Construction of Resilient Functions with Multiple Cryptographic Criteria[1]

Shaojing Fu Chao Li Bing sun
Department of Mathematic and System Science, NUDT, Changsha 410073

Abstract: In this paper, we describe a method to construct (n, m, t) resilient functions which satisfy multiple cryptographic criteria including high nonlinearity, good resiliency, high algebraic degree, and nonexistence of nonzero linear structure. Given a [u, m, t+1] linear code, we show that it is possible to construct (n, m, t) resilient functions with multiple good cryptographic criteria, where $2m \leqslant u < n$.

Key words: Resilient function; Linear Code; Nonlinearity; Linear structure

1 Introduction

Resilient functions have wide applications in quantum cryptographic key distribution, fault tolerant distributed computing, random sequence generation for stream ciphers, and S-box for block ciphers. It is now well accepted that for an (n, m, t) resilient function in symmetric cipher systems, it must satisfy the properties of high nonlinearity, high algebraic, and good resiliency, and good propagation character and so on. All of these parameters are important in resisting different kinds of attacks, so the research on cryptographic resilient functions is paid attention more and more[1,2,3,4,5]. However, we note that functions with good resiliency and high nonlinearity could imply some properties that lead to some cryptographic weakness, such as existence of linear structures. For example, the (n, m, t) resilient functions obtained from the paper [4, 6, 7], are all existence of nonzero linear structures [8]. Thus, Y.Z Wei turns to construct the (n, m, t) resilient functions which satisfy multiple cryptographic criteria including high nonlinearity, good resiliency, high algebraic degree, and nonexistence of nonzero linear structure [9]. But the method of construction in [9] has some mistakes.

In this paper, we point out the mistakes in [9], and describe an improved method to construct (n, m, t) resilient functions which satisfy multiple cryptographic criteria. The construction is based linear error-correcting code. Given a [u, m, t+1] linear code, we show that it is possible to construct (n, m, t) resilient functions with multiple cryptographic criteria, where $2m \leqslant u < n$.

[1]**Supported** by the National Natural Science Foundation of China (60573028) and State 863 Projects (2006AA701416)
E-mail: shaojing1984@yahoo.cn

2 Preliminaries

Let F_2 be the finite field with 2 elements, the vector space of n-tuples of element from F_2 is denoted by F_2^n, let $(F_2^n)^*$ be the nonzero vector of F_2^n .The addition operator over F_2 is denoted by +, representing additions modulo 2 . By V^n we mean the set of all Boolean functions on n variables. We interpret a Boolean function $f(x_1, x_2, \cdots, x_n)$ as the output column of its truth table, that is, a binary string of length 2^n having the form: $\{f(0, 0, \cdots, 0), f(0,0, \cdots, 1), \cdots, f(1,1, \cdots, 1)\}$. The weight of f is the number of ones in its output column, this is denoted by $wt(f)$. An n -variable function f is said to be balance if $wt(f)=2^{n-1}$.

An n-variable function f can be considered to be a multivariate polynomial over F_2. This polynomial can be express as a sum of products representation of all distinct kth-order ($k<n$) product terms of the variables. The number of variables in the highest order product term with nonzero coefficient is called the algebraic degree of f (abbr. $deg(f)$).

Functions with degree at most one are called affine functions. Affine functions with $f(0)=0$ are called linear functions. The set of all n-variable affine (respectively, linear) functions is denoted by A_n (respectively, L_n). The nonlinearity of an n-variable function f is the distance between f and the set of all n-variable affine functions, this is denoted by $nl(f)$.

The walsh transform of an n-variable function f is a real valued function defined as

$$W_f(u) = \sum_{x \in F_2^n} (-1)^{f(x)+x \cdot u}$$

where the dot product of vectors x and u is defined as $x \cdot u = x_1u_1 + x_2u_2 + \cdots + x_nu_n$. An n variable function f is called t-resilient if and only if $W_f(u) = 0$ for all u with $0 \le wt(u) \le t$, and f is said to have a linear structure, say a, iff $f(x+a)+f(x)$ is a constant function. Let us consider the function $F(x) = (f_1(x), f_2(x), \cdots, f_m(x))$ .Then the nonlinearity of F is defined as

$$nl(F) = \min\{ nl(\sum_{i=1}^{m} \tau_i f_i(x)) \mid \tau = (\tau_1, \cdots, \tau_m) \in (F_2^m)^* \}.$$

Similarly the algebraic degree of F is defined as

$$deg(F) = \min\{ deg(\sum_{i=1}^{m} \tau_i f_i(x)) \mid \tau = (\tau_1, \cdots, \tau_m) \in (F_2^m)^* \}.$$

F is said to be an (n, m, t) resilient function, iff $\sum_{i=1}^{m} \tau_i f_i(x)$ is an (n, 1, t) resilient function, for any $\tau \in (F_2^m)^*$. Moreover, a is said to be a linear structure *of* F, iff a is a linear structure of functions $\sum_{i=1}^{m} \tau_i f_i(x)$, for any $\tau \in (F_2^m)^*$.

Definition 1. A set D is called ***n-basis-set***, if it satisfies the following conditions:

1) $D \subset F_2^n$.

2) There exists $r_i \in D$, $i=1,2,\cdots,n$ such that $\{r_1, r_2, \cdots, r_n\}$ be a basis of F_2^n

3) There exists $i \ne j$ such that $r_i + r_j \in D$, where $1 \le i, j \le n$.

Lemma 1[9]**.** If D is an *n-basis-set*, then the function $f(x)=b \cdot x$ ($x \in D$) is not a constant function for any $b \in (F_2^n)^*$.

3 Construction of Resilient Functions with Multiple Cryptographic Criteria

In this section, we will provide a new method to get (*n*, *m*, *t*) resilient functions with multiple cryptographic criteria. Firstly, we remark that Lemma 2 in [9] is not correct. Here is a counter example:

Example 1. Consider a [7,3,3] linear code C with a basis {[1,0,0,1,0,1,1], [0,1,0,1,1,1,1], [0,0,1,0,1,0,1]}.then the dual of C(defined as $C^{\perp}$) is a [7,4,2] linear code which has a basis {[1,0,0,0,0,1,0], [0,1,0,0,1,1,1], [0,0,1,0,0,1,1],[0,0,0,1,0,1,0]}. It is easy to show that $C \cap C^{\perp}$={[1,1,1,0,0,0,1], [0,0,0,0,0,0,0]}. By computer search we know that a 7-*basis-set* D, such that $|D|=2^3$,$wt(x)\geq 2$, for any $x\in$ D can not be constructed by C and $C^{\perp}$.

Lemma 2. Let C be a [*u*, *m*, *t*+1] linear code. Then there exists a *u-basis-set* D, such that $|D|=2^q$, $wt(x)\geq t+1$, for any $x\in$ D, where $ln(u+4)\leq q\leq m$

Proof : Let $r_1=(0,1,1,\cdots,1)$, $r_2=(1,0,1,\cdots,1)$, $r_u=(1,1,\cdots,1,0)$, $r_{u+1}=(1,1,\cdots,1,1)$ where $r_1, r_2, \cdots, r_u$, $r_{u+1} \in F_2^u$.It is easy to show that$\{r_1+r_{u+1}, r_2+r_{u+1}, r_3+r_{u+1}, \cdots, r_u+r_{u+1}\}$is a basis of F_2^u , Now we define a set D ($|D|=2^q$) satisfies:

1) $r_1, r_2, r_3, \cdots, r_u, r_{u+1} \in D$

2)Let $c_1, c_2, c_1+c_2 \in D$ where $c_1, c_2 \in C$

3)And the remaining $2^q-(u+4)$ elements are chosen arbitrarily from C.

then D is a *u-basis-set*, such that $|D|=2^q$,$wt(x)\geq t+1$, for any $x\in$ D. □

Theorem 1. Let C be a [*u*, *m*, *t*+1] linear code. Let $f(x,y)=\varphi(x)\cdot y+g(x)$, $x\in F_2^q$, $y\in F_2^u$. Where $g(x)$ is a Boolean function on F_2^q, and$\varphi(x)$ is a bijection from F_2^q to the *u-basis-set* D (defined as in Lemma 2). Then the following results hold:

(1) $f(x,y)$ does not exist nonzero linear structure.

(2) $f(x,y)$ is an (n,1, t) resilient function with $n=u+q$

(3) $nl(f)= 2^{n-1}-2^{u-1}$

(4) $deg(f)\geq q$

Proof .

(1) $\forall (a,b)\in F_2^n$,where $a\in F_2^q, b\in F_2^u$

$D_f=f(x,y)+f(x+a,y+b)=g(x)+g(x+a)+[\varphi(x)+\varphi(x+a)]\cdot y+\varphi(x+a)\cdot b$

If $a=0$, $D_f=\varphi(x)\cdot b$, then from Lemma 1 we know that D_f is not a constant function

If $a\neq 0$, then $\varphi(x)+\varphi(x+a)\neq 0$ thus D_f is balance.

So $f(x, y)$ does not exist nonzero linear structure.

(2) Let $u=(u_1,u_2)$ $(u_1\in F_2^q, u_2\in F_2^u)$ with $0\leq wt(u)\leq t$

$$W_f(u) = \sum_{x,y} (-1)^{f(x,y)+(u_1,u_2)\cdot(x,y)}$$
$$= \sum_{x,y} (-1)^{\varphi(x)\cdot y + g(x) + u_1 \cdot x + u_2 \cdot y}$$
$$= \sum_{x} (-1)^{g(x)+u_1\cdot x} \sum_{y} (-1)^{(\varphi(x)+u_2)\cdot y}$$

$wt(u_2) \le t$ and $wt(\varphi(x)) \ge t+1$ by Lemma 2, then $\varphi(x)+u_2 \ne 0$ for all $x \in F_2^q$, so $W_f(u) = 0$ for all u with $0 \le wt(u) \le t$.

(3) $W_f(u) = \sum_{x,y} (-1)^{\varphi(x)\cdot y + g(x) + u_1 \cdot x + u_2 \cdot y} = \sum_{x} (-1)^{g(x)+u_1\cdot x} \sum_{y} (-1)^{(\varphi(x)+u_2)\cdot y}$

Since:

$$W_f(u) = \begin{cases} 0 & \text{If } \varphi(x)+u \ne 0 \text{ for all } x \in F_2^q \\ 2^u & \text{If } \exists x,\ \varphi(x)+u = 0 \end{cases}$$

So $nl(f) = 2^{n-1} - 2^{u-1}$

(4) Since g(x) is arbitrary over F_2^q, then the algebraic degree of $f(x,y)$ can exceed q. □

Lemma 3[9]**.** Let $\{c_0, c_1, \cdots, c_m\}$ be a basis of [u, m, t+1] linear code C. Let β be a primitive element in F_2^m and $\{1, \beta, \beta^2, \cdots, \beta^{m-1}\}$ be a basis of F_2^m. Define a bijection ϕ: $F_2^m \to$ C by

$$\phi(a_0\beta^0 + a_1\beta^1 + \cdots + a_{m-1}\beta^{m-1}) = a_0c_0 + a_1c_1 + \cdots + a_{m-1}c_{m-1}$$

Considers the matrices:

$$A = \begin{pmatrix} \phi(1) & \phi(\beta) & \cdots & \phi(\beta^{m-1}) \\ \phi(\beta) & \phi(\beta^2) & \cdots & \phi(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(\beta^{2^m-2}) & \phi(1) & \cdots & \phi(\beta^{m-2}) \end{pmatrix} \qquad B = \begin{pmatrix} \phi(1) & \phi(\beta) & \cdots & \phi(\beta^{m-1}) \\ \phi(\beta) & \phi(\beta^2) & \cdots & \phi(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(\beta^{m-1}) & \phi(\beta^m) & \cdots & \phi(\beta^{2m-2}) \end{pmatrix}$$

Then the following results hold:

(1)For any linear combination of columns (not all zero) of A, each nonzero codeword of C will appear exactly once.

(2)For any linear combination of columns (not all zero) of B, there exist a set of m nonzero codeword, which is always a basis of linear code C.

Lemma 4. Let C be a [u, m, t+1] linear code, then there exists a [u, u-m, t^*+1] linear code C^*, such that $C \cap C^* = \{0\}$, where $t^*+1 \ge 1$.

Proof. Let $\{c_0, c_1, \cdots c_{m-1}\}$ be a basis of [u, m, t+1] linear code C. It is easy to show that there exist $\{r_1, r_2, \cdots r_{u-m}\} \in GF(2)^u$–C such that $\{c_0, c_1, \cdots c_{m-1}, r_1, r_2, \cdots r_{u-m}\}$ is a basis of F_2^u, now we define a set C^* satisfying:

1) C^* is a linear code with length u.

2) $\{r_1, r_2, \cdots r_{u-m}\}$ is a basis of C^*.

Let $t^*=min\{wt(x)|x\in C^*\}-1$, then C^* is a $[u, u-m, t^*+1]$ linear code such that $C\cap C^*=\{0\}$. □

Lemma 5. Let C be a $[u, m, t+1]$ linear code and C^* be a $[u, u-m, t^*+1]$ linear code such that $C\cap C^*=\{0\}$.Then there exists a matrix $T_{2^q\times m}$ which has the property that every m nonzero codeword obtained in any linear combination of columns (not all zero) is still a *u-basis-set* D, such that $|D|=2^q$, $wt(x)\geq d$, for any $x\in D$, where $ln(u+1)\leq q\leq u-m$, $u\geq 2m$. $d=min(t+1, t^*+1)$.

Proof. Let $\{c_0, c_1, \cdots c_{m-1}\}$ be a basis of C and β be a primitive element in $F_2{}^m$. Let $\{r_1, r_2, \cdots r_{u-m}\}$ be a basis of C^* and β^* be a primitive element in $F_2{}^{u-m}$.

Define a bijection ϕ_1: $F_2{}^m \to C$ by

$$\phi_1(a_0\beta^0 + a_1\beta^1 + \cdots + a_{m-1}\beta^{m-1}) = a_0c_0 + a_1c_1 + \cdots + a_{m-1}c_{m-1}$$

Define a bijection ϕ_2: $F_2{}^m \to C^*$ by

$$\phi_2(a_0 + a_1\beta^* + \cdots + a_{u-m-1}\beta^{*u-m-1}) = a_0r_0 + a_1r_1 + \cdots + a_{u-m-1}r_{u-m-1}$$

Then we can obtain two matrices A_1 and A_2

$$A_1 = \begin{pmatrix} \phi_1(\beta^m) & \phi_1(\beta^{m+1}) & \cdots & \phi_1(\beta^{2m-1}) \\ \phi_1(\beta^{m+1}) & \phi_1(\beta^{m+2}) & \cdots & \phi_1(\beta^{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_1(\beta^{2^m-2}) & \phi_1(1) & \cdots & \phi_1(\beta^{m-2}) \end{pmatrix} \quad A_2 = \begin{pmatrix} \phi_2(\beta^{*(u-m)}) & \phi_2(\beta^{*(u-m+1)}) & \cdots & \phi_2(\beta^{*(u-1)}) \\ \phi_2(\beta^{*(u-m+1)}) & \phi_2(\beta^{*(u-m+2)}) & \cdots & \phi_2(\beta^{*u}) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_2(\beta^{*2^{u-m}-2}) & \phi_2(1) & \cdots & \phi_2(\beta^{*u-m-2}) \end{pmatrix}$$

Let

$$B_1 = \begin{pmatrix} \phi_1(1) & \phi_1(\beta) & \cdots & \phi_1(\beta^{m-1}) \\ \phi_1(\beta) & \phi_1(\beta^2) & \cdots & \phi_1(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_1(\beta^{m-1}) & \phi_1(\beta^m) & \cdots & \phi_1(\beta^{2m-2}) \end{pmatrix} \quad B_2 = \begin{pmatrix} \phi_2(1) & \phi_2(\beta^*) & \cdots & \phi_2(\beta^{*(m-1)}) \\ \phi_2(\beta^*) & \phi_2(\beta^{*2}) & \cdots & \phi_2(\beta^{*m}) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_2(\beta^{*(u-m-1)}) & \phi_2(\beta^{*(u-m)}) & \cdots & \phi_2(\beta^{*(u-2)}) \end{pmatrix}$$

$$T = \begin{pmatrix} (B_1^*)_{m\times m} \\ (B_2^*)_{(u-m)\times m} \\ (B_3^*)_{(2^q-u)\times m} \end{pmatrix}_{2^q\times m}$$

Where B_3 come from the row of A_1 and A_2 .

From the results of Lemma 3 and Lemma 4, it is easy to show that matrix T has the property that every 2^q nonzero codeword obtained in any linear combination of columns (not all zero) is still a *u-basis-set* D, such that $|D|=2^q$, $wt(x)\geq d$, for any $x\in D$. where $ln(u+1)\leq q\leq u-m$, $u\geq 2m$, $d=min(t+1, t^*+1)$. □

Theorem 2. Let C be a $[u, m, t+1]$ linear code and C^* be the $[u, u-m, t^*+1]$ obtained in Lemma 4. Let (n,m) function $F(x, y)=(f_1(x,y), f_2(x,y), \cdots f_m(x,y))$, where $f_i(x,y)=\varphi_i(x)\cdot y+g_i(x)$, $x\in F_2{}^q$, $y\in F_2{}^u$, $g_i(x)$ is any Boolean function on $F_2{}^q$, and $\varphi_i(x)$ is any bijection from $F_2{}^q$ to the ith column of matrix T (defined as in Lemma 5).

Then the following results hold:

(1) F(x, y) does not exist nonzero linear structures.

(2) F(x, y) is (n, m, t) resilient function with $d=min(t, t^*)$ and $n=u+q$.

(3) nl(F)= 2^{n-1} -2^{u-1}.

(4) $deg(F) \geq q-2$ for $max(\ (2m)^{1/2}, ln(u+1)) \leq q \leq m-1$, $deg(F) \geq q-1$ for $m \leq q \leq u-m$

Proof: Let $\tau = (\tau_1, \cdots, \tau_m) \in$ $(F_2{}^m)^*$. then $\sum_{i=1}^{m} \tau_i f_i(x, y) = \sum_{i=1}^{m} \tau_i \varphi_i(x) \cdot y + \sum_{i=1}^{m} \tau_i g_i(x)$

From Lemma 5 we can show that $\sum_{i=1}^{m} \tau_i \varphi_i(x)$ is a bijection from $F_2{}^q$ to a *u-basis-set* D,

where $|D|=2^q$, $wt(x) \geq d$, for any $x \in$ D.

Then from Theorem 1 we obtain :

(1) F(x, y) does not exist nonzero linear structures.

(2) F(x, y) is (n, m, t) resilient function with $d=min(t+1, t^*+1)$.

(3) nl(F)= 2^{n-1} -2^{u-1}.

Now we prove (4), Note that $g_i(x)$ is any Boolean function on $F_2{}^q$

If $m \leq q \leq u-m$ then for $1 \leq i \leq m$, define $g_i(x) = x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_q$, then $deg(\ \sum_{i=1}^{m} \tau_i g_i(x)\ )$ $=q-1$ for $\tau = (\tau_1, \cdots, \tau_m) \in (F_2{}^m)^*$

If $max(\ (2m)^{1/2}, ln(u+1)) \leq q \leq m-1$, define

$S=\{\ x_1 x_2 \cdots x_{k-1} x_{k+1} \cdots x_{l-1} x_{l+1} \cdots x_q \ \ | 0 \leq k,l \leq q$ and $k \neq l\ \} \bigcup \{\ x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_q \,| 1 \leq i \leq q\ \}$

$g_i(x)\ (1 \leq i \leq m)$ are m arbitrary element of S. then $deg(\ \sum_{i=1}^{m} \tau_i g_i(x)\ ) = q-2$,

for $(\tau_1, \cdots, \tau_m) \in (F_2{}^m)^*$ □

Construction Procedure:

Input: a [u, m, t+1] linear code C

Output: an (n, m, d) resilient function

1) Let $t^* = t$

2) Search to obtain a [u, u-m, t^*+1] linear code C^* such that $C \cap C^* = \{0\}$, if successful go to **4)**

3) $t^* = t^* - 1$

4) Obtain the matrix T (see Lemma 5)

5) Define $f_i(x,y)=\varphi_i(x) \cdot y + g_i(x)$, $x \in GF(2)^q$, $y \in GF(2)^u$ (defined as in Theorem 2)

6) output($f_1(x,y)$, $f_2(x,y)$, $\cdots$ $f_m(x,y)$)

However, the major problem with our method is the fact that such a construction is available through computer search (which becomes infeasible for a moderate cardinality of codes). Using the result in[10], we describe an easy way in some special cases.

Lemma 6[10] the number of disjoint [tm, m, t+1] linear code is lower bounded by

$$M^{lb}(tm, m, t+1) = (2^m - 2m) \sum_{i=0}^{t-2} (2m-1)^i (2^m - 1)^{t-2-i}$$

Theorem 3. Let C be a [2*m*, *m*, 3] linear code and *q* be an integer with $\max(\ (2m)^{1/2}, ln(2m+1)) \le q \le u-m$. Let $n=u+q$, then there exists (*n*,*m*) function $F(x, y)=(\ f_1(x,y), f_2(x,y), \cdots\ f_m(x,y)\ )$ such that:

(1) F(*x*, *y*) does not exist nonzero linear structures.

(2) F(*x*, *y*) is (*n*, *m*, 2) resilient function.

(3) $nl(F)= 2^{n-1} -2^{2m-1}$.

(4) $deg(F) \ge q-2$ for $max(\ (2m)^{1/2}, ln(2m+1)) \le q \le m-1$, $deg(F) \ge q-1$ for $m \le q \le u-m$

Proof: From Lemma 6**,** it is easy to show that $M^{lb}(2m, m, 3) = (2^m - 2m) \ge 2$,

Then we can construction another [*2m*, *m*, 3] linear code C^* such that $C \cap C^*=\{0\}$.

The remaining proof is similar to Theorem 2.

In the following table we compare (*n*, *m*, *t*) resilient functions obtained using the techniques presented in this paper with the existing results.

Table 1. comparison of (*n*, *m*, *t*) resilient functions with multiple cryptographic criteria

	Codes	Nonlinearity	Degree	Nonzero linear structure
[6]	A [*u*, *m*, *t*+1] linear code	$2^{n-1} -2^{u-1}$	$\ge q$	Exist
[7]	Some disjoint [*u*, *m*, *t*+1] linear codes	$\ge 2^{n-1} -2^{u-1}$	$\ge m$	Exist
Ours	A [*u*, *m*, *t*+1] linear code	$2^{n-1} -2^{u-1}$	$\ge q$	Not exist

4 Conclusion

In this paper, we point out the mistakes in [9], and describe an improved method for constructing of (*n*, *m*, *t*) resilient functions which satisfy multiple Cryptographic criteria. The construction is based on the use of linear error correcting code , our method provides a new idea in designing cryptographic functions. Besides, given a [*u*, *m*, *t*+1] linear code C, It will be of interest to find new methods to get a [*u*, *u-m*, t^*+1] linear code C^* that C and C^* are disjoint.

References

[1] A. Canteaut and C. Carlet. Propagation characteristics and correlation immunity of highly nonlinear boolean functions. Adv. in Cryptology EUROCRYPT‘2000, Springer-verlag, Lecture Notes in Computer Science, Vol. 1807,pp. 507–522,2000.

[2] Claude Carlet. On the propagation criterion of degree l and order k. Adv. in Cryptology EUROCRYPT‘98, Springer-verlag, Lecture Notes in Computer Science,pp. 463–474,1998.

[3] E. Pasalic. Degree optimized resilient boolean functions from Maiorana-MCFarland class. Cryptography and Code 2003, Springer-verlag, Lecture Notes in Computer Science, Vol. 2898, pp. 93–114,2003.

[4] K.Kurosawa and T.Satoh. Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria. Adv. in Cryptology EUROCRYPT‘97, Springer-verlag, Lecture Notes in Computer Science, Vol. 1233, pp. 434–449,1997.

[5] Y. Zheng and X.M. Zhang. On plateaued function. IEEE Trans.Inform.Theory ,Vol. 47,pp. 1215–1223,2001.

[6] E.Pasalic and S. Maitra. Linear code in generalized construction of resilient functions with very high nonlinearity. IEEE Trans. Inform.Theory,Vol. 48,pp. 2182–2192,2002.

[7] T.Johansson and E.Pasalic. A construction of resilient functions with high nonliearity. IEEE Trans. Inform.Theory ,Vol. 49,pp. 495–501,2003.

[8] Y.Z.Wei and Y.P.Hu. Reserch on linear structure of several cryptographic functions. J. of China Institute of Commu., Vol. 25,pp. 22–56,2004.

[9] Y.Z.Wei and Y.P.Hu. A construction of resilient functions with Satisfying Synthetical Cryptographic Criteria. IEEE ISOC ITW2005 on Coding and Complexity; pages 248-252.

[10] P. Charpin and E. Pasalic. Highly nonlinear resilient functions through disjoint codes in projective spaces. Designs, codes and cryptography, 37, 319-346, 2005.