Two Constructions of A^2-codes with Secrecy from Polynomials over Finite Fields *

Shangdi Chen, Xue Li,[†] Wenjing Tian

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

Abstract The authentication codes with arbitration are said to be A^2-codes. Two constructions of A^2-codes with secrecy from polynomials over finite fields are constructed to prevent communication systems from attacks which come from the opponent, the transmitter and the receiver. Parameters of the codes and probabilities of successful attacks are also computed. At last, two constructions are compared with an known one. It is important that a source state can't be recovered from the message without the knowledge of the transmitter's encoding rule or the receiver's decoding rule. It must be decoded before verification.

Key-words A^2-code; secrecy; finite field; polynomial

MSC 2010 05B25, 11E57, 94A60, 94A62

1 Introduction

As early as 1974, Gilbert, Macwilliams and Sloane[1] firstly constructed the authentication codes based on projective geometry over finite fields. In 1985, the information theory of authentication system was introduced by Simmons[2], who established three participants certification models, which include the transmitter, the receiver and the opponent based on trust between the transmitter and the receiver. They share common secret keys.

Confidentiality and authentication are two important aspects of information security. For authentication codes, there are authentication codes with secrecy and those without secrecy. In an authentication code without secrecy, a source

[*] Supported by the National Natural Science Foundation of China (No. 61179026), and the Fundamental Research Funds for the Central Universities (No. 3122016L005).

[†] Corresponding author. E-mail address: 1070558121@qq.com

state can be recovered from the encoded message without any secrecy keys, which is only used for authentication. For example, Wang and Xing[3,4] structured two constructions based on rank distance codes and algebraic curves over finite fields, respectively. In an authentication code with secrecy, a source state is hidden in the encoded message and can't be recovered without the secret key, which is used for both confidentiality and authentication. For instance, Stinson[5] introduced a construction based on combinatorial designs, and Ding[6] constructed some codes with secrecy based on trace functions.

But sometimes both the transmitter and the receiver are dishonest. In this case, they need an arbiter, an honest player, know all informations of the system. But he doesn't take part in communication and only adjust the dispute between them. As early as 1980's, Simmons[7,8] proposed authentication codes with arbitration to solve the distrust between the transmitter and the receiver. Adding an arbiter, four participants certification models were established, which are called authentication codes with arbitration, or A^2-codes for short.

In 1990's, Johansson[9,10] derived entropy based lower bounds on the cheating probabilities and the sizes of keys. In 2001, Kurosawa and Obana[11] given combinatorial bounds for them. In recent years, Gao, Chen, Nan and others[12–19] have constructed a lot of A^2-codes based on linear codes, projective geometry, singular symplectic geometry, pseudo-symplectic geometry and so on.

But A^2-codes with secrecy are rarely constructed. So a main goal is to construct A^2-codes with secrecy. It is hard to know the source state in an A^2-code with secrecy for an opponent when he observes a massage. Two constructions of A^2-codes with secrecy will be shown based on polynomials over finite fields in this paper.

The paper is structured as follows: The second part is preliminary knowledge about A^2-codes. In Section 3 and Section 4, we will construct two constructions of A^2-codes with secrecy from polynomials over finite fields, respectively. Parameters of the codes and probabilities of successful attacks are also calculated. In the last part, they are compared with an known one.

2 Preliminaries

Let $\mathscr{S}$, $\mathscr{E}_T$, $\mathscr{E}_R$ and $\mathscr{M}$ be four non-empty finite sets, which denote the set of source states, the set of transmitter's encoding rules, the set of receiver's decoding rules and the set of messages, respectively.

Definition 2.1. ([19]) *Let $f : \mathscr{S} \times \mathscr{E}_T \to \mathscr{M}$ and $g : \mathscr{M} \times \mathscr{E}_R \to \mathscr{S} \cup \{reject\}$ be two maps. The four tuple $(\mathscr{S}, \mathscr{E}_T, \mathscr{E}_R, \mathscr{M})$ is called authentication codes with arbitration (A^2-codes), if*

(1) *The maps f and g are surjective;*

(2) *For any $m \in \mathscr{M}$ and $e_t \in \mathscr{E}_T$, if there is an $s \in \mathscr{S}$ satisfying $f(s,e_t) = m$, then such an s is uniquely determined by the given m and e_t;*

(3) *$P(e_t,e_r) \neq 0$ and $f(s,e_t) = m$ imply that $g(m,e_r) = s$, otherwise, $g(m,e_r) = \{reject\}$. Where $P(e_t,e_r) \neq 0$ implies that any s encoded by e_t can be authenticated by e_r.*

Some notations are introduced as follows: Let $\mathscr{E}_R(m)$ denote the set of receiver's decoding rules for a given $m \in \mathscr{M}$, i.e., $\mathscr{E}_R(m) = \{e_r \mid g(m,e_r) \in \mathscr{S}\}$. Let $\mathscr{E}_T(m)$ denote the set of transmitter's encoding rules for a given $m \in \mathscr{M}$, i.e., $\mathscr{E}_T(m) = \{e_t \mid f(s,e_t) = m,\ s \in \mathscr{S}\}$. Then $\mathscr{M}(e_t)$ is the set of messages for a given $e_t \in \mathscr{E}_T$, i.e., $\mathscr{M}(e_t) = \{m \mid f(s,e_t) = m,\ s \in \mathscr{S}\}$; $\mathscr{M}(e_r)$ is the set of messages for a given $e_r \in \mathscr{E}_R$, i.e., $\mathscr{M}(e_r) = \{m \mid g(m,e_r) \in \mathscr{S}\}$. Similarly, let $\mathscr{E}_T(e_r)$ denote the set of transmitter's encoding rules for a given $e_r \in \mathscr{E}_R$, i.e., $\mathscr{E}_T(e_r) = \{e_t \mid f(s,e_t) \in \mathscr{M}(e_r)$, for any $s \in \mathscr{S}\}$; let $\mathscr{E}_R(e_t)$ denote the set of receiver's decoding rules for a given $e_t \in \mathscr{E}_T$, i.e., $\mathscr{E}_R(e_t) = \{e_r \mid g(m,e_r) \in \mathscr{S}$, for any $m \in \mathscr{M}(e_t)\}$.

Definition 2.2. ([10]) *A^2-codes include five attacks.*

(1) *The impersonation attack by the opponent: The opponent sends $m \in \mathscr{M}$ to the receiver, and succeeds if and only if m is accepted by the receiver as authentic. So the largest probability of the opponent's successful impersonation attack is*

$$P_I = \max_{m} \frac{|\mathscr{E}_R(m)|}{|\mathscr{E}_R|}.$$

(2) *The substitution attack by the opponent: The opponent observes $m \in \mathscr{M}$ which is sent by the transmitter, and replaces it with $m' \in \mathscr{M}$, where $m \neq m'$, and $s \in \mathscr{S}$ hidden in m is different from $s' \in \mathscr{S}$ hidden in m'. The opponent is successful if and only if m' is accepted by the receiver as authentic. So the largest probability of the opponent's successful substitution attack is*

$$P_S = \max_{\substack{m,\, m' \\ m \neq m'}} \frac{|\mathscr{E}_R(m) \cap \mathscr{E}_R(m')|}{|\mathscr{E}_R(m)|}.$$

(3) *The impersonation attack by the receiver: When the transmitter doesn't send message to the receiver, the receiver claims that he has received $m \in \mathscr{M}$ from the transmitter, and succeeds if and only if m can be generated by the transmitter using his encoding rule. So the largest probability of the receiver's successful impersonation attack is*

$$P_{R_0} = \max_{m,\, e_r} \frac{|\mathscr{E}_T(m) \cap \mathscr{E}_T(e_r)|}{|\mathscr{E}_T(e_r)|}.$$

(4) *The substitution attack by the receiver: The receiver receives $m \in \mathscr{M}$ from the transmitter, but claims that he has received $m' \in \mathscr{M}$, where $m \neq m'$, and $s \in \mathscr{S}$*

hidden in m is different from $s' \in \mathscr{S}$ hidden in m'. The receiver succeeds if and only if m' can be generated by the transmitter using his encoding rule. So the largest probability of the receiver's successful substitution attack is

$$P_{R_1} = \max_{\substack{m,\, m',\, e_r \\ m \neq m'}} \frac{|\mathscr{E}_T(m) \cap \mathscr{E}_T(m') \cap \mathscr{E}_T(e_r)|}{|\mathscr{E}_T(m) \cap \mathscr{E}_T(e_r)|}.$$

(5) *The impersonation attack by the transmitter: The transmitter sends $m \in \mathscr{M}$ to the receiver, and then denies that he has sent it. He succeeds if and only if m is accepted by the receiver as authentic, and m is not one of the messages that the transmitter can generate using his encoding rule. So the largest probability of the transmitter's successful impersonation attack is*

$$P_T = \max_{\substack{m,\, e_t \\ m \notin \mathscr{M}(e_t)}} \frac{|\mathscr{E}_R(m) \cap \mathscr{E}_R(e_t)|}{|\mathscr{E}_R(e_t)|}.$$

Theorem 2.1. ([10]) *For any A^2-codes, parameters of the codes and probabilities of successful attacks satisfy following relationships:*

$$|\mathscr{E}_R| \geq (P_I P_S P_T)^{-1},$$
$$|\mathscr{E}_T| \geq (P_I P_S P_{R_0} P_{R_1})^{-1},$$
$$|\mathscr{M}| \geq (P_I P_{R_0})^{-1} |\mathscr{S}|.$$

In particular, if all of equalities hold up, then authentication codes with arbitration (A^2-codes) are called perfect.

3 Construction I

3.1 The model

For a odd prime q, let $\mathbb{F}_q$ be a finite field with q elements, $\mathbb{F}_q{}^* = \mathbb{F}_q \setminus \{0\}$. $\mathbb{F}_q[x]$ denotes a set of polynomials over $\mathbb{F}_q$, $\mathbb{F}_q[x]_\omega = \left\{ \sum_{i=0}^{\omega-1} a_i x^i \;\middle|\; a_i \in \mathbb{F}_q \right\}$, where $3 \leq \omega < \frac{q}{2} + 1$.

The set of source states is

$$\mathscr{S} = \{ s \mid s \in \mathbb{F}_q \}.$$

The set of transmitter's encoding rules is

$$\mathscr{E}_T = \left\{ e_t = (P_1(x), P_2(x), P_3(x)) \;\middle|\; P_i(x) \in \mathbb{F}_q[x]_\omega,\ i = 1,2,3, \text{ where } P_1(x) \neq 0 \right\}.$$

The set of receiver's decoding rules is

$$\mathscr{E}_R = \left\{ e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \;\middle|\; \beta_0, \beta_2, \beta_3 \in \mathbb{F}_q,\ \beta_1 \in \mathbb{F}_q{}^* \right\}.$$

The set of messages is

$$\mathscr{M} = \left\{ m = (P(x), Q(x)) \;\middle|\; P(x), Q(x) \in \mathbb{F}_q[x]_\omega \right\}.$$

3.2 Operating rules

1. Key generation and distribution

(1) The key distribution center (KDC) randomly and privately chooses an transmitter's encoding rule $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$, and sends it to the transmitter as his key.

(2) The KDC randomly selects $\beta_0 \in \mathbb{F}_q$, such that $P_1(\beta_0) \neq 0$, and calculates

$$\beta_1 = P_1(\beta_0),\ \beta_2 = P_2(\beta_0),\ \text{and}\ \beta_3 = P_3(\beta_0),$$

respectively. The KDC sends $e_r = (\beta_0, \beta_1, \beta_2, \beta_3)$ to the receiver as his key.

2. Broadcast

For the source state $s \in \mathscr{S}$, the transmitter generates an authenticated message using his key

$$P(x) = sP_1(x) + P_2(x),\ Q(x) = sP_2(x) + P_3(x),$$

and sends $m = (P(x), Q(x))$ to the receiver, where s is hidden in m.

3. Verification

The receiver can verify the authenticity of the received message. He calculates

$$s = \beta_1{}^{-1}(P(\beta_0) - \beta_2),$$

and accepts the message $m = (P(x), Q(x))$, if and only if

$$Q(\beta_0) = s\beta_2 + \beta_3.$$

Lemma 3.1. *The construction above is well-defined authentication codes with arbitration (A^2-codes), that is*

(1) $f(s, e_t) = m \in \mathscr{M}$, *for all* $s \in \mathscr{S}$ *and* $e_t \in \mathscr{E}_T$;

(2) *For any* $m \in \mathscr{M}$ *and* $e_t \in \mathscr{E}_T$, *if there is an* $s \in \mathscr{S}$ *satisfying* $f(s, e_t) = m$, *then such an* s *is uniquely determined by the given* m *and* e_t.

Proof. (1) It is obvious. For any $f(s,e_t) = m$, s is hidden in m, which can't be recovered from the encoded m without e_t.

(2) Let $m = (P(x), Q(x)) \in \mathscr{M}$ and $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$. Assume that s and $s' \in \mathscr{S}$ and $f(s,e_t) = m = f(s',e_t)$, then

$$\begin{cases} P(x) = sP_1(x) + P_2(x), \\ Q(x) = sP_2(x) + P_3(x), \\ P(x) = s'P_1(x) + P_2(x), \\ Q(x) = s'P_2(x) + P_3(x). \end{cases} \Longleftrightarrow \begin{cases} (s'-s)P_1(x) = 0, \\ (s'-s)P_2(x) = 0. \end{cases}$$

As $P_1(x) \neq 0$, $s = s'$. s is an uniquely source state contained in m. □

3.3 Parameters of codes

Theorem 3.1. *Parameters of A^2-codes which are constructed above are*

$$|\mathscr{S}| = q,\ |\mathscr{E}_T| = q^{2\omega}(q^{\omega} - 1),\ |\mathscr{E}_R| = q^3(q-1),\ \textit{and}\ |\mathscr{M}| = q^{2\omega},$$

respectively.

Proof. For $s \in \mathbb{F}_q$, and $\mathscr{S} = \mathbb{F}_q$, the number of source states is

$$|\mathscr{S}| = |\mathbb{F}_q| = q.$$

For any $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$, let

$$P_1(x) = a_0 + a_1 x + \cdots + a_{\omega-1} x^{\omega-1} \neq 0,\ a_j \in \mathbb{F}_q,$$
$$P_2(x) = b_0 + b_1 x + \cdots + b_{\omega-1} x^{\omega-1},\ b_j \in \mathbb{F}_q,$$
$$P_3(x) = c_0 + c_1 x + \cdots + c_{\omega-1} x^{\omega-1},\ c_j \in \mathbb{F}_q,$$

where $j = 0, 1, \cdots, \omega - 1$, then the number of transmitter's encoding rules is

$$|\mathscr{E}_T| = q^{2\omega}(q^{\omega} - 1).$$

For any $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$, there are β_0, β_2 and $\beta_3 \in \mathbb{F}_q$, and $\beta_1 \in \mathbb{F}_q{}^*$. So the number of receiver's decoding rules is

$$|\mathscr{E}_R| = q^3(q-1).$$

For any $m = (P(x), Q(x)) \in \mathscr{M}$, let

$$P(x) = h_0 + h_1 x + \cdots + h_{\omega-1} x^{\omega-1},\ h_j \in \mathbb{F}_q,$$
$$Q(x) = g_0 + g_1 x + \cdots + g_{\omega-1} x^{\omega-1},\ g_j \in \mathbb{F}_q,$$

where $j = 0, 1, \cdots, \omega - 1$. For any $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$, if the transmitter randomly selects $s \in \mathscr{S}$, then $P_2(x) = P(x) - sP_1(x) \in \mathbb{F}_q[x]_{\omega}$, $P_3(x) = Q(x) - sP_2(x) \in \mathbb{F}_q[x]_{\omega}$, and $f(s,e_t) = (P(x), Q(x)) \in \mathbb{F}_q[x]_{\omega} \times \mathbb{F}_q[x]_{\omega}$. So the number of messages is

$$|\mathscr{M}| = q^{2\omega}.$$ □

3.4 Probabilities of successful attacks

Lemma 3.2. *For any $m \in \mathscr{M}$, the number of $e_r \in \mathscr{E}_R$ which is incidence with m is*

$$|\mathscr{E}_R(m)| = q^2(q-1).$$

Proof. Assume that $m = (P(x), Q(x)) \in \mathscr{M}$. For $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$,

$$e_r \in \mathscr{E}_R(m) \Longleftrightarrow \begin{cases} s = \beta_1{}^{-1}(P(\beta_0) - \beta_2), \\ Q(\beta_0) = s\beta_2 + \beta_3. \end{cases}$$

If β_0, β_1 *and* β_2 are fixed, β_3 will be sure. So the number of $e_r \in \mathscr{E}_R(m)$ is

$$|\mathscr{E}_R(m)| = q^2(q-1). \qquad \square$$

Lemma 3.3. *For any $m, m' \in \mathscr{M}$, and $m \neq m'$, the number of $e_r \in \mathscr{E}_R$ which is incidence with m and m' is*

$$q(q-1) \geq |\mathscr{E}_R(m) \cap \mathscr{E}_R(m')| \geq (q-1)(q-\omega+1).$$

Proof. Assume that $m = (P(x), Q(x)), m' = (P'(x), Q'(x)) \in \mathscr{M}$, where $P(x) \neq P'(x)$. $s \in \mathscr{S}$ hidden in m is different from $s' \in \mathscr{S}$ hidden in m' $(s \neq s')$. For $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$,

$$\begin{aligned} & e_r \in \mathscr{E}_R(m) \cap \mathscr{E}_R(m') \\ \Longleftrightarrow & \begin{cases} s = \beta_1{}^{-1}(P(\beta_0) - \beta_2), \\ Q(\beta_0) = s\beta_2 + \beta_3, \\ s' = \beta_1{}^{-1}(P'(\beta_0) - \beta_2), \\ Q'(\beta_0) = s'\beta_2 + \beta_3. \end{cases} \Longleftrightarrow \begin{cases} P'(\beta_0) - P(\beta_0) = (s'-s)\beta_1, \\ Q'(\beta_0) - Q(\beta_0) = (s'-s)\beta_2. \end{cases} \end{aligned}$$

From above, $\begin{cases} P'(x) - P(x) \neq 0, \\ P'(\beta_0) - P(\beta_0) \neq 0, \end{cases}$ so the number of β_0 is at least $q - \omega + 1$ and at most q. If β_0 and β_1 are fixed, β_2 and β_3 will be sure. So the number of $e_r \in \mathscr{E}_R(m) \cap \mathscr{E}_R(m')$ is

$$q(q-1) \geq |\mathscr{E}_R(m) \cap \mathscr{E}_R(m')| \geq (q-1)(q-\omega+1). \qquad \square$$

Lemma 3.4. *For any $e_r \in \mathscr{E}_R$, the number of $e_t \in \mathscr{E}_T$ which is incidence with e_r is*

$$|\mathscr{E}_T(e_r)| = q^{3(\omega-1)} \text{ or } 0.$$

Proof. Assume that $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$. For $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$,

$$e_t \in \mathscr{E}_T(e_r) \Longleftrightarrow \begin{cases} P_1(\beta_0) = a_0 + a_1\beta_0 + \cdots + a_{\omega-1}\beta_0{}^{\omega-1} = \beta_1 \neq 0, \\ P_2(\beta_0) = b_0 + b_1\beta_0 + \cdots + b_{\omega-1}\beta_0{}^{\omega-1} = \beta_2, \\ P_3(\beta_0) = c_0 + c_1\beta_0 + \cdots + c_{\omega-1}\beta_0{}^{\omega-1} = \beta_3. \end{cases}$$

$$\Longleftrightarrow \begin{cases} (\ 1, \beta_0, \cdots, \beta_0{}^{\omega-1}\ ) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{\omega-1} \end{pmatrix} = \beta_1, \\ (\ 1, \beta_0, \cdots, \beta_0{}^{\omega-1}\ ) \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{\omega-1} \end{pmatrix} = \beta_2, \\ (\ 1, \beta_0, \cdots, \beta_0{}^{\omega-1}\ ) \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{\omega-1} \end{pmatrix} = \beta_3. \end{cases} \Longleftrightarrow A \begin{pmatrix} a_0 \\ \vdots \\ a_{\omega-1} \\ b_0 \\ \vdots \\ b_{\omega-1} \\ c_0 \\ \vdots \\ c_{\omega-1} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix},$$

where

$$A = \begin{pmatrix} 1, \beta_0, \cdots, \beta_0{}^{\omega-1} & & \\ & 1, \beta_0, \cdots, \beta_0{}^{\omega-1} & \\ & & 1, \beta_0, \cdots, \beta_0{}^{\omega-1} \end{pmatrix}.$$

Then the rank of the matrix A is 3. So the number of $e_t \in \mathscr{E}_T(e_r)$ is

$$|\mathscr{E}_T(e_r)| = q^{3(\omega-1)} \text{ or } 0. \qquad \square$$

Lemma 3.5. *For any $e_r \in \mathscr{E}_R$ and $m \in \mathscr{M}$, the number of $e_t \in \mathscr{E}_T$ which is incidence with e_r and m is*

$$|\mathscr{E}_T(e_r) \cap \mathscr{E}_T(m)| = q^{(\omega-1)} \textit{ or } 0.$$

Proof. Assume that $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$ and $m = (P(x), Q(x)) \in \mathscr{M}$. For $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$,

$$e_t \in \mathscr{E}_T(e_r) \cap \mathscr{E}_T(m)$$

$$\Longleftrightarrow \begin{cases} P_1(\beta_0) = \beta_1 \neq 0, \\ P_2(\beta_0) = \beta_2, \\ P_3(\beta_0) = \beta_3, \\ P(x) = sP_1(x) + P_2(x), \\ Q(x) = sP_2(x) + P_3(x). \end{cases} \Longleftrightarrow \quad B \begin{pmatrix} a_0 \\ \vdots \\ a_{\omega-1} \\ b_0 \\ \vdots \\ b_{\omega-1} \\ c_0 \\ \vdots \\ c_{\omega-1} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ h_0 \\ \vdots \\ h_{\omega-1} \\ g_0 \\ \vdots \\ g_{\omega-1} \end{pmatrix},$$

where

$$B = \begin{pmatrix} 1,\beta_0,\cdots,{\beta_0}^{\omega-1} & & \\ & 1,\beta_0,\cdots,{\beta_0}^{\omega-1} & \\ & & 1,\beta_0,\cdots,{\beta_0}^{\omega-1} \\ sI^{(\omega)} & I^{(\omega)} & \\ & sI^{(\omega)} & I^{(\omega)} \end{pmatrix},$$

$I^{(\omega)}$ is an $\omega \times \omega$ identity matrix, and the rank of the matrix B is $2\omega+1$. So the number of $e_t \in \mathscr{E}_T(e_r) \cap \mathscr{E}_T(m)$ is

$$|\mathscr{E}_T(e_r) \cap \mathscr{E}_T(m)| = q^{(\omega-1)} \text{ or } 0. \qquad \square$$

Lemma 3.6. *For any $e_r \in \mathscr{E}_R$, $m, m' \in \mathscr{M}$ and $m \neq m'$, the number of $e_t \in \mathscr{E}_T$ which is incidence with e_r, m and m' is*

$$|\mathscr{E}_T(e_r) \cap \mathscr{E}_T(m) \cap \mathscr{E}_T(m')| = 1 \textit{ or } 0.$$

Proof. Assume $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$, $m = (P(x), Q(x))$, $m' = (P'(x), Q'(x)) \in \mathscr{M}$, where $P(x) \neq P'(x)$. $s \in \mathscr{S}$ hidden in m is different from $s' \in \mathscr{S}$ hidden in m' $(s = s')$. For $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$,

$$e_t \in \mathscr{E}_T(e_r) \cap \mathscr{E}_T(m) \cap \mathscr{E}_T(m') \Longleftrightarrow \begin{cases} P_1(\beta_0) = \beta_1 \neq 0, \\ P_2(\beta_0) = \beta_2, \\ P_3(\beta_0) = \beta_3, \\ P(x) = sP_1(x) + P_2(x), \\ Q(x) = sP_2(x) + P_3(x), \\ P'(x) = s'P_1(x) + P_2(x), \\ Q'(x) = s'P_2(x) + P_3(x). \end{cases}$$

$$\Longleftrightarrow C \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{\omega-1} \\ b_0 \\ b_1 \\ \vdots \\ b_{\omega-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{\omega-1} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ h_0 \\ \vdots \\ h_{\omega-1} \\ g_0 \\ \vdots \\ g_{\omega-1} \\ h'_0 \\ \vdots \\ h'_{\omega-1} \\ g'_0 \\ \vdots \\ g'_{\omega-1} \end{pmatrix},$$

where

$$C = \left(\begin{array}{ccc} 1,\beta_0,\cdots,{\beta_0}^{\omega-1} & & \\ & 1,\beta_0,\cdots,{\beta_0}^{\omega-1} & \\ & & 1,\beta_0,\cdots,{\beta_0}^{\omega-1} \\ sI^{(\omega)} & I^{(\omega)} & \\ & sI^{(\omega)} & I^{(\omega)} \\ s'I^{(\omega)} & I^{(\omega)} & \\ & s'I^{(\omega)} & I^{(\omega)} \end{array} \right),$$

and the rank of the matrix C is 3ω. So the number of $e_t \in \mathscr{E}_T(e_r) \cap \mathscr{E}_T(m) \cap \mathscr{E}_T(m')$ is

$$|\mathscr{E}_T(e_r) \cap \mathscr{E}_T(m) \cap \mathscr{E}_T(m')| = 1 \; or \; 0. \qquad \square$$

Lemma 3.7. *For any $e_t \in \mathscr{E}_T$, the number of $e_r \in \mathscr{E}_R$ which is incidence with e_t is*

$$q \geq |\mathscr{E}_R(e_t)| \geq q - \omega + 1.$$

Proof. Assume that $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$. For $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$,

$$e_r \in \mathscr{E}_R(e_t) \Longleftrightarrow \begin{cases} P_1(\beta_0) = \beta_1 \neq 0, \\ P_2(\beta_0) = \beta_2, \\ P_3(\beta_0) = \beta_3. \end{cases} .$$

As $P_1(x) \neq 0$, the number of β_0 is at least $q - \omega + 1$ and at most q. If β_0 is fixed, β_1, β_2 and β_3 will be determined. So the number of $e_r \in \mathscr{E}_R(e_t)$ is

$$q \geq |\mathscr{E}_R(e_t)| \geq q - \omega + 1. \qquad \square$$

Lemma 3.8. *For any $e_t \in \mathscr{E}_T$, $m \in \mathscr{M}$ and $m \notin \mathscr{M}(e_t)$, the number of $e_r \in \mathscr{E}_R$ which is incidence with e_t and m is*

$$|\mathscr{E}_R(e_t) \cap \mathscr{E}_R(m)| \leq \omega - 1.$$

Proof. Assume that $m = (P(x), Q(x)) \in \mathscr{M}$ and $e_t = (P_1(x), P_2(x), P_3(x)) \in \mathscr{E}_T$. For $e_r = (\beta_0, \beta_1, \beta_2, \beta_3) \in \mathscr{E}_R$,

$$e_r \in \mathscr{E}_R(e_t) \cap \mathscr{E}_R(m) \quad \Longleftrightarrow \begin{cases} P_1(\beta_0) = \beta_1 \neq 0, \\ P_2(\beta_0) = \beta_2, \\ P_3(\beta_0) = \beta_3, \\ s = {\beta_1}^{-1}(P(\beta_0) - \beta_2), \\ Q(\beta_0) = s\beta_2 + \beta_3, \\ (P(x), Q(x)) \neq (sP_1(x) + P_2(x), sP_2(x) + P_3(x)). \end{cases}$$

As $P(x) \neq sP_1(x)+P_2(x)$ or $Q(x) \neq sP_2(x)+P_3(x)$, there is

$$\begin{cases} P(x)-P_2(x)-sP_1(x) \neq 0 \text{ or } Q(x)-P_3(x)-sP_2(x) \neq 0, \\ P(\beta_0)-P_2(\beta_0)-sP_1(\beta_0)=0, \\ Q(\beta_0)-P_3(\beta_0)-sP_2(\beta_0)=0. \end{cases}$$

$$\begin{pmatrix} h_0-b_0-sa_0 & h_1-b_1-sa_1 & \cdots & h_{\omega-1}-b_{\omega-1}-sa_{\omega-1} \\ g_0-c_0-sb_0 & g_1-c_1-sb_1 & \cdots & g_{\omega-1}-c_{\omega-1}-sb_{\omega-1} \end{pmatrix} \begin{pmatrix} 1 \\ \beta_0 \\ \vdots \\ {\beta_0}^{\omega-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Let

$$D = \begin{pmatrix} h_0-b_0-sa_0 & h_1-b_1-sa_1 & \cdots & h_{\omega-1}-b_{\omega-1}-sa_{\omega-1} \\ g_0-c_0-sb_0 & g_1-c_1-sb_1 & \cdots & g_{\omega-1}-c_{\omega-1}-sb_{\omega-1} \end{pmatrix},$$

the rank of the matrix D is 1 or 2. So the number of β_0 is at most $\omega-1$. If β_0 is fixed, β_1, β_2 and β_3 will be confirmed. So the number of $e_r \in \mathscr{E}_R(e_t) \cap \mathscr{E}_R(m)$ is

$$|\mathscr{E}_R(e_t) \cap \mathscr{E}_R(m)| \leq \omega-1. \qquad \square$$

Theorem 3.2. *In A^2-codes with secrecy constructed above, if $e_t \in \mathscr{E}_T$ and $e_r \in \mathscr{E}_R$ are chosen according to a uniform probability distribution, the largest probabilities of success for different types of attacks are*

$$P_I = \frac{1}{q},\ P_S = \frac{1}{q},\ P_{R_0} = \frac{1}{q^{2(\omega-1)}},\ P_{R_1} = \frac{1}{q^{(\omega-1)}},\ \textit{and}\ P_T = \frac{\omega-1}{q-\omega+1},$$

respectively.

Proof. By Theorem 3.1 and Lemma 3.2, there is

$$P_I = \max_m \frac{|\mathscr{E}_R(m)|}{|\mathscr{E}_R|} = \frac{q^2(q-1)}{q^3(q-1)} = \frac{1}{q}.$$

From Lemma 3.2 and Lemma 3.3, there is

$$P_S = \max_{\substack{m,\,m' \\ m \neq m'}} \frac{|\mathscr{E}_R(m) \cap \mathscr{E}_R(m')|}{|\mathscr{E}_R(m)|} = \frac{q(q-1)}{q^2(q-1)} = \frac{1}{q}.$$

Based on Lemma 3.4 and Lemma 3.5, there is

$$P_{R_0} = \max_{m,\,e_r} \frac{|\mathscr{E}_T(m) \cap \mathscr{E}_T(e_r)|}{|\mathscr{E}_T(e_r)|} = \frac{q^{(\omega-1)}}{q^{3(\omega-1)}} = \frac{1}{q^{2(\omega-1)}}.$$

By Lemma 3.5 and Lemma 3.6, there is

$$P_{R_1} = \max_{\substack{m,\,m',\,e_r \\ m \neq m'}} \frac{|\mathscr{E}_T(m) \cap \mathscr{E}_T(m') \cap \mathscr{E}_T(e_r)|}{|\mathscr{E}_T(m) \cap \mathscr{E}_T(e_r)|} = \frac{1}{q^{(\omega-1)}}.$$

From Lemma 3.7 and Lemma 3.8, there is

$$P_T = \max_{\substack{m,\, e_t \\ m \notin \mathscr{M}(e_t)}} \frac{|\mathscr{E}_R(m) \cap \mathscr{E}_R(e_t)|}{|\mathscr{E}_R(e_t)|} = \frac{\omega - 1}{q - \omega + 1}.$$

□

4 Construction II

4.1 The model

For a odd prime q, let $\mathbb{F}_q$ be a finite field with q elements, $\mathbb{F}_q{}^* = \mathbb{F}_q \setminus \{0\}$. $\mathbb{F}_q[x]$ denotes a set of polynomials over $\mathbb{F}_q$, $\mathbb{F}_q[x]_\omega = \left\{ \sum_{i=0}^{\omega-1} a_i x^i \;\middle|\; a_i \in \mathbb{F}_q \right\}$, where $4 \le \omega < \frac{q}{2} + 1$.

The set of source states is

$$\mathscr{S} = \{s \mid s \in \mathbb{F}_q\}.$$

The set of transmitter's encoding rules is

$$\mathscr{E}_T = \left\{ e_t = (P_1(x), P_2(x), P_3(x), P_4(x)) \;\middle|\; P_i(x) \in \mathbb{F}_q[x]_\omega,\ P_1(x) \neq 0,\ i = 1,2,3,4 \right\}.$$

The set of receiver's decoding rules is

$$\mathscr{E}_R = \left\{ e_r = (\beta_0, \beta_1, \beta_2, \beta_3, \beta_4) \;\middle|\; \beta_0, \beta_2, \beta_3, \beta_4 \in \mathbb{F}_q,\ \beta_1 \in \mathbb{F}_q{}^* \right\}.$$

The set of messages is

$$\mathscr{M} = \left\{ m = (P(x), Q(x)) \;\middle|\; P(x), Q(x) \in \mathbb{F}_q[x]_\omega \right\}.$$

4.2 Operating rules

1. Key generation and distribution

(1) The key distribution center (KDC) randomly and privately chooses an transmitter's encoding rule $e_t = (P_1(x), P_2(x), P_3(x), P_4(x)) \in \mathscr{E}_T$, and sends it to the transmitter as his key.

(2) The KDC randomly selects $\beta_0 \in \mathbb{F}_q$, such that $P_1(\beta_0) \neq 0$, and calculates

$$\beta_1 = P_1(\beta_0),\ \beta_2 = P_2(\beta_0),\ \beta_3 = P_3(\beta_0), \text{ and } \beta_4 = P_4(\beta_0),$$

respectively. The KDC sends $e_r = (\beta_0, \beta_1, \beta_2, \beta_3, \beta_4)$ to the receiver as his key.

2. Broadcast

For the source state $s \in \mathscr{S}$, the transmitter generates an authenticated message using his key

$$P(x) = sP_1(x) + P_2(x),\ Q(x) = sP_3(x) + P_4(x),$$

and sends $m = (P(x), Q(x))$ to the receiver, where s is hidden in m.

3. Verification

The receiver can verify the authenticity of the received message. He calculates

$$s = \beta_1{}^{-1}(P(\beta_0) - \beta_2),$$

and accepts the message $m = (P(x), Q(x))$, if and only if

$$Q(\beta_0) = s\beta_3 + \beta_4.$$

Lemma 4.1. *The construction above is well-defined authentication codes with arbitration (A^2-codes), that is*

(1) $f(s, e_t) = m \in \mathscr{M}$, *for all* $s \in \mathscr{S}$ *and* $e_t \in \mathscr{E}_T$;

(2) *For any* $m \in \mathscr{M}$ *and* $e_t \in \mathscr{E}_T$, *if there is an* $s \in \mathscr{S}$ *satisfying* $f(s, e_t) = m$, *then such an* s *is uniquely determined by the given* m *and* e_t.

Proof. (1) It is obvious. For any $f(s, e_t) = m$, s is hidden in m, which can't be recovered from the encoded m without e_t.

(2) Let $m = (P(x), Q(x)) \in \mathscr{M}$ and $e_t = (P_1(x), P_2(x), P_3(x), P_4(x)) \in \mathscr{E}_T$. Assume that s and $s' \in \mathscr{S}$ and $f(s, e_t) = m = f(s', e_t)$, then

$$\begin{cases} P(x) = sP_1(x) + P_2(x), \\ Q(x) = sP_3(x) + P_4(x), \\ P(x) = s'P_1(x) + P_2(x), \\ Q(x) = s'P_3(x) + P_4(x). \end{cases} \Longleftrightarrow \begin{cases} (s' - s)P_1(x) = 0, \\ (s' - s)P_3(x) = 0. \end{cases}$$

As $P_1(x) \neq 0$, $s = s'$. s is an uniquely source state contained in m. □

4.3 Parameters and Probabilities of successful attacks

Because the second construction is similar to the first one, proofs are deleted.

Theorem 4.1. *Parameters of A^2-codes which are constructed above are*

$$|\mathscr{S}| = q,\ |\mathscr{E}_T| = q^{3\omega}(q^{\omega} - 1),\ |\mathscr{E}_R| = q^4(q - 1),\ \text{and}\ |\mathscr{M}| = q^{2\omega},$$

respectively.

Lemma 4.2. *Some relative parameters of A^2-codes which are constructed above are:*

(1) *For any $m \in \mathscr{M}$, the number of $e_r \in \mathscr{E}_R$ which is incidence with m is*

$$|\mathscr{E}_R(m)| = q^3(q-1);$$

(2) *For any $m, m' \in \mathscr{M}$, and $m \neq m'$, the number of $e_r \in \mathscr{E}_R$ which is incidence with m and m' is*

$$q^2(q-1) \geq |\mathscr{E}_R(m) \cap \mathscr{E}_R(m')| \geq q(q-1)(q-\omega+1);$$

(3) *For any $e_r \in \mathscr{E}_R$, the number of $e_t \in \mathscr{E}_T$ which is incidence with e_r is*

$$|\mathscr{E}_T(e_r)| = q^{4(\omega-1)} \text{ or } 0;$$

(4) *For any $e_r \in \mathscr{E}_R$ and $m \in \mathscr{M}$, the number of $e_t \in \mathscr{E}_T$ which is incidence with e_r and m is*

$$|\mathscr{E}_T(e_r) \cap \mathscr{E}_T(m)| = q^{2(\omega-1)} \text{ or } 0;$$

(5) *For any $e_r \in \mathscr{E}_R$, $m, m' \in \mathscr{M}$ and $m \neq m'$, the number of $e_t \in \mathscr{E}_T$ which is incidence with e_r, m and m' is*

$$|\mathscr{E}_T(e_r) \cap \mathscr{E}_T(m) \cap \mathscr{E}_T(m')| = 1 \text{ or } 0;$$

(6) *For any $e_t \in \mathscr{E}_T$, the number of $e_r \in \mathscr{E}_R$ which is incidence with e_t is*

$$q \geq |\mathscr{E}_R(e_t)| \geq q-\omega+1;$$

(7) *For any $e_t \in \mathscr{E}_T$, $m \in \mathscr{M}$ and $m \notin \mathscr{M}(e_t)$, the number of $e_r \in \mathscr{E}_R$ which is incidence with e_t and m is*

$$|\mathscr{E}_R(e_t) \cap \mathscr{E}_R(m)| \leq \omega - 1.$$

Theorem 4.2. *In A^2-codes with secrecy constructed above, if $e_t \in \mathscr{E}_T$ and $e_r \in \mathscr{E}_R$ are chosen according to a uniform probability distribution, the largest probabilities of success for different types of attacks are*

$$P_I = \frac{1}{q}, \; P_S = \frac{1}{q}, \; P_{R_0} = \frac{1}{q^{2(\omega-1)}}, \; P_{R_1} = \frac{1}{q^{2(\omega-1)}}, \text{ and } P_T = \frac{\omega-1}{q-\omega+1},$$

respectively.

5 Concluding remarks

For communication systems, we need new constructions of A^2-codes which are safe, cost-effective and highly efficient. But most of A^2-codes are without secrecy. In our two constructions of A^2-codes, a source state is hidden in the message, which can't be recovered from the message without the knowledge of the transmitter's encoding rule or the receiver's decoding rule. Compared with most of A^2-codes, it greatly improved security.

The security of authentication codes could be also measured by the maximum probabilities of successful attacks. It means that the smaller probabilities of successful attacks, the higher security of authentication codes. The economy of authentication codes could be measured by the storage. It means that the smaller storage, the more economical efficiency of authentication codes. Polynomials are easier implemented than others using computer programs. So maybe our constructions are higher effective. Now let's compare our constructions with Kong and Nan's construction. In [14], when $n = q + 1$, the number of source states of their construction is q as the same as ours. The specific result is listed as the Table 1.

Table 1: The Comparison of Three A^2-codes

	Kong and Nan's [14]	Construction I	Construction II
$\lvert\mathscr{S}\rvert$	q	q	q
$\lvert\mathscr{E}_T\rvert$	$q^{q(q+1)}\prod_{i=1}^{q+1}(q^i-1)^2$	$q^{2\omega}(q^{\omega}-1)$	$q^{3\omega}(q^{\omega}-1)$
$\lvert\mathscr{E}_R\rvert$	$q^{q(q+1)}\prod_{i=1}^{q+1}(q^i-1)^2$	$q^3(q-1)$	$q^4(q-1)$
$\lvert\mathscr{M}\rvert$	$q^{(q+1)^2}-1-q^{\frac{q(q+1)}{2}}\prod_{i=1}^{q+1}(q^i-1)$	$q^{2\omega}$	$q^{2\omega}$
P_I	$\frac{q-1}{(q^{(q+1)}-1)^2}$	$\frac{1}{q}$	$\frac{1}{q}$
P_S	$\frac{1}{q(q+1)}$	$\frac{1}{q}$	$\frac{1}{q}$
P_{R_0}	$\frac{1}{q^2}$	$\frac{1}{q^{2(\omega-1)}}$	$\frac{1}{q^{2(\omega-1)}}$
P_{R_1}	$\frac{1}{q(q+1)}$	$\frac{1}{q^{(\omega-1)}}$	$\frac{1}{q^{2(\omega-1)}}$
P_T	1	$\frac{\omega-1}{q-\omega+1}$	$\frac{\omega-1}{q-\omega+1}$

Compared our two constructions, the more transmitter's encoding rules or the receiver's decoding rules, the lower probabilities of successful attacks. Compared with constructed authentication codes in [14], P_I and P_S of their construction are smaller than ours. But in our constructions, a source state is hidden in the massage and which must be decoded before verification. It's very hard for an opponent to know the source state. Meanwhile, our $|\mathscr{E}_T|$, $|\mathscr{E}_R|$ and other probabilities of successful attacks are smaller than theirs. So our constructions are more economical, and they are better than theirs to protect against attacks from insiders. So our constructions are more better.

References

[1] E.N. Gilbert, F.J. Macwilliams, N.J.A. Sloane, Codes which detect deception, Bell Labs Technical Journal. 53 (3) (1974) 405 - 424.

[2] G.J. Simmons, Authentication theory/coding theory, Advances in Cryptology, Volume 196 of the series Lecture Notes in Computer Science. 196 (1985) 411-432.

[3] R. Safavi-Naini, H. Wang, C. Xing, Linear authentication codes: bounds and constructions, IEEE Transactions on Information Theory. 49 (4) (2003) 866-872.

[4] C. Xing, H. Wang, K.Y. Lam, Constructions of authentication codes from algebraic curves over finite fields, IEEE Transactions on Information Theory. 46 (3) (2000) 886 - 892.

[5] D.R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, Journal of Cryptology. 1 (2) (1988) 119-127.

[6] C.S. Ding, A. Salomaa, P. Solé, X.J. Tian, Three constructions of authentication/secrecy codes, Journal of Pure and Applied Algebra. 196 (2-3) (2005) 149-168.

[7] G.J. Simmons, Message authentication with arbitration of transmitter/receiver disputes, Advance in Cryptology-Eurocrypt'87, Lecture Notes in Computer Science 304, Springer-Verlag, Berlin. (1988) 151-165.

[8] G.J. Simmons, A cartesian product construction for unconditionally secure authentication codes that permit arbitration, Journal of Cryptology. 2 (2) (1990) 77-104.

[9] T. Johansson, Lower bounds on the probability of deception in authentication with arbitration, IEEE Transcations on Information Theory. 40 (5) (1994) 1573-1585.

[10] T. Johansson, Further results on asymmetric authentication schemes, Information and Computation. 151 (1-2) (1999) 100-133.

[11] K. Kurosawa, S. Obana, Combinatorial bounds for authentication codes with arbitration, Designs, Codes and Cryptography. 22 (2) (2001) 265-281.

[12] S.D. Chen, D.W. Zhao, New construction of authentication codes with arbitration from pseudo-symplectic geometry over finite fields, Ars Combinatoria. (2) (2013) 453-465.

[13] Y. Gao, X.H. Shi, H.L. Wang, A construction of authentication codes with arbitration from singular symplectic geometry over finite fields, Acta Scientiarum Naturalium Universitatis Nankaiensis. 41 (6) (2008) 72-77.

[14] D.B. Kong, J.Z. Nan, Using normal form of matrices over finite fields to construct authentication codes with arbitration, Journal of Natural Science of Heilongjiang University. 27 (3) (2010) 341-346.

[15] W.J. Li, J.Z. Nan, A construction of authentication codes with arbitration from vector spaces over finite fields, Journal of Mathematical Research and Exposition. 31 (2) (2011) 269-278.

[16] S.D. Chen, L.Z. Chang, Two constructions of multi-sender authentication codes with arbitration based linear codes, Wseas Transactions on Mathematics. 11 (12) (2012) 1103-1113.

[17] Y. Gao, L.W. Chang, A new construction of A^2 authentication codes from singular pseudo-symplectic geometry over finite fields, Journal of Combinatorial Mathematics and Combinatorial Computing. 81 (2012) 65-81.

[18] D.Y. Pei, Y. Li, Y. Wang, R. Safavi-Naini, Characterization of optimal authentication codes with arbitration, Information Security and Privacy. (1999) 303-313.

[19] S.D. Chen, X.L. Zhang, Three constructions of perfect authentication codes from projective geometry over finite fields, Applied Mathematics and Computation. 253 (1) (2015) 308-317.

[20] W.Ogata, K. Kurosawa, D.R. Stinson, H. Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, Discrete Mathematics. 279 (1-3) (2004) 384-405.