2014

Concatenations of the Hidden Weighted Bit Function and their Cryptographic Properties

Wang, Qichun; Tan, Chick How; Stnic, Pantelimon

Advances in Mathematics of Communications, Volume 8, No. 2, 2014, pp. 153-165.
https://hdl.handle.net/10945/42533

Advances in Mathematics of Communications
Volume 8, No. 2, 2014, 153–165
doi:10.3934/amc.2014.8.153

CONCATENATIONS OF THE HIDDEN WEIGHTED BIT FUNCTION AND THEIR CRYPTOGRAPHIC PROPERTIES

Qichun Wang and Chik How Tan

Temasek Laboratories
National University of Singapore
117411, Singapore

Pantelimon Stănică

Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943-5216, USA

(Communicated by Joan-Josep Climent)

Abstract. To resist Binary Decision Diagrams (BDD) based attacks, a Boolean function should have a high BDD size. The hidden weighted bit function (HWBF), introduced by Bryant in 1991, seems to be the simplest function with exponential BDD size. In [28], Wang et al. investigated the cryptographic properties of the HWBF and found that it is a very good candidate for being used in real ciphers. In this paper, we modify the HWBF and construct two classes of functions with very good cryptographic properties (better than the HWBF). The new functions are balanced, with almost optimum algebraic degree and satisfy the strict avalanche criterion. Their nonlinearity is higher than that of the HWBF. We investigate their algebraic immunity, BDD size and their resistance against fast algebraic attacks, which seem to be better than those of the HWBF too. The new functions are simple, can be implemented efficiently, have high BDD sizes and rather good cryptographic properties. Therefore, they might be excellent candidates for constructions of real-life ciphers.

1. Introduction

To resist the main known attacks, Boolean functions used in real ciphers should be balanced, with high algebraic degree, with high algebraic immunity, with high nonlinearity and with good immunity to fast algebraic attacks. It would be better if the function is non-normal and satisfies the strict avalanche criterion. Up to now, many classes of Boolean functions with high algebraic immunity have been introduced [4, 5, 6, 10, 11, 15, 16, 22, 23, 25, 26, 27, 30, 31, 32, 34]. However, none of them can gather all the necessary criteria and be implemented efficiently. Moreover, none of them took BDD-based attacks into consideration.

To resist BDD-based attacks, which were first introduced by Krause in 2002 [14], a Boolean function should have a high BDD size. It is known that an n variable symmetric Boolean function has a BDD size $O(n^2)$ [13], and therefore it is weak against BDD-based attacks. The hidden weighted bit function (HWBF), proposed by Bryant [1], looks like a symmetric function, but in fact, it has an exponential

2010 *Mathematics Subject Classification:* 11T71.
Key words and phrases: Hidden weighted bit function, algebraic immunity, nonlinearity, strict avalanche criterion, BDD-based attack.
The first author is supported by NSFC (Grant No. 61202463).

BDD size and its VLSI implementation has low area-time complexity [1]. In [13], Knuth reproved Bryant's theorem stating that the HWBF has a large BDD size, regardless of how one reorders its variables. Therefore, the HWBF can resist BDD-based attacks and could be implemented efficiently.

In [28], Wang et al. investigated the cryptographic properties of the HWBF and found that it has overall very good cryptographic properties: balancedness, optimum algebraic degree, strict avalanche criterion, good algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks. Since the HWBF has a high BDD size and can be implemented very efficiently, it is a potential candidate for the stream cipher construction.

In this paper, we modify the HWBF and construct two classes of functions with very good cryptographic properties (better than those of the HWBF). The new functions are balanced, with almost optimum algebraic degree and satisfying the strict avalanche criterion. Their nonlinearity is higher than that of the HWBF. We investigate their algebraic immunity, BDD size and their resistance against fast algebraic attacks, which seem to be better than those of the HWBF too. The new functions are simple, can be implemented efficiently, have high BDD sizes and rather good cryptographic properties. Therefore, they might be excellent candidates for stream ciphers constructions.

The paper is organized as follows. In Section 2, the necessary background is established. We introduce a concatenation of two hidden weighted bit functions in Section 3. In Section 4, we give the other concatenation of four functions. We end in Section 5 with conclusions.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. We let B_n be the set of all n-variable Boolean functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2$.

Any Boolean function $f \in B_n$ can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$, called the algebraic normal form (ANF)

$$f(x_1, \ldots, x_n) = \sum_{K \subseteq \{1,2,\ldots,n\}} a_K \prod_{k \in K} x_k.$$

The algebraic degree of f is the number of variables in the highest order term with nonzero coefficient and is denoted by $\deg(f)$.

A Boolean function is *affine* if there are no term of degree strictly greater than 1 in the ANF. The set of all affine functions is denoted by A_n.

Let

$$1_f = \{x \in \mathbb{F}_2^n | f(x) = 1\},\ 0_f = \{x \in \mathbb{F}_2^n | f(x) = 0\},$$

be the support of a Boolean function f, and its complement function $f + 1$, respectively. The cardinality of 1_f is called the *Hamming weight* of f, and will be denoted by $wt(f)$. The *Hamming distance* between two functions f and g is the Hamming weight of $f + g$, and will be denoted by $d(f, g)$. We say that an n-variable Boolean function f is *balanced* if $wt(f) = 2^{n-1}$.

Let $f \in B_n$. The *nonlinearity* of f is the distance from the set of all n-variable affine functions, that is,

$$nl(f) = \min_{g \in A_n} d(f, g).$$

The nonlinearity of an n-variable Boolean function is bounded above by $2^{n-1} - 2^{n/2-1}$, and a function is said to be *bent* if it achieves this bound. Clearly, bent

functions exist only for even n and it is known that the algebraic degree of a bent function is bounded above by $\frac{n}{2}$ [2, 9, 24]. The *r-order nonlinearity*, denoted by $nl_r(f)$, is the distance from the set of all n-variable functions of algebraic degrees at most r.

For any $f \in B_n$, a nonzero function $g \in B_n$ is called an *annihilator* of f if fg (the function defined by $fg(x) = f(x)g(x)$) is null, and the *algebraic immunity* of f, denoted by $\mathcal{AI}(f)$, is the minimum value of d such that f or $f+1$ admits an annihilator of degree d [19]. It is known that the algebraic immunity of an n-variable Boolean function is bounded above by $\lceil \frac{n}{2} \rceil$ [8].

To resist algebraic attacks, a Boolean function f should have a high algebraic immunity, which implies that the nonlinearity of f is also not very low since, according to Lobanov's bound [17]

$$nl(f) \geq 2 \sum_{i=0}^{\mathcal{AI}(f)-2} \binom{n-1}{i}.$$

To resist fast algebraic attacks, a high algebraic immunity is not sufficient. If we can find g of low degree and h of algebraic degree not much larger than $n/2$ such that $fg = h$, then f is considered to be weak against fast algebraic attacks [7, 12]. The higher order nonlinearities of a function with high (fast) algebraic immunity is also not very low [2, 18, 21, 29].

The *Walsh transform* of a given function $f \in B_n$ is the integer-valued function over $\mathbb{F}_2^n$ defined by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x},$$

where $\omega \in \mathbb{F}_2^n$ and $\omega \cdot x$ is an inner product, for instance, $\omega \cdot x = \omega_1 x_1 + \omega_2 x_3 + \cdots + \omega_n x_n$. It is easy to see that a Boolean function f is balanced if and only if $W_f(0) = 0$. Moreover, the nonlinearity of f can be determined by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|.$$

The autocorrelation function of $f \in B_n$ is defined by

$$C_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+\alpha)}.$$

Also, f satisfies the strict avalanche criterion if $C_f(\alpha) = 0$, for $wt(\alpha) = 1$ [33].

A truth table of order n is a binary string of length 2^n. A bead of order n is a truth table β of order n that does not have the form $\alpha\alpha$ for any string α of length 2^{n-1}. The beads of a Boolean function are the subtables of its truth table that happens to be beads. The BDD size of a Boolean function f, denoted by $B(f)$, is the number of beads that f has. To resist BDD-based attacks, a Boolean function should have a large BDD size, regardless of how one reorders its variables.

3. Concatenation of two functions

Let a, b be integers. Define "$\boxplus$" as follows:

$$a \boxplus b = \begin{cases} n & \text{if } n|(a+b), \\ a+b \pmod{n} & \text{otherwise.} \end{cases}$$

Lemma 3.1. *If* $1 \leq d \leq n$ *and* $(n, d) = 1$, *then the set* $\{1 \boxplus (k*d) \mid k = 1, 2, \ldots, n\} = \{1, 2, \ldots, n\}$.

Proof. Let $G = \{1, 2, ..., n\}$. Clearly, $(G, \boxplus)$ is a cyclic group of order n with 1 as a generator. Since $(n, d) = 1$, $d * 1 = 1 \boxplus 1 \boxplus \cdots \boxplus 1 = d$ is also a generator, and the result follows. □

Let $h \in B_n$ be the hidden weighted bit function. That is,

$$h(x) = \begin{cases} 0 & \text{if } x = 0, \\ x_{wt(x)} & \text{otherwise.} \end{cases}$$

It is known that h is balanced, with the optimum algebraic degree and satisfying the strict avalanche criterion [28].

Let $\widehat{h}(x_1, \ldots, x_n) = h(S_{\lfloor \frac{n}{2} \rfloor}(x)) = h(x_{\lfloor \frac{n}{2} \rfloor + 1}, \ldots, x_{\lfloor \frac{n}{2} \rfloor})$, where

$$S_{\lfloor \frac{n}{2} \rfloor}(x) = (x_{1 \boxplus \lfloor \frac{n}{2} \rfloor}, \ldots, x_{n \boxplus \lfloor \frac{n}{2} \rfloor}).$$

Let $||$ denote the concatenation. We consider the function $h_1 \in B_{n+1}$ as a concatenation of two functions:

$$h_1(x_1, \ldots, x_{n+1}) = h(x_1, \ldots, x_n) || \widehat{h}(x_1, \ldots, x_n). \tag{1}$$

In fact, we can construct a family of functions in the form of $h(x)||h(S_i(x))$, where $1 \le i \le n-1$. These functions possess the similar cryptographic properties, and the function has the best nonlinearity when $i = \lfloor \frac{n}{2} \rfloor$. For that reason, we only consider $h(x)||h(S_{\lfloor \frac{n}{2} \rfloor}(x))$ here. Moreover, if we take $h(x)$ to be any balanced function with optimum algebraic degree and some other good cryptographic properties, then some of the following theorems (e.g. Theorem 3.2) still hold. In particular, we can take $h(x)$ to be the Carlet-Feng function. One can certainly ask about the cryptographic properties of $h(x)||h(S_i(x))$, for other functions h, and we leave this as an open problem.

Theorem 3.2. *The function $h_1 \in B_{n+1}$ $(n \ge 3)$ defined by (1) is balanced and*

$$\deg(h_1) = \begin{cases} n & \text{if } n \equiv 1, 2, 3 \pmod 4, \\ \ge n - 1 & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

Proof. Since h is balanced, then the concatenation of two balanced functions is also a balanced function. Hence the first claim is proven.

Clearly, $h_1(x_1, \ldots, x_{n+1}) = x_{n+1}(h(x_1, \ldots, x_n) + \widehat{h}(x_1, \ldots, x_n)) + h(x_1, \ldots, x_n)$. Therefore, $\deg(h_1) \ge n - 1$. We now prove that $\deg(h_1) = n$, for $n \equiv 1, 2, 3 \pmod 4$. That is, $g = h(x_1, \ldots, x_n) + \widehat{h}(x_1, \ldots, x_n)$ is of degree $n - 1$. Let $1_h = \{(b_{i1} + 1, b_{i2} + 1, \ldots, b_{in} + 1), 1 \le i \le 2^{n-1}\}$. Then the coefficient of the monomial $x_1 x_2 \cdots x_{k-1} x_{k+1} \cdots x_n$ in the ANF of h equals (see e.g. [2, 9])

$$\begin{aligned} \sum_{i=1}^{2^{n-1}} b_{ik} &= \sum_{j=1}^{n} |\{x|\ wt(x) = j,\ x_j = 1 \text{ and } x_k = 0\}| \\ &= \sum_{\substack{j=1 \\ j \ne k}}^{n-1} \binom{n-2}{j-1} \equiv 2^{n-2} - \binom{n-2}{k-1} \pmod 2. \end{aligned}$$

Case 1: $n \equiv 2 \pmod 4$, $n \ge 3$.

Since $\sum_{i=1}^{2^{n-1}} b_{i1} = 2^{n-2} - 1 \equiv 1 \pmod 2$ (if $n \ge 3$) and $\sum_{i=1}^{2^{n-1}} b_{i,\frac{n}{2}+1} = 2^{n-2} - \binom{n-2}{\frac{n}{2}} \equiv 0 \pmod 2$, the coefficient of the monomial $x_1 \cdots x_{\frac{n}{2}} x_{\frac{n}{2}+2} \cdots x_n$ in the ANF of g equals 1, and the result follows.

Case 2: $n \equiv 1, 3 \pmod 4$.

Since $\deg(h) = n-1$ and h contains the monomial $x_2x_3\cdots x_n$, if $\deg(g) < n-1$, then $\widehat{h}(x_1,\ldots,x_n) = h(S_{\lfloor \frac{n}{2} \rfloor}(x))$ also contains $x_2x_3\cdots x_n$, and thus $h(x_1,...,x_n)$ contains the monomial $x_1\cdots x_{\lfloor \frac{n}{2} \rfloor+1}x_{\lfloor \frac{n}{2} \rfloor+3}\cdots x_n$. Since $(n, \lfloor \frac{n}{2} \rfloor + 1) = 1$, then by Lemma 3.1, the ANF of h contains all the monomials of degree $n-1$. That is, $\sum_{i=1}^{2^{n-1}} b_{ij} \equiv 1 \pmod 2$, for $1 \le j \le n$. However, $\sum_{i=1}^{2^{n-1}} b_{in} = 2^{n-2} \equiv 0 \pmod 2$, which is a contradiction and the result follows. □

Lemma 3.3. *If $f_1, f_2 \in B_n$ satisfy the strict avalanche criterion and f_1+f_2 is a balanced function, then the concatenation $f = f_1||f_2$ also satisfies the strict avalanche criterion.*

Proof. We need to prove that $f(x) + f(x+\alpha)$ is balanced, for $\alpha = (\alpha_1,\ldots,\alpha_{n+1})$, $wt(\alpha) = 1$ and $\alpha_k = 1$, where $1 \le k \le n+1$.

Case 1: $\alpha_k = 1$, for $1 \le k \le n$. That is, $\alpha_{n+1} = 0$.

Since f_1 and f_2 satisfy the strict avalanche criterion, we have

$$\begin{aligned}&\sum_{x\in\mathbb{F}_2^{n+1}} (-1)^{f(x)+f(x+\alpha)}\\ &= \sum_{\substack{x\in\mathbb{F}_2^n\\ x_{n+1}=0}} (-1)^{f_1(x)+f_1(x+\widehat{\alpha})} + \sum_{\substack{x\in\mathbb{F}_2^n\\ x_{n+1}=1}} (-1)^{f_2(x)+f_2(x+\widehat{\alpha})} = 0,\end{aligned}$$

where $\widehat{\alpha} = (\alpha_1,\ldots,\alpha_n)$. Hence, $f(x) + f(x+\alpha)$ is balanced.

Case 2: $\alpha_{n+1} = 1$.

Since $f_1 + f_2$ is balanced, we have

$$\begin{aligned}&\sum_{x\in\mathbb{F}_2^{n+1}} (-1)^{f(x)+f(x+\alpha)}\\ &= \sum_{\substack{x\in\mathbb{F}_2^n\\ x_{n+1}=0}} (-1)^{f_1(x)+f_2(x)} + \sum_{\substack{x\in\mathbb{F}_2^n\\ x_{n+1}=1}} (-1)^{f_2(x)+f_1(x)} = 0,\end{aligned}$$

and the result follows. □

Theorem 3.4. *The function $h_1 \in B_{n+1}$ defined by (1) satisfies the strict avalanche criterion.*

Proof. Since $h(x)$ and $\widehat{h}(x)$ satisfy the strict avalanche criterion, by Lemma 3.3, we need to prove that $h(x) + \widehat{h}(x)$ is balanced. Clearly,

$$\begin{aligned}|0_h \cap 0_{\widehat{h}}| &= \sum_{i=0}^{n} |\{x|\ wt(x) = i \text{ and } x_i = x_{i\boxplus\lfloor \frac{n}{2} \rfloor} = 0\}|,\\ &= \sum_{i=0}^{n-2} \binom{n-2}{i} = 2^{n-2}.\end{aligned}$$

Similarly,

$$\begin{aligned}|1_h \cap 1_{\widehat{h}}| &= \sum_{i=0}^{n} |\{x|\ wt(x) = i \text{ and } x_i = x_{i\boxplus\lfloor \frac{n}{2} \rfloor} = 1\}|,\\ &= \sum_{i=2}^{n} \binom{n-2}{i-2} = 2^{n-2}.\end{aligned}$$

Hence, $|0_{h+\widehat{h}}| = |0_h \cap 0_{\widehat{h}}| + |1_h \cap 1_{\widehat{h}}| = 2^{n-1}$, and the result follows. □

Remark 3.5. From the proof of Theorem 3.4, it is easy to see that $h(x)+h(S_i(x))$ is balanced, for $1 \le i < n$. Then by Lemma 3.3, $h(x)||h(S_i(x))$ also satisfies the strict avalanche criterion.

Lemma 3.6 (Lemma 1 of [28]). *Let $\omega = (\omega_1, \ldots, \omega_n)$, $wt(\omega) = 1$ and $\omega_k = 1$. Then*

$$W_h(\omega) = 4\binom{n-2}{k-1}.$$

We now show a similar result for our constructed function h_1.

Lemma 3.7. *Let $\omega = (\omega_1, \ldots, \omega_{n+1})$ and $wt(\omega) = 1$. Then*

$$W_{h_1}(\omega) \le \begin{cases} 4\binom{n-2}{\frac{n-2}{2}} & \text{for } n \text{ even}, \\ 4\left(\binom{n-2}{\frac{n-1}{2}} + 1\right) & \text{for } n \text{ odd} \end{cases}$$

which is a tight bound.

Proof. Let $1 \le k \le n+1$ and $\omega_k = 1$. Let $\widehat{\omega} = (\omega_1, \ldots, \omega_n)$.

Case 1: $k = n+1$.

Since $h(x)$ and $\widehat{h}(x)$ are both balanced, we have

$$\begin{aligned} W_{h_1}(\omega) &= \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{h_1(x)+x_{n+1}} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{h(x)} + \sum_{x \in \mathbb{F}_2^n} (-1)^{\widehat{h}(x)+1} = 0. \end{aligned}$$

Case 2: $1 \le k \le n$.

By Lemma 3.6, we have

$$\begin{aligned} W_{h_1}(\omega) &= \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{h_1(x)+\omega \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{h(x)+\widehat{\omega} \cdot x} + \sum_{x \in \mathbb{F}_2^n} (-1)^{\widehat{h}(x)+\widehat{\omega} \cdot x} \\ &= 4\binom{n-2}{k-1} + 4\binom{n-2}{k \boxplus (n - \lfloor \frac{n}{2} \rfloor) - 1}, \end{aligned}$$

If n is even, then

$$W_{h_1}(\omega) \le 4\binom{n-2}{\frac{n-2}{2}},$$

and the equality can be achieved when $k = n$ or $\frac{n}{2}$. If n is odd, then

$$W_{h_1}(\omega) \le 4\left(\binom{n-2}{\frac{n-1}{2}} + 1\right),$$

and the equality can be achieved when $k = \frac{n+1}{2}$, and the result follows. □

Lemma 3.8. *Let $2 \le k \le n$ and $wt(\omega) = k$. Then*

$$W_{h_1}(\omega) \le \begin{cases} 4\binom{n-2}{\frac{n-2}{2}} & \text{for } n \text{ even}, \\ 4\left(\binom{n-2}{\frac{n-1}{2}} + 1\right) & \text{for } n \text{ odd}. \end{cases}$$

Proof. Let $\omega = (\omega_1, \omega_2, \ldots, \omega_{n+1})$ and $\omega_i = 1$ if $i \in \{s_1, s_2, \ldots, s_k\}$. Let $\widehat{\omega} = (\omega_1, \ldots, \omega_n)$. We have

$$\begin{aligned} W_{h_1}(\omega) &= \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{h_1(x)+\omega \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{h(x)+\widehat{\omega} \cdot x} + \sum_{x \in \mathbb{F}_2^n} (-1)^{\widehat{h}(x)+\widehat{\omega} \cdot x + \omega_{n+1}}. \end{aligned}$$

If $\omega_{n+1} = 0$, then $W_{h_1}(\omega) = W_h(\widehat{\omega}) + W_{\widehat{h}}(\widehat{\omega})$. By [28], we have

$$W_h(\widehat{\omega}) = 2 \sum_{i \in \{s_1, s_2, \ldots, s_k\}}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} (C_2 - C_1),$$

and

$$W_{\widehat{h}}(\widehat{\omega}) = 2 \sum_{i \in \{s_1 \boxplus \lfloor \frac{n}{2} \rfloor, \ldots, s_k \boxplus \lfloor \frac{n}{2} \rfloor\}}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} (C_2 - C_1),$$

where $d_i = 2\lfloor \frac{i-1}{2} \rfloor + 1$ and

$$C_1 = \binom{k-1}{2j-1}\binom{n-k+1}{i-2j+1}, \; C_2 = \binom{k+1}{2j-1}\binom{n-k-1}{i-2j+1}.$$

Let

$$\begin{aligned} I_1 &= \left\{ i \mid i \boxplus \lfloor \frac{n}{2} \rfloor \in \{s_1, s_2, \ldots, s_k\} \right\} \\ I_2 &= \{s_1, s_2, \ldots, s_k\} - I_1 \\ I_3 &= \left\{ i \boxplus \lfloor \frac{n}{2} \rfloor \mid i \in I_1 \right\} \\ I_4 &= \left\{ i \boxplus \lfloor \frac{n}{2} \rfloor \mid i \in I_2 \right\}. \end{aligned}$$

Then

$$W_{h_1}(\omega) = 2 \sum_{i \in I_2 \cup I_4} \sum_{j=1}^{\frac{d_i+1}{2}} (C_2 - C_1) + 2 \sum_{i \in I_1 \cup I_3} \sum_{j=1}^{\frac{d_i+1}{2}} (C_2 - C_1).$$

For $1 \le k \le n-1$, let

$$S_k = \max |\{ \sum_{i \in T_k} \sum_{j=1}^{\frac{d_i+1}{2}} (C_1 - C_2)\}|,$$

where T_k runs over all k-element subsets of $\{1, 2, ..., n\}$. We have $S_k = S_{n-k}$ and S_k decreases at first and then increases. Therefore, $|W_{h_1}(\omega)|$ achieves the maximum value when $k = \frac{n-1}{2}$ for n odd and $k = \frac{n-2}{2}$ for n even. Then we have

$$|W_{h_1}(\omega)| \le \begin{cases} 4\binom{n-2}{\frac{n-2}{2}} & \text{for } n \text{ even}, \\ 4\left(\binom{n-2}{\frac{n-1}{2}} + 1\right) & \text{for } n \text{ odd}. \end{cases}$$

The proof for the case $\omega_{n+1} = 1$ is similar, and the result follows. □

Lemma 3.9 (Lemma 3 of [28])**.** *Let $wt(\omega) = n$. Then $W_h(\omega) = 0$.*

Lemma 3.10. *Let $wt(\omega) = n + 1$. Then $W_{h_1}(\omega) = 0$.*

TABLE 1. Algebraic immunity and nonlinearity of h and h_1

n	$\mathcal{AI}(h)$	$\mathcal{AI}(h_1)$	$nl(h)$	$nl(h_1)$
6	3	3	20	24
7	3	4	44	52
8	4	4	88	106
9	4	4	186	216
10	4	5	372	440
11	5	5	772	884
12	5	6	1544	1794
13	5	6	3172	3592
14	5	6	6344	7266
15	6	6	12952	14536

Proof. Let $\widehat{\omega} = (\omega_1, \ldots, \omega_n) = (1, \ldots, 1)$. By Lemma 3.9, we have

$$W_{h_1}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{h(x)+\widehat{\omega}\cdot x} + \sum_{x \in \mathbb{F}_2^n} (-1)^{\widehat{h}(x)+\widehat{\omega}\cdot x+1} = 0 + 0 = 0,$$

and the result follows. □

Theorem 3.11. *For the function $h_1 \in B_{n+1}$ defined by (1), we have*

$$nl(h_1) = \begin{cases} 2^n - 2\binom{n-2}{\frac{n-2}{2}} & \text{for } n \text{ even,} \\ 2^n - 2\left(\binom{n-2}{\frac{n-1}{2}} + 1\right) & \text{for } n \text{ odd.} \end{cases}$$

Proof. By Lemmas 3.7, 3.8 and 3.10, we have

$$\max_{\omega \in \mathbb{F}_2^{n+1}} |W_{h_1}(\omega)| = \begin{cases} 4\binom{n-2}{\frac{n-2}{2}} & \text{for } n \text{ even,} \\ 4\left(\binom{n-2}{\frac{n-1}{2}} + 1\right) & \text{for } n \text{ odd,} \end{cases}$$

and the result follows. □

Theorem 3.12. *We have*

$$\mathcal{AI}(h_1) \geq \left\lfloor \frac{n}{3} \right\rfloor + 1.$$

Proof. Since h and $\widehat{h}$ are affine equivalent, they have the same algebraic immunity, which is $\geq \lfloor \frac{n}{3} \rfloor + 1$ by Theorem 4 of [28]. Then by Proposition 1 of [4], $\mathcal{AI}(h_1) \geq \lfloor \frac{n}{3} \rfloor + 1$. □

It seems that $\mathcal{AI}(h_1) \geq \mathcal{AI}(h)$ and in some cases $\mathcal{AI}(h_1) > \mathcal{AI}(h)$, which can be found in Table 1, where $h, h_1 \in B_n$.

Let $\deg(g_1) = d < \mathcal{AI}(h_1)$ and $h_1 \cdot g_1 = g_2$. We expect that $\deg(g_2)$ is as high as possible for any g_1 of low degree. The optimum case for a Boolean function to resist fast algebraic attacks is that $\deg(g_1) + \deg(g_2) = n + 1$ for any g_1 of degree $\deg(g_1) \leq \mathcal{AI}(h_1)$. Let $\deg(g_2) = e$. For $6 \leq n + 1 \leq 13$, in Table 2, we give the lowest possible values of (d, e). Compared with the HWBF, in most cases, the function h_1 has a better behavior against fast algebraic attacks.

To resist BDD-based attacks, a Boolean function should have a high BDD size. In Table 3, one can find BDD size of the majority function maj, the hidden weighted

TABLE 2. Behavior of the function h_1 against Fast Algebraic Attacks

n	6	7	8	9	10	11	12	13
(d, e)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)	(1,9)	(1,10)	(1,10)
	(2,3)	(2,4)	(2,5)	(2,5)	(2,7)	(2,8)	(2,9)	(2,9)
		(3,4)	(3,4)	(3,4)	(3,6)	(3,6)	(3,8)	(3,8)
					(4,5)	(4,5)	(4,6)	(4,7)
							(5,6)	(5,6)

TABLE 3. BDD size of maj, h and h_1

n	$B(maj)$	$B(h)$	$B(h_1)$
6	14	25	27
7	18	40	42
8	22	57	67
9	27	85	95
10	32	121	136
11	38	172	198
12	44	240	290
13	51	335	388
14	58	459	517
15	66	630	737
16	74	856	959

bit function h and the modified function h_1, with the standard ordering of variables. Clearly, as a symmetric Boolean function, the majority function has a very small BDD size. Although the BDD size of h is big, the BDD size of the modified function h_1 is even bigger than that of h.

4. Concatenation of four functions

Let $h \in B_n$ be the hidden weighted bit function. Let $h_2 \in B_{n+2}$ and $h_2(x_1, \ldots, x_{n+2}) = h(x)||h(S_{\lfloor \frac{n}{2} \rfloor}(x))||h(S_{\lfloor \frac{n}{4} \rfloor}(x))||h(S_{\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{2} \rfloor}(x))$. Clearly, h_2 is a balanced function.

Lemma 4.1. *The sum of the two halves of h_2, that is, $\widetilde{h} = (h(x)||h(S_{\lfloor \frac{n}{2} \rfloor}(x))) + (h(S_{\lfloor \frac{n}{4} \rfloor}(x))||h(S_{\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{2} \rfloor}(x)))$ is balanced.*

Proof. Clearly, $\widetilde{h} = (h(x) + h(S_{\lfloor \frac{n}{4} \rfloor}(x)))||(h(S_{\lfloor \frac{n}{2} \rfloor}(x)) + h(S_{\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{2} \rfloor}(x)))$. By Remark 1, $h(x)+h(S_{\lfloor \frac{n}{4} \rfloor}(x))$ and $h(S_{\lfloor \frac{n}{2} \rfloor}(x))+h(S_{\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{2} \rfloor}(x))$ are balanced functions, and the result follows. □

By Lemmas 3.3 and 4.1, it is easy to see that h_2 satisfies the strict avalanche criterion.

Lemma 4.2. *Let $\omega = (\omega_1, \ldots, \omega_{n+2})$ and $wt(\omega) = 1$. Then*

$$W_{h_2}(\omega) \leq 4 \max_{1\leq k\leq n} \left\{ \binom{n-2}{k-1} + \binom{n-2}{k \boxplus (n - \lfloor \frac{n}{2} \rfloor) - 1} + \binom{n-2}{k \boxplus (n - \lfloor \frac{n}{4} \rfloor) - 1} + \binom{n-2}{k \boxplus (n - \lfloor \frac{n}{4} \rfloor - \lfloor \frac{n}{2} \rfloor) - 1} \right\},$$

which is a tight bound.

Proof. Let $\widehat{\omega} = (\omega_1, \ldots, \omega_n)$. Consider $\omega_k = 1$ for $1 \leq k \leq n+2$.

Case 1: $k = n+1$ or $n+2$.

Since h, $h(S_{\lfloor \frac{n}{2} \rfloor})$, $h(S_{\lfloor \frac{n}{4} \rfloor})$ and $h(S_{\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{2} \rfloor})$ are all balanced, we have

$$\begin{aligned} W_{h_2}(\omega) &= \sum_{x \in \mathbb{F}_2^{n+2}} (-1)^{h_2(x)+x_k} \\ &= \sum_{\substack{x \in \mathbb{F}_2^n \\ x_{n+1}=x_{n+2}=0}} (-1)^{h(x)+x_k} + \sum_{\substack{x \in \mathbb{F}_2^n \\ x_{n+1}+1=x_{n+2}=0}} (-1)^{h(S_{\lfloor \frac{n}{2} \rfloor}(x))+x_k} \\ &\quad + \sum_{\substack{x \in \mathbb{F}_2^n \\ x_{n+1}=x_{n+2}+1=0}} (-1)^{h(S_{\lfloor \frac{n}{4} \rfloor}(x))+x_k} \\ &\quad + \sum_{\substack{x \in \mathbb{F}_2^n \\ x_{n+1}=x_{n+2}=1}} (-1)^{h(S_{\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{2} \rfloor}(x))+x_k} \\ &= 0. \end{aligned}$$

Case 2: $1 \leq k \leq n$.

By Lemma 3.6, we have

$$\begin{aligned} W_{h_2}(\omega) &= \sum_{x \in \mathbb{F}_2^N} (-1)^{h_2(x)+\omega \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{h(x)+\widehat{\omega} \cdot x} + \sum_{x \in \mathbb{F}_2^n} (-1)^{h(S_{\lfloor \frac{n}{2} \rfloor}(x))+\widehat{\omega} \cdot x} \\ &\quad + \sum_{x \in \mathbb{F}_2^n} (-1)^{h(S_{\lfloor \frac{n}{4} \rfloor}(x))+\widehat{\omega} \cdot x} + \sum_{x \in \mathbb{F}_2^n} (-1)^{h(S_{\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{2} \rfloor}(x))+\widehat{\omega} \cdot x} \\ &= 4\binom{n-2}{k-1} + 4\binom{n-2}{k \boxplus (n - \lfloor \frac{n}{2} \rfloor) - 1} + 4\binom{n-2}{k \boxplus (n - \lfloor \frac{n}{4} \rfloor) - 1} \\ &\quad + 4\binom{n-2}{k \boxplus (n - \lfloor \frac{n}{4} \rfloor - \lfloor \frac{n}{2} \rfloor) - 1}, \end{aligned}$$

and the result follows. □

Similarly, as for h_1, one can find some other cryptographic properties for h_2, and we gather these in the following theorem, whose proof we omit.

Theorem 4.3. *The Boolean function $h_2 \in B_{n+2}$ is a balanced function, it satisfies the strict avalanche criterion, has degree $\deg(h_2) \geq n-1$, $\mathcal{AI}(h_2) \geq \lfloor \frac{n}{3} \rfloor + 1$ and*

$$nl(h_2) = 2^{n+1} - 2 \max_{1\leq k\leq n} \left\{ \binom{n-2}{k-1} + \binom{n-2}{k \boxplus (n - \lfloor \frac{n}{2} \rfloor) - 1} + \binom{n-2}{k \boxplus (n - \lfloor \frac{n}{4} \rfloor) - 1} + \binom{n-2}{k \boxplus (n - \lfloor \frac{n}{4} \rfloor - \lfloor \frac{n}{2} \rfloor) - 1} \right\}.$$

TABLE 4. Algebraic immunity, nonlinearity and BDD size of h_2

$n+2$	$\mathcal{AI}(h_2)$	$nl(h_2)$	$B(h_2)$
10	5	448	137
11	5	896	196
12	6	1820	280
13	6	3658	383
14	6	7508	571
15	7	15018	782

TABLE 5. Behavior of the function h_2 against Fast Algebraic Attacks

$n+2$	(d,e)				
10	(1,7)	(2,6)	(3,5)	(4,5)	
11	(1,9)	(2,8)	(3,7)	(4,6)	
12	(1,10)	(2,9)	(3,8)	(4,7)	(5,6)
13	(1,11)	(2,10)	(3,9)	(4,8)	(5,6)

In Table 4, one can find the algebraic immunity, nonlinearity and BDD size of $h_2 \in B_{n+2}$ for $10 \le n+2 \le 15$. Clearly, the BDD size of h_2 is better than that of h, $\mathcal{AI}(h_2) \ge \mathcal{AI}(h_1)$ and the nonlinearity of h_2 is much higher than that of h and h_1. In Table 5, one can find the behavior of the function h_2 against fast algebraic attacks, which is better than that of h, as well.

We have the following well-known results.

Proposition 4.4. *Let $p_1(x_1,\ldots,x_l) \in B_l$ be balanced, $p_2(x_{l+1},\ldots,x_{l+m}) \in B_m$ and $p = p_1 + p_2$ be the direct sum of p_1 and p_2. Then we have*

1) $\deg(p) = \max\{\deg(p_1), \deg(p_2)\}$.

2) $\mathcal{AI}(p) \ge \max\{\mathcal{AI}(p_1), \mathcal{AI}(p_2)\}$.

3) $nl(p) = 2^m nl(p_1) + 2^l nl(p_2) - 2nl(p_1)nl(p_2)$.

Recall that the fast correlation attack has an on-line complexity proportional to $\left(\frac{1}{\epsilon}\right)^2$, where $\epsilon = \frac{1}{2} - \frac{nl(f)}{2^n}$ is the so-called bias [20]. In consideration of the implementation efficiency, we compare the 16-variable Carlet–Feng function with the 256-variable HWBF. Let f_c be the 16-variable Carlet–Feng function discussed by [26], $\widetilde{h} = h_{256} + x_{257}x_{258} + x_{259}x_{260} + x_{261}x_{262} + x_{263}x_{264} + x_{265}x_{266} + x_{267}x_{268} + x_{269}x_{270} + x_{271}x_{272}$, $\widetilde{h_1} = h_{1_{256}} + x_{257}x_{258} + x_{259}x_{260} + x_{261}x_{262} + x_{263}x_{264} + x_{265}x_{266} + x_{267}x_{268} + x_{269}x_{270} + x_{271}x_{272}$ and $\widetilde{h_2} = h_{2_{256}} + x_{257}x_{258} + x_{259}x_{260} + x_{261}x_{262} + x_{263}x_{264} + x_{265}x_{266} + x_{267}x_{268} + x_{269}x_{270} + x_{271}x_{272}$. Then, the bias of f_c is $\epsilon = 0.0036$, while by Proposition 1, the bias of $\widetilde{h}$ is $\epsilon = 0.0001$, the bias of $\widetilde{h_1}$ is $\epsilon = 0.00005$ and the bias of $\widetilde{h_2}$ is $\epsilon = 0.000025$. Clearly, the behavior of $\widetilde{h}$ and $\widetilde{h_1}$ against fast correlation attacks is better than that of f_c, and $\widetilde{h_2}$ has the best behavior among all of them. We have $\mathcal{AI}(f_c) = 8$, while the other three functions have algebraic immunities at least 86. The Carlet–Feng function also has an exponential BDD size. However, $B(f_c) < 2^{15}$, and it is much smaller than the BDD sizes of the other three functions.

Example 4.5. Let $h, h_1, h_2 \in B_{12}$. Then they are all balanced and satisfy the strict avalanche criterion. $\deg(h) = \deg(h_1) = \deg(h_2) = 11$; $\mathcal{AI}(h) = 5$ and $\mathcal{AI}(h_1) = \mathcal{AI}(h_2) = 6$; $nl(h) = 1544$, $nl(h_1) = 1794$ and $nl(h_2) = 1820$; $B(h) = 240$, $B(h_1) = 290$ and $B(h_2) = 280$. Comparing it with h, h_1 has a better behavior and h_2 has the best behavior against fast algebraic attacks (it is noticed that $h_2 \in B_{12}$ has the optimum algebraic immunity and the optimum behavior against fast algebraic attacks). Clearly, all these cryptographic properties of h_1 and h_2 are better than those of h.

5. Conclusion

This paper modifies the HWBF and constructs two infinite classes of functions with very good cryptographic properties (better than those of the HWBF). To summarize, the new functions are balanced, have almost optimum algebraic degree and satisfy the strict avalanche criterion. Their nonlinearity is higher than that of the HWBF. We investigate their algebraic immunity, BDD size and their resistance against fast algebraic attacks, which seem to be better than those of the HWBF, too. Since the new functions can be implemented very efficiently, they can be used with a large number of variables, which allows reaching very good cryptographic properties. The new functions could be excellent candidates for stream ciphers constructions.

Acknowledgments

We would like to thank the anonymous reviewers for their valuable suggestions and comments that improved the quality of this paper.

References

[1] R. E. Bryant, On the complexity of VLSI implementations and graph representations of Boolean functions with application to integer multiplication, *IEEE Trans. Comput.*, **40** (1991), 205–213.

[2] C. Carlet, On the higher order nonlinearities of algebraic immune functions, in *Advances in Cryptology – CRYPTO 2006*, Springer-Verlag, 2006, 584–601.

[3] C. Carlet, Boolean functions for cryptography and error correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Cambridge Univ. Press, 2010, 257–397.

[4] C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra, Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, *IEEE Trans. Inf. Theory*, **52** (2006), 3105–3121.

[5] C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, in *Advances in Cryptology – ASIACRYPT 2008*, Springer-Verlag, 2008, 425–440.

[6] C. Carlet and K. Feng, An infinite class of balanced vectorial Boolean functions with optimum algebraic immunity and good nonlinearity, in *IWCC 2009*, Springer-Verlag, 2009, 1–11.

[7] N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, in *Advances in Cryptology – CRYPTO 2003*, Springer-Verlag, 2003, 176–194.

[8] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in *Advances in Cryptology – EUROCRYPT 2003*, Springer-Verlag, 2003, 345–359.

[9] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Elsevier-Academic Press, New York, 2009.

[10] D. K. Dalai, K. C. Maitra and S. Maitra, Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity, in *Proceedings of FSE 2005*, Springer-Verlag, 2005, 98–111.

[11] D. K. Dalai, S. Maitra and S. Sarkar, Basic theory in construction of Boolean functions with maximum possible annihilator immunity, *Des. Codes Cryptogr.*, **40** (2006), 41–58.

[12] P. Hawkes and G. G. Rose, Rewriting variables: the complexity of fast algebraic attacks on stream ciphers, in *Advances in Cryptology – CRYPTO 2004*, Springer-Verlag, 2004, 390–406.
[13] D. E. Knuth, *The Art of Computer Programming: Bitwise Tricks & Techniques; Binary Decision Diagrams*, Addison-Wesley Professional, Boston, 2009.
[14] M. Krause, BDD-based cryptanalysis of keystream generators, in *Advances in Cryptology – EUROCRYPT 2002*, Springer-Verlag, 2002, 222–237.
[15] N. Li and W. F. Qi, Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity, in *Advances in Cryptology – ASIACRYPT 2006*, Springer-Verlag, 2006, 84–98.
[16] N. Li, L. Qu, W. Qi, G. Feng, C. Li and D. Xie, On the construction of Boolean functions with optimal algebraic immunity, *IEEE Trans. Inf. Theory*, **54** (2008), 1330–1334.
[17] M. S. Lobanov, Exact relation between nonlinearity and algebraic immunity, *Discrete Math. Appl.*, **16** (2006), 453–460.
[18] M. S. Lobanov, Exact relations between nonlinearity and algebraic immunity, *J. Appl. Ind. Math.*, **3** (2009), 367–376.
[19] W. Meier, E. Pasalic and C. Carlet, Algebraic attacks and decomposition of Boolean functions, in *Advances in Cryptology – EUROCRYPT 2004*, Springer-Verlag, 2004, 474–491.
[20] W. Meier and O. Staffelbach, Fast correlation attacks on stream ciphers, in *Advances in Cryptology – EUROCRYPT '88*, Springer-Verlag, 1988, 301–314.
[21] S. Mesnager, Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity, *IEEE Trans. Inf. Theory*, **54** (2008), 3656–3662.
[22] E. Pasalic, Almost fully optimized infinite classes of Boolean functions resistant to (fast) algebraic cryptanalysis, in *Proceedings of ICISC 2008*, Springer-Verlag, 2009, 399–414.
[23] P. Rizomiliotis, On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation, *IEEE Trans. Inf. Theory*, **56** (2010), 4014–4024.
[24] O. S. Rothaus, On bent functions, *J. Comb. Theory Ser. A*, **20** (1976), 300–305.
[25] C. Tan and S. Goh, Several classes of even-variable balanced Boolean functions with optimal algebraic immunity, *IEICE Trans. Fund.*, **E94.A** (2011), 165–171.
[26] D. Tang, C. Carlet and X. Tang, Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks, *IEEE Trans. Inf. Theory*, **59** (2013), 653–664.
[27] Z. Tu and Y. Deng, A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity, *Des. Codes Cryptogr.*, **60** (2011), 1–14.
[28] Q. Wang, C. Carlet, P. Stănică and C. Tan, Cryptographic properties of the hidden weighted bit function, *Discrete Appl. Math.*, to appear.
[29] Q. Wang, T. Johansson and H. Kan, Some results on fast algebraic attacks and higher-order non-linearities, *IET Inform. Secur.*, **6** (2012), 41–46.
[30] Q. Wang, J. Peng, H. Kan and X. Xue, Constructions of cryptographically significant Boolean functions using primitive polynomials, *IEEE Trans. Inf. Theory*, **56** (2010), 3048–3053.
[31] Q. Wang and C. H. Tan, A new method to construct Boolean functions with good cryptographic properties, *Inform. Proc. Lett.*, **113** (2013), 567–571.
[32] Q. Wang and C. H. Tan, Balanced Boolean functions with optimum algebraic degree, optimum algebraic immunity and very high nonlinearity, *Discrete Appl. Math.*, **1673** (2014), 25–32.
[33] A. F. Webster and S. E. Tavares, On the design of S-boxes, in *Advances in Cryptology – CRYPTO '85*, Springer-Verlag, 1985, 523–534.
[34] X. Zeng, C. Carlet, J. Shan and L. Hu, More balanced Boolean functions with optimal algebraic immunity, and good nonlinearity and resistance to fast algebraic attacks, *IEEE Trans. Inf. Theory*, **57** (2011), 6310–6320.

Received January 2013; revised September 2013.

E-mail address: tslwq@nus.edu.sg
E-mail address: tsltch@nus.edu.sg
E-mail address: pstanica@nps.edu