A new construction of resilient functions over *GF*(*p*) with good cryptographic properties

Kai-Qun Huang
Department of Computer Science & Information Engineering
National Chiao Tung University
huangkc@csie.nctu.edu.tw

Jen-Chun Chang
Department of Computer Science & Information Engineering
National Taipei University
jcchang@csie.nctu.edu.tw

Rong-Jaye Chen
Department of Computer Science & Information Engineering
National Chiao Tung University
rjchen@csie.nctu.edu.tw

Abstract*-A common structure of key stream generator for stream ciphers consisting of several linear feedback shift registers*(*LFSR*) *combined by a combining function. The combining function plays an important role in the cryptographic security of stream ciphers. Most combining functions are resilient functions. In this paper we first show some lemmas about the cryptographic properties of functions over the Galois Field GF*(*p*) *where p is a prime. These lemmas are useful for demonstrations and constructions of resilient functions. Finally, we propose a new strategy to construct resilient functions. The nonlinearity, algebraic degree, and the order of correlation immunity of these resilient functions are also discussed.*

Keywords: Stream Cipher, Resilient Function, Affine function, Nonlinearity, Correlation Immunity.

1. Introduction

The main component of a stream cipher is a key stream generator which consists of several linear feedback shift registers(LFSR) and functions. Filter generators, combination generators and clock-control generators are three common kinds of key stream generators for stream ciphers. Among these three kinds of generators, combination generators are most widely used. This kind of generator uses several LFSRs combined by a nonlinear function, i.e., combining function *f*. If the function *f* is not properly chosen, then the combination generator combined by *f* can be attacked from common attacks, such as linear synthesis attack[8], correlation attack[10], and best affine approximation attack[3]. There are at least four criteria that *f* should fulfill. These criteria are balancedness, high algebraic degree, high nonlinearity, and high order of correlation immunity.

All of these criteria are important in resisting various kinds of attacks. Many research results have been published on these criteria. Firstly, K. Gopalakrishnan and D. R. Stinson [4] demonstrated that three different characterizations of *t* th-order correlation immune functions and resilient functions where the random variable is over the Galois Field *GF*(*q*) and *q* is a prime power. In the following year P. Camion and A. Canteaut[1] generalized the results of Gopalakrishnan and Stinson. They gave an orthogonal array characterization and a Fourier transform characterization for resilient functions over any finite field. Moreover, they also constructed new resilient functions by composition of resilient functions of small order. Next in 1998, M. Liu, P. Lu, and G. L. Mullen[7] showed the tradeoff among algebraic degree and order of correlation immunity over some special finite fields. They proved that (n-1)-th resilient functions with n variables over *GF*(3) have a unique algebraic degree 1. Besides, they also designed a kind of (*n*-1)-th resilient functions with n variables over *GF*(*q*), where *q* is greater than 3. However, the most recent papers written by Y. Hu and G. Xiao[5][6] concentrate on the construction of resilient functions which have some restrictions on order of correlation immunity. The authors design not only 1-output functions but also m-output functions over *GF*(*q*), where m is greater than 1.

In this correspondence, we first show some lemmas about the cryptographic properties of functions over *GF*(*p*) where *p* is a prime. These lemmas are useful for demonstrations and constructions of resilient functions. Furthermore, we give a new construction method for constructing resilient functions. The nonlinearity, algebraic degree, and the order of correlation immunity of these resilient functions are also discussed.

This paper is organized as follows. In Section 2, we introduce some basic definitions and notations. In Section 3, we give new results for resilient functions over *GF*(*p*). In Section 4, we propose a new construction of resilient functions over *GF*(*p*). We also discuss the nonlinearity, algebraic degree, and the order of correlation immunity of these resilient functions. In Section 5 we make a conclusion.

2. Basic Notations

This work was supported by the National Science Council, R.O.C. , under contracts no. NSC 93-2213-E-009-010- and no. NSC93-2213-E-305-003-.

We review some relevant definitions, notations and former results in the area of our concern. By $GF(p)$ we mean the Galois Field with p elements, where p is a prime. Let $[GF(p)]^n$ denote the set of n-tuples of elements from $GF(p)$. Let $u = (u_1,u_2,\ldots,u_n)$ and $x = (x_1, x_2, \ldots,x_n)$ be two vectors in $GF(p)$. The scalar product of u and x, denoted by $u \cdot x$, is defined by $u \cdot x = u_1x_1+u_2x_2+\ldots+u_nx_n$, where multiplication and addition are over $GF(p)$. We interpret a function f: $[GF(p)]^n \rightarrow GF(p)$ as $f(x)$. Then f can be uniquely expressed in algebraic normal form(ANF):

$$f(x)=\sum_{k_1=0}^{q-1}\sum_{k_2=0}^{q-1}\cdots\sum_{k_n=0}^{q-1}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$$

where each coefficient is a constant in $GF(p)$. The *algebraic degree* of f, denoted by $deg(f)$, is defined as the number of variables in its longest term when it is represented in the algebraic normal form.

Let $\delta=(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_s)$ be a vector in $[GF(p)]^s$ with $s \geqq 1$. Then the notation δ' is defined as follows

$$\delta'=\sum_{j=1}^{s}\varepsilon_j p^{s-j}.$$

Suppose f is an n-variable function over $GF(p)$ and w is the p-th root of unity in the field of complex numbers C. Then the *truth table* of f, denoted by T_f, is defined as follows

$$(f(\delta_0), f(\delta_1),\ldots, f(\delta_{p^n-1}))$$

where δ_j is in $[GF(p)]^n$. The $b \cdot T_f$ and $b + T_f$ are defined as follows

$$(b\cdot f(\delta_0), b\cdot f(\delta_1),\ldots, b\cdot f(\delta_{p^n-1}))$$

and

$$(b + f(\delta_0), b + f(\delta_1),\ldots, b + f(\delta_{p^n-1}))$$

where multiplication and addition are over $GF(p)$ and b is a constant in $GF(p)$. In addition, the *walsh-hadamard transform* for an n-variable function f over $GF(p)$ is defined as follows

$$F_f(a,b,u)=\sum_x w^{au\cdot x+bf(x)}$$

where a is a nonzero constant in $GF(p)$, b is a constant in $GF(p)$.

An n-variable affine function l over $GF(p)$ is a function that has algebraic degree at most one, i.e., it takes the form of $l(x) = u \cdot x+c$, where c is a constant in $GF(p)$. Furthermore, l is called a linear function if c=0. By $A_p(n)$ (respectively $L_p(n)$) we denote the set of all affine(respectively linear) functions over $GF(p)$. The *Hamming weight* of a string s in $GF(p)$, denoted by $HW(s)$, is the number of nonzero elements in s. The *Hamming distance* between two string s_1 and s_2, denoted by $HD(s_1,s_2)$, is the number of the different elements in the same position. The Hamming distance between two n-variable functions $f(x)$ and $g(x)$ over $GF(p)$ is defined by $HD(f,g) = HD(T_f , T_g)$. Then the nonlinearity of n-variable function f, denoted by N_f, is defined as follows

$$N_f = \min_{l\in A_p(n)}\{HD(T_f,T_l)\}.$$

Furthermore, suppose that f be a function over $GF(p)$. If $\Pr[f(x)=z]=1/p^n$, then f is said to be balanced. And then f is a t-th order correlation immune function if for any vector $(a_1,\ldots,a_t)\in[GF(p)]^n$ and any $z\in GF(p)$

$$\#\{x \mid x=(x_1,\ldots,x_n)\in F_q, x_{j_1}=a_1,\ldots,x_{j_t}=a_t, f(x)=z\}=q^{n-t}$$

where $t \geqq 1$. f is said to be a t-resilient function if f is t-th order correlation immune and balanced.

Finally we introduce a notation which is used throughout the rest of the paper. Given any vectors $\delta=(\varepsilon_1,\varepsilon_2,...,\varepsilon_s)\in[GF(p)]^s$, we define a s-variable function over $GF(p)$ by

$$Z_{\delta'}(y)=\prod_{i=1}^{s}\prod_{j=0|j\neq\varepsilon_i}^{p-1}\frac{(y_i-j)}{(\varepsilon_i-j)}$$

where multiplication and subtraction are over $GF(p)$, $y = (y_1,y_2,\ldots,y_n)$ and δ' is defined before. Note that since $Z_{\delta'}(y)=1$ if and only if $y=\delta'$.

3. New Results for Resilient functions

In [5], the authors did not discuss the nonlinearity of the constructing functions presented at the theorem 5. From the definition of nonlinearity mentioned above, it is not difficult to compute a lower bound of nonlinearity for this construction method. The following lemma explains this result.

*Lemma*1: Let $2 \leqq t \leqq n$ and A be any subset of $GF(p)$. Suppose that nonlinearity of f_1 and f_2 be denoted by N_{f_1} and N_{f_2} respectively, where $f_1$and f_2 are two n-variable functions over $GF(p)$. If we construct an $(n+1)$-variable function f defined as follows

$$h(x_1,\ldots,x_{n+1})=\prod_{a\in A}(x_{n+1}-a)f(x_1,\ldots,x_n)+\prod_{a\in F_q-A}(x_{n+1}-a)g(x_1,\ldots,x_n),$$

then $N_f \geq \#A\cdot N_{f_1}+(p-\#A)\cdot N_{f_2}$, where $\#A$ is the number of elements in set A.

Proof:

Note that for any affine function $\gamma\in A_p(n+1)$, we can write the truth table of γ in the form

$$T_l \,\|\, T_l+b \,\|\, T_l+2b \,\|\cdots\|\, T_l+(p-1)b,$$

where $l\in A_p(n)$, b = 0, 1, …, p-1 and $\|$ is a concatenation operator. And from the constructing method of function f, we can also write the truth table of f in the form

$$c_0\cdot T_{h_0} \,\|\, c_1\cdot T_{h_1} \,\|\ldots\|\, c_{p-1}\cdot T_{h_{p-1}},$$

where $h_k\in\{T_{f_1},T_{f_2}\}$, c_k is a nonzero constant in $GF(p)$, and k = 0, 1, …, p-1. Then,

$$HD(T_f, T_\gamma) = \sum_{k=0}^{p-1} HD(T_l + kb, c_k \cdot T_{h_k})$$
$$= \sum_{k|T_{h_k}=T_{f1}} HD(T_l + kb, c_k \cdot T_{h_k}) + \sum_{k|T_{h_k}=T_{f2}} HD(T_l + kb, c_k \cdot T_{h_k})$$

Since for all k= 0, 1, …, p-1, the inverse of c_j modulo p is existing. Hence, we can imply as follows

$$HD(T_f, T_\gamma) = \sum_{k|T_{h_k}=T_{f1}} HD(c_k^{-1}(T_l + kb)), T_{h_k}) + \sum_{k|T_{h_k}=T_{f2}} HD(c_k^{-1}(T_l + kb), T_{h_k})$$

By the definition of nonlinearity, we know that

$HD(c_k^{-1}(T_l + kb)), T_{h_k}) \geq N_{f_1}$ or N_{f_2}.

Then

$$HD(T_f, T_\gamma) \geq \sum_{k=1}^{\#A} N_{f_1} + \sum_{k=1}^{p-\#A} N_{f_2}$$
$$= \#A \cdot N_{f_1} + (p - \#A) \cdot N_{f_2}$$ □

In [4], K. Gopalakrishnan and D. R. Stinson raise a method that can test for correlation immune functions over $GF(p)$ by walsh-hadamard transform. Here we describe a relationship between the nonliearity and walsh-hadamrad transform of a function f over $GF(p)$.

Lemma 2: Let f be an n-variable function over $GF(p)$. Then the nonlinearity of the function f can express as

$$N_f = p^n - \frac{1}{p} \cdot \max_{u \in [GF(p)]^n} \left\{ \sum_{c=0}^{p-1} F_f(a, -a, u) \right\}$$

where $a \in GF(p)/\{0\}$.

Proof:

First, we consider that

$$F_f(a, -a, u) = \sum_x w^{a(u \cdot x - f(x))}$$
$$= \sum_{y \in \{x | u \cdot x = f(x)\}} w^{a(y \cdot u - f(y))} + \sum_{y \in \{x | u \cdot x \neq f(x)\}} w^{a(y \cdot u - f(y))}.$$

Let $\psi = \#\{x \mid x \cdot u = f(x)\}$, then $F_f(a,-a,u)$ can simplify as

$$F_f(c, -c, u) = \psi + \sum_{y \in \{x | u \cdot x \neq f(x)\}} w^{c(d_y)}$$

where $d_y = y \cdot u - f(y)$ for all $y \in \{x \mid u \cdot x \neq f(x)\}$.

Then,

$$\sum_{a=0}^{p-1} F_f(a, -a, u) = \sum_{a=0}^{p-1} (\psi + \sum_{y \in \{x | u \cdot x \neq f(x)\}} w^{a(d_y)})$$
$$= p\psi + \sum_{y \in \{x | u \cdot x \neq f(x)} \sum_{a=0}^{p-1} w^{a(d_y)} = p\eta$$

$$\Rightarrow \psi = \frac{1}{p} \cdot \sum_{c=0}^{p-1} F_f(c, -c, u) \cdot$$

From the definition of nonlinearity, we know that

$$N_f = \min_{u \in [GF(p)]^n} \{HD(T_f, T_{u \cdot x})\}$$
$$= \min_{u \in [GF(p)]^n} \{\#\{x \mid u \cdot x \neq f(x)\}\}$$
$$= \min_{u \in [GF(p)]^n} \left\{ p^n - \frac{1}{p} \sum_{a=0}^{p-1} F_f(a, -a, u) \right\}$$
$$= p^n - \frac{1}{p} \max_{u \in [F_p]^n} \left\{ \sum_{a=0}^{p-1} F_f(a, -a, u) \right\}$$ □

4. A New Construction of Resilient Functions over *GF*(*p*)

In this section, we present our construction method of resilient functions over $GF(p)$. We use lemmas in section 3 to prove the properties of resilient functions.

First we review a result in [4] that can test for correlation immune function over $GF(p)$.

Lemma 3[4]: For all $a, b \in GF(p)$ with $a \neq 0$, f is a t-th correlation immune function with n variables over $GF(p)$ if and only if

$F_f(a, b, u) = 0$

for all $u \in [GF(p)]^n$ such that $1 \leqq HW(u) \leqq t$. □

Now, we construct new resilient functions over $GF(p)$. The following theorem explains this construction method.

*Theorem*1: Let

(1) n, s and t be three positive integers with $n \geqq 4$, $1 \leqq s \leqq n$-3, $1 \leqq t < n$-s.

(2) $f_{\delta'}$ be a t-th resilient function with (n-s) variables over $GF(p)$ for all $\delta \in (GF[p])^s$.

(3) $N_{f_{\delta'}}$ be the nonlinearity of $f_{\delta'}$ for all $\delta \in (GF[p])^s$.

We now define a function f: $[GF(p)]^n \rightarrow GF(p)$ by

$$f(y, x) = \sum_{\delta \in [GF(p)]^s} Z_{\delta'}(y) f_{\delta'}(x)$$

where $y = (y_1, y_2, \ldots, y_s)$ and $x = (x_1, x_2, \ldots, x_{n-s})$. Then the following holds:

(1) f is a t-th resilient function.

(2) $N_f \geq \sum_{\delta \in [GF(p)]^n} N_{f_{\delta'}}$.

Proof:

(1) First, we show that $f(y,x)$ is balanced. Since $f_{\delta'}$ is a resilient function. Hence $\#\{x \mid f_{\delta'}(x) = z\} = p^{n-s-1}$ for all $z \in GF(p)$. Then we have

$$\#\{x \mid f(y, x) = z\} = \sum_{\delta'=0}^{p^s-1} \#\{x \mid f_{\delta'} = z\} = p^s \cdot p^{n-s-1} = p^{n-1}$$
$$= p^s \cdot p^{n-s-1} = p^{n-1}.$$

It is clear that $f(y,x)$ is balanced.

Next, we prove that $f(y,x)$ is a t-th correlation immune function. Let w be the p-th root of unity in C. For all $a, b \in GF(p)$ with $a \neq 0$ and any $(c, d) \in [GF(p)]^n$ with $c \in [GF(p)]^s$, $d \in [GF(p)]^{n-s}$, $1 \leqq WH(c,d) \leqq t$, we note that

$$F_f(a,b,(c,d)) = \sum_{y,x} w^{a(c,d)\cdot(y,x)+bf(y,x)}$$
$$= \sum_{y,x} w^{a(c\cdot y+d\cdot x)+b(\sum_{\delta} Z_{\delta'}(y) f_{\delta'}(x))}$$
$$= \sum_{y} w^{a(c\cdot y)} \sum_{x} w^{a(d\cdot x)+b(\sum_{\delta} Z_{\delta'}(y) f_{\delta'}(x))}.$$

For all η in $[GF(p)]^s$, we know that

$$f(\eta,x) = f_{\eta'}(x).$$

Further, $0 \leqq WH(d) \leqq t$. To find $F_f(a,b,(c,d))$, we consider the following cases:

Case1: $1 \leqq WH(d) \leqq t$

Since $f(\eta,x)$ is a t-th resilient function. Through Lemma 3 we obtain

$$\sum_{x} w^{a(d\cdot x)+b(f(\eta,x))} = 0.$$

This result implies that $F_f(a,b,(c,d)) = 0$.

Case2: $WH(d)=0$

Let $b \neq 0$. We obtain

$$\sum_{x} w^{a(d\cdot x)+b(f(\eta,x))} = 0$$

because $f(\eta,x)$ is balanced. This result also imply that $F_f(a,b,(c,d)) = 0$.

Besides, let $b = 0$. We obtain

$$\sum_{x} w^{a(d\cdot x)+b(f(\eta,x))} = p^{n-s}.$$

Then

$$F_f(a,b,(c,d)) = \sum_{y} w^{a(c\cdot y)} \cdot p^{n-s} = 0$$

because $a(u \cdot x)$ is a linear function with $a \neq 0$, $WH(c) = t$.

From case1 and case2, we know

$$F_f(a,b,(c,d)) = 0$$

for $1 \leqq WH(c,d) \leqq t$. By Lemma 3, $f(y,x)$ is a t-th correlation immune function.

(2) Let $\kappa \in A_p(s)$ and $l \in A_p(n-s)$. Note that for any affine function $\gamma \in A_p(n)$, we can write the truth table of γ in the form

$$T_l \,||\, T_l + \kappa(0,0,\cdots,1) \,||\, T_l + \kappa(0,0,\cdots,2) \,||\cdots$$
$$||\, T_l + \kappa(p-1, p-1,\cdots, p-1)$$

where $||$ is a concatenation operator. And we can also write the truth table of f in the form

$$T_{f_0} \,||\, T_{f_1} \,||\ldots||\, T_{f_{p^n-1}}.$$

Then

$$HD(T_f, T_\gamma) = \sum_{k\in[GF(p)]^s} HD(T_l + \kappa(k), T_{f_{k'}})$$

By the definition of nonlinearity, we know that

$$HD(T_f, T_\gamma) = \sum_{\delta\in[GF(p)]^s} HD(T_l + \kappa(\delta), T_{f_{\delta'}}).$$

Then we obtain

$$N_f \geq \sum_{\delta\in[GF(p)]^n} N_{f_{\delta'}}.$$

□

*Theorem*2: Let

(1) n, s and t be three positive integers with $n \geqq 4$, $1 \leqq s \leqq n-3$, $1 \leqq t < n-s$.

(2) $\delta = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_s) \in [GF(p)]^s$.

(3) $\theta_{n,s,t} = \{u_{\delta'} \in [GF(p)]^{n-s} \mid HW(u_{\delta'}) \geq t+1\}$.

(4) $t_d = \#\{\delta \mid u_{\delta'} = d, d \in [GF(p)]^{n-s}\}$ and $t = \max_d \{t_d\}$.

(5) $u_\delta(i)$ be the i-th component of $u_{\delta'}$.

(6) $T(i) = \sum_{\delta} \left(\prod_{i=1}^{s} \prod_{j=0 | j\neq\varepsilon_i}^{p-1} \frac{1}{(\varepsilon_i - j)} \right) u_{\delta'}(i) \bmod p$.

We now define a function f: $[GF(p)]^n \to GF(p)$ by

$$f(y,x) = \sum_{\delta\in[GF(p)]^s} Z_{\delta'}(y)(u_{\delta'}\cdot x)$$

where $y = (y_1, y_2, \ldots, y_s)$ and $x = (x_1, x_2, \ldots, x_{n-s})$. Then the following holds:

(1) f is a t-th resilient function.

(2) $N_f = (p-1)(p^{n-1} - t\cdot p^{n-s-1})$.

(3) If $T(i) \neq 0$ for $1 \leq i \leq n-s$, then $deg(f)=(p-1)s+1$.

Proof:

(1) Since $u_{\delta'}\cdot x$ is a t-th resilient function for all $\delta \in (GF[p])^s$. By Theorem 1-(1) we know f is a t-th resilient function.

(2) For all $a \in GF(p)/\{0\}$ and any $(c,d) \in [GF(p)]^n$ with $c \in [GF(p)]^s$, $d \in [GF(p)]^{n-s}$, we note that

$$\sum_{a=0}^{p-1} F_f(a,-a,(c,d))$$
$$= \sum_{a=0}^{p-1} \sum_{y,x} w^{a(c,d)\cdot(y,x)-af(y,x)}$$
$$= p^n + \sum_{a=1}^{p-1} \sum_{y,x} w^{a\left(c\cdot y+d\cdot x-\sum_{\delta} Z_{\delta'}(y)(u_{\delta'}\cdot x)\right)}$$
$$= p^n + \sum_{a=1}^{p-1} \sum_{y} w^{a(c\cdot y)} \sum_{x} w^{a\left(d\cdot x-\sum_{\delta} Z_{\delta'}(y)(u_{\delta'}\cdot x)\right)}.$$

Further, $0 \leqq WH(d) \leqq t$ and $f(\eta,x) = u_{\eta'}\cdot x$ for all η in $[GF(p)]^s$. Then we know that

$$\sum_{x} w^{a(d\cdot x)-a(f(\eta,x))} = \begin{cases} p^{n-s} & , d = f(\eta,x) \\ 0 & , d \neq f(\eta,x) \end{cases}.$$

Therefore we can imply that

$$\sum_{a=0}^{p-1} F_f(a,-a,(c,d)) = p^n + p^{n-s} \sum_{a=1}^{p-1} \sum_{y | d=u_{\eta'})} w^{a(c\cdot y)}. \qquad \text{(a)}$$

Hence,

$$\max_{(c,d)} \left\{ \sum_{a=0}^{p-1} F_f(a,-a,(c,d)) \right\} \leq p^n + p^{n-s} \sum_{a=1}^{p-1} \max_d \{t_d\}$$
$$= p^n + p^{n-s}(p-1)t.$$

If we let $c = 0$ in (a), it follows that

$$\max_{(c,d)} \left\{ \sum_{a=0}^{p-1} F_f(a,-a,(c,d)) \right\} \geq \max_{(0,d)} \left\{ \sum_{a=0}^{p-1} F_f(a,-a,(0,d)) \right\}$$
$$= p^n + p^{n-s}(p-1)t.$$

Therefore

$$\sum_{a=0}^{p-1} F_f(a,-a,(c,d)) = p^n + p^{n-s}(p-1)t.$$

By Lemma 2,

$$N_f = p^n - \frac{1}{p}(p^n + p^{n-s}(p-1)t)$$
$$= (p-1)(p^{n-1} - t \cdot p^{n-s-1}).$$

(3) We know

$$f(y,x) = \sum_{\delta \in [GF(p)]^s} Z_{\delta'}(y)(u_{\delta'} \cdot x).$$

If $T(i) \neq 0$ for some i, then the term $y_1^{p-1} y_2^{p-1} \cdots y_s^{p-1} x_i$ is not cancelled. Hence the algebraic degree of f is $(p\text{-}1)s+1$. □

*Example*1: Choose $p = 3$, $n = 5$, $s = 1$ and $t = 2$ in Theorem 2. Choose

$$\theta_{4,1,2} = \{u_0 = (2,2,1,0), u_1 = (1,1,2,1), u_0 = (0,1,1,1)\}.$$

This implies that t=1. Next the function f: $[GF(3)]^4 \rightarrow GF(3)$ is defined as follows.

$$f(y,x) = \frac{(y_1-1)(y_1-2)}{(0-1)(0-2)}(2x_1 + 2x_2 + x_3) + \frac{(y_1-0)(y_1-2)}{(1-0)(1-2)}(x_1 + x_2 + 2x_3 + x_4) + \frac{(y_1-0)(y_1-1)}{(2-0)(2-1)}(x_2 + x_3 + x_4).$$

Then f is 2-th resilient function and the nonliearty of f is

$$= (p-1)(p^{n-1} - t \cdot p^{n-s-1}) = 108.$$

And since

$$T(1) = \frac{1}{(0-1)(0-2)} \cdot 2 + \frac{1}{(1-0)(1-2)} \cdot 1 (\mathrm{mod}\, 3)$$
$$= 1 (\mathrm{mod}\, 3).$$

By Theorem 2-(3), $deg(f)$ = (3-1)1+1 = 3. □

For p = 2 the resilient functions constructed by Theorem 2 will coincide with those given in [2].

5. Conclusion

In this paper, we consider functions over $GF(p)$. A new relationship between nonlinearity and walsh-hadamard transform of f has been provided. Furthermore, we have constructed new resilient functions over $GF(p)$ and discussed the nonlinearity and algebraic degree of these functions. In the future, we are interested in constructing functions with better nonlinearity and algebraic degree than those in our method. In addition, we will look for the optimal nonlinearity of resilient functions for input parameters p, n, t.

References

[1] P. Camion, and A. Canteaut, "Construction of t-resilient functions over a finite alphabet," in Advances in Cryptology-EUROCRYPT'96 (Lecture Notes in Computer Science) Berlin, Germany:Springer-Verlag, Vol. 1070, pp. 283-293, 1996.

[2] S. Cheet, S. Lee, D. Lee, and S. H. Sung, "On the correlation immune functions and their nonlinearity," in Advances in Cryptology-ASIACRYPT'96 (Lecture Notes in Computer Science) Berlin, Germany:Springer-Verlag, vol. 1163, pp. 232-243, 1996.

[3] C. Ding, G. Xia, and W. Shan, The stability theory of stream ciphers, Number 561, Lecture Notes in Computer Science, Springer-Verlag, 1991.

[4] K. Gopalakrishnan, and D. R. Stinson, "Three characterizations of non-binary correlation-immune and resilient functions," International Journal of Designs, Codes and Cryptography 5, pp.241-251, 1995.

[5] Y. Hu, and G. Xiao, "Correlation immune over finite fields," IEEE Transaction on Information Theory, vol. 44, no. 3, pp. 1273-1276, May, 1998.

[6] Y. Hu, and G. Xiao, "Resilient functions over finite fields", IEEE Transaction on Information Theory, vol. 49, no. 8, pp. 2040-2046, August, 2003.

[7] M. Liu, P. Lu, and G. L. Mullen, "Correlation immune functions over finite fields," IEEE Transaction on Information Theory, vol. 44, pp. 1273-1276, May 1998.

[8] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of applied cryptography, Boca Raton, FL:CRC, 1997.

[9] J. Seberry, and X. M. Zhang, "Highly nonlinear 0-1 balanced boolean functions satisfying strict avalanche criterion," in Advances in Cryptology-AUSCRYPT'92 (Lecture Notes in Computer Science) Berlin, Germany:Srpinger-Verlag, vol. 718, pp. 145-155, 1993.

[10] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," IEEE Transaction on Computers, vol. C-34, pp. 81-85, 1985.