i)}{\prod_{i=1}^{r} (q^i - (-1)^i) \prod_{i=1}^{m-r} (q^{2i} - 1)}. \tag{1}$$

It is known that [6] the number of subspaces of type (m_1, r_1) contained in a given subspace of type (m, r) denoted $N(m_1, r_1; m, r; n)$, is equal to

$$N(m_1, r_1; m, r; n) = \sum_{k=\max(0,[\frac{2m_1-r-r_1+1}{2}])}^{\min(m-r,m_1-r_1)} q^{r_1(r+r_1-2m_1+2k)+2(m_1-k)(m-r-k)}$$

$$\times \frac{\prod_{i=r+r_1-2m_1+2k+1}^{r} (q^i - (-1)^i) \prod_{i=m-r-k+1}^{m-r} (q^{2i} - 1)}{\prod_{i=1}^{r_1} (q^i - (-1)^i) \prod_{i=1}^{m_1-r_1-k} (q^{2i} - 1) \prod_{i=1}^{k} (q^{2i} - 1)}. \tag{2}$$

And it is also known that [10] the number of subspaces of type (m, r) containing a given subspace of type (m_1, r_1) denoted by $N'(m_1, r_1; m, r; n)$ is equal to

$$N'(m_1, r_1; m, r; n) = \sum_{k=\max(0,[\frac{2m_1-r-r_1+1}{2}])}^{\min(m-r,m_1-r_1)} q^{(n-2m+r)(r+r_1-2m_1+2k)+2(n-m-k)(m_1-r-k)}$$
$$\times \frac{\prod_{i=r+r_1-2m_1+2k+1}^{n-2m_1+r_1} (q^i - (-1)^i) \prod_{i=m_1-r_1-k+1}^{m_1-r_1} (q^{2i} - 1)}{\prod_{i=1}^{n-2m+r} (q^i - (-1)^i) \prod_{i=1}^{m-r-k} (q^{2i} - 1) \prod_{i=1}^{k} (q^{2i} - 1)}. \tag{3}$$

Moreover, the number of m-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_{q^2}$, denoted by $N(m, n)$ is known to be

$$N(m, n) = \frac{\prod_{i=n-m+1}^{n} (q^{2i} - 1)}{\prod_{i=1}^{m} (q^{2i} - 1)} \tag{4}$$

(Cf. [6], for instance).

Let u and v be vectors in $V_n(\mathbb{F}_{q^2})$. They are said to be *orthogonal*, if

$$u\bar{v}^T = 0$$

A vector u orthogonal to itself is called an *isotropic vector*; a nonzero isotropic vector u generates a 1-dimensional totally isotropic subspace $\langle u \rangle$. A vector u not orthogonal to itself is called a *nonisotropic vector* and it generates a 1-dimensional nonisotropic subspace $\langle u \rangle$. For any subspace, P, let

$$P^\perp = \{x \in V_n(\mathbb{F}_{q^2}) | x\bar{v}^T = 0, \text{ for all } v \in P\}$$

and call $P^\perp$ the dual subspace of P. Clearly, if P is a subspace of type (m, r) then $P^\perp$ is a subspace of type $(n - m, n - 2m + r)$. For any vector v, we denote $v^\perp = \langle v \rangle^\perp$.

Two $n \times n$ Hermitian matrices H and H' are said to be *congruent*, if there is an $n \times n$ nonsingular matrix Q such that $H' = QH\bar{Q}^T$. It is known that [1] $I^{(n)}$ is congruent to

$$\begin{bmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{bmatrix} \text{ if } n = 2\nu,$$

or

$$\begin{bmatrix} 0 & I^{(\nu)} & \\ I^{(\nu)} & 0 & \\ & & 1 \end{bmatrix} \text{ if } n = 2\nu + 1.$$

Denote these two matrices by $H_{2\nu}$ and $H_{2\nu+1}$, respectively. We introduce the notation $H_{2\nu+\delta}$, where $\delta = 0$ or 1, to cover these two cases. Define the unitary group of degree $2\nu + \delta$ with respect to $H_{2\nu+\delta}$ over $\mathbb{F}_{q^2}$ by

$$U_{2\nu+\delta}(\mathbb{F}_{q^2}) = \{U \in GL_{2\nu+\delta}(\mathbb{F}_{q^2}) \mid UH_{2\nu+\delta}\bar{U}^T = H_{2\nu+\delta}\},$$

and define an action of $U_{2\nu+\delta}(\mathbb{F}_{q^2})$ on $V_{2\nu+\delta}(\mathbb{F}_{q^2})$ by

$$V_{2\nu+\delta}(\mathbb{F}_{q^2}) \times U_{2\nu+\delta}(\mathbb{F}_{q^2}) \to V_{2\nu+\delta}(\mathbb{F}_{q^2})$$

$$((x_1, x_2, \ldots, x_{2\nu+\delta}), U) \mapsto (x_1, x_2, \ldots, x_{2\nu+\delta})U,$$

then we obtain the unitary space with respect to $H_{2\nu+\delta}$.

Let $n = 2\nu + \delta$ and Q be a $(2\nu + \delta) \times (2\nu + \delta)$ nonsingular matrix such that

$$QH_{2\nu+\delta}\,\bar{Q}^T = I^{(2\nu+\delta)},$$

then we have a group isomorphism

$$U_n(\mathbb{F}_{q^2}) \to U_{2\nu+\delta}(\mathbb{F}_{q^2})$$

$$U \mapsto Q^{-1}UQ$$

and an equivariant vector space isomorphism

$$V_n(\mathbb{F}_{q^2}) \to V_{2\nu+\delta}(\mathbb{F}_{q^2})$$

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1, x_2, \ldots, x_{2\nu+\delta})Q.$$

Therefore in studying unitary spaces we may choose either the unitary space with respect to $I^{(n)}$ or the unitary space with respect to $H_{2\nu+\delta}$.

Notice that in the unitary space $V_{2\nu+\delta}(\mathbb{F}_{q^2})$ with respect to $H_{2\nu+\delta}$, an m-dimensional subspace P is defined to be of type (m, r) if the rank of $PH_{2\nu+\delta}\bar{P}^T$ is r, two vectors u and v of $V_{2\nu+\delta}(\mathbb{F}_{q^2})$ are said to be orthogonal if $uH_{2\nu+\delta}\bar{v}^T = 0$, and the dual subspace $P^\perp$ of a subspace P is defined to be

$$P^{\perp} = \{x \in V_{2\nu+\delta}(\mathbb{F}_{q^2}) | xH_{2\nu+\delta}\bar{v}^T = 0, \text{ for all } v \in P\}.$$

3. Construction I

Let $1 \le m < m_0 \le [(n-1)/2]$, $0 \le 2r_1 \le 2m_1 \le n + r_1$, and $0 \le n - 2m_0 - r_1 \le 2(n - m_0 - m_1)$. Let P_0 be a fixed m_0-dimensional totally isotropic subspace of the n-dimensional unitary space $V_n(\mathbb{F}_{q^2})$. Then $P_0^{\perp}$ is a subspace of type $(n - m_0, n - 2m_0)$. The source states are the m-dimensional subspaces of P_0. The encoding rules are the subspaces of type (m_1, r_1) which are contained in $P_0^{\perp}$ and intersect P_0 at (0). The messages are the subspaces of type $(m + m_1, r_1)$ which are contained in $P_0^{\perp}$ and intersect P_0 in m-dimensional subspaces. Given a source state s and an encoding rule e, the join $s + e$ of the subspaces s and e is regarded as the message into which the source state s is encoded under e.

At first we shall prove

LEMMA 1. *Construction I yields a Cartesian authentication code.*

Proof. Let s be a source state and e an encoding rule. Then s is an m-dimensional subspace Q of P_0 and e is a subspace R of type (m_1, r_1) contained in $P_0^{\perp}$ and $R \cap P_0 = (0)$. Clearly $Q + R$ is a subspace of dimension $m + m_1$. Since $Q\bar{Q}^T = 0$ and $P_0\bar{R}^T = 0$, the rank of

$$\begin{pmatrix} Q \\ R \end{pmatrix} \overline{\begin{pmatrix} Q \\ R \end{pmatrix}}^T = \begin{pmatrix} 0 & \\ & R\bar{R}^T \end{pmatrix} \tag{5}$$

is equal to the rank of $R\bar{R}^T$, which is r_1. Thus $Q + R$ is a subspace of type $(m + m_1, r_1)$. Clearly $(Q + R) \cap P_0 = Q$ is of dimension m. Hence $Q + R$ is a message. Therefore we have a well-defined map

$$f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$$

$$(s, e) \mapsto \langle s, e \rangle.$$

Next, we prove that the map f is surjective. Let P be a message, that is a subspace of type $(m + m_1, r_1)$ which is contained in $P_0^{\perp}$ and intersects P_0 in an m-dimensional subspace. Let $Q = P \cap P_0$. Then Q is an m-dimensional subspace of P_0, hence is a source state. Let R be a complementary subspace of Q in P, i.e., $P = Q + R$. Clearly $\dim R = m_1$. Since $P\bar{P}^T$ is of rank r_1, from (5) we deduce that $R\bar{R}^T$ is also of rank r_1. Hence R is a subspace of type (m_1, r_1). Since $P \cap P_0 = Q$, $R \cap P_0 = (0)$. Therefore R is an encoding rule. Since $Q + R = P$, f is surjective.

Now let Q' be another source state which is encoded into P under an encoding rule R', i.e., $P = Q' + R'$. As a source state, $Q' \subset P_0$. Hence $Q' \subset P \cap P_0 = Q$. Therefore $Q' = Q$. This proves that the source state Q is uniquely determined by P and the independence of Q from R.

Let us now compute the size parameters of the code.

LEMMA 2.

$$|\mathcal{S}| = N(m, m_0),$$

where $N(m, m_0)$ *is given by (4).*

LEMMA 3.

$$|\mathcal{E}| = q^{2m_0m_1} N(m_1, r_1; n - 2m_0),$$

where $N(m_1, r_1; n - 2m_0)$ *is given by* (1).

Proof. $|\mathcal{E}|$ is equal to the number of subspaces of type (m_1, r_1) contained in $P_0^{\perp}$, which interests P_0 at (0). Let $n = 2\nu + \delta$, where $\delta = 0$ or 1. By the transitivity of the unitary group $U_{2\nu+\delta}(\mathbb{F}_{q^2})$ on the set of subspaces of the same type, we can assume that

$$P_0 = (I^{(m_0)}\ 0^{(m_0,\nu-m_0)}\ 0^{(m_0)}\ 0^{(m_0,\nu-m_0)}\ 0^{(m_0,\delta)})$$

which will be shortened as

$$P_0 = \begin{array}{cccccc} (& I^{(m_0)} & 0 & 0 & 0 & 0\ ) \\ & m_0 & \nu - m_0 & m_0 & \nu - m_0 & \delta \end{array} \tag{6}$$

where the m_0, $\nu - m_0$, ..., under $I^{(m_0)}$, 0, ..., signify that $I^{(m_0)}$, 0, ... are matrices with m_0 columns, $\nu - m_0$ columns, ..., respectively. Then

$$P_0^{\perp} = \begin{pmatrix} I^{(m_0)} & 0 & 0 & 0 & 0 \\ 0 & I^{(\nu-m_0)} & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-m_0)} & 0 \\ 0 & 0 & 0 & 0 & I^{(\delta)} \end{pmatrix} \tag{7}$$

Let R be a subspace of type (m_1, r_1) contained in $P_0^{\perp}$ such that $R \cap P_0 = (0)$. Since $R \subset P_0^{\perp}$, R is of the form

$$R = \begin{array}{cccccc} (& R_1 & R_2 & 0 & R_4 & R_5\ ) \\ & m_0 & \nu - m_0 & m_0 & \nu - m_0 & \delta \end{array} \tag{8}$$

Since $R \cap P_0 = (0)$,

$$(R_2\ \ R_4\ \ R_5)$$

is of rank m_1. Thus $(R_2\ R_4\ R_5)$ is a subspace of type (m_1, r_1) in the $(2(\nu - m_0) + \delta)$-dimensional unitary space. Consequently

$$|\mathcal{E}| = q^{2m_0m_1}N(m_1, r_1; n - 2m_0).$$

□

LEMMA 4. *The number of encoding rules contained in a message is*

$$q^{2mm_1}.$$

Proof. Let P be a message, i.e., a subspace of type $(m + m_1, r_1)$ contained in $P_0^{\perp}$ such that $P \cap P_0$ is of dimension m. Let $Q = P \cap P_0$ and R be a complementary subspace of Q in P, i.e., $P = Q \dot{+} R$. By the proof of Lemma 1, Q is the unique source state contained in P and R is an encoding rule contained in P. Following the notation of Lemma 3, we can assume that

$$Q = \begin{array}{cccccc} (I^{(m)} & 0^{(m,m_0-m)} & 0 & 0 & 0 & 0) \\ m & m_0 - m & \nu - m_0 & m_0 & \nu - m_0 & \delta \end{array}$$

and

$$R = \begin{array}{cccccc} (R_1 & R_2 & 0 & R_4 & R_5) & m_1 \\ m_0 & \nu - m_0 & m_0 & \nu - m_0 & \delta & \end{array}$$

where m_1 signifies that all the matrices $R_1, R_2, \ldots$ have m_1 row, and (R_2, R_4, R_5) is a subspace of type (m_1, r_1) in the $(2(\nu - m_0) + \delta)$-dimensional unitary space. Then

$$P = \begin{array}{c} \left(\begin{array}{ccccc} (I^{(m)}\ 0) & 0 & 0 & 0 & 0 \\ R_1 & R_2 & 0 & R_4 & R_5 \end{array} \right) \begin{array}{c} m \\ m_1 \end{array} \\ \begin{array}{ccccc} m_0 & \nu - m_0 & m_0 & \nu - m_0 & \delta \end{array} \end{array}$$

Clearly, the number of encoding rules contained in P is q^{2mm_1}. □

LEMMA 5. $|\mathcal{M}| = q^{2(m_0-m)m_1} N(m, m_0) N(m_1, r_1; n - 2m_0)$.

Proof. By Lemma 1, each message contains a unique source state. By Lemma 4, each message contains q^{2mm_1} encoding rules. Thus

$$|\mathcal{M}| = \frac{|\mathcal{S}|\ |\mathcal{E}|}{q^{2mm_1}}.$$

□

LEMMA 6. *Let P_1 and P_2 be two distinct messages and let Q_1 and Q_2 be the unique source states contained in P_1 and P_2, respectively. Let dim $(Q_1 \cap Q_2) = s$. Assume that P_1 and P_2 have an encoding rule in common, then the number of encoding rules contained in both P_1 and P_2 is q^{2m_1s}.*

Proof. Let $Q_1 \cap Q_2 = Q_0$. Then there exist $(m - s)$-dimensional subspaces Q_1' and Q_2' of Q_1 and Q_2, respectively, such that

$$Q_1 = Q_0 \dot{+} Q_1', \qquad Q_2 = Q_0 \dot{+} Q_2', \qquad \text{and} \qquad Q_1' \cap Q_2' = (0),$$

where $\dot{+}$ denotes the direct sum. Let R be an encoding rule contained in both P_1 and P_2. Then

$$P_1 = Q_1 \dot{+} R = Q_0 \dot{+} Q_1' \dot{+} R,$$

$$P_2 = Q_2 \dot{+} R = Q_0 \dot{+} Q_2' \dot{+} R.$$

Let $n = 2\nu + \delta$, where $\delta = 0$ or 1, and consider the $(2\nu + \delta)$-dimensional unitary space with respect to $H_{2\nu+\delta}$. As in Lemma 3 we can assume that P_0, $P_0^\perp$, and R have matrix representations (6), (7), and (8), respectively, where

$$(R_2\ R_4\ R_5)$$

is a subspace of type (m_1, r_1) in the $(2(\nu - m_0) + \delta)$-dimensional unitary space. We can also assume that

$$Q_0 = \begin{array}{cccccccl} (& I^{(s)} & 0^{(s,m_0-s)} & 0 & 0 & 0 & 0\ ) & s \\ & s & m_0 - s & \nu - m_0 & m_0 & \nu - m_0 & \delta & \end{array}$$

Let

$$B = \begin{array}{cccccccl} (& B_1 & 0 & 0 & 0 & 0 & 0\ ) & m_1 \\ & s & m_0 - s & \nu - m_0 & m_0 & \nu - m_0 & \delta & \end{array} \tag{9}$$

Denote the subspace generated by the row vectors of the matrix B also by B. Then the subspace B is contained in Q_0. Clearly, $B + R$ is an encoding rule contained in both P_1 and P_2.

Conversely, let R' be an encoding rule contained in both P_1 and P_2. For any $\nu \in R'$, write

$$\nu = u_1 + u_1' + w_1,\ u_1 \in Q_0,\ u_1' \in Q_1',\ w_1 \in R,$$

$$\nu = u_2 + u_2' + w_2,\ u_2 \in Q_0,\ u_2' \in Q_2',\ w_2 \in R,$$

Since the sum $P_0 + R$ is direct, $u_1 + u_1' \in Q_1 \subseteq P_0$, and $u_2 + u_2' \in Q_2 \subseteq P_0$, we have necessarily $u_1 + u_1' = u_2 + u_2'$ and $w_1 = w_2$. It follows that $u_1 + u_1' = u_2 + u_2' \in Q_1 \cap Q_2 = Q_0$. Therefore $u_1' = u_2' = 0$ and $u_1 = u_2$. Hence every vector in R' is of the form $u_0 + w$, where $u_0 \in Q_0$ and $w \in R$. Thus R' has a matrix representation of form

$$R' = B + R$$

where B is of the form (9). Therefore the number of encoding rules contained in both P_1 and P_2 is $q^{2m_1 s}$. □

Assume now that the encoding rules are chosen according to a uniform probability distribution, let us compute P_I and P_S. By Lemmas 3 and 4, we have

$$P_I = \frac{1}{q^{2(m_0-m)m_1}N(m_1, r_1; n - 2m_0)}.$$

Suppose now that P_1 and P_2 are two distinct messages containing an encoding rule in common. Let Q_1 and Q_2 be the unique source states which are contained in P_1 and P_2, respectively. Assume then $\dim(Q_1 \cap Q_2) = s$, then $0 \le s \le m - 1$. By Lemmas 4 and 6, we have

$$P_S(P_2|P_1) = \frac{1}{q^{2m_1(m-s)}} \le \frac{1}{q^{2m_1}}$$

Clearly, given any source state Q_1 there is a source state Q_2 such that $\dim(Q_1 \cap Q_2) = m - 1$. Hence

$$P_S = \frac{1}{q^{2m_1}}.$$

Summarizing, we obtain

THEOREM 7. *Construction I yields a Cartesian authentication code with size parameters*

$$|\mathcal{S}| = N(m, m_0),$$
$$|\mathcal{E}| = q^{2m_0 m_1}N(m_1, r_1; n - 2m_0),$$
$$|\mathcal{M}| = q^{2(m_0-m)m_1}N(m, m_0)N(m_1, r_1; n - 2m_0),$$

where $N(m, m_0)$ and $N(m_1, r_1; n - 2m_0)$ are given by (4) *and* (1) *respectively. Assume that the encoding rules are chosen according to a uniform probability distribution, then the probabilities of a successful impersonation attack P_I and of a successful substitution attack P_S are given by*

$$P_I = \frac{1}{q^{2(m_0-m)m_1}N(m_1, r_1; n - 2m_0)}$$

and

$$P_S = \frac{1}{q^{2m_1}}$$

respectively. □

COROLLARY 8. *If in Construction I we take $(m_1, r_1) = (1, 1)$, i.e., the encoding rules are the 1-dimensional non-isotropic subspaces contained in $P_0^{\perp}$, then we obtain an authentication code with size parameters*

$$|\mathcal{S}| = \frac{\prod_{i=m_0-m+1}^{m_0} (q^{2i} - 1)}{\prod_{i=1}^{m} (q^{2i} - 1)},$$

$$|\mathcal{E}| = \frac{q^{n-1}(q^{n-2m_0} - (-1)^{n-2m_0})}{q+1},$$

$$|\mathcal{M}| = \frac{q^{n-2m-1}(q^{n-2m_0} - (-1)^{n-2m_0}) \prod_{i=m_0-m+1}^{m_0} (q^{2i} - 1)}{(q+1)\prod_{i=1}^{m} (q^{2i} - 1)},$$

and probabilities of successful attacks

$$P_I = \frac{1}{\dfrac{q^{n-2m-1}(q^{n-2m_0} - (-1)^{n-2m_0})}{q+1}}, \quad P_S = \frac{1}{q^2}.$$

□

In view of the combinatorial lower bounds $P_I \geq k/v$ and $P_S \geq (k-1)/(v-1)$ (here $k = |\mathcal{S}|$ and $v = |\mathcal{M}|$), for the authentication code of Corollary 8 if we require the order of magnitude of P_S as a function of q to be optimal, we obtain necessarily: n odd, $m_0 = (n-1)/2$, and $m = (n-3)/2$. Thus we have an authentication code with size parameters

$$|\mathcal{S}| = \frac{q^{2n-2} - 1}{q^2 - 1}, \qquad |\mathcal{E}| = q^{n-1}, \qquad |\mathcal{M}| = \frac{q^2(q^{2n-2} - 1)}{q^2 - 1}$$

for which P_I is optimal and P_S is nearly optimal.

COROLLARY 9. *If in Construction I we take $(m_1, r_1) = (1, 0)$, i.e., the encoding rules are the 1-dimensional totally isotropic subspaces contained in $P_0^\perp$ but not contained in P_0, then we obtain an authentication code with size parameters*

$$|\mathcal{S}| = \frac{\prod_{i=m_0-m+1}^{m_0} (q^{2i} - 1)}{\prod_{i=1}^{m} (q^{2i} - 1)},$$

$$|\mathcal{E}| = \frac{q^{2m_0} \prod_{i=n-2m_0-1}^{n-2m_0} (q^i - (-1)^i)}{q^2 - 1},$$

$$|\mathcal{M}| = \frac{q^{2(m_0-m)} \prod_{i=n-2m_0-1}^{n-2m_0} (q^i - (-1)^i) \prod_{i=m_0-m+1}^{m_0} (q^{2i} - 1)}{(q^2 - 1) \prod_{i=1}^{m} (q^{2i} - 1)},$$

and probabilities of successful attacks

$$P_I = \frac{1}{\dfrac{q^{2(m_0-m)} \prod_{i=n-2m_0-1}^{n-2m_0} (q^i - (-1)^i)}{q^2 - 1}}, \quad P_S = \frac{1}{q^2}.$$

□

It should be remarked that in Corollary 9, when n is odd and $m_0 = (n - 1)/2$, we get $|\mathcal{E}| = |\mathcal{M}| = 0$, which is not interesting. Thus the case when n is odd and $m_0 = (n - 1)/2$ should be excluded.

Moreover, Construction I can be generalized as follows.

Generalized Construction I. Let $2r_0 \le 2m_0 \le n + r_0$ and P_0 be a fixed subspace of type (m_0, r_0) in the n-dimensional unitary space over $\mathbb{F}_{q^2}$. Then $P_0^\perp$ is a subspace of type $(n - m_0, n - 2m_0 + r_0)$. Assume that (m, r) satisfies $2r \le 2m \le n + r$ and $0 \le r_0 - r \le 2(m_0 - m)$, and that (m_1, r_1) satisfies $2r_1 \le 2m_1 \le n + r_1$ and $0 \le n - 2m_0 + r_0 - r_1 \le 2(n - m_0 - m_1)$. The source states are the subspaces of type (m, r) contained in P_0. The encoding rules are the subspaces of type (m_1, r_1) which are contained in $P_0^\perp$

and intersect P_0 at (0). The messages are the subspaces of type $(m + m_1, r + r_1)$ having the property that each of them is the join of a subspace of type (m, r) contained in P_0 and a subspace of type (m_1, r_1) which is contained in $P_0^{\perp}$ and intersects P_0 at (0). Given a source state s and an encoding rule e, the join $s + e$ of the subspaces s and e can be proved to be a message and is defined to be the message into which s is encoded under e.

It can be proved in the same way as Lemma 1 that Generalized Construction I yields a Cartesian authentication code. The size parameters and the probabilities P_I and P_S can also be computed.

4. Construction II

Let $2r \leq 2m \leq n + r$. Let v_0 be a fixed nonzero isotropic vector of $V_n(\mathbb{F}_{q^2})$. Take the set of subspaces of type (m, r) containing v_0 and orthogonal to v_0 as the set $\mathcal{S}$ of source states, the set of 2-dimensional nonisotropic subspaces containing v_0 as the set $\mathcal{E}$ of encoding rules, and the set of subspaces of type $(m + 1, r + 2)$ containing v_0 and not orthogonal to v_0 as the set $\mathcal{M}$ of messages. Given a source state s (i.e., a subspace of type (m, r) containing v_0 and orthogonal to v_0) and an encoding rule e (i.e., a 2-dimensional nonisotropic subspace containing v_0), the join $s + e$ of the subspaces s and e is clearly a message and is regarded as the message into which s is encoded under e.

LEMMA 10. *Construction II results in a Cartesian authentication code.*

Proof. Let P be any message, i.e., a subspace of type $(m + 1, r + 2)$ containing v_0 and not orthogonal to v_0. Since $P \not\subseteq v_0^{\perp}$, there is a vector $u \in P$ such that $v_0\bar{u}^T = 1$. Then $R = \langle v_0, u\rangle$ is a 2-dimensional nonisotropic subspace containing v_0 and contained in P. Hence R is an encoding rule contained in P. Thus $V_n(\mathbb{F}_{q^2}) = R^{\perp} \dot{+} R$ and hence $P = (P \cap R^{\perp}) \dot{+} R$. Let $Q_0 = P \cap R^{\perp}$. Clearly $\dim Q_0 = m - 1$. Since Q_0 is orthogonal to R and the ranks of the subspaces P and R are $r + 2$ and 2, respectively, Q_0 is of type $(m - 1, r)$. Let $Q = \langle v_0\rangle \dot{+} Q_0$, then Q is a subspace of type (m, r) contained in P. Hence Q is a source state. Clearly $Q + R = P$, i.e., the source state Q is encoded under the encoding rule R into the message P.

Let Q' be another source state encoded to P under an encoding rule R'. Any vector $x \in Q'$ can be written in the direct sum decomposition

$$P = \langle v_0\rangle \dot{+} Q_0 + \langle u\rangle$$

as $x = \lambda v_0 + w + \mu u$, where $\lambda, \mu \in \mathbb{F}_{q^2}$ and $w \in Q_0$. Since Q' is orthogonal to v_0, $v_0\bar{x}^T = 0$. Thus $\mu = 0$, and $x \in Q$, hence $Q' \subset Q$. Since $\dim Q' = \dim Q = m$, $Q' = Q$. □

Let us now compute the size parameters of this code.

LEMMA 11.

$$|\mathcal{S}| = N(m-1, r; 2(\nu-1)+\delta),$$

where $N(m-1, r; 2(\nu-1)+\delta)$ *is given by* (1).

Proof. Let $n = 2\nu + \delta$, where $\delta = 0$ or 1 and consider the $(2\nu+\delta)$-dimensional unitary space with respect $H_{2\nu+\delta}$. Let Q be a source state. Since $v_0 \in Q$ and $v_0 H_{2\nu+\delta} \bar{Q}^T = 0$, we can assume that

$$v_0 = (1, 0, 0, \ldots, 0)$$

and

$$Q = \begin{array}{c} \left(\begin{array}{ccccc} 1 & 0\ldots0 & 0 & 0\ldots0 & 0 \\ 0 & Q_1 & 0 & Q_2 & Q_3 \end{array}\right) \begin{array}{c} 1 \\ m-1 \end{array} \\ \begin{array}{ccccc} 1 & \nu-1 & 1 & \nu-1 & \delta \end{array} \end{array}$$

It can be readily verified that

$$(Q_1 \quad Q_2 \quad Q_3)$$

is a subspace of type $(m-1, r)$ in the $(2(\nu-1)+\delta)$-dimensional unitary space over $\mathbb{F}_{q^2}$. Therefore

$$|\mathcal{S}| = N(m-1, r; 2(\nu-1)+\delta).$$

□

LEMMA 12. *The number of encoding rules is*

$$|\mathcal{E}| = q^{2n-4}.$$

Proof. The number of 2-dimensional subspaces containing v_0 is $(q^{2(n-1)} - 1)/(q^2 - 1)$. If $\langle v_0, u\rangle$ is a 2-dimensional totally isotropic subspace containing v_0, then $u\bar{v}_0^T = 0$. Since the solution space of $u\bar{v}_0^T = 0$ is of dimension $n - 1$ and contains v_0, the number of 2-dimensional totally isotropic subspaces containing v_0 is $(q^{2(n-2)} - 1)/(q^2 - 1)$.

Thus

$$|\mathcal{E}| = \frac{q^{2(n-1)} - 1}{q^2 - 1} - \frac{q^{2(n-2)} - 1}{q^2 - 1} = \frac{q^{2n-2} - q^{2n-4}}{q^2 - 1} = q^{2n-4}. \qquad \square$$

LEMMA 13. *The number of encoding rules contained in a message is*

$$q^{2(m-1)}.$$

Proof. Let P be a message, Q be the unique source state contained in P, and $R = \langle v_0, u\rangle$, where $v_0\bar{u}^T = 1$, be an encoding rule contained in P. Then $P = Q + R$. Let Q_0 be a complementary subspace of $\langle v_0\rangle$ in P. Then

$$P = Q_0 \dot{+} \langle v_0\rangle \dot{+} \langle u\rangle.$$

A 2-dimensional nonisotropic subspace containing v_0 and contained in P can be written in the form $\langle v_0, w + u\rangle$, where $w \in Q_0$. But $\dim Q_0 = m - 1$, hence the number of encoding rules contained in P is $q^{2(m-1)}$. □

LEMMA 14.

$$|\mathfrak{M}| = q^{2(n-m-1)}N(m - 1, r; 2(\nu - 1) + \delta),$$

where $N(m - 1, r; 2(\nu - 1) + \delta)$ *is given by* (1).

Proof. Same as Lemma 5. □

Now assuming that the encoding rules are chosen according to a uniform probability distribution, we compute the probabilities of a successful impersonation attack P_I and of a successful substitution attack P_S. It follows immediately from Lemmas 12 and 13 that

$$P_I = \frac{q^{2(m-1)}}{q^{2n-4}} = \frac{1}{q^{2(n-m-1)}}.$$

To compute P_S we need the following Lemma

LEMMA 15. *Let* P_1 *and* P_2 *be two distinct messages and* Q_1 *and* Q_2 *be the unique source states contained in them, respectively. Let* $Q_1 \cap Q_2 = Q_0$ *and* $\dim Q_0 = s$, *then* $1 \le s \le m - 1$. *Assume that* P_1 *and* P_2 *have an encoding rule* $\langle v_0, u\rangle$, *where* $v_0\bar{u}^T = 1$, *in common. Then* $P_1 \cap P_2 = \langle Q_0, u\rangle$, $\dim(P_1 \cap P_2) = s + 1$, *and the number of encoding rules contained in both* P_1 *and* P_2 *is* $q^{2(s-1)}$.

Proof. Since $v_0 \in Q_1$ and $v_0 \in Q_2$, $v_0 \in Q_0$ and $s \ge 1$. Since $P_1 \ne P_2$, we have $Q_1 \ne Q_2$ and $s \le m - 1$. Let Q_1' and Q_2' be complementary subspaces of Q_0 in Q_1 and Q_2, respectively, i.e.,

$$Q_1 = Q_0 \dot{+} Q_1', \qquad Q_2 = Q_0 \dot{+} Q_2', \qquad \text{and} \qquad Q_1' \cap Q_2' = (0).$$

Clearly we have

$$P_1 = Q_0 \dot{+} Q_1' \dot{+} \langle u\rangle, \qquad P_2 = Q_0 \dot{+} Q_2' \dot{+} \langle u\rangle,$$

and $\langle Q_0, u\rangle \subset P_1 \cap P_2$. Let w be any vector of $P_1 \cap P_2$. Since $w \in P_i (i = 1, 2)$, w can be expressed uniquely as $w = w_i + w_i' + C_i u$, where $w_i \in Q_0$, $w_i' \in Q_i'$ and $c_i \in \mathbb{F}_{q^2} (i = 1, 2)$. Then $w\bar{v}_0^T = c_1 u\bar{v}_0^T = c_2 u\bar{v}_0^T$. Since $u\bar{v}_0^T \neq 0$, we have $c_1 = c_2$. Thus $w_1 + w_1' = w_2 + w_2' \in Q_1 \cap Q_2 = Q_0$. Consequently, $w_1' = w_2' = 0$ and $w_1 = w_2$. Therefore $w = w_1 + c_1 u \in \langle Q_0, u\rangle$. Hence $P_1 \cap P_2 = \langle Q_0, u\rangle$, $\dim (P_1 \cap P_2) = s + 1$, and the number of encoding rules contained in $P_1 \cap P_2$ is $q^{2(s-1)}$. □

Suppose now that P_1 and P_2 are two distinct messages containing an encoding rule in common and $\dim(P_1 \cap P_2) = s + 1$, where $1 \leq s \leq m - 1$. By Lemma 15 the number of encoding rules contained in $P_1 \cap P_2$ is

$$q^{2(s-1)}.$$

Hence

$$P_S(P_2 | P_1) = \frac{1}{q^{2(m-s)}} \leq \frac{1}{q^2}.$$

However, we have

LEMMA 16. *Let Q_1 be a source state, then there is a source state Q_2 such that* $\dim(Q_1 \cap Q_2) = m - 1$.

Proof. Let $n = 2\nu + \delta$, where $\delta = 0$ or 1, and consider the $(2\nu + \delta)$-dimensional unitary space with respect to $H_{2\nu+\delta}$. Consider the case when r is even, write $r = 2r'$. By the transitivity of $U_{2\nu+\delta}(\mathbb{F}_{q^2})$ we can assume that

$$v_0 = (1, 0, 0, \ldots, 0)$$

and

$$Q_1 = \begin{array}{c} \begin{pmatrix} I^{(m-r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r')} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r')} & 0 & 0 \end{pmatrix} \\ \begin{matrix} m-r & \quad r' & \quad \nu+r'-m & \quad m-r & \quad r' & \quad \nu+r'-m & \quad \delta \end{matrix} \end{array}.$$

Then

$$Q_2 = \begin{array}{c} \begin{pmatrix} I^{(m-r-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & I^{(r')} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(r')} & 0 & 0 \end{pmatrix} \\ \begin{matrix} m-r-1 & \quad 1 & \quad r' & \quad \nu+r'-m & \quad m-r-1 & \quad 1 & \quad r' & \quad \nu+r'-m & \quad \delta \end{matrix} \end{array}$$

is also a source state and $\dim (Q_1 \cap Q_2) = m - 1$. The case when r is odd can be treated in a similar way. □

From Lemmas 15 and 16 it follows immediately that

$$P_S = \frac{1}{q^2}.$$

Summarizing, we have

THEOREM 17. *Construction II yields a Cartesian authentication code with the following size parameters*

$$|\mathcal{S}| = N(m-1, r; 2(\nu-1)+\delta),$$
$$|\mathcal{E}| = q^{2n-4},$$
$$|\mathcal{M}| = q^{2(n-m-1)}N(m-1, r; 2(\nu-1)+\delta),$$

where $N(m-1, r; 2(\nu-1)+\delta)$ *is given by* (1).

Suppose that the encoding rules are chosen according to a uniform probability distribution, then the probabilities of a successful impersonation attack P_1 *and of a successful substitution attack* P_S *are given by*

$$P_I = \frac{1}{q^{2(n-m-1)}},\ P_S = \frac{1}{q^2},$$

respectively. □

COROLLARY 18. *If we take* $(m, r) = (m, 0)$ *in construction II, then we obtain an authentication code with size parameters*

$$|\mathcal{S}| = \frac{\prod_{i=n-2m+1}^{n-2} (q^i - (-1)^i)}{\prod_{i=1}^{m-1} (q^{2i} - 1)},$$

$$|\mathcal{E}| = q^{2n-4},$$

$$|\mathcal{M}| = q^{2(n-m-1)} \frac{\prod_{i=n-2m+1}^{n-2} (q^i - (-1)^i)}{\prod_{i=1}^{m-1} (q^{2i} - 1)},$$

and probabilities of successful attacks

$$P_I = \frac{1}{q^{2(n-m-1)}}, \ P_S = \frac{1}{q_2}.$$

□

For the authetication code in Corollary 18 if we require that the order of magnitude of P_S as a function of q to be optimal, we obtain necessarily: $n = 4$ and $m = 2$. Thus we have an authentication code with size parameters $|\mathcal{S}| = q + 1$, $|\mathcal{E}| = q^4$, $|\mathcal{M}| = q^2(q + 1)$, for which P_I is optimal and P_S is nearly optimal.

5. Construction III

Let $0 < m \leq r_0$ and $2r_0 \leq 2m_0 \leq n + r_0$. Let v_0 be a fixed nonzero isotropic vector in the n-dimensional unitary space over $\mathbb{F}_{q^2}$, P_0 be a fixed subspace of type (m_0, r_0) containing v_0 and assume that $v_0 \notin P_0^\perp$. The source states are the m-dimensional nonisotropic subspaces, contained in P_0 and containing v_0. The encoding rules are the 2-dimensional nonisotropic subspaces not contained in P_0 but containing v_0. The messages are $(m + 1)$-dimensional subspaces, which contain v_0 and intersect P_0 in m-dimensional nonisotropic subspaces. Denote the set of source states, the set of encoding rules, and the set of messages by $\mathcal{S}$, $\mathcal{E}$, and $\mathcal{M}$, respectively. Given an $s \in \mathcal{S}$ and an $e \in \mathcal{E}$, we shall prove below that the join $s + e$ of s and e is a message and we call it the message into which s is encoded under e.

LEMMA 19. *Construction III yields a Cartesian authentication code.*

Proof. Let s be a source state and e an encoding rule. Then s is an m-dimensional nonisotropic subspace Q contained in P_0 and containing v_0, and e is a 2-dimensional nonisotropic subspace R not contained in P_0 but containing v_0. Clearly, $Q \cap R = \langle v_0 \rangle$ and $\dim(Q \cap R) = 1$. By dimension formula, $\dim(Q + R) = m + 1$. Define $P = Q + R$. Then P is an $(m + 1)$-dimensional subspace. Clearly, $v_0 \in P$ and

$$P \cap P_0 = (Q + R) \cap P_0 = Q + (R \cap P_0) = Q + \langle v_0 \rangle = Q.$$

Hence P is a message.

Now let P be a message. Let $Q = P \cap P_0$. By definition, Q is an m-dimensional nonisotropic subspace. Since $v_0 \in P$ and $v_0 \in P_0$, $v_0 \in Q$. Therefore Q is a source state. Since $P \neq P_0$, there is a vector $v \in P$ but $v \notin P_0$. If $\langle v_0, v \rangle$ is nonisotropic, let $R = \langle v_0, v \rangle$, then R is an encoding rule contained in P. Suppose that $v_0 \bar{v}^T = 0$. Since $v_0 \in Q$ and Q is nonisotropic, there is a vector $u \in Q$ such that $v_0 \bar{u}^T = 1$. Then $u + v \in P$, $u + v \notin P_0$, and $\langle v_0, u + v \rangle$ is nonisotropic. Set $R = \langle v_0, u + v \rangle$. Then $R \in \mathcal{E}$ and $R \subseteq P$. In both cases we have $P = Q + R$.

We can also prove that the source state Q is uniquely determined by the message P in the same way as Lemma 1. Therefore a Cartesian authentication code is obtained. □

To compute the size parameters of the code, we need the following auxiliary result.

LEMMA 20. *The number of subspace of type* (m_0, r_0) *containing* v_0 *and not orthogonal to* v_0 *is*

$$q^{2(n-m_0)}N(m_0 - 2, r_0 - 2; n - 2),$$

where $N(m_0 - 2, r_0 - 2; n - 2)$ *is given by* (1),

Proof. Let $n = 2\nu + \delta$, where $\delta =$ o or 1, and consider the unitary space with respect to $H_{2\nu+\delta}$. Without loss of generality we can assume that

$$v_0 = (1, 0, 0, \ldots, 0).$$

Let P be a subspace of type (m_0, r_0) containing v_0 and not orthogonal to v_0. Then there is a vector $u \in P$ such that $v_0 H_{2\nu+\delta}\bar{u}^T = 1$. Thus we can assume that

$$u = (0, \underbrace{*, \ldots, *}_{\nu-1}, 1, \underbrace{*, \ldots, *}_{\nu-1}, \underbrace{*}_{\delta}).$$

Then we can assume that P has a matrix representation of the form

$$P = \begin{array}{c} \left(\begin{array}{ccccc} 1 & 0\ldots0 & 0 & 0\ldots0 & 0 \\ 0 & *\ldots* & 1 & *\ldots* & * \\ 0 & P_1 & 0 & P_2 & P_3 \end{array}\right) \begin{array}{c} 1 \\ 1 \\ m_0 - 2 \end{array} \\ \begin{array}{ccccc} 1 & \nu - 1 & 1 & \nu - 1 & \delta \end{array} \end{array} \tag{10}$$

It can be readily verified that

$$(P_1 \;\; P_2 \;\; P_3) \tag{11}$$

is a subspace of type $(m_0 - 2, r_0 - 2)$ in the $(2(\nu - 1) + \delta)$-dimensional unitary space. The number of subspaces of type $(m_0 - 2, r_0 - 2)$ in the $(2(\nu - 1) + \delta)$-dimensional unitary space is denoted by $N(m_0 - 2, r_0 - 2; n - 2)$ and is given by (1). By the transitivity of the unitary group on the set of subspaces of the same type, it is sufficient to compute the number of subspaces of the form (10), with a fixed (11) of type $(m_0 - 2, r_0 - 2)$. For simplicity we consider only the case $r_0 - 2$ is even and write $r_0 - 2 = 2r'$. We choose

$$(P_1\, P_2\, P_3) = \begin{pmatrix} I^{(r')} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r')} & 0 & 0 & 0 \\ 0 & I^{(m_0-r_0)} & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Then we can assume that P has a matrix representation of the form

$$\begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & * & 1 & 0 & * & * & * \\ 0 & I^{(r')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(r')} & 0 & 0 & 0 \\ 1 & 0 & I^{(m_0-r_0)} & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} 1 & r' & m_0 - r_0 & \nu + r_0/2 - m_0 & 1 & r' & m_0 - r_0 & \nu + r_0/2 - m_0 & \delta. \end{matrix}\end{array} \tag{12}$$

Clearly the number of subspaces of type (m_0, r_0) whose matrix representations are of the form (12) is $q^{2(n-m_0)}$. The case when $r_0 - 2$ is odd can be treated in a similar way, and we obtain the same conclusion. Therefore the number of subspaces of type (m_0, r_0) containing v_0 and not orthogonal to v_0 is

$$q^{2(n-m_0)}N(m_0 - 2, r_0 - 2; n - 2).$$

□

Let us now compute the size parameters of the code.

LEMMA 21.

$$|\mathcal{S}| = \frac{N'(1, 0; m, m; n)N'(m, m; m_0, r_0; n)}{q^{2(n-m_0)}N(m_0 - 2, r_0 - 2; n - 2)},$$

where $N'(1, 0; m, m; n)$ *and* $N'(m, m; m_0, r_0; n)$ *are given by* (3) *and* $N(m_0 - 2, r_0 - 2; n - 2)$ *is given by* (1).

Proof. $|\mathcal{S}|$ is the number of m-dimensional nonisotropic subspaces contained in P_0 and containing v_0. We count for every m-dimensional nonisotropic subspace containing v_0 the number of subspaces of type (m_0, r_0) containing this given m-dimensional nonisotropic subspace. This count equals to $N'(m, m; m_0, r_0; n)$. The sum for all the $N'(1, 0; m, m; n)$ m-dimensional nonisotropic subspaces containing v_0 is equal to

$$N'(1, 0; m, m; n)N'(m, m; m_0, r_0; n), \tag{13}$$

which must be equal to the overall count obtained by counting for every subspaces of type (m_0, r_0) containing v_0 and not orthogonal to v_0 the number of m-dimensional nonisotropic subspaces containing v_0 that it contains. By Lemma 20 the latter is

$$|\mathcal{S}|\; q^{2(n-m_0)}N(m_0 - 2, r_0 - 2; n - 2). \tag{14}$$

From the equality of (13) and (14) Lemma 21 follows.

LEMMA 22. $|\mathcal{E}| = q^{2(m_0-2)}(q^{2(n-m_0)} - 1)$.

Proof. $|\mathcal{E}|$ is equal to the number of 2-dimensional nonisotropic subspaces not contained in P_0 but containing v_0. Since $v_0 \notin P_0^{\perp}$, there is a vector $v \in P_0$ such that $v_0\bar{v}^T = 1$. Let U be a complementary subspace of $\langle v_0, v\rangle$ in P_0, and let W be a complementary subspace of P_0 in $V_n(\mathbb{F}_{q^2})$. Then

$$V_n(\mathbb{F}_{q^2}) = \langle v_0\rangle + \langle v\rangle + U + W.$$

Let $\langle v_0, x\rangle$ be an encoding rule, we can assume that

$$x = \lambda v + u + w, \tag{15}$$

where $\lambda \in \mathbb{F}_{q^2}$, $u \in U$, $w \in W$ and $w \neq 0$. We must have $v_0\overline{(\lambda v + u + w)}^T \neq 0$, i.e., $\lambda + v_0\overline{(u + w)}^T \neq 0$. For any nonzero vector $w \in W$ and any vector $u \in U$, there are $q^2 - 1$ values λ in $\mathbb{F}_{q^2}$ such that $\langle v_0, x\rangle$ is an encoding rule. All together we obtain

$$(q^{2(n-m_0)} - 1)q^{2(m_0-2)}(q^2 - 1)$$

encoding rules of the form $\langle v_0, x\rangle$, where x is of the form (15). Two encoding rules $\langle v_0, x\rangle$ and $\langle v_0, x'\rangle$, where x and x' are of the form (15) coincide if and only if x and x' are proportional. Hence

$$|\mathcal{E}| = \frac{(q^{2(n-m_0)} - 1)q^{2(m_0-2)}(q^2 - 1)}{q^2 - 1} = q^{2(m_0-2)}(q^{2(n-m_0)} - 1).$$

□

LEMMA 23. *The number of encoding rules contained in a message is*

$$q^{2(m-2)}(q^2 - 1).$$

Proof. Similar to the proof of Lemma 13. □

LEMMA 24.

$$|\mathcal{M}| = \frac{(q^{2(n-m_0)} - 1)N'(1, 0; m, m; n)N'(m, m; m_0, r_0; n)}{q^{2(n+m-2m_0)}(q^2 - 1)N(m_0 - 2, r_0 - 2; n - 2)}.$$

Proof. Same as Lemma 5. □

Now assume that the encoding rules are chosen according to a uniform probability distribution. Let us compute the probabilities of a successful impersonation attack P_I and of a successful substitution attack P_S. From Lemmas 22 and 23 we have

$$P_I = \frac{1}{\dfrac{q^{2(m_0-m)}(q^{2(n-m_0)}-1)}{q^2-1}}.$$

To compute P_S, we need

LEMMA 25. *Let P_1 and P_2 be two distinct messages which contain an encoding rule in common, and let Q_1 and Q_2 be the unique source states contained in P_1 and P_2, respectively. Assume that $\dim(Q_1 \cap Q_2) = s$, then $1 \leq s \leq m-1$ and the number of encoding rules contained in both P_1 and P_2 is either*

$$q^{2(s-2)}(q^2-1) \quad \text{or} \quad q^{2(s-1)}.$$

Proof. Let $R = \langle v_0, u\rangle$, where $v_0\bar{u}^T = 1$, be a common encoding rule contained in both P_1 and P_2. Then

$$P_1 = Q_1 \dotplus \langle u\rangle, \qquad P_2 = Q_2 \dotplus \langle u\rangle.$$

Let $Q_1 \cap Q_2 = Q_0$, then $\dim Q_0 = s$. Since $v_0 \in Q_1 \cap Q_2$, $s \geq 1$. Since $P_1 \neq P_2$, $s \leq m-1$. There exist subspaces Q_1' and Q_2' of Q_1 and Q_2, respectively, such that

$$Q_1 = Q_0 \dotplus Q_1', \qquad Q_2 = Q_0 \dotplus Q_2'.$$

Then

$$P_1 = Q_0 \dotplus Q_1' \dotplus \langle u\rangle, \qquad P_2 = Q_0 \dotplus Q_2' \dotplus \langle u\rangle.$$

Clearly, $\langle v_0, v+u\rangle$, where $v \in Q_0$ and $v_0\overline{(v+u)}^T \neq 0$, is an encoding rule contained in both P_1 and P_2. Conversely, let $\langle v_0, w\rangle$ be an encoding rule contained in both P_1 and P_2. We can express w in two ways

$$w = v_1 + v_1' + \lambda_1 u, \qquad v_1 \in Q_0, \qquad v_1' \in Q_1', \qquad \lambda_1 \in \mathbb{F}_{q^2},$$

$$w = v_2 + v_2' + \lambda_2 u, \qquad v_2 \in Q_0, \qquad v_2' \in Q_2', \qquad \lambda_2 \in \mathbb{F}_{q^2},$$

Since $P_0 + < u >$ is a direct sum, $\lambda_1 = \lambda_2$. Thus $v_1 + v_1' = v_2 + v_2' \in Q_1 \cap Q_2 = Q_0$. It follows that $v_1' = v_2' = 0$ and $v_1 = v_2$. Hence $\langle v_0, w\rangle = \langle v_0, v+u\rangle$, where $v \in Q_0$.

Let us enumerate the number of encoding rules contained in both P_1 and P_2. At first, we notice that $\langle v_0, v+u\rangle$ and $\langle v_0, v'+u\rangle$, where $v, v' \in Q_0$, is the same 2-dimensional subspace if and only if $v - v' = \lambda v_0$, where $\lambda \in \mathbb{F}_{q^2}$. Thus the number of encoding rules contained in both P_1 and P_2 is equal to the number of encoding rules of the form $\langle v_0, v+u\rangle$, where $v \in Q_0$, divided by q^2. Then we distinguish the following two cases:

(a) $v_0\bar{Q}_0^T \neq 0$. $\langle v_0, v + u\rangle$, where $v \in Q_0$, is an encoding rule if and only if $v_0\overline{(v + u)}^T \neq 0$, i.e., if and only if $v_0\bar{v}^T \neq -1$. The number of solutions of $v_0\bar{x}^T = -1$ in Q_0 is $q^{2(s-1)}$. Hence the number of encoding rules contained in both P_1 and P_2 is

$$(q^{2s} - q^{2(s-1)})/q^2 = q^{2(s-2)}(q^2 - 1).$$

(b) $v_0\bar{Q}_0^T = 0$. For any $v \in Q_0$, we have $v_0\overline{(v + u)}^T = 1$. Thus $\langle v_0, v + u\rangle$ is an encoding rule contained in both P_1 and P_2. Therefore the number of encoding rules contained in both P_1 and P_2 is

$$q^{2s}/q^2 = q^{2(s-1)}.$$

□

From Lemmas 23 and 25 it follows immediately that

$$P_S = \frac{1}{q^2 - 1}.$$

Summarizing, we obtain

THEOREM 26. *Construction III results in a Cartesian authentication code with size parameters*

$$|\mathcal{S}| = \frac{N'(1, 0; m, m; n)N'(m, m; m_0, r_0; n)}{q^{2(n-m_0)}N(m_0 - 2, r_0 - 2; n - 2)},$$

$$|\mathcal{E}| = q^{2(m_0-2)}(q^{2(n-m_0)} - 1),$$

$$|\mathcal{M}| = \frac{(q^{2(n-m_0)} - 1)N'(1, 0; m, m; n)N'(m, m; m_0, r_0; n)}{q^{2(n+m-2m_0)}(q^2 - 1)N(m_0 - 2, r_0 - 2; n - 2)}.$$

Assume that the encoding rules are chosen with a uniform probability distribution and denote the probabilities of a successful impersonation attack and of a successful substitution attack by P_I and P_S, respectively, then

$$P_I = \frac{1}{\dfrac{q^{2(m_0-m)}(q^{2(n-m_0)} - 1)}{q^2 - 1}},$$

$$P_S = \frac{1}{q^2 - 1}.$$

□

For the authentication code resulted from Construction III if we require the order of magnitude of P_I and P_S as functions of q to be optimal, we obtain necessarily $m = n - 2$.

Construction III can be generalized as follows:

Generalized construction III. Let $2r_0 \leq 2m_0 \leq n + r_0$, $2r \leq 2m \leq n + r$, and $0 \leq r_0 - r \leq 2(m_0 - m)$. Let v_0 be a fixed nonzero isotropic vector in the n-dimensional unitary space over $\mathbb{F}_{q^2}$, let P_0 be a fixed subspace of type (m_0, r_0) containing v_0, and assume that $v_0 \notin P_0^\perp$. The source states are the subspaces of type (m, r) contained in P_0, containing v_0 and not orthogonal to v_0. The encoding rules are the 2-dimensional nonisotropic subspaces not contained in P_0 but containing v_0. The messages are the $(m + 1)$-dimensional subspaces which intersect P_0 in a subspace of type (m, r) containing v_0 and not orthogonal to v_0. Given a source state s and an encoding rule e, the join $s + e$ of the subspaces s and e can be proved to be a message and is defined to be the message into which s is encoded under e.

It can be proved in the same way as Lemma 19 that Generalized Construction III yields a Cartesian authentication code. Its size parameters and probabilities P_I and P_S can also be computed.

References

1. L.E. Dickson, *Linear Groups*, Teubner, Leipzig, 1990.
2. J. Dieudonné, *Sur les groupes classiques*, Hermann, Paris, 1948.
3. E.N. Gilbert, F.J. MacWilliams, and N.J.A. Sloane, Codes which detect deception, *Bell System Technical Journal*, Vol. 53 (1974), pp. 405-424.
4. G.J. Simmons, Authentication theory/coding theory, *Advances in Cryptology, Proceedings of Crypto 84, Lecture Notes in Computer Science 196*, Springer-Verlag, Berlin, New York, (1985), pp. 411-431.
5. G.J. Simmons, A Cartesian product construction for unconditionally secure authentication codes that permit arbitration, *Journal of Cryptology*, Vol. 3 (1990), pp. 77-104.
6. Zhe-xian Wan, Some Anzahl theorems in finite singular symplectic, unitary and orthogonal geometries, accepted for publication in *Discrete Mathematics*.
7. Zhe-xian Wan, On the unitary invariants of a subspace of a vector space over a finite field, *Chinese Science Bulletin*, Vol. 37 (1992), pp. 705-707.
8. Zhe-xian Wan, *Geoemetry of Classical Groups over Finite Fields*, Studentlitteratur, Lund, 1993.
9. Zhe-xian Wan and Benfu Yang, Studies in finite geometry and the construction of incomplete block designs III. Some Anzahl theorems in unitary geometry over finite fields and their applications, *Acta Mathematica Sinica* Vol. 15 (1965), pp. 533-544. (in Chinese.) English Translation: *Chinese Mathematics* Vol. 7 (1965), pp. 252-264.
10. Benfu Yang and Wendi Wei, Finite unitary geometry and PBIB designs I, *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol. 6 (1989), pp. 51-61.