# Three Constructions of Authentication Codes from Power Function over Finite Fields with Perfect Secrecy

*Xiuli Wang*[1], *Shangdi Chen*[1], *Maoyuan Zhou*[2,1]

(*Science college, Civil Aviation University of China, Tianjin 300300, China* )[1]
(*School of Mathematical Sciences, Nankai University,Tianjin 300071, China* )[2]

Email:xlwang@cauc.edu.cn

**Abstract:** In this paper, we present three algebraic constructions of authentication codes from power function over finite fields with secrecy and realize an application of some properties about authentication codes in [1]. The first and the third class are optimal. Some of the codes in the second class are optimal, and others in the second class are asymptotically optimal. All authentication codes in the three classes provide perfect secrecy.
**Key words:** authentication codes, cryptography, rings, perfect nonlinear mappings, secrecy
**2000 MR Subject Classification:** 94A60

## §1. Introduction

The authentication model introduced by Simmons [12] involves three parties: a transmitter, a receiver, and an opponent. The transmitter wants to send some information (called source state) to the receiver using a public communication channel. To provide confidentiality and/or authenticity for the source state to be transmitted to the receiver, the sender and receiver need to share a secret key $k \in \mathcal{K}$, where $\mathcal{K}$ is the key space. Each secret key $k$ will then specify a secret one-to-one transformation $E_k$ , which transforms a source state $s$ into a message $m = E_k(s)$. All the possible messages $m$ form a space $\mathcal{M}$, which is called the message space. All the encoding rules form the encoding rule space $\mathcal{E} = \{E_k : k \in \mathcal{K}\}$. The source state space and the key space are associated with a probability distribution. An authentication code is defined by the four-tuple $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$. There are two types of authentication codes: authentication codes with secrecy and

those without secrecy. In an authentication code with secrecy, a source state $s$ is sent to the receiver in an encrypted form. In this case, the secret key $k$ shared by both the sender and receiver is used for both encryption and authentication purpose. In an authentication code without secrecy, a source state is sent to the receiver in plaintext. In this case, the secret key is used only for authentication purpose. In this paper, we consider only authentication codes with secrecy. It is possible that more than one message can be used to determine a source state (this is called splitting). In this paper, we consider only authentication codes without splitting. An authentication code with secrecy is used as follows. After encoding the source state $s$ with $E_k$ , the sender sends the message $m = E_k(s)$ to the receiver through the public communication channel. When receiving $m'$, the receiver will check the authenticy of the received message first. If it is authentic, the receiver will then recover the source state $s$ with the shared secret key $k$ and the encoding rule $E_k$. Otherwise, the receiver will reject the message.

Within Simmons authentication model, we assume that an opponent can insert his message into the channel, and can substitute an observed message $m$ with another message $m'$. We consider two kinds of attacks, the impersonation and substitution attacks. In the impersonation attack an opponent inserts his message into the channel and wishes to make the receiver accept it as authentic. In a substitution attack the opponent observed a message sent by the transmitter and will replace it with his message $m' \neq m$ hoping that the receiver accepts it as authentic. We use $P_I$ and $P_S$ to denote the maximum success probabilities with respect to the two attacks. Authentication codes with secrecy have been considered in [8, 9]. Most known constructions are combinatorial. In this paper, we present three algebraic constructions of authentication codes with secrecy. The first and the third class are optimal. Some of the codes in the second class are optimal, and others in the second class are asymptotically optimal. All authentication codes in the three classes provide perfect secrecy.

For all the authentication codes described in this paper, all the keys are used equally likely, and all source states are used with equal probability. Since there is a one-to-one mapping from the key space to the encoding rule space for all the authentication codes in this paper, all the encoding rules are used equally likely, and the number of keys and the number of distinct encoding rules are always the same.

## §2. Encoding Matrix, Perfect Secrecy and Authentication Perpendicular Arrays

Given an authentication code $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$, we define a $|\mathcal{K}| \times |\mathcal{S}|$ matrix, where the rows are indexed by the keys (equivalently the encoding rules),

the columns are indexed by the source states, and the entry in row k and column s is $E_k(s)$. This matrix is called the encoding matrix or authentication matrix. In this paper, for all the authentication codes, we assume that each secret key (and thus each encoding rule) is used for encoding only one source state. This is the same as in the Vernam one-time-pad system. As made clear before, we consider only the impersonation and substitution attacks in this paper. We say that an authentication code offers perfect secrecy if any observed message m gives zero information about the corresponding source state $s$, i.e., $p(s\backslash m) = p(s)$. This is exactly Shannon definition of perfect secrecy [10]. Shannon proved that if a code offers perfect secrecy, then

$$|\mathcal{K}| = |\mathcal{E}| \geq |\mathcal{S}|$$

An authentication perpendicular array $\mathbf{APA_1}(1, u, v)$ is a $v \times u$ array, $A$, of $v$ symbols, which satisfies the following properties:

$c1$. Every row of A contains u distinct symbols.

$c2$. Every column of A contains each of the v symbols exactly once.

Authentication perpendicular arrays $\mathbf{APA_1}(1, |\mathcal{S}|, |\mathcal{K}|)$, $|\mathcal{S}| < |\mathcal{K}|$, can be used to construct authentication codes with perfect secrecy and with $P_I = |\mathcal{S}|/|\mathcal{M}|$ [3].

LEMMA 1. (Stinson [3]). If the encoding matrix of an authentication code with secrecy is an $\mathbf{APA_1}(1, |\mathcal{S}|, |\mathcal{K}|)$, $|\mathcal{S}| < |\mathcal{K}|$, then the code offers perfect secrecy and $P_I = |\mathcal{S}|/|\mathcal{M}|$.

This lemma will be used frequently in the sequel. For the generalization of perfect secrecy into L-fold secrecy and the use of general perpendicular arrays for the construction of authentication codes with L-fold secrecy, we refer to Stinson [3].

## §3. Bounds on Authentication Codes

We summarize some of the known bounds needed in the sequel. We also use $\mathcal{M}$ , $\mathcal{E}$ and $\mathcal{S}$ to denote the random variable of the messages, encoding rules, and source states. We use $\mathcal{M}^r$ to denote the random variables of the first $r$ messages, and $H(\mathcal{E}\backslash\mathcal{M}^r)$ the conditional entropy of $\mathcal{E}$ given that the first $r$ messages have been observed.

LEMMA 2. [Brickel [2]]. In any authentication system without splitting,

$$P_S \geq 2^{H(\mathcal{M})-H(\mathcal{E})-H(\mathcal{S})}.$$

The following is called the information-theoretic bound [6,7,8].

LEMMA 3. In any authentication code,

$$P_I \geq 2^{H(\mathcal{E}\backslash\mathcal{M})-H(\mathcal{E})}, \quad P_S \geq 2^{H(\mathcal{E}\backslash\mathcal{M}^2)-H(\mathcal{E}\backslash\mathcal{M})}.$$

The following are combinatorial bounds [4,5].

LEMMA 4. In any authentication system without splitting,

$$P_I \geq \frac{|\mathcal{S}|}{|\mathcal{M}|} \text{ and } P_S \geq \frac{|\mathcal{S}|-1}{|\mathcal{M}|-1}$$

If both equalities are achieved, then $|\mathcal{E}| \geq |\mathcal{M}|$.

# §4. Construction I

Let $n$ and $m$ be two positive integers such that $m \mid n$, it means that $m$ is a factor of $n$. Let $p(x)$ be a power function $x^s$ from $GF(q^n)$ to $GF(q^m)$. We use $\mathcal{S}$, $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{E}$ to denote the source state space, key space, message space, and encoding rule space, respectively. Define

$$\begin{cases} (\mathcal{S}, \mathcal{K}, \mathcal{M}) = (GF(q^n), GF(q^n) \times GF(q^m), GF(q^n) \times GF(q^m)) \\ \mathcal{E} = \{E_k | k \in \mathcal{K}\}, \end{cases} \tag{1}$$

where for any $k = (k_1, k_2) \in \mathcal{K}$ and $s \in \mathcal{S}$,

$E_k(s) = (s + k_1, p(sk_1) + k_2)$

We denote $m_1 = s + k_1$ and $m_2 = p(sk_1) + k_2$. The first part is the encrypted message. The second part $m_2$ is the redundant part for authentication.

**4.1 The parameters and properties of the codes**

THEOREM 5. The authentication code of (1) provides perfect secrecy. Furthermore, we have

$P_I = \frac{1}{q^m}$, $P_S = \frac{1}{q^m}$.

*proof.* We first prove that the encoding matrix of this authentication code is an authentication perpendicular array $\mathbf{APA_1}(1, |\mathcal{S}|, |\mathcal{K}|)$, where $|\mathcal{S}| = q^n$ and $|\mathcal{K}| = q^{n+m}$. For every fixed key $k = (k_1, k_2)$, $E_k$ is a one-to-one mapping. Hence each row of the encoding matrix contains $q^n = |\mathcal{S}|$ distinct symbols of $\mathcal{M}$. Hence condition $(c1)$ is satisfied.

On the other hand, for every fixed source state $s$ and any pair $(a, b) \in GF(q^n) \times GF(q^m)$, the equation

$E_k(s) = (s + k_1, p(sk_1) + k_2) = (a, b)$ appears exactly once in each column of the encoding matrix, and condition $(c1)$ is satisfied.

Since both $(c1)$ and $(c2)$ are satisfied, by definition the encoding matrix is an $\mathbf{APA_1}(1, |\mathcal{S}|, |\mathcal{K}|)$. It then follows from Lemma 1 that this authentication code provides perfect secrecy and $P_I = \frac{|\mathcal{S}|}{|\mathcal{M}|} = \frac{1}{q^m}$.

We now consider the substitution attack and compute $P_S$. An opponent has observed one message

$$m_1 = s + k_1, \ m_2 = p(sk_1) + k_2. \tag{2}$$

This message gives $\log_2 q^m$ bits of information about the key $k = (k_1, k_2)$, but gives no information about $k_1$. The opponent wants to replace $m$ with another message $m' = (m_1', m_2')$, where $m_1 \neq m_1'$. He wishes to analyze the whole system and to choose a message $m'$ such that the success probability is maximal.

Whatever $m' = (m_1', m_2')$ the opponent chooses, there is a pair $(\delta_1, \delta_2)$ such that $(m_1', m_2') = (m_1 + \delta_1, m_2 + \delta_2)$, where $\delta_1 \neq 0$. Thus the substitution attack is equivalent to adding an element $\delta_1 \neq 0$ to $m_1$, and an element $\delta_2$ to $m_2$. This is successful if and only if

$p(sk_1) + k_2 + \delta_2 = p((s + \delta_1)k_1) + k_2$,

which is equivalent to

$p(\delta_1 k_1) = \delta_2$.

Hence

$P_S = \max_{\delta_1 \neq 0, \delta_2} Pr[p(\delta_1 k_1) = \delta_2]$.

Note that the observed message gives no information about $k_1$. We obtain

$Pr[p(\delta_1 k_1) = \delta_2] = \frac{q^{n-m}}{q^n} = \frac{1}{q^m}$

for any fixed $\delta_1 \neq 0$ and $\delta_2$. Hence

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

This completes the proof.

### 4.2. Optimality of the Codes

Clearly, $P_I = \frac{1}{q^m}$ meets the lower bound on $P_I$ given in Lemma 4. Note that all encoding rules are equally likely and all source states are equally likely. Then all messages are used with equal probability. It follows that

$H(\mathcal{S}) = \log_2 q^{n+m}$, $H(\mathcal{E}) = \log_2 q^{n+m}$, $H(\mathcal{M}) = \log_2 q^n$.

Hence $2^{H(\mathcal{M}) - H(\mathcal{E}) - H(\mathcal{S})} = 1/q^n$.

If $n = m$, the code of (1) is optimal with respect to the bound on $P_S$ given in Lemma 2.

We now compare the $P_S$ of Theorem 5 with the information-theoretic bound of Lemma 3. We first determine $H(\mathcal{E}\backslash\mathcal{M})$. Suppose that a message $m = (m_1, m_2) = (s + k_1, p(sk_1) + k_2)$ has been observed. Then we have

$k_2 = m_2 - p(k_1(m_1 - k_1))$.

Hence

$H(\mathcal{E}\backslash\mathcal{M}) = \log_2 q^n$.

We now determine $H(\mathcal{E}\backslash\mathcal{M}^2)$. Suppose that two distinct messages

$m = m_1 + m_2 = (s + k_1, p(sk_1) + k_2)$ and

$m' = m_1' + m_2' = (s' + k_1, p(s'k_1) + k_2)$

have been observed. Since $m \neq m'$, the uncertainty of $k_1$ is $\log_2 q^{n-m}$. So

$H(\mathcal{E}\backslash\mathcal{M}^2) = \log_2 q^{n-m}$.

Combining the formulas for $H(\mathcal{E}\backslash\mathcal{M})$ and $H(\mathcal{E}\backslash\mathcal{M}^2)$ yields

$P := 2^{H(\mathcal{E}\backslash\mathcal{M}^2) - H(\mathcal{E}\backslash\mathcal{M})} = \frac{1}{q^m}$.

This is the lower bound on $P_S$ given in Lemma 3. Hence the code of (1) is optimal with respect to the bound on given in Lemma 3 in all cases.

Thus we have arrived at the following conclusions.

THEOREM 6. The code of (1) is optimal with respect to the bound on $P_S$ given in Lemma 3. In addition, it is also optional with respect to

the bound on $P_S$ given in Lemma 2 in the case $n = m$. Furthermore, it is optimal with respect to the bound on $P_I$ given in Lemma 4.

# §5. Construction II

let $n$ and $m$ be two positive integers such that $m \backslash n$. Let $p(x)$ be a power function from $GF(q^n)$ to $GF(q^m)$. We use $\mathcal{S}$, $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{E}$ to denote the source state space, key space, message space, and encoding rule space, respectively. Define

$$\begin{cases} (\mathcal{S}, \mathcal{K}, \mathcal{M}) = (GF(q^n)^*, GF(q^n)^* \times GF(q^m), GF(q^n)^* \times GF(q^m)) \\ \mathcal{E} = \{E_k | k \in \mathcal{K}\}, \end{cases} \tag{3}$$

where for any $k = (k_1, k_2) \in \mathcal{K}$ and $s \in \mathcal{S}$,

$E_k(s) = (sk_1, p(s + k_1) + k_2)$.

We denote $m_1 = sk_1$ and $m_2 = p(s + k_1) + k_2$. The first part is the encrypted message. The second part $m_2$ is the redundant part for authentication.

**5.1 The parameters and properties of the codes**

THEOREM 7. The authentication code of (3) provides perfect secrecy. Furthermore, we have

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

*proof.* Similarly as in the proof of Theorem 5, we can show that the encoding matrix of this authentication code is an authentication perpendicular array $\mathbf{APA_1}(1, |\mathcal{S}|, |\mathcal{K}|)$, where $|\mathcal{S}| = q^n - 1$ and $|\mathcal{K}| = (q^n - 1)q^m$. It then follows from Lemma 1 that this authentication code provides perfect secrecy and $P_I = \frac{|\mathcal{S}|}{|\mathcal{M}|} = \frac{1}{q^m}$.

We now consider the substitution attack and compute $P_S$. An opponent has observed one message $m = (m_1, m_2)$, where

$$m_1 = sk_1, \ m_2 = p(s + k_1) + k_2. \tag{4}$$

This message gives $\log_2 q^m$ bits of information about the key $k = (k_1, k_2)$, but no information at all about the source state $s$ and $k_1$. The opponent wants to replace $m$ with another message $m' = (m'_1, m'_2)$, where $m_1 \neq m'_1$. He wishes to select an $m'$ such that the success probability is maximal.

Whatever $m'$ the opponent chooses, there is always a pair $(\delta_1, \delta_2)$ such that $(m'_1, m'_2) = (m_1\delta_1, m_2 + \delta_2)$, where $\delta_1 \neq \{0, 1\}$. Thus the substitution attack is equivalent to multiplying an element $\delta_1 \neq 1$ to $m_1$, adding an element $\delta_2$ to $m_2$. This is successful if and only if

$p(s + k_1) + k_2 + \delta_2 = p((s\delta_1) + k_1) + k_2$, which is equivalent to

$p[(\delta_1 - 1)s] = \delta_2$. Hence

$$P_S = \max_{\delta_1 \notin \{0,1\}, \delta_2} Pr[p[(\delta_1 - 1)s] = \delta_2].$$

Note that the observed message gives no information about $s$. Hence

$$Pr[p[(\delta_1 - 1)s] = 0] = \frac{q^{n-m}-1}{q^n-1}$$

for any $\delta_1 \notin \{0,1\}$ and

$$Pr[p[(\delta_1 - 1)s] = 0] = \frac{q^{n-m}-1}{q^n-1}$$

for any $\delta_1 \notin \{0,1\}$ and $\delta_2 \neq 0$. Hence

$$P_S = \frac{1}{q^m} + \frac{1}{q^m(q^n-1)}.$$

This completes the proof.

**5.2. Optimality of the Codes**

Clearly, $P_I = \frac{1}{q^m}$ meets the lower bound on $P_I$ given in Lemma 4. Hence the code is optimal with respect to impersonation attack.

If $n = m$, then $P_S = 2^{H(\mathcal{E}\backslash\mathcal{M}^2)-H(\mathcal{E}\backslash\mathcal{M})-H(\mathcal{S})} = 1/q^n$, which meets the bound of Lemma 2. Hence the code is optimal with respect to both attacks. If $n > m$, we can prove that

$$P := 2^{H(\mathcal{E}\backslash\mathcal{M}^2)-H(\mathcal{E}\backslash\mathcal{M})} = \frac{(q^{n-m}-1)^{1/q^m}(q^{n-m})^{q^m-1/q^m}}{q^n-1}$$

is the lower bound on $P_S$ given in Lemma 3.

Note that

$$\lim_{q\to\infty} \frac{P}{P_S} = \lim_{q\to\infty} \frac{P}{q^{n-m}/q^n-1} = \lim_{q\to\infty} \frac{(q^{n-m}-1)^{1/q^m}(q^{n-m})^{q^m-1/q^m}}{q^{n-m}} = 1$$

Hence the code of (3) is asymptotically optimal with respect to the bound on $P_S$ given in Lemma 3.

Thus we have proved the following conclusions.

THEOREM 8. The code of (3) is optimal. If $n > m$ , it is optimal with respect to the lower bound on $P_I$ given in Lemma 4, and it is asymptotically optimal with respect to the bound on $P_S$ given in Lemma 3.

# §6. Construction III

Let $(A,+)$ and $(B,+)$ be two finite abelian groups, and let $\Pi$ be a homomorphism from $A$ to $B$. We construct an authentication code $(\mathcal{S},\mathcal{K},\mathcal{M},\mathcal{E})$ by defining

$$(\mathcal{S},\mathcal{K},\mathcal{M},\mathcal{E}) = (A, A\times B, A\times B, \{E_k | k\in\mathcal{K}\}), \tag{5}$$

where for any $k = (k_1,k_2) \in \mathcal{K}$ and $s \in \mathcal{S}$,

$E_k(s) = (s + k_1, \Pi(s) + k_2)$

We denote $m_1 = s + k_1$ and $m_2 = \Pi(s) + k_2$. The first part is the encrypted message. The second part $m_2$ is the redundant part for authentication.

**6.1 The parameters and properties of the codes**

THEOREM 9. Let $(A,+)$ and $(B,+)$ be two finite abelian groups, and let $\Pi$ be a homomorphism from $A$ to $B$. Then for the authentication code of (5), we have

$P_I = \frac{1}{|B|}$,
$P_S = \max_{\delta_1 \neq 0, \delta_2} Pr[\Pi(s+\delta_1) - \Pi(s) = \delta_2]$.

In addition, the authentication code provides perfect secrecy.

*proof*. Similarly as in the proof of Theorem 5, we can show that the encoding matrix of this authentication code is an $\mathbf{APA_1}(1, |\mathcal{S}|, |\mathcal{K}|)$, where $|\mathcal{S}| = |\mathcal{A}|$ and $|\mathcal{K}| = |A||B|$. It then follows from Lemma 1 that this authentication code provides perfect secrecy and $P_I = \frac{|\mathcal{S}|}{|\mathcal{M}|} = \frac{1}{|B|}$.

We now consider the substitution attack and compute $P_S$. An opponent has observed one message $m = (m_1, m_2)$, where

$$m = s + k_1, \ m_2 = \Pi(s) + k_2. \tag{6}$$

He wants to replace $m$ with another message $m' = (m_1', m_2')$, where $m_1 \neq m_1'$. Note the observed message gives no information about $s$ and $k_1$, although it gives information about $(k_1, k_2)$.

Whatever $m' = (m_1', m_2')$ the opponent chooses, there is always a pair $(\delta_1, \delta_2)$ such that $(m_1', m_2') = (m_1, m_2) + (\delta_1, \delta_2)$. Hence the substitution attack is equivalent to adding an element $\delta_1 \neq 1$ to $m_1$, and an element $\delta_2$ to $m_2$. This is successful if and only if $\Pi(s) + k_2 + \delta_2 = \Pi(s + \delta_1) + k_2$, which is equivalent to $\Pi(s + \delta_1) - \Pi(s) = \delta_2$. Then the formula for $P_S$ follows.

By Theorem 9, the probability $P_I$ is independent of the choice of $\Pi$. However, the probability $P_S$ depends totally on the mapping $\Pi$. In the sequel, we construct codes by choosing proper mapping $\Pi$ with general framework. To this end, we need optimal nonlinear functions. Clearly, the codes provide perfect secrecy and this does not depend on the properties of $\Pi$.

### 6.2 A General Construction Using Perfect Nonlinear Function

Let $f$ be a mapping from an abelian group $(A, +)$ to $(B, +)$. The derivatives are defined as $D_a f(x) = f(x + a) - f(x)$. A robust measure of the nonlinearity of function is given by

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} Pr(D_a f(x) = b), \tag{7}$$

where $Pr(E)$ denotes the probability of the occurrence of event $E$.

It can be proved that $P_f \geq 1/|B|$ [11]. If the equality is achieved, we say that function $f : A \to B$ has perfect nonlinearity. In this case $|B|$ must divide $|A|$.

COROLLARY 10. Let $(A, +)$ and $(B, +)$ be two finite abelian groups, and let $\Pi$ be a homomorphism (clearly it is a perfect nonlinear mapping) from $A$ to $B$. Then for the authentication code of (5), we have

$P_I = \frac{1}{|B|}$, $P_S = \frac{1}{|B|}$.

In addition, the authentication code provides perfect secrecy, and this does not depend on the perfect nonlinearity of $\Pi$ .

*proof.* The constructions follow from Theorem 9 and perfect nonlinearity of $\Pi$.

**6.3 Optimality of the Codes of Theorem 9**

Clearly, $P_I = \frac{1}{|B|}$ meets the lower bound on $P_I$ given in Lemma 4. Thus it is optimal against impersonation attack. We now prove that $P_S = \frac{1}{|B|}$ meets the bound on $P_S$ given in Lemma 3. To this end, we need to compute $H(\mathcal{E}\backslash\mathcal{M})$ and $H(\mathcal{E}\backslash\mathcal{M}^2)$.

Assume that one message $(m_1, m_2) = (s + k_1, \Pi(s) + k_2)$ has been observed. We have then

$$m_2 - k_2 = \Pi(m_1 - k_1).$$

Thus the uncertainty of $k = (k_1, k_2)$ is $\log_2 |A|$.

Suppose that two message $(m_1, m_2) = (s+k_1, \Pi(s)+k_2)$ and $(m_1', m_2') = (s' + k_1, \Pi(s') + k_2)$ have been observed. Both the two messages depend on $k_1$. Then we obtain $m_2 = \Pi(m_1 - k_1) + k_2$, $m_2' = \Pi(m_1' + k_1) + k_2$ which gives

$$\Pi(m_1 - k_1) - \Pi(m_1' - k_1) = m_2 - m_2'. \tag{8}$$

Since $m_1 \neq m_1'$ and $\Pi$ has perfect nonlinearity, (8) has exactly $|A|/|B|$ solution $k_1$. Hence $H(\mathcal{E}\backslash\mathcal{M}^2) = \log_2(|A|/|B|)$.

Thus the bound on $P_S$ given in Lemma 3 is

$$P := 2^{H(\mathcal{E}\backslash\mathcal{M}^2) - H(\mathcal{E}\backslash\mathcal{M})} = \frac{1}{|B|}.$$

Hence the code of Theorem 9 is optimal with respect to the bound on $P_S$ given in Lemma 3.

In summary, we have proved the following.

THEOREM 11. The code of Theorem 9 is optimal against both impersonation and substitution attacks.

# §7. Concluding Remarks

We remark that in the definition of the encoding algorithm $E_k$ in Constructions I and II, the trace function in [1] has been replaced by power function in this paper. Construction III is a promising application of perfect nonlinear mappings in the construction of authentication codes with secrecy, because it gives optimal authentication codes whenever $\Pi$ is perfect nonlinear, and $\Pi$ has been replaced by homomorphism in this paper.

Although the authentication codes constructed here are for providing both secrecy and authenticity at the same time, they can also be used as authentication codes without secrecy. To this end, in all the three constructions, we set $k_1 = 1$ and make $k_1$ public.

The implementation of these authentication/secrecy codes involves the arithmetic of power function between two fields and also realize an application of some properties about these authentication/secrecy codes from a

trace function between two fields in [1], and the computation of the values of power function. The homomorphism in the authentication code of (5) involves a number of multiplications and additions over a field, and its values can be computed efficiently in both hardware and software. Hence the perfect nonlinear functions used in Construction III can also be implemented efficiently.

Note that the authentication/secrecy codes presented in this paper provide perfect secrecy and are optimal against the impersonation and substitution attacks with respect to certain bounds on $P_I$ and $P_S$.

Highly nonlinear functions are used to construct authentication codes without secrecy in Chanson et al.[11], here we use them to construct optimal authentication codes with secrecy from homomorphism between two abelian groups within the framework of Construction III.

**ACKNOWLEDGMENT** We would like to thank the referees for their valuable suggestions. This paper is partially supported by NSF of China(61179026)and Civil Aviation University of China (2010kys06).

## [References]

[1] C. Ding and X. Tian. "Three Constructions of Authentication Codes with Perfect Secrecy ", Designs, Codes and Cryptography, 33, 227-239, 2004.

[2] E. F. Brickel, A few results in message authentication, Congressus Numerantium, Vol. 43 (1984) pp. 141-154.

[3] D.R.Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, J. Cryptology, Vol.1 (1988) pp. 119-127.

[4] J.L.Massey, CryptographyA Selective Survey, Digital Communications, North-Holland (1986) pp. 3-21.

[5] R.S.Rees and D. R. Stinson, Combinatorial characterizations of authentication codes, Designs, Codes and Cryptography, Vol.7(1996) pp. 239-259.

[6] D. Pei, Information-theoretic bounds for authentication codes and block designs, J. Cryptology, Vol.8 (1995) pp.177-188.

[7] U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, J. Cryptology, Vol. 6 (1993) pp. 135-156.

[8] A. Sgarro, Information-theoretic bounds for authentication frauds, J. Computer Security, Vol.2(1993) pp.53-63.

[9] T. Johansson,Authentication codes for non trusting parties obtained from rank metric codes, Des., Codes Cryptogr., vol.6, pp.205-218, 1995.

[10] C.E.Shannon, Communication theory of secrecy systems, Bell System Tech. J., Vol. 28 (1949)pp. 656-715.

[11] S. Chanson,C. Ding and A. Salomaa,Cartesian authentication codes from functions with optimal nonlinearity,Theoretical Computer Science,Vol.290(2003)pp.1737-1752.

[12] G.J.Simmons, Authentication theory/coding theory, Advances in Cryptology:Crypto'84, Lecture Notes in Computer Science,Vol.196(1984)pp.119-127.