STRICT AVALANCHE CRITERION OVER FINITE FIELDS

YUAN LI AND T.W.CUSICK

Abstract. Boolean functions on $GF(2)$ which satisfy the Strict Avalanche Criterion (SAC) play an important role in the art of information security. In this paper, we extend the conception SAC to finite fields $GF(p)$. A necessary and sufficient condition is given by using spectral analysis. Also, based on an interesting permutation polynomial theorem, we prove various facts about $(n-1)$-th order SAC functions on $GF(p)$. We also construct many such functions.

1. Introduction

Resilient functions, bent functions and functions which satisfy SAC have important cryptographic applications. SAC was introduced by Webster and Tavares [16] in connection with a study of the design of S-boxes. A Boolean function in n variables is said to satisfy SAC if complementing any one of the n input bits results in changing the output bit with probability exactly one half. Forré [5] extended this conception by defining the higher order SAC. A Boolean function of n variables satisfies the SAC of order k ($SAC(k)$), $0 \le k \le n-2$, if whenever k input bits are fixed arbitrarily, the resulting function of $n-k$ variables satisfies SAC. The properties of SAC functions have been well studied (see [1], [2], [3], [8], [9], [17]). Recently, Cusick and Yuan [4] described a method to find k-th order symmetric SAC functions for any k, $k \le n-2$. On the other hand, it's natural to extend the various cryptographic conceptions from $GF(2)$ to $GF(p)$ or $GF(p)^n$. For example, [14] and [19] studied the resilient functions on $GF(p)$. Also, [7], [11], [12] investigated the generalized bent functions on $GF(p)^n$. In this paper, we firstly introduce the definition of SAC on $GF(p)$. Similar to [5], we give a spectral analysis, and a necessary and sufficient condition for SAC is given. Based on an interesting result which was independently proved by three research groups between 1989 and 1990, we prove various facts about $(n-1)$-order SAC on $GF(p)$. In contrust, on $GF(2)$ the highest order of SAC is only $n-2$. Using some elementary number theory, we construct many $SAC(n-1)$ functions. Section 2 will list some well known results about Fourier transform. Section 3 will introduce the definition of SAC and discuss its spectral analysis. In section 4, an explanation of SAC is given from a different point of view. We give the definition of higher order SAC in section 5 and a spectral analysis is provided for $SAC(1)$. In section 6 we construct many $SAC(n-1)$ functions. Some open questions are listed in section 7.

Key words and phrases. Fourier transform, cryptography, Boolean functions, algebraic normal form, strict avalanche criterion, resilience, bent functions, permutation polynomials, finite field, quadratic residue, Legendre symbol,

2. Fourier Transform of n variables polynomial functions on $GF(p)$

In this paper, p is always an odd prime.

If f: $GF(p)^n \longrightarrow GF(p)$, then f can be uniquely expressed in the following form:

$$f(x_1, x_2, ..., x_n) = \sum_{k_1=0}^{p-1} \sum_{k_2=0}^{p-1} ... \sum_{k_n=0}^{p-1} a_{k_1 k_2 ... k_n} {x_1}^{k_1} {x_2}^{k_2} ... {x_n}^{k_n} \tag{1}$$

Each coefficient $a_{k_1 k_2 ... k_n} \in GF(p)$ is a constant. This form is called the algebraic normal form of f. The largest $k_1 + k_2 + ... + k_n$ with $a_{k_1 k_2 ... k_n} \neq 0$ is called the algebraic degree of f.

Let $A = \{f | GF(p)^n \longrightarrow GF(p)\}$, $B = \{\widehat{f} | GF(p)^n \longrightarrow C\}$, where C is the complex numbers. Then

$$F_{\widehat{f}}(x) = \sum_{y \in GF(p)^n} \widehat{f}(y) w^{-xy}$$

is called the Fourier transform of $\widehat{f}(x)$, where $w = e^{2\pi i/p}$, $x = (x_1, x_2, ..., x_n)$, $y = (y_1, y_2, ..., y_n)$, $xy = \sum_{k=1}^{n} x_k y_k$.

Some of the following results about the Fourier transform may be "folk lore", but for completeness, we present the proofs.

Lemma 1. $F_{F_{\widehat{f}}}(x) = p^n \widehat{f}(-x)$

Proof.

$$F_{F_{\widehat{f}}}(x) = \sum_{y \in GF(p)^n} F_{\widehat{f}}(y) w^{-xy} = \sum_{y \in GF(p)^n} (\sum_{z \in GF(p)^n} \widehat{f}(z) w^{-yz}) w^{-xy}$$
$$= \sum_{z \in GF(p)^n} (\sum_{y \in GF(p)^n} w^{-(z+x)y}) \widehat{f}(z)$$

The inner sum will vanish if $z \neq -x$, hence, $F_{F_{\widehat{f}}}(x) = p^n \widehat{f}(-x)$. □

If $\widehat{f} = w^f$, we have

$$p^n w^{f(-x)} = \sum_{y \in GF(p)^n} F_{w^f}(y) w^{-xy}, \quad w^{f(x)} = p^{-n} \sum_{y \in GF(p)^n} F_{w^f}(y) w^{xy}.$$

Of course, we have

$$F_{w^f}(x) = \sum_{y \in GF(p)^n} w^{f(x) - xy}$$

Let $\widehat{f} * \widehat{g} : \quad x \longrightarrow \sum_{y \in GF(p)^n} \widehat{f}(x-y) \widehat{g}(y)$. Clearly, $(\widehat{f} * \widehat{g})(x) = (\widehat{g} * \widehat{f})(x)$ and $((\widehat{f} * \widehat{g}) * \widehat{h})(x) = (\widehat{f} * (\widehat{g} * \widehat{h}))(x)$.

Lemma 2. $F_{\widehat{f} * \widehat{g}}(x) = F_{\widehat{f}}(x) F_{\widehat{g}}(x)$

Proof.

$$F_{\widehat{f} * \widehat{g}}(x) = \sum_{y \in GF(p)^n} (\widehat{f} * \widehat{g})(y) w^{-yx} = \sum_{y \in GF(p)^n} (\sum_{z \in GF(p)^n} \widehat{f}(y-z) \widehat{g}(z)) w^{-yx}$$
$$= \sum_{z \in GF(p)^n} (\sum_{y \in GF(p)^n} \widehat{f}(y-z) w^{-yx}) \widehat{g}(z) = \sum_{z \in GF(p)^n} (\sum_{u \in GF(p)^n} \widehat{f}(u) w^{-x(u+z)}) \widehat{g}(z)$$

$$= \sum_{z\in GF(p)^n} (\sum_{u\in GF(p)^n} \widehat{f}(u)w^{-xu})\widehat{g}(z)w^{-xz} = F_{\widehat{f}}(x)F_{\widehat{g}}(x)$$

□

Lemma 3. $F_{\widehat{f}} * F_{\widehat{g}} = p^n F_{\widehat{f}\widehat{g}}$

Proof.

$$(F_{\widehat{f}} * F_{\widehat{g}})(x) = \sum_{y\in GF(p)^n} F_{\widehat{f}}(x-y)F_{\widehat{g}}(y)$$

$$= \sum_{y\in GF(p)^n} (\sum_{s\in GF(p)^n} \widehat{f}(s)w^{-s(x-y)})(\sum_{t\in GF(p)^n} \widehat{g}(t)w^{-ty})$$

$$= \sum_{s\in GF(p)^n} \sum_{t\in GF(p)^n} \widehat{f}(s)\widehat{g}(t)w^{-sx} \sum_{y\in GF(p)^n} w^{y(s-t)}.$$

The inner sum will vanish if $s \neq t$, hence,

$$(F_{\widehat{f}} * F_{\widehat{g}})(x) = p^n \sum_{s\in GF(p)^n} \widehat{f}(s)\widehat{g}(s)w^{-sx} = p^n F_{\widehat{f}\widehat{g}}(x)$$

□

Lemma 4. $\widehat{h} = \widehat{f} * \widehat{g}$ *if and only if* $F_{\widehat{h}} = F_{\widehat{f}}F_{\widehat{g}}$

Proof. Necessity is Lemma 2.

From $F_{\widehat{h}} = F_{\widehat{f}}F_{\widehat{g}}$, we have $F_{F_{\widehat{h}}} = F_{F_{\widehat{f}}F_{\widehat{g}}}$. By Lemma 1 and Lemma 3,
$p^n\widehat{h}(-x) = p^{-n}(F_{F_{\widehat{f}}} * F_{F_{\widehat{g}}}) = p^{-n}(p^n\widehat{f}(-x) * p^n\widehat{g}(-x)) \iff$
$\widehat{h}(-x) = \widehat{f}(-x) * \widehat{g}(-x) = (\widehat{f} * \widehat{g})(-x) \iff \widehat{h} = \widehat{f} * \widehat{g}$ □

Lemma 5. $\widehat{h} = \widehat{f}\widehat{g} \iff F_{\widehat{h}} = p^{-n}F_{\widehat{f}} * F_{\widehat{g}}$

Proof. Necessity is Lemma 3.

If $F_{\widehat{h}} = p^{-n}F_{\widehat{f}} * F_{\widehat{g}}$, then $F_{F_{\widehat{h}}}(x) = F_{p^{-n}F_{\widehat{f}}*F_{\widehat{g}}}(x)$. By Lemma 1 and Lemma 2,
$p^n\widehat{h}(-x) = p^{-n}F_{F_{\widehat{f}}*F_{\widehat{g}}}(x) = p^{-n}F_{F_{\widehat{f}}}(x)F_{F_{\widehat{g}}}(x) = p^{-n}p^n\widehat{f}(-x)p^n\widehat{g}(-x)$
$\Longrightarrow \widehat{h}(-x) = \widehat{f}(-x)\widehat{g}(-x) \Longrightarrow \widehat{h}(x) = \widehat{f}(x)\widehat{g}(x)$. □

3. Strict Avalanche Criterion and Spectral Analysis

Let $wt(\alpha)$ be the Hamming weight of α, i.e., the number of nonzero components of α, $\alpha \in GF(p)^n$.

Definition 1. $f(x): \quad GF(p)^n \longrightarrow GF(p)$ fulfills Strict Avalanche Criterion (SAC) if and only if $prob(f(x+\alpha) = f(x) + a) = \frac{1}{p}$ for any $a \in GF(p)$ and any $\alpha \in GF(p)^n$ with $wt(\alpha) = 1$.

In fact, $f(x)$ fulfills SAC means $f(x+\alpha) - f(x)$ is a balanced function if $wt(\alpha) = 1$. Note that f is a permutation on $GF(p)$ if $n = 1$.

Lemma 6. *$f(x)$ fulfills SAC $\iff$ $\sum_{x\in GF(p)^n} w^{f(x+\alpha)-f(x)} = 0$, for any α with $wt(\alpha) = 1$.*

Proof. Let $n_j = \#\{x|f(x+\alpha)-f(x)=j\}$, $j=0,1,...,p-1$. Because of the identity $w^0+w^1+...+w^{p-1}=0$, we have
$\sum_{x\in GF(p)^n} w^{f(x+\alpha)-f(x)} = n_0w^0+n_1w^1+...+n_{p-1}w^{p-1}=0 \iff$
$(n_0-n_{p-1})w^0+(n_1-n_{p-1})w^1+...+(n_{p-2}-n_{p-1})w^{p-2}=0 \iff$
$n_0-n_{p-1}=n_1-n_{p-1}=...=n_{p-2}-n_{p-1}=0$ since the minimal polynomial of w is $x^{p-1}+...+x+1 \iff n_0=n_1=...=n_{p-1} \iff$
$f(x+\alpha)-f(x)$ is a balanced function.

□

Lemma 7.

$$h(x)=\sum_{y\in GF(p)^n} w^{f(y+x)-f(y)} \iff F_h(x)=F_{w^f}(x)F_{w^{-f}}(-x)$$

Proof. "$\Longrightarrow$"

$$F_h(x)=\sum_{y\in GF(p)^n} h(y)w^{-xy}=\sum_{y\in GF(p)^n}(\sum_{z\in GF(p)^n} w^{f(z+y)-f(z)})w^{-xy}$$

$$=\sum_{z\in GF(p)^n}(\sum_{y\in GF(p)^n} w^{f(z+y)-xy})w^{-f(z)}=\sum_{z\in GF(p)^n}(\sum_{s\in GF(p)^n} w^{f(s)-x(s-z)})w^{-f(z)}$$

$$=\sum_{z\in GF(p)^n} F_{w^f}(x)w^{-f(z)+xz}=F_{w^f}(x)F_{w^{-f}}(-x).$$

"$\Longleftarrow$"

$$F_{F_h}(x)=F_{F_{w^f}(x)F_{w^{-f}}(-x)}$$

By Lemma 1 and Lemma 5, we have

$$p^nh(-x)=p^{-n}F_{F_{w^f}(x)}*F_{F_{w^{-f}}(-x)}=p^{-n}(p^nw^{f(-x)}*p^nw^{-f(x)}).$$

Hence,

$$h(-x)=w^{f(-x)}*w^{-f(x)}=\sum_{y\in GF(p)^n} w^{f(-(x-y))}w^{-f(y)}=\sum_{y\in GF(p)^n} w^{f(y-x)}w^{-f(y)},$$

So,

$$h(x)=\sum_{y\in GF(p)^n} w^{f(y+x)-f(y)}$$

□

Now, we can prove the following spectral characterization of SAC.

Theorem 1. *f(x) fulfills SAC* $\iff F_{F_{w^f}(x)F_{w^{-f}}(-x)}(s)=0$, *when* $wt(s)=1$.
$\iff \sum_{x\in GF(p)^n} F_{w^f}(x)F_{w^{-f}}(-x)w^{-\delta x_i}=0$, *for all* $i\in\{1,2,...,n\}$ *and any* $\delta\in GF(p)^*$. $\iff \sum_{x:x_i=0} F_{w^f}(x)F_{w^{-f}}(-x)=\sum_{x:x_i=1} F_{w^f}(x)F_{w^{-f}}(-x)=......$
$=\sum_{x:x_i=p-1} F_{w^f}(x)F_{w^{-f}}(-x)$.

Proof. By Lemma 7, $h(x)=\sum_{y\in GF(p)^n} w^{f(y+x)-f(y)} \iff F_h(x)=F_{w^f}(x)F_{w^{-f}}(-x)$
$\Longrightarrow F_{F_h}(s)=F_{F_{w^f}(x)F_{w^{-f}}(-x)}(s) \Longrightarrow p^nh(-s)=F_{F_{w^f}(x)F_{w^{-f}}(-x)}(s)$
$\Longrightarrow h(s)=p^{-n}F_{F_{w^f}(x)F_{w^{-f}}(-x)}(-s)$.
By Lemma 6, $f(x)$ fulfills $SAC \iff h(s)=0$ when $wt(s)=1 \iff$
$F_{F_{w^f}(x)F_{w^{-f}}(-x)}(-s)=0$ for any s with $wt(s)=1 \iff F_{F_{w^f}(x)F_{w^{-f}}(-x)}(s)=0$ for any s with $wt(s)=1 \iff \sum_{x\in GF(p)^n} F_{w^f}(x)F_{w^{-f}}(-x)w^{-sx}=0$ for any s with

$wt(s) = 1 \iff \sum_{x\in GF(p)^n} F_{w^f}(x)F_{w^{-f}}(-x)w^{-\delta x_i} = 0$ for any $i \in \{1, 2, , ..., n\}$ and for any $\delta \in GF(p)^*$, where x_i is the ith component of vector $x \iff$
$\sum_{x:x_i=0} F_{w^f}(x)F_{w^{-f}}(-x)w^{-\delta(0)} + \sum_{x:x_i=1} F_{w^f}(x)F_{w^{-f}}(-x)w^{-\delta(1)} + ...$
$+ \sum_{x:x_i=p-1} F_{w^f}(x)F_{w^{-f}}(-x)w^{-\delta(p-1)} = 0 \iff \sum_{x:x_i=0} F_{w^f}(x)F_{w^{-f}}(-x)=$
$\sum_{x:x_i=1} F_{w^f}(x)F_{w^{-f}}(-x)=......$ $\sum_{x:x_i=p-1} F_{w^f}(x)F_{w^{-f}}(-x)$ (the last step is same as the proof of lemma 6 since
$\{-\delta(0), -\delta(1), ..., -\delta(p-1)\} = \{0, 1, ..., p-1\}$ when $\delta \neq 0$). □

Let $\widehat{f} = w^f$, $\widehat{g} = w^{-f}$ in Lemma 3, we have

Theorem 2.

$$F_{w^f} * F_{w^{-f}}(\alpha) = \begin{cases} p^{2n} & \alpha = 0 \\ 0 & \alpha \neq 0 \end{cases}$$

i.e.

$$\sum_{x\in GF(p)^n} F_{w^f}(x)F_{w^{-f}}(\alpha - x) = \begin{cases} p^{2n} & \alpha = 0 \\ 0 & \alpha \neq 0 \end{cases}$$

Similar to the situation on $GF(2)$, we have the following simple results.

Theorem 3. *$f(x)$ fulfills SAC if and only if $g(x) = f(\sigma x + c)$ fulfills SAC, where σ is a permutation on $GF(p)^n$, $c \in GF(p)^n$.*

Theorem 4. *$f(x)$ fulfills SAC if and only if $af(x) + b$ fulfills SAC, where $a \neq 0$, $b \in GF(p)$.*

Theorem 5. *If $f(x)$ and $g(y)$ are SAC over $GF(p)^{n_1}$ and $GF(p)^{n_2}$ respectively, then $h(z) = f(x) + g(y)$ is SAC over $GF(p)^{n_1+n_2}$, where $z = (x, y)$.*

4. Spectral Symmetries of SAC-Fulfilling Functions

Definition 2. A function f: $GF(p)^n \longrightarrow GF(p)$ is said to be $\frac{1}{p}$-dependent in its i-th input component x_i if and only if $prob(f(x + \alpha_i) = f(x) + a) = \frac{1}{p}$ for any $a \in GF(p)$, $b \in GF(p)^*$ such that $\alpha_i = (0, ...0, b, 0, ...0)$, where b is the i-th component.

It is clear that f fulfills SAC if and only if it is $\frac{1}{p}$-dependent in each of its input components. Similar to Lemma 6, we have $f(x)$ is $\frac{1}{p}$- dependent in its i-th input if and only if $\sum_{x\in GF(p)^n} w^{f(x+\alpha_i)-f(x)} = 0$ for any $b \in GF(p)^*$ such that $\alpha_i = (0, ..., 0, b, 0, ..., 0)$, where b is the i-th component.

Now, we can give a spectral characterization.

Theorem 6. *If*

$$F_{w^f}(x)F_{w^{-f}}(-x) = F_{w^f}(x + c)F_{w^{-f}}(-x - c) \tag{2}$$

for any $c \in I_{i_1 i_2 ... i_m} = \{(c_1, ..., c_n)|c_i \neq 0 \Longrightarrow i \in \{i_1, ..., i_m\}\}$, then $f(x)$ is $\frac{1}{p}$-dependent in the input components $x_{i_1}, x_{i_2}, ..., x_{i_m}$.

Proof. Let $x' \in GF(p)^m$, $x' = (x'_1, ..., x'_m)$,
$S_{x'} = \{x \in GF(p)^n | x_{i_1} = x'_1, ..., x_{i_m} = x'_m\}$, then

$$GF(p)^n = \bigcup_{x'\in GF(p)^m} S_{x'}, S_{x'_1} \bigcap S_{x'_2} = \phi \iff x'_1 \neq x'_2.$$

Because of (2), we can write

$$\sum_{x\in S_{x'}} F_{w^f}(x)F_{w^{-f}}(-x) = \sum_{x\in S_{x'+c'}} F_{w^f}(x)F_{w^{-f}}(-x)$$

for any $x' \in GF(p)^m$ and any $c' \in GF(p)^m$. Let $x' = (0, x'')$, $x'' \in GF(p)^{m-1}$, $c' = (j, c'')$, $c'' \in I_{i_2...i_m}$, $1 \le j \le p-1$, we have

$$\sum_{x\in S_{(0,x'')}} F_{w^f}(x)F_{w^{-f}}(-x) = \sum_{x\in S_{(j,x''+c'')}} F_{w^f}(x)F_{w^{-f}}(-x)$$

for any $x'' \in GF(p)^{m-1}$, $c'' \in GF(p)^{m-1}$. Hence,

$$\sum_{x''\in GF(p)^{m-1}} \sum_{x\in S_{(0,x'')}} F_{w^f}(x)F_{w^{-f}}(-x) = \sum_{x''\in GF(p)^{m-1}} \sum_{x\in S_{(j,x''+c'')}} F_{w^f}(x)F_{w^{-f}}(-x)$$

which means

$$\sum_{x:x_{i_1}=0} F_{w^f}(x)F_{w^{-f}}(-x) = \sum_{x:x_{i_1}=j} F_{w^f}(x)F_{w^{-f}}(-x), j \in \{1, 2, ..., p-1\}.$$

By the proof of Theorem 1, we know $f(x)$ is $\frac{1}{p}$-dependent in the i_1th input component. By symmetric reason, we get the same result for $x_{i_2}, ..., x_{i_m}$. □

5. *SAC* of High Order

Definition 3. f: $GF(p)^n \longrightarrow GF(p)$ is said to fulfill SAC of order m ($SAC(m)$) if any function obtained from $f(x)$ by keeping m of its input components constant fulfills the SAC as well (this must be true for any choice of the position, and any values of the m constant components).

When $p \ge 3$, we have $SAC(n-1)$ functions, which is impossible for $p = 2$. For example, $f(x_1, ..., x_n) = a_1x_1^2 + ... + a_nx_n^2$, where $a_i \in GF(p)^*$.

Theorem 7. *$f(x)$ fulfills $SAC(m)$ implies $f(x)$ fulfills $SAC(m-1)$, $1 \le m \le n-1$.*

Proof. Let $f^{c_1\cdots c_k}_{i_1\ldots i_k}$ be the function resulted from f by fixing x_{i_j} to constant c_j, $c_j \in GF(p)$, $j = 1, 2, ...k$. Let $\alpha \in GF(p)^{n-m+1}$ and $wt(\alpha) = 1$, consider

$V = \sum_{x\in GF(p)^{n-m+1}} w^{f^{c_1\cdots c_{m-1}}_{i_1\cdots i_{m-1}}(x+\alpha)-f^{c_1\cdots c_{m-1}}_{i_1\cdots i_{m-1}}(x)}$, without lost of generality, let $\alpha = (a, 0, ..., 0) = (\alpha', 0)$, $a \in GF(p)^*$, $\alpha' \in GF(p)^{n-m}$, $x = (x', \delta)$, $x' \in GF(p)^{n-m}$, $wt(\alpha') = 1$. Then,

$$V = \sum_{\delta=0}^{p-1} \sum_{x'\in GF(p)^{n-m}} w^{f^{c_1\cdots c_{m-1}\delta}_{i_1\cdots i_{m-1}j_{n-m+1}}(x'+\alpha')-f^{c_1\cdots c_{m-1}\delta}_{i_1\cdots i_{m-1}j_{n-m+1}}(x')}$$

By Lemma 6, each of the p inner sums is zero since f fulfills $SAC(m)$. Hence, $V = 0$, and f fulfills $SAC(m-1)$ since each $f^{c_1\ldots c_{m-1}}_{i_1\ldots i_{m-1}}$ fulfills SAC by Lemma 6. □

In the following, we will give a spectral characterization for $SAC(1)$.

Let l_j: $GF(p) \longrightarrow C$, $0 \le j \le p-1$ be defined by

$$l_j(x) = \begin{cases} 1 & x = j \\ 0 & x \ne j. \end{cases}$$

Then we have

$w^{f(x)} = \sum_{j=0}^{p-1} l_j(x_i) w^{f_i^j(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)}$ for any i, where f_i^j is obtained from $f(x)$ by keeping the i-th component of x constant and equal to j. Hence,

$$F_{w^f}(u) = \sum_{j=0}^{p-1} \sum_{x \in GF(p)^n} l_j(x_i) w^{f_i^j(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)} w^{-ux}$$

$$= \sum_{j=0}^{p-1} \sum_{x:x_i=j} w^{f_i^j} w^{-u'x'} w^{-ju_i}$$

for any i, where $u = (u_1, \ldots, u_n)$, $u' = (u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n)$, $x' = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. So,

$$F_{w^f}(u) = \sum_{j=0}^{p-1} w^{-ju_i} \sum_{x:x_i=j} w^{f_i^j - u'x'} = \sum_{j=0}^{p-1} w^{-ju_i} F_{w^{f_i^j}}(u')$$

$$= F_{w^{f_i^0}}(u') + w^{-u_i} F_{w^{f_i^1}}(u') + \ldots + w^{-(p-1)u_i} F_{w^{f_i^{p-1}}}(u'),$$

$u_i \in GF(p)$, $u_i = 0, 1, \ldots, p-1$. In matrix form, we get

$$\begin{pmatrix} F_{w^f}(u)|_{u_i=0} \\ F_{w^f}(u)|_{u_i=1} \\ . \\ . \\ . \\ F_{w^f}(u)|_{u_i=p-1} \end{pmatrix} = M \begin{pmatrix} F_{w^{f_i^0}}(u') \\ F_{w^{f_i^1}}(u') \\ . \\ . \\ . \\ F_{w^{f_i^{p-1}}}(u') \end{pmatrix},$$

where

$$M = M^T = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & w^{-1} & \ldots & w^{-(p-1)} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & w^{-(p-1)} & \ldots & w^{-(p-1)(p-1)} \end{pmatrix}.$$

Let

$$N = N^T = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & w & \ldots & w^{(p-1)} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & w^{p-1} & \ldots & w^{(p-1)(p-1)} \end{pmatrix}.$$

We have $MN = Diag\{p, p, \ldots, p\}$, $M^{-1} = p^{-1}N$. So,

$$(3) \qquad \begin{pmatrix} F_{w^{f_i^0}}(u') \\ F_{w^{f_i^1}}(u') \\ . \\ . \\ . \\ F_{w^{f_i^{p-1}}}(u') \end{pmatrix} = M^{-1} \begin{pmatrix} F_{w^f}(u)|_{u_i=0} \\ F_{w^f}(u)|_{u_i=1} \\ . \\ . \\ . \\ F_{w^f}(u)|_{u_i=p-1} \end{pmatrix}$$

On the other hand, $w^{-f(x)} = \sum_{j=0}^{p-1} l_j(x_i) w^{-f_i^j(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)}$ for any i.

$$F_{w^{-f}}(-u) = \sum_{j=0}^{p-1} \sum_{x:x_i=j} w^{-f_i^j} w^{u'x'} w^{ju_i}$$

$$= \sum_{j=0}^{p-1} w^{ju_i} \sum_{x:x_i=j} w^{-f_i^j + u'x'} = \sum_{j=0}^{p-1} w^{ju_i} F_{w^{-f_i^j}}(-u')$$

$$= F_{w^{-f_i^0}}(-u') + w^{u_i} F_{w^{-f_i^1}}(-u') + ... + w^{(p-1)u_i} F_{w^{-f_i^{p-1}}}(-u'),$$

In matrix form, we have

$$\begin{pmatrix} F_{w^{-f}}(-u)|_{u_i=0} \\ F_{w^{-f}}(-u)|_{u_i=1} \\ . \\ . \\ . \\ F_{w^{-f}}(-u)|_{u_i=p-1} \end{pmatrix} = N \begin{pmatrix} F_{w^{-f_i^0}}(-u') \\ F_{w^{-f_i^1}}(-u') \\ . \\ . \\ . \\ F_{w^{-f_i^{p-1}}}(-u') \end{pmatrix},$$

or

$$\begin{pmatrix} F_{w^{-f_i^0}}(-u') \\ F_{w^{-f_i^1}}(-u') \\ . \\ . \\ . \\ F_{w^{-f_i^{p-1}}}(-u') \end{pmatrix} = N^{-1} \begin{pmatrix} F_{w^{-f}}(-u)|_{u_i=0} \\ F_{w^{-f}}(-u)|_{u_i=1} \\ . \\ . \\ . \\ F_{w^{-f}}(-u)|_{u_i=p-1} \end{pmatrix} \tag{4}$$

From (3) and (4), we get $F_{w^{f_i^j}}(u')F_{w^{-f_i^j}}(-u') =$
$p^{-1}(\sum_{r=0}^{p-1} w^{rj} F_{w^f}(u)|_{u_i=r}) p^{-1}(\sum_{s=0}^{p-1} w^{-sj} F_{w^{-f}}(-u)|_{u_i=s})$
$=p^{-2} \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} w^{(r-s)j} F_{w^f}(u)|_{u_i=r} F_{w^{-f}}(-u)|_{u_i=s}$,
where $u' = (u_1, ..., u_{i-1}, u_{i+1}, ..., u_n)$. From Theorem 1, we get

Theorem 8. *f(x): $GF(p)^n \longrightarrow GF(p)$ fulfills $SAC(1)$ if and only if*

$$\sum_{\substack{u':u_t=0 \\ t\neq i}} \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} w^{(r-s)j} F_{w^f}(u)|_{u_i=r} F_{w^{-f}}(-u)|_{u_i=s} =$$

$$\sum_{\substack{u':u_t=1 \\ t\neq i}} \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} w^{(r-s)j} F_{w^f}(u)|_{u_i=r} F_{w^{-f}}(-u)|_{u_i=s} =$$

....

$$\sum_{\substack{u':u_t=p-1 \\ t\neq i}} \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} w^{(r-s)j} F_{w^f}(u)|_{u_i=r} F_{w^{-f}}(-u)|_{u_i=s} =$$

for any i, any $t \in I - \{i\}$ and any $j \in GF(p)$.

By (3) and (4), we get the following

Theorem 9. *For any f(x): $GF(p)^n \longrightarrow GF(p)$, we have*

$$\sum_{j=0}^{p-1} F_{w^{f_i^j}}(u') F_{w^{-f_i^j}}(-u') = p^{-1} \sum_{j=0}^{p-1} (F_{w^f}(u) F_{w^{-f}}(-u))|_{u_i=j}$$

for any $i \in \{1, 2, ..., n\}$.

6. Construction and Characterization of $SAC(n-1)$ over $GF(p)$

In 1989 and 1990, three groups ([6], [10], [15]) independently proved the following interesting result about permutation polynomials.

Theorem 10. *Suppose $f(x)$ is a polynomial on $GF(p)$. If $f(x+\alpha)-f(x)$ is a permutation for any $\alpha \neq 0$, then f must be quadratic.*

From this theorem, we immediately have

Theorem 11. *$f(x_1,...,x_n) : GF(p)^n \longrightarrow GF(p)$, if f is $SAC(n-1)$, then the degree of each x_i must be 2. Actually, we have the following:*
$f(x_1,...,x_n)=f_{i1}(x_1,...,x_{i-1},x_{i+1},...,x_n)x_i^2+f_{i2}(x_1,...,x_{i-1},x_{i+1},...,x_n)x_i+$ $f_{i3}(x_1,...,x_{i-1},x_{i+1},...,x_n)$, where f_{i1} is never zero, f_{i3} is $SAC(n-2)$ for $i=1,2,...,n$.

Proof. By Definition 3, $f(c_1,...c_{i-1},x_i,c_{i+1},...,c_n)$ is SAC for any $c_1,...,c_{i-1},c_{i+1},...,c_n$ and hence must be quadratic because of Theorem 10. So, the coefficient f_{i1} is never zero. Also, f_{i3} must be $SAC(n-2)$ since $f_{i3}=f(x_1,...,x_{i-1},0,x_{i+1},...,x_n)$. □

We introduce a "big oh" notation for $f(x)$:
If the degree of each x_i is at most one, i.e. $f(x_1,...x_n)=\sum_{S\subset I} d_S \prod_{i\in S} x_i$, where $I=\{1,2,...,n\}$, then we write f as "big oh" of $x_1,...,x_n$, i.e. $f=O(x_1,...x_n)$. Obviously, $O(x_1,...,x_n)+O(x_1,...,x_n)=O(x_1,...,x_n)$, $O(x_1,...,x_k)+O(x_{k+1},...,x_t)=O(x_1,...,x_t)$.

Theorem 12. *If $f(x_1,x_2)$ is SAC(1), then $f(x_1,x_2)$ must be*
1)$a_1x_1^2+a_2x_2^2+O(x_1,x_2)$, $a_1,a_2\in GF(p)^*$, or
2)$a(x_1^2+bx_1+c)(x_2^2+dx_2+e)+O(x_1,x_2)$, where $a\neq 0$, $x_1^2+bx_1+c$ and $x_2^2+dx_2+e$ are never zero, i.e. $x_1^2+bx_1+c=(x+b_1)^2-r_1$, $x_2^2+dx_2+e=(x_2+d_2)^2-r_2$, with Legendre symbol $(\frac{r_i}{p})=-1$, $i=1,2$.

Proof. $f(x_1,x_2)=x_1^2f_1(x_2)+x_1f_2(x_2)+f_3(x_2)$, $f_1(x_2)=a_1x_2^2+b_1x_2+c_1$, $f_2(x_2)=a_2x_2^2+b_2x_2+c_2$, $f_3(x_2)=a_3x_2^2+b_3x_2+c_3$. Since $f(0,x_2)=f_3(x_2)$ is SAC, $f_3(x_2)$ must be quadratic, i.e. $a_3\neq 0$. $f_1(x_2)$ is never zero by Theorem 11.

Case 1 $f_1(x_2)=c_1\neq 0$ $(a_1=0)$:
$f(x_1,x_2)=c_1x_1^2+x_1(a_2x_2^2)+a_3x_2^2+O(x_1,x_2)$. If $a_2\neq 0$, $f(-a_2^{-1}a_3,x_2)$ is not quadratic for x_2, hence, not SAC, a contradiction. So, $a_2=0$, $f(x_1,x_2)=c_1x_1^2+a_3x_2^2+O(x_1,x_2)$ which belongs to 1).

Case 2 $(a_1\neq 0)$ $f_1(x_2)=a_1x_2^2+b_1x_2+c_1=a_1[(x_2+b')^2-r_1]$, $(\frac{r_1}{p})=-1$:
$f(x_1,x_2)=x_1^2(a_1x_2^2+b_1x_2+c_1)+x_1(a_2x_2^2)+a_3x_2^2+O(x_1,x_2)$
$=a_1x_1^2[(x_2+b')^2-r_1]+a_2x_1[(x_2+b')^2-r_1]+a_3[(x_2+b')^2-r_1]+O(x_1,x_2)$
$=(a_1x_1^2+a_2x_1+a_3)[(x_2+b')^2-r_1]+O(x_1,x_2)$.
Because $f(x_1,x_2)=(a_1x_1^2+a_2x_1+a_3)x_2^2+(b_1x_1^2+b_2x_1+b_3)x_2+(c_1x_1^2+c_2x_1+c_3)$, $a_1x_1^2+a_2x_1+a_3$ is the coefficient of x_2^2, hence, never zero. So, $f(x_1,x_2)$ belongs to 2). □

In fact, we have determined all the $SAC(n-1)$ functions for $n=1,2$. We will give some constructions for $n\geq 3$.

CONSTRUCTION 1 $(n\geq 3,\ p\geq 3)$
$I=\{1,2,...,n\}$, $I_i=\{i_1,i_2,...,i_{r_i}\}$, $i=1,2,...,t$. $I_i\cap I_j=\phi$ if $i\neq j$,

$I_1 \cup I_2 \cup ... \cup I_t = I$. Let $f(x_1, ..., x_n) = a \prod_{i=1}^{t} (l_i^2 - \alpha_i)$, where α_i are nonsquares, i.e. $(\frac{\alpha_i}{p}) = -1$, $a \in GF(p)^*$, $l_i = a_{i1}x_{i_1} + a_{i2}x_{i_2} + ... + a_{ir_i}x_{i_{r_i}} + b_i$, $a_{ij} \in GF(p)^*$, $j = 1, 2, ...r_i$, $i = 1, 2, ...t$, then f is obviously $SAC(n-1)$.

In general, we have

Theorem 13. *Let $I=\{1, 2, ..., n\}=I_1 \cup I_2$, $I_1 \cap I_2 = \phi$, $I_2 = J_1 \cup ... \cup J_s$, $J_i \cap J_j = \phi$ if $i \neq j$. Let $J_k = \{k_1, ..., k_{r_k}\}$, $k = 1, 2, ..., s$, using CONSTRUCTION 1 to construct f_k on $x_{k_1}, ..., x_{k_{r_k}}$, then*

$f(x_1, ..., x_n) = \sum_{i \in I_1} a_i x_i^2 + \sum_{j=1}^{s} f_j + O(x_1, ..., x_n)$ is $SAC(n-1)$.

CONSTRUCTION 2 $(n \geq 3,\ p \geq 3)$

Step 1: Choose any $b_1, b_2, ..., b_n, c_0, d_0$ from $GF(p)$.

Step 2: Choose any nonsquare r_1, r_2.

Step 3: If $b_i = 0$, choose any $\bar{b}_i$ from $GF(p)^*$, if $b_i \neq 0$, let $\bar{b}_i = 0$.

Step 4: Choose a_i such that

$$a_i \neq \begin{cases} -b_i^2(k^2 - r_2) & \text{if } b_i \neq 0 \\ -\bar{b}_i^2(k^2 - r_1) & \text{if } b_i = 0. \end{cases}$$

for $k = 0, 1, ..., \frac{p-1}{2}$, $i = 1, 2, ..., n$.

Step 5: Let $f(x_1, ..., x_n)$

$=a_1x_1^2 + ... + a_nx_n^2 + [(b_1x_1 + ... + b_nx_n + c_0)^2 - r_1][(\bar{b}_1x_1 + ...\bar{b}_nx_n + d_0)^2 - r_2]$.

f is obviously $SAC(n-1)$.

Generally, we have

Theorem 14. *Let $I = \{1, 2, ..., n\} = I_1 \cup I_2 \cup ... \cup I_s$, $I_i \cap I_j = \phi$ if $i \neq j$, $|I_j| = t_j$, $\sum_{j=1}^{s} t_j = n$, $I_j = \{j_1, j_2, ...j_{t_j}\}$, $j = 1, 2, ...s$. Using CONSTRUCTION 2 to construct f_j on $x_{j_1}, x_{j_2}, ..., x_{j_{t_j}}$, then*

$f(x_1, ..., x_n) = \sum_{j=1}^{s} f_j + O(x_1, ..., x_n)$ is $SAC(n-1)$.

Let A_1 be the set of all the functions of Theorem 13. Let A_2 be the set of all the functions of Theorem 14. We have

Theorem 15. $A_1 \subsetneqq A_2 \subsetneqq A_1$

Proof. It's not hard to prove that if there exist i with $a_i \neq 0$, then the functions of A_2 don't belong to A_1. On the other hand, $f(x_1, ..., x_n) = (x_1^2 - r_1)...(x_n^2 - r_n) \in A_1$, where the r_i are nonsquares for $i = 1, 2, ..., n$. For any function from A_2, its algebraic degree is at most $max(4, n)$. Hence, f doesn't belong to A_2 since its algebraic degree is $2n$. $\square$

Theorem 16. *The maximal algebraic degree of $SAC(n-1)$ functions is $2n$.*

Proof.

$$f(x_1, x_2, ..., x_n) = \sum_{k_1=0}^{p-1} \sum_{k_2=0}^{p-1} ... \sum_{k_n=0}^{p-1} a_{k_1 k_2 ... k_n} {x_1}^{k_1} {x_2}^{k_2} ... {x_n}^{k_n},$$

we know $k_j \leq 2$ for each j by theorem 11, hence $deg(f) \leq 2n$. On the other hand, $(x_1^2 - r_1)...(x_n^2 - r_n)$ has degree $2n$, where $(\frac{r_i}{p}) = -1$. $\square$

7. Some Open Questions

We have the following open questions:

Q1: Do CONSTRUCTION 1 and 2 give all the $SAC(n-1)$ functions?

Q2: Does $f = a\prod_{i=1}^{n}[(a_i x_i + b_i)^2 - r_i] + O(x_1, ..., x_n)$ give all the $SAC(n-1)$ functions with degree $2n$?

Q3: Are there any $SAC(k)$ $(0 \leq k \leq n-2)$ functions such that the degrees for some x_i are more than 2?

This paper was finished on Mar,2004.

References

[1] Luke O'Connor " An Upper Bound on the Number of Functions Satisfying the Strict Avalanche Criterion", *Information Processing Letters* 52 (1994), pp. 325-327.

[2] T.W.Cusick, "Boolean Functions Satisfying a Higher Order Strict Avalanche Criterion", *Advances in Cryptology,Eurocrypt'93*, pp. 102-117.

[3] T.W. Cusick, Pantelimon Stănică " Bounds on the Number of Functions Satisfying the Strict Avalanche Criterion", *Information Processing Letters* 60 (1996), pp. 215-219.

[4] T.W.Cusick and Yuan Li "k-th Order Symmetric SAC Boolean Functions and Bisecting Binomial Coefficients", *Discrete Applied Mathematics* 149 (2005), pp. 73-86.

[5] Forré. R, "The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition", *Advances in Cryptology, Crypto'88*, pp. 450-468.

[6] David Gluck, " A Note On Permutation Polynomials And Finite Geometries", *Discrete Mathematics* (8) pp. 97-100 1990.

[7] Habong Chung and P.V.Kumar, " A New General Construction for Generalized Bent Functions", *IEEE Transactions on Information Theory* Vol. 35, No. 1,January 1989. pp. 206-209.

[8] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng "Improving the Strict Avalanche Characteristics of Cryptographic Functions", *Information Processing Letters* 50 (1994), pp. 37-41.

[9] S.Lloyd, "Counting Binary Functions with Certain Cryptographic Properties". *Journal of Cryptology*, 5: pp. 107-131, 1992.

[10] Yutaka Hiramine, " A Conjecture On Affine Planes of Prime Order", *J. Combinatorial Theory (A)*, 52, pp. 44-50, 1989.

[11] Keqin Feng And Fengmei Liu, "New Results On The Nonexistence of Generalized Bent Functions", *IEEE Transactions on Information Theory* Vol. 49, No. 11, November 2003, pp. 3066-3071.

[12] P.V.Kumar, R.A.Scholtz, and L. R. Welch, "Generalized Bent Functions and Their Properties", *J. Combinatorial Theory (A)*, Vol. 40, pp. 90-107, 1985.

[13] R.Lidl and H.Niederreiter, "Finite Fields"(Encyclopedia of Mathematics and Its Applications, vol. 20). Reading, MA: Addison-Wesley, 1984

[14] Mulan Liu, Peizhong Lu and Gary L. Mullen, "Correlation-Immune Functions over Finite Fields", *IEEE Transactions on Information Theory* vol 44, No 3, May 1998, pp. 1273-1276.

[15] L.Ronyiai and T.Szonyi, "Planar Functions Over Finite Fields", *Combinatorica* 9(3) (1989), pp. 315-320.

[16] A.F.Webster and S.E.Tavares, "On the Design of S-Boxes", *Advances in Cryptology, Crypto'85*, Lect. Notes. Comp. Sci:218, Springer Verlag, 1986, pp. 523-534.

[17] A.M. Youssef, S.E. Tavares " Comment on "Bounds on the Number of Functions Satisfying the Strict Avalanche Criterion"", *Information Processing Letters* 60 (1996), pp. 271-275.

[18] Yuan Li and T. W. Cusick, " Linear Structures of Symmetric Functions over Finite Fields", *Information Processing Letters*, accepted.

[19] Yupu Hu and Guozhen Xiao "Resilient Functions Over Finite Fields", *IEEE Transactions on Information Theory* Vol 49, No. 8, August 2003, pp. 2040-2046

SUNY Department of Mathematics, 244 Mathematics Building, Buffalo, NY 14260

E-mail address: email:yuanli@buffalo.edu, cusick@buffalo.edu