Additive Autocorrelation of Resilient Boolean Functions

Guang Gong [1] and Khoongming Khoo [2]

[1] Department of Electrical and Computer Engineering, [2] Department of Combinatorics and Optimization,
University of Waterloo, Waterloo, Ontario N2L 3G1, Canada.
[1] ggong@calliope.uwaterloo.ca, [2] kkhoo@math.uwaterloo.ca

Abstract. In this paper, we introduce a new notion called the *dual function* for studying Boolean functions. First, we discuss general properties of the dual function that are related to resiliency and additive autocorrelation. Second, we look at preferred functions which are Boolean functions with the lowest 3-valued spectrum. We prove that if a balanced preferred function has a dual function which is also preferred, then it is resilient, has high nonlinearity and optimal additive autocorrelation. We demonstrate four such constructions of optimal Boolean functions using the Kasami, Dillon-Dobbertin, Segre hyperoval and Welch-Gong Transformation functions. Third, we compute the additive autocorrelation of some known resilient preferred functions in the literature by using the dual function. We conclude that our construction yields highly nonlinear resilient functions with better additive autocorrelation than the Maiorana-McFarland functions. We also analysed the saturated functions, which are resilient functions with optimized algebraic degree and nonlinearity. We show that their additive autocorrelation have high peak values, and they become linear when we fix very few bits. These potential weaknesses have to be considered before we deploy them in applications.

1 Introduction

Resiliency and high nonlinearity are two of the most important prerequisites of Boolean functions when used as combiners in stream cipher systems. Resiliency ensures the cipher is not prone to correlation attack [22] while high nonlinearity offers protection against linear approximation attack [16]. Another criteria, studied in many recent papers, is low additive autocorrelation [23–26]. This ensures that the output of the function is complemented with a probability close to 1/2 when any number of input bits are complemented. As a result, the cipher is not prone to differential-like cryptanalysis [1]. This is a more practical condition than the propagation criteria of order k which, in the case of high nonlinearity, may cause linear structures to occur (as pointed out in [24]).

In this paper, we study the autocorrelation and resiliency properties of Boolean functions with 3-valued spectrum. This is an important class of functions with many applications in cryptography, for example see [2, 4, 5, 20, 27]. We give several new constructions of resilient Boolean functions with high nonlinearity and optimally low additive autocorrelation. Then we show that our construction yields functions with better additive autocorrelation than known highly nonlinear resilient functions. Our findings are summarized in the following paragraphs.

First, we introduce a new notion called the *dual function*, which is defined as the characteristic function of the Hadamard transform. This notion turns out to be a very useful tool for studying functions with 3-valued spectrum. For such functions, we show that propagation criteria of order k and correlation immunity of order k are dual concepts. From this, we deduce that a function with 3-valued spectrum is correlation immune of order 1 if and only if its dual function is not affine.

Second, we look at preferred functions which have the lowest 3-valued spectrum $0, \pm 2^{(n+1)/2}$. We prove that, if a balanced preferred function $f(x)$ has a dual function that is non-affine or preferred, then $f(x)$ has several optimal cryptographic properties like 1-resiliency, high nonlinearity and optimal additive autocorrelation. We present some functions used in the construction of certain Hadamard difference sets, which achieve these properties. They include the Kasami functions, the Dillon-Dobbertin functions, the Segre hyperoval functions and the Welch-Gong Transformation functions [7–9, 11]. Moreover, some of these functions have high algebraic degree (for algebraic complexity) and large linear span (which offers protection against an interpolation attack [13]).

Third, we compute the additive autocorrelation of some known resilient functions with high nonlinearity. We show that our constructed functions have better additive autocorrelation than resilient preferred functions based on the Maiorana-McFarland construction [3]. We also investigate an important class of functions with 3-valued spectrum: the saturated functions constructed in [20] (which are resilient functions optimizing Siegenthaler and Sarkar-Maitra inequality). We compute a lower bound for the additive autocorrelation which improves on a bound given in [23]. We show that they have very high additive autocorrelation close to 2^n. Moreover an n-bit saturated function becomes linear when we fix just very few bits ($\log_2(n)$ or less bits). Thus, although a saturated function satisfies some very strong cryptographic properties, it may lead to a rigid structure which causes other weaknesses to occur.

2 Definitions and Preliminaries

The trace function $Tr : GF(2^n) \rightarrow GF(2)$ is defined as $Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$. It is a linear function and is basic to the representation of polynomial functions $f : GF(2^n) \rightarrow GF(2)$.

The *Hadamard Transform* of a polynomial function $f : GF(2^n) \rightarrow GF(2)$ is defined by $\hat{f}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{Tr(\lambda x) + f(x)}$.

There is a natural correspondence between polynomial functions $f : GF(2^n) \rightarrow GF(2)$ and Boolean functions $g : GF(2)^n \rightarrow GF(2)$. Let $\{\alpha_0, \ldots, \alpha_{n-1}\}$ be a basis of $GF(2^n)$ and $g(\underline{x})$ be the Boolean function representation of $f(x)$, then this correspondence is given by

$$g(x_0, \ldots, x_{n-1}) = f(x_0\alpha_0 + \cdots + x_{n-1}\alpha_{n-1}).$$

The *Hadamard Transform* of a Boolean function $f : GF(2)^n \rightarrow GF(2)$ is $\hat{f}(w) = \sum_{x \in GF(2)^n} (-1)^{w \cdot x + f(x)}$. This is equivalent to the definition for the corresponding polynomial function over $GF(2^n)$ [17].

We say the function $f : GF(2)^n \rightarrow GF(2)$ has 3-*valued spectrum* if its Hadamard Transform $\hat{f}(\lambda)$ only takes on the values $0, \pm 2^i$.

Definition 1. *Let n be odd and $f : GF(2)^n \rightarrow GF(2)$. If $\hat{f}(w)$ only takes on the values $0, \pm 2^{(n+1)/2}$, then we say f is* preferred.

Remark 1. It is desirable for a Boolean function to have low Hadamard transform. We deduce from Parseval's equation: $\sum_w \hat{f}(w)^2 = 2^{2n}$ that a preferred function has the lowest Hadamard transform among functions with 3-valued spectrum. That is the reason they are called preferred functions in [12].

The *nonlinearity* of a function $f : GF(2)^n \rightarrow GF(2)$ is defined as $N_f = min_{\{a \text{ affine function}\}} |\{x | f(x) \neq a(x)\}|$. A high nonlinearity is desirable as it offers protection against linear approximation based attacks [16, 22].

A Boolean function $f : GF(2)^n \rightarrow GF(2)$ is *kth order correlation immune*, denoted $CI(k)$, if $\hat{f}(w) = 0$ for all $1 \leq wt(w) \leq k$ where $wt(w)$ is the number of ones in the binary representation of w. Correlation immunity offers protection against correlation attack [22]. Furthermore, if f is balanced and $CI(k)$, we say f is resilient of order k.

The *additive autocorrelation at a* is defined as $\Delta_f(a) = \sum_x (-1)^{f(x)+f(x+a)}$. We say f satisfies the *propagation criteria of order k*, denoted $PC(k)$, if $\Delta_f(a) = 0$ for all $1 \leq wt(a) \leq k$. If $\Delta_f(a) = \pm 2^n$, then a is called a *linear structure* of f which is undesirable.

Definition 2. *The* additive autocorrelation *of f is $\Delta_f := max_{a \neq 0} |\Delta_f(a)|$.*

Remark 2. This value is also called the *maximum indicator* in [24]. For a balanced function f, we want Δ_f to be low so that any change in the input bits will complement the output with probability close to $1/2$. It was conjectured by Zhang and Zheng in [24, Conjecture 1] that $\Delta_f \geq 2^{(n+1)/2}$ for a balanced function $f : GF(2)^n \rightarrow GF(2)$. Although this conjecture was later disproved by Clark et. al. when n is even (see [6, Table 3]), it still holds when n is odd. Thus, we make the following definition.

Definition 3. *Let n be odd and $f : GF(2)^n \rightarrow GF(2)$ be balanced. f has* optimal additive autocorrelation *if $\Delta_f = 2^{(n+1)/2}$.*

The *linear span*, denoted $LS(f)$, of a polynomial function $f(x) = \sum_i \beta_i x^{s_i}$, $\beta_i \in GF(2^n)$, is the number of monomials x^{s_i} in its polynomial representation. We want it to be high to defend against interpolation attacks [13]. The *algebraic degree*, denoted $deg(f)$, of the corresponding Boolean function is given by the maximum weight of the exponents $\max_i wt(s_i)$ (see [17]). We want it to be high so that algebraic analysis is complex.

3 Cryptographic Properties of the Dual Function

Definition 4. *Let $f : GF(2)^n \to GF(2)$. Its* dual function *σ_f is defined as*

$$\sigma_f(w) = \begin{cases} 0 & \textit{if } \hat{f}(w) = 0 \\ 1 & \textit{if } \hat{f}(w) \neq 0. \end{cases}$$

Remark 3. From Parseval's equation: $\sum_w \hat{f}(w)^2 = 2^{2n}$, we see that $\sigma_f(w)$ has weight $2^{2(n-i)}$ if f has 3-valued spectrum $0, \pm 2^i$.

Next, we show that the Hadamard transform of the dual function is proportional to the additive autocorrelation of a function with 3-valued spectrum. It can be applied to derive several useful results in the next few subsections.

Lemma 1. *If $f : GF(2)^n \to GF(2)$ is a Boolean function with 3-valued spectrum $0, \pm 2^i$, then for all $a \neq 0$*

$$\Delta_f(a) = -2^{2i-(n+1)}\widehat{\sigma_f}(a).$$

Proof. We make use of the well known Wiener-Khintchine theorem (e.g. see [2, Lemma 1]): $\hat{f}(w)^2 = \sum_a \Delta_f(a)(-1)^{a \cdot w}$. By applying inverse Hadamard transform[1], we have the equivalent formula:

$$\Delta_f(a) = 1/2^n \sum_w \hat{f}(w)^2(-1)^{a \cdot w}. \tag{1}$$

By definition, $\hat{f}(w)^2 = 2^{2i}\sigma_f(w)$. Substituting this in equation (1), we get

$$\Delta_f(a) = 2^{2i-n} \sum_w \sigma_f(w)(-1)^{a \cdot w}.$$

By noting that $2\sigma_f(w) = 1 - (-1)^{\sigma_f(w)}$, we get

$$\Delta_f(a) = 2^{2i-(n+1)} \left(\sum_w (-1)^{a \cdot w} - \sum_w (-1)^{\sigma_f(w) + a \cdot w} \right).$$

This is $-2^{2i-(n+1)}\widehat{\sigma_f}(a)$ when $a \neq 0$ and 2^n when $a = 0$. □

3.1 Correlation Immunity and Non-Affine Dual Function

In this section, we derive several useful results on correlation immunity from Lemma 1.

Proposition 1. *Let $f : GF(2)^n \to GF(2)$ be a Boolean function with 3-valued spectrum $0, \pm 2^i$. Then f is $PC(k)$ if and only if σ_f is $CI(k)$.*

[1] The inverse Hadamard transform is the formula: $F(w) = \sum_x f(x)(-1)^{w \cdot x} \Longrightarrow f(x) = 1/2^n \sum_w F(w)(-1)^{w \cdot x}$

Proof. f is $PC(k) \iff \Delta_f(a) = 0$ for $1 \leq wt(a) \leq k \iff \widehat{\sigma_f}(a) = 0$ for $1 \leq wt(a) \leq k$ (by Lemma 1) $\iff \sigma_f$ is $CI(k)$. □

We need the following result from [2] for proving correlation immunity of Boolean functions.

Proposition 2. *(Canteaut, Carlet, Charpin and Fontaine [2, Theorem 7]) Let $f : GF(2^n) \to GF(2)$ be a polynomial function with 3-valued spectrum $0, \pm 2^i$. Then there exists a basis of $GF(2^n)$ such that the Boolean representation of f is $CI(1)$ if and only if f is not $PC(n-1)$ under any basis representation.*

Remark 4. We stated Proposition 2 in a modified form (from the original in [2]) so that it applies to polynomial functions. From the proof of Proposition 2, we see that the set $\{\lambda | \hat{f}(\lambda) = 0\}$ contains n linearly independent vectors. Based on these n vectors, Gong and Youssef gave an algorithm to find a basis of $GF(2^n)$ such that the Boolean form of f is 1-resilient in [11]. Proposition 2 was proven in another form by Zheng and Zhang [27, Theorem 2]. A related result concerning resilient preferred functions can be found in [15, Section 3].

Theorem 1 is a corollary of Proposition 1 and 2. Some applications can be found in Section 4.

Theorem 1. *Let $f : GF(2^n) \to GF(2)$ be a polynomial function with 3-valued spectrum $0, \pm 2^i$. Then there exists a basis of $GF(2^n)$ such that the Boolean representation of $f(x)$ is $CI(1)$ if and only if σ_f is not affine.*

Proof. f is $CI(1)$ in some basis $\iff f$ is not $PC(n-1)$ in any basis (by Proposition 2) $\iff \sigma_f$ is not $CI(n-1)$ in any basis (by Proposition 1) $\iff \sigma_f$ is not affine. □

3.2 Computing Additive Autocorrelation from the Dual Function

In this section, we derive formulas to compute the additive autocorrelation of functions with 3-valued spectrum.

Proposition 3. *Let $f : GF(2)^n \to GF(2)$ has 3-valued spectrum $0, \pm 2^i$. Then $\Delta_f \leq 2^{2i-1} - 2^{2i-n} N_{\sigma_f}$. Thus N_{σ_f} is high $\Longrightarrow \Delta_f$ is low.*

Proof. By Lemma 1, we have $\widehat{\sigma_f}(a) = -2^{n+1-2i} \Delta_f(a)$ for $a \neq 0$. By substituting this in the formula $N_{\sigma_f} = 2^{n-1} - 1/2 \max_a |\widehat{\sigma_f}(a)|$, we see that Δ_f is

$$\max_{a \neq 0} |\Delta_f(a)| = 2^{2i-(n+1)} \max_{a \neq 0} |\widehat{\sigma_f}(a)| \leq 2^{2i-(n+1)} \max_{a} |\widehat{\sigma_f}(a)| = 2^{2i-1} - 2^{2i-n} N_{\sigma_f}.$$

□

Low additive autocorrelation, i.e. toggling any number of input bits will result in the output being complemented with probability close to 1/2, is a useful generalization of the propagation criteria of order k. The next theorem shows when low additive autocorrelation can be achieved. Some applications can be found in Section 4.

Theorem 2. *If $f : GF(2)^n \rightarrow GF(2)$ is a balanced preferred function and σ_f is preferred, then $\Delta_f = 2^{(n+1)/2}$ and $\Delta_f(a) = 0$ for $2^{n-1} - 1$ a's. That is, f has optimal additive autocorrelation.*

Proof. By Lemma 1, $\widehat{\sigma_f}(a) = -\Delta_f(a)$ for $a \neq 0$ when f is preferred. σ_f is preferred means $\widehat{\sigma_f}(a) = 0, \pm 2^{(n+1)/2}$ which implies $\Delta_f(a) = 0, \pm 2^{(n+1)/2}$ for all $a \neq 0$. Thus, $\Delta_f = 2^{(n+1)/2}$.

Let v be the number of elements a such that $\widehat{\sigma_f}(a) = 0$. By Parseval's equation and the fact that σ_f is preferred, we have

$$\sum_a \widehat{\sigma_f}(a)^2 = 2^{2n} \Longrightarrow (2^n - v)2^{n+1} = 2^{2n} \Longrightarrow v = 2^{n-1}.$$

From remark 3, $\widehat{\sigma_f}(0) = 0$ because σ_f is balanced (note that $\Delta_f(0) = 2^n$). Therefore $\widehat{\sigma_f}(a) = 0$ for $2^{n-1} - 1$ non-zero a's. By Lemma 1, $\Delta_f(a) = 0$ for $2^{n-1} - 1$ elements a's. □

3.3 Nonlinearity and Algebraic Degree

Proposition 4 follows easily from the following relation:

$$N_f = 2^{n-1} - 1/2 \max_w |\hat{f}(w)|. \tag{2}$$

Proposition 4. *A function $f : GF(2)^n \rightarrow GF(2)$ with 3-valued spectrum $0, \pm 2^i$ have nonlinearity $2^{n-1} - 2^{i-1}$. By remark 1, a preferred function has the highest nonlinearity $2^{n-1} - 2^{(n-1)/2}$ among functions with 3-valued spectrum.*

Remark 5. In Section 4 and 5.1, we will concentrate on resilient preferred functions. Their nonlinearity $2^{n-1} - 2^{(n-1)/2}$ is considered high among resilient functions according to Carlet [3]. Sarkar and Maitra constructed resilient functions with nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ [19, Theorem 6]. But their construction only works when $n \geq 41$ for 1-resilient functions and $n \geq 55$ for 2-resilient functions.

From [27], if $f : GF(2)^n \rightarrow GF(2)$ satisfies $\hat{f}(\lambda) \equiv 0 \pmod{2^i}$ for all λ, then $deg(f) \leq n - i + 1$. The following proposition follows easily.

Proposition 5. *A function with 3-valued spectrum $0, \pm 2^i$ satisfies $deg(f) \leq n - i + 1$. By remark 1, the preferred functions have maximal bound for algebraic degree: $deg(f) \leq (n+1)/2$ among functions with 3-valued spectrum.*

4 Construction of Resilient Highly Nonlinear Boolean Functions with Optimal Additive Autocorrelation

Our main result in this section is to construct four classes of Boolean functions with desirable cryptographic properties, from functions used in the construction of Hadamard difference sets. This is achieved by applying Theorem 3 and 4, which are corollaries of Theorem 1, Theorem 2 and Proposition 4.

Theorem 3. *If $f : GF(2^n) \to GF(2)$ is a balanced preferred function such that its dual σ_f is non-affine, then*

1. *f is resilient of order 1 for some basis conversion.*
2. *f has high nonlinearity $2^{n-1} - 2^{(n-1)/2}$.*

Theorem 4. *If $f : GF(2^n) \to GF(2)$ is a balanced preferred function such that its dual σ_f is preferred, then*

1. *f is resilient of order 1 for some basis conversion.*
2. *f has high nonlinearity $2^{n-1} - 2^{(n-1)/2}$.*
3. *f has optimal additive autocorrelation, i.e. $\Delta_f = 2^{(n+1)/2}$ and $\Delta_f(a) = 0$ for $2^{n-1} - 1$ a's.*

Our first construction is based on a class of Kasami functions whose Hadamard transform distribution is found by Dillon.

Lemma 2. *(Kasami-Dillon [7, 14]) Let n be odd, $\gcd(n, 3) = 1$ and $f : GF(2^n) \to GF(2)$ be defined by $f(x) = Tr(x^d)$ where $d = 2^{2k} - 2^k + 1$, $3k \equiv 1 \pmod{n}$. Then f is preferred and satisfies*

$$\hat{f}(\lambda) = \begin{cases} 0 & \text{if } Tr(\lambda^{2^k+1}) = 0 \\ \pm 2^{(n+1)/2} & \text{if } Tr(\lambda^{2^k+1}) = 1. \end{cases}$$

Theorem 5. *The Kasami function $f(x)$ in Lemma 2 is 1-resilient, $N_f = 2^{n-1} - 2^{(n-1)/2}$ and $\Delta_f = 2^{(n+1)/2}$. Moreover, the algebraic degree is $deg(f) = \lceil n/3 \rceil + 1$.*

Proof. By Lemma 2, f is balanced because $\hat{f}(0) = 0$. Also by Lemma 2, $\sigma_f(x) = Tr(x^{2^k+1})$ which is preferred by [10]. Therefore, we can apply Theorem 4 because f is balanced and both functions f, σ_f are preferred.

For any k, the degree of f is $wt(2^{2k} - 2^k + 1) = k + 1$ for $1 \leq k \leq (n-1)/2$ and $wt(2^{2k} - 2^k + 1) = (n - k) + 1$ when $(n-1)/2 \leq k \leq n - 1$ [14]. When $3k \equiv 1 \pmod{n}$, $k \equiv \pm \lceil n/3 \rceil \pmod{n}$. Therefore $deg(f) = \lceil n/3 \rceil + 1$ in this case. □

Our next construction is based on a class of functions from the construction of cyclic Hadamard difference sets by Dillon and Dobbertin [8].

Lemma 3. *(Dillon-Dobbertin [8]) Let n be odd. Define $f : GF(2^n) \to GF(2)$ by*

$$f(x) = \begin{cases} 0 & \text{if } x^{2^k+1} \in Im(\Delta_k) \\ 1 & \text{if } x^{2^k+1} \notin Im(\Delta_k). \end{cases}$$

where $\Delta_k(x) = (x+1)^d + x^d + 1$, $d = 2^{2k} - 2^k + 1$ and $\gcd(k, n) = 1$. Then $f(x)$ is preferred and satisfies

$$\hat{f}(\lambda) = \begin{cases} 0 & \text{if } Tr(\lambda^{\frac{2^k+1}{3}}) = 0 \\ \pm 2^{(n+1)/2} & \text{if } Tr(\lambda^{\frac{2^k+1}{3}}) = 1. \end{cases}$$

Theorem 6. *Let $f(x)$ be the Dillon-Dobbertin function in Lemma 3*

1. *$f(x)$ is 1-resilient and $N_f = 2^{n-1} - 2^{(n-1)/2}$.*
2. *Furthermore, if $k = 3$ or $3k \equiv 1 \pmod{n}$, then $f(x)$ is 1-resilient, $N_f = 2^{n-1} - 2^{(n-1)/2}$ and $\Delta_f = 2^{(n+1)/2}$.*
3. *If $3k \equiv 1 \pmod{n}$, then $LS(f) = 5n$ where*

$$f(x) = Tr(x^3 + x^{2^k+1} + x^{2^{2k+1}+1} + x^{2^{2k}+2^{k+1}+1} + x^{2^{2k+1}+2^{k+1}+3}). \qquad (3)$$

The algebraic degree satisfies $deg(f) = 4$ for $n \neq 5$. $deg(f) = 3$ for $n = 5$.

Proof. 1. By Lemma 3, f is balanced because $\hat{f}(0) = 0$. Also by Lemma 3, f is preferred and the dual function is $\sigma_f(x) = Tr(x^{(2^k+1)/3})$ which is not affine. Therefore, we can apply Theorem 3.

2. If $k = 3$, then $(2^k + 1)/3 = 3$ and $\sigma_f(x) = Tr(x^3)$ which is preferred by [10]. If $3k \equiv 1 \pmod{n}$, then $2^{3k} + 1 \equiv 2 + 1 \equiv 3 \pmod{2^n - 1}$. Therefore

$$(2^k + 1)/3 \equiv (2^k + 1)/(2^{3k} + 1) \equiv 1/(2^{2k} - 2^k + 1) \equiv d^{-1} \pmod{2^n - 1}.$$

where $d = 2^{2k} - 2^k + 1$. Therefore the dual function is $\sigma_f(x) = Tr(x^{d^{-1}})$ which is preferred by the following argument:
We define $g(x) := Tr(x^d)$ which is preferred from [14]. This implies $\sigma_f(x)$ is preferred from the following computation.

$$\widehat{\sigma_f}(\lambda) = \sum_x (-1)^{Tr(x^{d^{-1}})+Tr(\lambda x)} = \sum_y (-1)^{Tr(\lambda^{-d^{-1}} y)+Tr(y^d)} = \hat{g}(\lambda^{-d^{-1}}).$$

where we let $x = \lambda^{-1} y^d$. Therefore, we can apply Theorem 4 because f is balanced and both functions f, σ_f are preferred.

3. $f(x)$ is a 2^k+1-decimation of the characteristic function $b_k(x)$ of the Hadamard difference set B_k in [8, 9], i.e. $f(x) = b_k(x^{2^k+1})$. When $3k \equiv 1 \pmod{n}$, the trace representation of $b_k(x)$ in [8, 9] is

$$b_k(x) = Tr(x^{2^{2k}+2^k+1} + x^{2^{2k}+2^k-1} + x^{2^{2k}-2^k+1} + x^{2^k+1} + x).$$

The exponents of $f(x)$ in Equation 3 are obtained by multiplying all the exponents of $b_k(x)$ by $2^k + 1$, and noting that $3k \equiv 1 \pmod{n}$ implies $2^{3k} \equiv 2$ modulo $2^n - 1$. When we expand the 5 trace terms of $f(x)$, we get $5n$ monomials, i.e. $LS(f) = 5n$.
The maximum weight of the exponents of $f(x)$ in Equation 3 is 4 which comes from the exponent $2^{2k+1} + 2^{k+1} + 3$ for $n > 5$. Thus, $deg(f) = 4$. For $n = 5$, we can verify $deg(f) = 3$.

□

Our final construction is based on the hyperoval functions in [7].

Lemma 4. *(Hyperoval [7]) Let n be odd. Define $f : GF(2^n) \rightarrow GF(2)$ by*

$$f(x) = \begin{cases} 0 \ \textit{if } x \in Im(D_k) \\ 1 \ \textit{if } x \notin Im(D_k) \end{cases}$$

where $D_k(x) = x + x^k$ is a 2-to-1 map on $GF(2^n)$. Then $f(x)$ satisfies $\hat{f}(\lambda) = \hat{g}(\lambda^{\frac{k-1}{k}})$ where $g(x) = Tr(x^k)$.

The known values of k for which $x + x^k$ is a 2-to-1 map are $k = 2$ (Singer), $k = 6$ (Segre) and two cases due to Glynn. We will consider the Segre case $k = 6$.

Theorem 7. *Let $f(x)$ be the Segre hyperoval function for $k = 6$ in Lemma 4. Then $f(x)$ is 1-resilient and $N_f = 2^{n-1} - 2^{(n-1)/2}$.*

Proof. We see from Lemma 4 that when $k = 6$, f is balanced because $\hat{f}(0) = \hat{g}(0) = 0$ where $g(x) = Tr(x^6) = Tr(x^3)$. f is preferred because g is preferred [10] and $\hat{f}(\lambda) = \hat{g}(\lambda^{5/6})$ by Lemma 4. By the distribution of $\hat{g}$ from [10] and Lemma 4,

$$\hat{f}(\lambda) = \hat{g}(\mu) = \begin{cases} 0 & \text{if } Tr(\mu) = 0 \\ \pm 2^{(n+1)/2} & \text{if } Tr(\mu) = 1 \end{cases}$$

where $\mu = \lambda^{5/6}$. Therefore, $\sigma_f(x) = Tr(x^{5/6})$ which is not affine. Thus, we can apply Theorem 3 because f is a balanced preferred function and σ_f is not affine. □

The Welch-Gong Transformation functions also corresponds to optimal Boolean function with low additive autocorrelation in the following remark.

Remark 6. In [11], the Welch-Gong Transformation function was shown to have good cryptographic properties: 1-resiliency, high nonlinearity $2^{n-1} - 2^{(n-1)/2}$, high algebraic degree $deg(f) = \lceil n/3 \rceil + 1$ and large linear span $LS(f) = n(2^{\lceil n/3 \rceil} - 3)$. A description of the function can be found in [11, Section 2].

Here, we remark that the Welch-Gong function has the additional property of optimal additive autocorrelation. This is because the Welch-Gong Transformation function $f(x)$ is a balanced preferred function and its dual function is $\sigma_f(x) = Tr(x^{d^{-1}})$, $d = 2^{2k} - 2^k + 1$ where $3k \equiv 1 \pmod{n}$ [11, Lemma 2]. By the same reason as in Theorem 6 part (2), we can apply Theorem 4 because f is balanced and both f, σ_f are preferred.

We present Table 1 to summarize our results and example 1 to demonstrate our construction.

Example 1. Let $GF(2^7)^*$ be generated by the element α satisfying $\alpha^7 + \alpha + 1 = 0$. Define $f : GF(2^7) \rightarrow GF(2)$ by $f(x) = Tr_1^7(x^3 + x^5 + x^9 + x^{19} + x^{29})$, which is the Dillon-Dobbertin function of Theorem 6 with $3k \equiv 1 \mod 7$, i.e. $k = 5$ (we have reduced the exponents of f to their cyclotomic coset leaders). By

Table 1. Cryptographic Properties of Preferred Functions

Kasami* (Theorem 5)	Dillon-Dobbertin* (Theorem 6)	Segre hyperoval* (Theorem 7)	Welch-Gong* (Remark 6)
Balance	Balance	Balance	Balance
High Nonlinearity	High Nonlinearity	High Nonlinearity	High Nonlinearity
Resiliency	Resiliency	Resiliency	Resiliency
Optimal Additive Autocorrelation	Optimal Additive Autocorrelation	-	Optimal Additive Autocorrelation
For odd n, $3 \not| n$	For odd $n \geq 5$	For odd $n \geq 5$	For odd n, $3 \not| n$
$deg(f) = \lceil n/3 \rceil + 1$	$deg(f) = 3, 4$ when $k = 3^{-1}$	-	$deg(f) = \lceil n/3 \rceil + 1$ $LS(f) = n(2^{\lceil n/3 \rceil} - 3)$

***Remark:** All the functions listed in Table 1 satisfies 2-level (multiplicative) autocorrelation, i.e. $C_f(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(x)+f(\lambda x)} = 0$ for all $\lambda \neq 1$ [7–9], for applications in pseudorandom number generation and communication systems.

applying Algorithm 1 of [11] with the 7 linearly independent vectors $\{\alpha^i | i = 1, 2, 3, 4, 5, 6, 13\}$ satisfying $\hat{f}(\alpha^i) = 0$, a 1-resilient Boolean form of f is given by

$$\begin{aligned} g(x_6, x_5, x_4, x_3, x_2, x_1, x_0) &= x_6x_3x_1x_0 + x_5x_4x_1x_0 + x_5x_3x_2x_0 \\ &+ x_5x_3x_1x_0 + x_4x_3x_2x_1 + x_6x_5x_3 + x_6x_5x_0 + x_6x_4x_0 + x_6x_2x_1 + x_5x_4x_2 \\ &+ x_5x_3x_2 + x_5x_1x_0 + x_4x_3x_1 + x_4x_2x_1 + x_4x_1x_0 + x_3x_2x_0 + x_3x_1x_0 \\ &+ x_2x_1x_0 + x_5x_4 + x_5x_3 + x_5x_2 + x_5x_0 + x_4x_3 + x_4x_2 + x_4x_0 + x_3x_1 \\ &+ x_3x_0 + x_2x_1 + x_2x_0 + x_1x_0 + x_6 + x_4 + x_2 + x_1 + x_0. \end{aligned}$$

g is a Boolean function with 7 input bits, is 1-resilient and has algebraic degree 4, which is highest among all preferred functions by Proposition 5. The nonlinearity is $2^6 - 2^3 = 56$ which is optimal among 7-bit Boolean functions, see [18]. The additve autocorrelation is optimal, given by $\Delta_f = 2^{(7+1)/2} = 16$.

5 Additive Autocorrelation of Known Resilient Functions with High Nonlinearity

5.1 Comparison with Known Resilient Preferred Functions

In the known literature, there were many constructions for resilient preferred functions. Some examples include [2, 3, 11, 21]. A common construction belong to the Maiorana-McFarland class, see [3] for a summary. We present in Proposition 6 a general construction for Maiorana-McFarland resilient preferred functions.

Proposition 6. *(Carlet [3, page 555]) Let n be odd and $f : GF(2)^n \to GF(2)$ be defined by*

$$f(x, y) = x \cdot \phi(y) + g(y), \;\; x \in GF(2)^{(n+1)/2}, y \in GF(2)^{(n-1)/2}. \qquad (4)$$

where g is any $(n-1)/2$-bit Boolean function, and $\phi : GF(2)^{\frac{n-1}{2}} \to GF(2)^{\frac{n+1}{2}}$ is an injection such that $wt(\phi(y)) \geq k+1$. Then f is a k-resilient function with nonlinearity $2^{n-1} - 2^{(n-1)/2}$.

The above construction is quite useful. When $n \equiv 1 \pmod 4$, we can construct $(n-1)/4$-resilient functions having nonlinearity $2^{n-1} - 2^{(n-1)/2}$ from it.

We will show that the function $f(x, y)$ in Proposition 6 is preferred, and deduce its dual function and additive autocorrelation in Theorem 8. We define the *characteristic function* $\chi_A(x)$ on a set A to be: $\chi_A(x) = 1$ if $x \in A$ and 0 otherwise. We also denote the image set of ϕ by $Im(\phi)$.

Theorem 8. *Let $f(x, y)$ be the function defined in Proposition 6. Then it is preferred with dual function $\sigma_f(x, y) = \chi_{Im(\phi)}(x)$. The additive autocorrelation of f satisfies $\Delta_f \geq 2^{(n-1)/2}\sqrt{2^{n+1}/(2^{(n+1)/2} - 1)}$ which is approximately $2^{3n/4} > 2^{(n+1)/2}$.*

Proof. From [3], the Hadamard transform of f is:

$$\begin{aligned}\hat{f}(a, b) &= \sum_{y}(-1)^{g(y)+b\cdot y}\sum_{x}(-1)^{x\cdot(a+\phi(y))} = 2^{(n+1)/2}\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)+b\cdot y} \\ &= \begin{cases} 0 \text{ , if } a \notin Im(\phi), \\ \pm 2^{(n+1)/2} \text{ , if } a \in Im(\phi), \end{cases}\end{aligned}$$

because ϕ is injective. Therefore, f is preferred and $\sigma_f(x, y) = \chi_{Im(\phi)}(x)$. To find the additive autocorrelation of f, we can compute $\widehat{\sigma_f}$:

$$\begin{aligned}\widehat{\sigma_f}(a, b) &= \sum_{x,y}(-1)^{\chi_{Im(\phi)}(x)+a\cdot x+b\cdot y} = \sum_{y}(-1)^{b\cdot y}\sum_{x}(-1)^{\chi_{Im(\phi)}(x)+a\cdot x} \\ &= \begin{cases} 0 \text{ , if } b \neq 0, \\ 2^{(n-1)/2}\widehat{\chi_{Im(\phi)}}(a) \text{ , if } b = 0. \end{cases}\end{aligned}$$

Note that $\widehat{\chi_{Im(\phi)}}(0) = 0$ because $\chi_{Im(\phi)}$ is balanced. Therefore, by Parseval's equation: $\sum_{a\neq 0}\widehat{\chi_{Im(\phi)}}(a)^2 = 2^{n+1}$ and Lemma 1: $\Delta_f = max_{(a,b)\neq(0,0)}|\widehat{\sigma_f}(a, b)|$,

$$\Delta_f = 2^{(n-1)/2}\max_{a\neq 0}|\widehat{\chi_{Im(\phi)}}(a)| \geq 2^{(n-1)/2}\sqrt{2^{n+1}/(2^{(n+1)/2} - 1)}.$$

This lower bound is approximately $2^{n/2} \times \sqrt{2^{n/2}} = 2^{3n/4}$. □

Remark 7. We note that for n odd, Canteaut et. al. [2, Corollary 3] constructed 1-resilient preferred functions that can achieve all algebraic degree between 2 and $(n + 1)/2$ by restricting a Maiorana-McFarland bent function to a hyperplane. The dual function and additive autocorrelation can be computed by a method similar to the proof of Theorem 8.

By Theorem 8, we see that the Maiorana-McFarland construction of resilient preferred functions have higher (worse) additive autocorrelation than our constructed functions from Table 1. Moreover, the Maiorana-McFarland function in equation (4) becomes linear when we fix $(n-1)/2$ input bits y. Our construction can avoid this possible weakness:

Example 2. The construction of Proposition 6 for a 7-bit 1-resilient preferred function with nonlinearity 56 is

$$f(x,y) = x \cdot \phi(y) + g(y), \;\; x \in GF(2)^4, y \in GF(2)^3.$$

where $\phi : GF(2)^3 \to GF(2)^4$ is an injection such that $wt(\phi(y)) \geq 2$.

f becomes linear when we fix three bits $y = (y_0, y_1, y_2)$. In comparison, our 1-resilient preferred function in example 1 is not linear when we fix any three bits. By Theorem 8, we deduce that $\Delta_f \geq \lceil 2^3 \times \sqrt{2^8/(2^4-1)} \rceil = 34$ while the additive autocorrelation of our function in example 1 is 16.

5.2 Potential Weaknesses of Saturated Functions

In this section, we investigate an important class of Boolean functions with 3-valued spectrum. They are the saturated functions introduced by Sarkar and Maitra [20]. If an n-bit Boolean function f have algebraic degree d, then the maximal order of resiliency it can achieve is $k := n - 1 - d$ by Siegenthaler's inequality [22]. If the order of resiliency is k, then the maximal nonlinearity it can achieve is $2^{n-1} - 2^{k+1}$ by Sarkar-Maitra inequality [20, Theorem 2]. When both these conditions are achieved, we say f is a *saturated function* and it necessarily have 3-valued spectrum $0, \pm 2^{k+2}$ [20]. Fix $d \geq 2$, Sarkar and Maitra constructed an infinite class of saturated functions having algebraic degree d in [20]. They denoted their class of functions by $SS(d-2)$.

Proposition 7. *([20, Theorem 5] Sarkar and Maitra) Construction for functions in $SS(d-2)$. Fix $d \geq 2$, let $n = r + s + t$ where $r = 2^{d-1} - 1$, $s = d - 1$ and $t \geq 0$. Define $f : GF(2)^n \to GF(2)$ by*

$$f(x,y,z) = x \cdot \phi(y) + g(y) + z_0 + \cdots + z_{t-1}, \;\; x \in GF(2)^r, y \in GF(2)^s, z \in GF(2)^t. \tag{5}$$

where $g : GF(2)^s \to GF(2)$ is any function and $\phi : GF(2)^s \to GF(2)^r$ is an injection such that $wt(\phi(y)) \geq r - 1$ for all $y \in GF(2)^s$. Then $deg(f) = d$, f is k-resilient having nonlinearity $2^{n-1} - 2^{k+1}$ where $k = n - 1 - d$. f necessarily has 3-valued spectrum $0, \pm 2^{k+2}$.

The Boolean functions in Proposition 7 achieve two very desirable properties, maximal resiliency and nonlinearity, for applications in stream cipher systems. However, we will see in Theorem 9 that they have certain weaknesses that have to be considered in applications.

A good lower bound for the additive autocorrelation of a general k-resilient function[2] is given by Tarannikov et. al. in [23, Theorem 4]. In Theorem 9, we give a better (sharper) bound for the function in Proposition 7.

Theorem 9. *Fix $d \geq 2$, let $f(x, y, z)$ be a function in $SS(d-2)$ as defined in Proposition 7.*

1. *When $t = 0$, $\Delta_f \geq (1 - \frac{2}{n})2^n$. This bound is sharper than a general bound obtained by [23, Theorem 4]. Thus Δ_f has an asymptotic linear structure: $\Delta_f / 2^n \to 1$ as $n \to \infty$.*
2. *When $t \geq 1$, $\Delta_f = 2^n$ and the function has linear structures at $(0, 0, a)$ for all $a \in GF(2)^t$.*

Furthermore, when we fix $log_2(n)$ or less input bits, f becomes linear.

Proof. 1. When $t = 0$, we do not have any z-terms in equation (5):

$$\begin{aligned}\Delta_f(a,b) &= \sum_{x,y}(-1)^{x\cdot\phi(y)+g(y)+(x+a)\cdot\phi(y+b)+g(y+b)} \\ &= \sum_{y}(-1)^{a\cdot\phi(y+b)+g(y)+g(y+b)}\sum_{x}(-1)^{x\cdot(\phi(y)+\phi(y+b))} \\ &= \begin{cases} 0 \text{ , if } b \neq 0, \\ 2^r\sum_y(-1)^{a\cdot\phi(y)} \text{ , if } b = 0. \end{cases}\end{aligned}$$

Note that $|\{x \in GF(2)^r | wt(x) \geq r-1\}| = r + 1 = 2^s = |Im(\phi)|$. Therefore we necessarily have $Im(\phi) = \{x \in GF(2)^r | wt(x) \geq r-1\}$ and $\{100\ldots0 \cdot \phi(y) | y \in GF(2)^s\} = \{0, 1, 1, \ldots, 1, 1\}$. This implies

$$|\Delta_f(100\ldots0, 000\ldots0)| = 2^r\left|\sum_y(-1)^{100\ldots0\cdot\phi(y)}\right| = 2^n - 2^{n-s+1}.$$

Therefore, $\Delta_f \geq 2^n - 2^{n-s+1} \geq 2^n - 2^{n-\log_2(n)+1} = (1-2/n)2^n$. The last inequality is true because $n = r+s = 2^s - 1 + s \Longrightarrow 2^s \leq n \Longrightarrow s \leq \log_2(n)$. By [23, Theorem 4], $\Delta_f \geq \left(\frac{2k-n+3}{n+1}\right)2^n = \left(1 - \frac{2(s+1)}{n+1}\right)2^n$ where $k = r-2$ is the order of resiliency of f. It is easy to see by elementary algebra that their lower bound $\left(1 - \frac{2(s+1)}{n+1}\right)2^n$ is not as sharp as our bound $\left(1 - \frac{2}{n}\right)2^n$.

2. When $t \geq 1$, $\Delta_f(0, 0, a) = 2^{s+r}\sum_z(-1)^{11\ldots1\cdot z+11\ldots1\cdot(z+a)} = \pm2^{s+r+t} = \pm2^n$.

It is easy to see that equation (5) becomes linear when we fix y which has $s \leq log_2(n)$ bits. □

Remark 8. We have used the direct approach for computing additive autocorrelation in Theorem 9 because it gives sharper bounds than by using dual functions.

[2] We note that such a lower bound was first given by Zheng and Zhang in [26, Theorem 2]. Later this bound was improved by Tarannikov et. al. in [23, Theorem 4] for functions with order of resiliency $\geq (n-3)/2$.

The saturated functions constructed by Proposition 7 are 'nearly linear' because they become linear when we fix very few ($\leq log_2(n)$) bits. Moreover, they have linear structures or asymptotic linear structures for the case $t = 0$. We see that although the resilient functions in Proposition 7 optimize Siegenthaler [22] and Sarkar-Maitra [20, Theorem 2] inequality. These strong conditions may cause the function to have linear-like structure.

6 Conclusion

We have introduced the dual function as a useful concept in the study of functions with 3-valued spectrum and derived several useful results for such functions. Then we constructed highly nonlinear resilient Boolean functions with optimal additive autocorrelation from functions used in the construction of Hadamard difference sets. Finally, we showed that our constructions have better additive autocorrelation than known highly nonlinear resilient Boolean functions.

7 Acknowledgement

We would like to thank Shaoquan Jiang for proofreading this paper and his many useful suggestions. We would also like to thank Douglas R. Stinson for proofreading an earlier version of the paper. Finally, we would like to thank the referees for their helpful comments. Research for this paper is supported by NSERC grant RG-PIN 227700-00. Khoongming Khoo's research is supported by a postgraduate scholarship from DSO National Laboratories, Singapore.

References

1. E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", *Journal of Cryptology*, vol. 4, 1991.
2. A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, "Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions", LNCS 1807, *Eurocrypt'2000*, pp. 507-522, Springer-Verlag, 2000.
3. C. Carlet, "A Larger Class of Cryptographic Boolean Functions via a Study of the Moriana-McFarland Construction", LNCS 2442, *Crypto'2002*, pp. 549-564, Springer Verlag, 2002.
4. C. Carlet and E. Prouff, "On Plateaued Functions and their Constructions", *Proceedings of FSE 2003*, Springer-Verlag, 2003.
5. F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis", LNCS 950, *Eurocrypt'94*, pp.356-365, Springer-Verlag, 1995.
6. J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan, "Evolving Boolean Functions satisfying Multiple Criteria", LNCS 2551, *Indocrypt 2002*, pp. 246-259, Springer-Verlag, 2002.
7. J.F. Dillon, "Multiplicative Difference Sets via Characters", *Designs, Codes and Cryptography*, vol. 17, pp. 225-235, 1999.
8. J.F. Dillon and H. Dobbertin, "Cyclic Difference Sets with Singer Parameters", preprint, 12 August 1999.

9. H. Dobbertin, "Kasami Power Functions, Permutation Polynomials and Cyclic Difference Sets", *N.A.T.O.-A.S.I. Workshop: Difference Sets, Sequences and their Correlation Properties*, Bad Windsheim, Aug 3-14, 1998.
10. R. Gold, "Maximal Recursive Sequences with 3-valued Cross Correlation Functions", *IEEE Transactions on Information Theory*, vol. 14, pp. 154-156, 1968.
11. G. Gong and A.M. Youssef, "Cryptographic Properties of the Welch-Gong Transformation Sequence Generators", *IEEE Trans. Inform. Theory*, vol.48 no.11, pp. 2837-2846, Nov 2002.
12. T. Helleseth and P.V. Kumar, "Sequences with Low Correlation", Chapter in *Handbook of Coding Theory*, North-Holland, 1998.
13. T. Jacobsen, L. Knudsen, "The Interpolation Attack on Block Ciphers", LNCS 1267, *Fast Software Encryption*, pp.28-40, Springer-Verlag, 1997.
14. T. Kasami, "The Weight Enumerators for several Classes of Subcodes of Second Order Binary Reed Muller Codes, *Information and Control* 18, pp. 369-394, 1971.
15. K. Khoo and G. Gong, "New Constructions for Highly Nonlinear and Resilient Boolean Functions", LNCS 2727, *ACISP 2003*, pp. 498-509, 2003.
16. M. Matsui, "Linear cryptanalysis method for DES cipher", LNCS 765, *Eurocrypt'93*, pp. 386-397, 1994.
17. F.J. McWilliams and N.J.A. Sloane, *Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
18. N.J Patterson and D.H. Wiedemann, "The Covering Radius of the $(2^{15}, 16)$ Reed-Muller Code is at least 16276", *IEEE Trans. Inform. Theory*, vol. 29 no. 3, pp. 354-356, May 1983.
19. P. Sarkar and S. Maitra, "Construction of Nonlinear Boolean Functions with Important Cryptographic Properties", LNCS 1807, *Eurocrypt'2000*, pp. 485-506, Springer-Verlag, 2000.
20. P. Sarkar and S. Maitra, "Nonlinearity Bounds and Constructions of Resilient Boolean Functions", LNCS 1880, *Crypto'2000*, pp. 515-532, Springer Verlag, 2000.
21. J. Seberry, X.M. Zhang and Y. Zheng, "On Constructions and Nonlinearity of Correlation Immune Functions", LNCS 765, *Eurocrypt'93*, pp. 181-199, 1994.
22. T. Siegenthaler, "Decrypting a Class of Stream Ciphers using Ciphertexts only", *IEEE Transactions on Computers*, vol. C34, no. 1, pp. 81-85, 1985.
23. Y. Tarannikov, P. Korolev and A. Botev, "Autocorrelation Coefficients and Correlation Immunity of Boolean Functions", LNCS 2248, *Asiacrypt 2001*, pp. 460-479, Springer-Verlag, 2001.
24. X.M. Zhang and Y. Zheng, "GAC - The Criterion for Global Avalanche Criteria of Cryptographic Functions", *Journal for Universal Computer Science*, vol. 1 no. 5, pp. 316-333, 1995.
25. X.M. Zhang and Y. Zheng, "Autocorrelations and New Bounds on the Nonlinearity of Boolean Functions", LNCS 1070, *Eurocrypt'96*, pp. 294-306, Springer-Verlag, 1996.
26. Y. Zheng and X.M. Zhang, "New Results on Correlation Immune Functions", LNCS 2015, *ICISC 2000*, pp. 264-274, Springer-Verlag, 2001.
27. Y. Zheng and X.M. Zhang, "Relationships between Bent Functions and Complementary Plateaued Functions", LNCS 1787, *ICISC'99*, pp. 60-75, Springer-Verlag, 1999.