Cryptographic Properties of the Hidden Weighted Bit Function

Qichun Wang[a], Claude Carlet[b], Pantelimon Stănică[c], Chik How Tan[a]

[a] *Temasek Laboratories, National University of Singapore, 117411, Singapore. E-mails: {tslwq,tsltch}@nus.edu.sg*
[b] *LAGA, Department of Mathematics, University of Paris 8 (and Paris 13 and CNRS), Saint-Denis cedex 02, France. E-mail: claude.carlet@univ-paris8.fr*
[c] *Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA. Email: pstanica@nps.edu*

Abstract

The hidden weighted bit function (HWBF), introduced by R. Bryant in IEEE Trans. Comp. 40 and revisited by D. Knuth in Vol. 4 of The Art of Computer Programming, is a function that seems to be the simplest one with exponential Binary Decision Diagram (BDD) size. This property is interesting from a cryptographic viewpoint since BDD-based attacks are receiving more attention in the cryptographic community. But, to be usable in stream ciphers, the functions must also satisfy all the other main criteria. In this paper, we investigate the cryptographic properties of the HWBF and prove that it is balanced, with optimum algebraic degree and satisfies the strict avalanche criterion. We calculate its exact nonlinearity and give a lower bound on its algebraic immunity. Moreover, we investigate its normality and its resistance against fast algebraic attacks. The HWBF is simple, can be implemented efficiently, has a high BDD size and rather good cryptographic properties, if we take into account that its number of variables can be much larger than for other functions with the same implementation efficiency. Therefore, the HWBF is a good candidate for being used in real ciphers. Indeed, contrary to the case of symmetric functions, which allow such fast implementation but also offer to the attacker some specific possibilities due to their symmetry, its structure is not suspected to be related to such dedicated attacks.

Keywords: Hidden weighted bit function, algebraic immunity, nonlinearity, BDD-based attack.

1. Introduction

To resist the main known attacks, Boolean functions used in stream ciphers should have good cryptographic properties: balancedness, high algebraic degree, high algebraic immunity, high nonlinearity and good immunity to fast algebraic attacks. Up to now, many classes of Boolean functions with high algebraic immunity have been introduced [1, 5, 6, 7, 8, 13, 14, 22, 23, 28, 29, 30, 31, 36, 37, 38, 41, 42, 43]. However, most of them do not satisfy all the necessary criteria and the few classes which do satisfy, are not very efficiently implementable; moreover, none of the papers studying these classes took BDD-based attacks into consideration.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
23 DEC 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cryptographic Properties of the Hidden Weighted Bit Function	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Department of Applied Mathematics,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The hidden weighted bit function (HWBF), introduced by R. Bryant in IEEE Trans. Comp. 40 and revisited by D. Knuth in Vol. 4 of The Art of Computer Programming, is a function that seems to be the simplest one with exponential Binary Decision Diagram (BDD) size. This property is interesting from a cryptographic viewpoint since BDDbased attacks are receiving more attention in the cryptographic community. But, to be usable in stream ciphers, the functions must also satisfy all the other main criteria. In this paper, we investigate the cryptographic properties of the HWBF and prove that it is balanced, with optimum algebraic degree and satis es the strict avalanche criterion. We calculate its exact nonlinearity and give a lower bound on its algebraic immunity. Moreover, we investigate its normality and its resistance against fast algebraic attacks. The HWBF is simple, can be implemented e ciently, has a high BDD size and rather good cryptographic properties, if we take into account that its number of variables can be much larger than for other functions with the same implementation e ciency. Therefore the HWBF is a good candidate for being used in real ciphers. Indeed, contrary to the case of symmetric functions, which allow such fast implementation but also o er to the attacker some speci c possibilities due to their symmetry, its structure is not suspected to be related to such dedicated attacks.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**15**	

BDD-based attacks were first introduced by Krause in 2002 [20]. They might be efficient against LFSR-based generators [20, 21, 34, 35]. To resist BDD-based attacks, a Boolean function should have a high BDD size.

The hidden weighted bit function (HWBF) was proposed by Bryant [2]. It is an easily defined function that has an exponential BDD size, but has a VLSI implementation with low area-time complexity [2]. In [19], 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. However, many other cryptographic properties of the HWBF were still unknown.

In this paper, we investigate the important cryptographic properties of this function and show that it is balanced, with optimum algebraic degree and satisfies the strict avalanche criterion. We calculate exactly its nonlinearity and give a lower bound on its algebraic immunity. These two parameters are not at an optimal level (but they are not low either). The function would then not be a good choice as a filter function (in a stream cipher) if it was implemented with a number of variables which is usual for other functions such as the Carlet–Feng function [7] (say, between 16 and 20 variables). But its very simple structure allows using it with many more variables (at least twice) and then the values of the nonlinearity and of the algebraic immunity allow good resistance to the main attacks while the function has still a much faster hardware implementation, which allows the stream cipher to be in the same time robust against the main known attacks and fast. This is also the case of some symmetric functions (whose output depend only on the Hamming weight of the input), but the specificity of symmetric functions represents a threat since it has the reputation of allowing dedicated attacks. The structure of the HWBF function is almost as simple as that of symmetric functions but the fact that, for a given Hamming weight different from 0 and n of the input, the output is non-constant (and is even almost balanced in the case of Hamming weights near $n/2$, that is, for most probable ones), the function represents a better tradeoff between robustness and speed. We also investigate the normality and give some computational results on the resistance of the HWBF against fast algebraic attacks, revealing that the HWBF displays good behavior against fast algebraic attacks.

The paper is organized as follows. In Section 2, the necessary background is established. We then investigate the cryptographic properties of the HWBF in Section 3. We end in Section 4 with conclusions.

2. Preliminaries

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

Cosets of vector subspaces are also called *flats*. Let $f \in B_n$ and E be any flat. If the restriction of f to E, denoted by $f|_E$, is constant (respectively affine), then E is called a constant (respectively affine) flat for f.

Any Boolean function $f \in B_n$ can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1, \cdots, x_n]$,

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

which is called its algebraic normal form (ANF). The algebraic degree of f, denoted by $\deg(f)$, is the number of variables in the highest order term with nonzero coefficient.

A Boolean function is *affine* if there exists 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, respectively, its complement. 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 its 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 $\frac{n}{2}$ [4, 33]. The *r-order nonlinearity*, denoted by $nl_r(f)$, is its distance from the set of all n-variable functions of algebraic degrees at most r.

A Boolean function $f \in B_n$ is called *k-normal* (respectively, *k-weakly-normal*) if there exist a k-dimensional constant (respectively, affine) flat for f. If $k = \lceil \frac{n}{2} \rceil$, f is simply called a *normal* (respectively, *weakly-normal*) function.

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 [25]. It is known that the algebraic immunity of an n-variable Boolean function is bounded above by $\lceil \frac{n}{2} \rceil$ [11].

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 [24]:

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

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 [10, 17]. The higher order nonlinearities of a function with high (fast) algebraic immunity is also not very low [3, 27, 40].

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, $\omega \cdot x = \omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$. 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 $wt(\alpha) = 1$.

For convenience, we denote the largest odd m such that $m \leq n$ by d_n, that is, $d_n = 2\lfloor \frac{n-1}{2} \rfloor + 1$.

3. Cryptographic properties of the hidden weighted bit function

The *hidden weighted bit function* (HWBF) [2] in n-variables $h \in B_n$ is defined as follows:

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

We shall use h_n if we need to emphasize the number of variables that h depends on.

If we let $h' \in B_n$ be defined by

$$h'(x) = \begin{cases} 1 & \text{if } x = (1, 1, \ldots, 1), \\ x_{wt(x)+1} & \text{otherwise,} \end{cases}$$

that is, $h'(x_1, x_2, \ldots, x_n) = h(x_2, \ldots, x_n, x_1)$, then h_{n+1} is the *concatenation* $h_{n+1} = h_n || h'_n$.

Let $n = 4k + 1$. Set $x_{k+1} = x_{k+2} = \ldots = x_{2k} = 0$ and $x_{2k+1} = x_{2k+2} = \ldots = x_{3k+1} = 1$. Then the obtained subfunction from h_n is the $2k$-variable majority function, which has the optimum algebraic immunity k (see [13]).

Theorem 1. *The HWBF h is balanced and has algebraic degree $n-1$ (optimum for a balanced function), for $n \geq 3$.*

Proof. Clearly,

$$|1_h| = \sum_{i=1}^{n} |\{x|\ wt(x) = i \text{ and } x_i = 1\}| = \sum_{i=1}^{n} \binom{n-1}{i-1} = 2^{n-1},$$

and the first claim is proven.

We know (see e.g. [4, 12]) that the coefficient of a monomial $x^u = \prod_{i=1}^{n} x_i^{u_i}$ in the algebraic form of f equals $\sum_{x \preceq u} f(x) \pmod 2$ where $x \preceq u$ means $x_i \leq u_i$ for $i = 1, \ldots, n$.

We deduce that the coefficient of the monomial $x_1 x_2 \cdots x_{k-1} x_{k+1} \cdots x_n$ (of degree $n-1$) equals $\sum_{j=1}^{n} |\{x|\ wt(x) = j,\ x_j = 1 \text{ and } x_k = 0\}| = \sum_{\substack{j=1 \\ j \neq k}}^{n-1} \binom{n-2}{j-1} = 2^{n-2} - \binom{n-2}{k-1} \pmod 2$. In particular, for $k = n-1$, the coefficient equals 1, for $n \geq 3$. Hence, $\deg(h) = n-1$. □

Theorem 2. *The HWBF h satisfies the strict avalanche criterion.*

Proof. We need to prove that $h(x)+h(x+\alpha)$ is balanced, for $\alpha=(\alpha_1,\ldots,\alpha_n)$, $wt(\alpha)=1$, say $\alpha_k=1$, where $1\le k\le n$. Since $h(x)$ and $h(x+\alpha)$ are both balanced, it is sufficient to prove that $|1_{h(x)}\cap 1_{h(x+\alpha)}|=2^{n-1}-|1_{h(x)}\cap 0_{h(x+\alpha)}|=2^{n-2}$. Clearly, if $x_k=1$ then $wt(x+\alpha)=wt(x)-1$ and if $x_k=0$ then $wt(x+\alpha)=wt(x)+1$. Hence, separating the cases $wt(x)=i<k, i=k, i=k+1$ and $i>k+1$, we have

$$\begin{aligned}
& |\{x|x_k=1,\ h(x)=h(x+\alpha)=1\}| \\
= & \sum_{i=3}^{k-1}\binom{n-3}{i-3}+\binom{n-2}{k-2}+0+\sum_{i=k+2}^{n}\binom{n-3}{i-3} \\
& \text{(since if } i\neq k,k+1 \text{ for instance, then } wt(x)=i \text{ and } wt(x+\alpha)=i+1) \\
= & 2^{n-3}-\binom{n-3}{k-3}-\binom{n-3}{k-2}+\binom{n-2}{k-2}=2^{n-3},
\end{aligned}$$

and, separating the cases $i<k-1, i=k-1, i=k$ and $i>k$, we have

$$\begin{aligned}
& |\{x|x_k=0,\ h(x)=h(x+\alpha)=1\}| \\
= & \sum_{i=2}^{k-2}\binom{n-3}{i-2}+\binom{n-2}{k-2}+0+\sum_{i=k+1}^{n-1}\binom{n-3}{i-2} \\
= & 2^{n-3}-\binom{n-3}{k-3}-\binom{n-3}{k-2}+\binom{n-2}{k-2}=2^{n-3}.
\end{aligned}$$

Therefore, $|1_{h(x)}\cap 1_{h(x+\alpha)}|=2^{n-2}$, and the result follows. □

3.1. Nonlinearity

Lemma 1. *Let $\omega=(\omega_1,\ldots,\omega_n)\in\mathbb{F}_2^n$ with $wt(\omega)=1$. Then*

$$W_h(\omega)\le 4\binom{n-2}{\lceil\frac{n-2}{2}\rceil},$$

and the bound is tight.

Proof. Let $1\le k\le n$ and $\omega_k=1$. We have

$$\begin{aligned}
W_h(\omega) &= \sum_{x\in\mathbb{F}_2^n}(-1)^{h(x)+\omega\cdot x}=1+\sum_{i=1}^{n}\sum_{wt(x)=i}(-1)^{x_i+x_k} \\
&= 1+2^n-1-2|\bigcup_{i=1}^{n}\{x|\ wt(x)=i \text{ and } x_i+x_k=1\}|
\end{aligned}$$

Since

$$|\{x|\ wt(x)=i \text{ and } x_i+x_k=1\}|=\begin{cases}0 & \text{if } i=k \text{ or } n,\\ 2\binom{n-2}{i-1} & \text{otherwise,}\end{cases}$$

we have

$$\begin{aligned}
W_h(\omega) &= 2^n-4\left(\sum_{i=1}^{n-1}\binom{n-2}{i-1}-\binom{n-2}{k-1}\right) \\
&= 4\binom{n-2}{k-1},
\end{aligned}$$

and the result follows. □

Lemma 2. *Let $\omega \in \mathbb{F}_2^n$ with $wt(\omega) = k$, $2 \le k \le n-1$. Then*

$$W_h(\omega) \le 4\binom{n-2}{\lceil \frac{n-2}{2} \rceil}.$$

Proof. Let $\omega_i = 1$ if $i \in \{s_1, s_2, \ldots, s_k\}$. We have

$$\begin{aligned} W_h(\omega) &= 1 + \sum_{i=1}^{n} \sum_{wt(x)=i} (-1)^{x_i + x_{s_1} + x_{s_2} + \cdots + x_{s_k}} \\ &= 2^n - 2|\bigcup_{i=1}^{n} \{x|\ wt(x) = i \text{ and } x_i + x_{s_1} + x_{s_2} + \cdots + x_{s_k} = 1\}| \\ &= 2^n - 2\sum_{i=1}^{n} |A_i|, \end{aligned}$$

where $A_i = \{x|\ wt(x) = i \text{ and } x_i + x_{s_1} + x_{s_2} + \cdots + x_{s_k} = 1\}$. Now, we compute $|A_i|$ as follows.

We use the convention that $\binom{a}{b}$ is 0 if $b > a$. If $i \notin \{s_1, s_2, \ldots, s_k\}$, then

$$|A_i| = \binom{k+1}{1}\binom{n-k-1}{i-1} + \binom{k+1}{3}\binom{n-k-1}{i-3} + \cdots + \binom{k+1}{d_i}\binom{n-k-1}{i-d_i}.$$

If $i \in \{s_1, s_2, \ldots, s_k\}$, then

$$|A_i| = \binom{k-1}{1}\binom{n-k+1}{i-1} + \binom{k-1}{3}\binom{n-k+1}{i-3} + \cdots + \binom{k-1}{d_i}\binom{n-k+1}{i-d_i}.$$

Therefore, we have

$$\begin{aligned} \sum_{i=1}^{n} |A_i| &= \sum_{\substack{i=1 \\ i \notin \{s_1, s_2, \ldots, s_k\}}}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} \binom{k+1}{2j-1}\binom{n-k-1}{i-2j+1} \\ &\quad + \sum_{\substack{i=1 \\ i \in \{s_1, s_2, \ldots, s_k\}}}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} \binom{k-1}{2j-1}\binom{n-k+1}{i-2j+1}. \end{aligned}$$

Since

$$\begin{aligned} & \sum_{i=1}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} \binom{k+1}{2j-1}\binom{n-k-1}{i-2j+1} \\ = & \sum_{j=1}^{\lceil \frac{n}{2} \rceil} \sum_{i=2j-1}^{n} \binom{k+1}{2j-1}\binom{n-k-1}{i-2j+1} \\ = & \sum_{j=1}^{\lceil \frac{n}{2} \rceil} \binom{k+1}{2j-1} 2^{n-k-1}, \text{ since } n-2j+1 \ge n-k-1 \\ = & \ 2^{n-1}, \text{ since } 2\left\lceil \frac{n}{2} \right\rceil - 1 \ge k+1 \text{ if } n \text{ is odd and, if } n \text{ is even,} \end{aligned}$$

then $2\lceil \frac{n}{2} \rceil - 1 = n-1$ is the highest odd integer $\leq k+1$. Next, we have

$$\begin{aligned}\sum_{i=1}^{n} |A_i| &= 2^{n-1} + \sum_{\substack{i=1 \\ i\in\{s_1,s_2,\ldots,s_k\}}}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} (C_1 - C_2) \\ &= 2^{n-1} - \sum_{\substack{i=1 \\ i\notin\{s_1,s_2,\ldots,s_k\}}}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} (C_1 - C_2),\end{aligned}$$

where

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

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

$$S_k = \max |\{ \sum_{\substack{i=1 \\ i\in\{s_1,s_2,\ldots,s_k\}}}^{n} \sum_{j=1}^{\frac{d_i+1}{2}} (C_1 - C_2)\}|.$$

It is easy to verify that $S_k = S_{n-k}$ and S_k decreases initially and then increases. That is, S_k achieves the maximum value when $k=1$ and achieves the minimum value when $k = \lceil \frac{n}{2} \rceil$. Hence, by Lemma 1,

$$S_k \leq 2\binom{n-2}{\lceil \frac{n-2}{2} \rceil}.$$

Therefore,

$$2^{n-1} - 2\binom{n-2}{\lceil \frac{n-2}{2} \rceil} \leq \sum_{i=1}^{n} |A_i| \leq 2^{n-1} + 2\binom{n-2}{\lceil \frac{n-2}{2} \rceil},$$

and the result follows. □

Lemma 3. *Let $\omega \in \mathbb{F}_2^n$ with $wt(\omega) = n$. Then $W_h(\omega) = 0$.*

Proof. We have

$$\begin{aligned}W_h(\omega) &= 1 + \sum_{i=1}^{n} \sum_{wt(x)=i} (-1)^{x_i + x_1 + x_2 + \cdots + x_n} \\ &= 2^n - 2|\bigcup_{i=1}^{n} \{x|\ wt(x) = i \text{ and } x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n = 1\}| \\ &= 2^n - 4\left(\binom{n-1}{1} + \binom{n-1}{3} + \binom{n-1}{5} + \cdots + \binom{n-1}{d_{n-1}}\right) \\ &= 0.\end{aligned}$$

□

Theorem 3. *If h is the HWBF defined on $\mathbb{F}_2^n$, then*

$$nl(h) = 2^{n-1} - 2\binom{n-2}{\lceil \frac{n-2}{2} \rceil}.$$

Proof. By Lemmas 1–3 we have

$$\max_{\omega \in \mathbb{F}_2^n} |W_h(\omega)| = 4\binom{n-2}{\lceil \frac{n-2}{2} \rceil},$$

and the result follows. □

Remark 1. *For n odd,*

$$nl(h) = 2\sum_{i=0}^{\frac{n-3}{2}} \binom{n-1}{i} + \binom{n-1}{\frac{n-1}{2}} - 2\binom{n-2}{\frac{n-3}{2}} = 2\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 2} \binom{n-1}{i},$$

which is exactly Lobanov's bound on the nonlinearity for n-variable functions with optimum algebraic immunity (albeit the HWBF function does not have optimal algebraic immunity).

3.2. Algebraic immunity

The algebraic immunity of the HWBF is a non-decreasing sequence of n.
To prove this, let us first recall a known result:

Lemma 4 (Proposition 1 of [6])**.** *Let f, g be two Boolean functions in the variables $x_1, \ldots, x_n$ with $\mathcal{AI}(f) = \mathcal{AI}(g) = d$, and let $h = (1 + x_{n+1})f + x_{n+1}g \in B_{n+1}$. Then $d \leq \mathcal{AI}(h) \leq d + 1$.*

Note that we know also from [6] that $\mathcal{AI}(h) = d$ if and only if there exists $f_1, g_1 \in B_n$ of algebraic degree d such that $\{f \cdot f_1 = 0, g \cdot g_1 = 0\}$ or $\{(1+f) \cdot f_1 = 0, (1+g) \cdot g_1 = 0\}$ and $\deg(f_1 + g_1) \leq d-1$, but we shall not need to use it here. Clearly, $\mathcal{AI}(h_n) = \mathcal{AI}(h'_n)$. Lemma 4 immediately implies the next result.

Lemma 5. *We have $\mathcal{AI}(h_{n+1}) \geq \mathcal{AI}(h_n)$.*

We next bound the algebraic immunity from below.

Theorem 4. *We have*

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

Proof. We show that, if $h \cdot g = 0$ or $(h+1) \cdot g = 0$ for $g \in B_n$ such that $\deg(g) \leq d = \lfloor \frac{n}{3} \rfloor$, then $g = 0$.

We first assume that $(h + 1) \cdot g = 0$. Let

$$g = \sum_{\substack{K \subseteq \{1,2,\ldots,n\} \\ |K| \leq d}} a_K \prod_{k \in K} x_k.$$

Then $g(x) = 0$, for any x such that $h(x) = 0$. We denote $a_\emptyset$ by a_0 and $a_{\{i_1,\ldots,i_k\}}$ by $a_{i_1 i_2 \ldots i_k}$.

Since $g(0,\ldots,0) = 0$, we have $a_0 = 0$. Since $g(0,1,0,\ldots,0) = 0$ then $a_2 = 0$. Similarly, we have $a_3 = \ldots = a_n = 0$. Since $g(0,0,1,1,0,\ldots,0) = 0$ then $a_{34} = 0$. Similarly, we have $a_{35} = \ldots = a_{n-1,n} = 0$.

In general, let $wt(x) = i$, $x_1 = x_2 = \ldots = x_i = 0$ and $x_{s_1} = x_{s_2} = \ldots = x_{s_i} = 1$, where $i+1 \leq s_1 < s_2 < \ldots < s_i \leq n$. Then $h(x) = x_i = 0$. Therefore, $g(x) = 0$; moreover, $g(y) = 0$ for every $y \preceq x$; then $a_{s_1,s_2,\ldots,s_i} = 0$. Hence, we obtain

$$\begin{aligned} g(x) &= a_1x_1 \\ &+ a_{12}x_1x_2 + \cdots + a_{1n}x_1x_n + a_{23}x_2x_3 + \cdots + a_{2n}x_2x_n \\ &\qquad \text{(i.e. the degree 2 terms containing } x_1 \text{ or } x_2) \\ &+ a_{123}x_1x_2x_3 + \cdots + a_{3,n-1,n}x_3x_{n-1}x_n \\ &\qquad \text{(i.e. the degree 3 terms containing } x_1, x_2, \text{ or } x_3) \\ &+ \cdots \\ &+ a_{12\ldots d}x_1x_2\cdots x_d + \cdots + a_{d,n-d+2,\ldots,n}x_dx_{n-d+2}\cdots x_n. \\ &\qquad \text{(i.e. the degree n terms containing } x_1, \text{ or } x_2, \ldots, \text{ or } x_d) \end{aligned}$$

The following Claims 2–4 will prove that all these coefficients of g must be 0. In the proof, the following Claim 1 will be frequently used.

Claim 1: For $k \geq 1$; $i > k$ and $i+1 \leq s_1 < s_2 < \ldots < s_{i-1} \leq n$, we have

$$a_{k,s_1,s_2,\ldots,s_{i-1}} = \sum_{\substack{|J|=k-1 \\ J \subseteq \{s_1,\ldots,s_{i-1}\}}} a_{k,J}.$$

In particular, $a_{13} = \ldots = a_{1n} = a_{134} = \ldots = a_{1,n-d+2,\ldots,n} = a_1$.

Proof: Since $g(1,0,1,0,\ldots 0) = 0$, we have $a_{13} = a_1$. Similarly, $a_{14} = \ldots = a_{1n} = a_1$. In general, let $wt(x) = i > 1$, $x_1 = x_{s_1} = x_{s_2} = \ldots = x_{s_{i-1}} = 1$, where $i+1 \leq s_1 < s_2 < \ldots < s_{i-1} \leq n$. Then $h(x) = x_i = 0$. Therefore, $g(x) = 0$ and by induction, $a_{1,s_1,s_2,\ldots,s_{i-1}} = a_1 + a_{1,s_1} + \cdots + a_{1,s_{i-1}} + a_{1,s_1,s_2} + \cdots + a_{1,s_{i-2},s_{i-1}} + \cdots + a_{1,s_2,\ldots,s_{i-1}} = a_1 + a_1 + \cdots + a_1 = a_1$, since $\binom{i-1}{0} + \binom{i-1}{1} + \cdots + \binom{i-1}{i-2} = 2^{i-1} - 1$. Consider $x = (0,1,0,1,1,0,\ldots,0)$. Then $h(x) = x_3 = 0$. Therefore, $g(x) = 0$ and $a_{245} = a_{24} + a_{25}$. In general, let $wt(x) = i > 2$, $x_2 = x_{s_1} = x_{s_2} = \ldots = x_{s_{i-1}} = 1$, where $i+1 \leq s_1 < s_2 < \ldots < s_{i-1} \leq n$. Then $h(x) = x_i = 0$. Therefore, $g(x) = 0$ and by induction, $a_{2,s_1,s_2,\ldots,s_{i-1}} = a_{2,s_1} + a_{2,s_2} + \cdots + a_{2,s_{i-1}} + a_{2,s_1,s_2} + \cdots + a_{2,s_{i-2},s_{i-1}} + \cdots + a_{2,s_2,\ldots,s_{i-1}} = a_{2,s_1} + \cdots + a_{2,s_{i-1}}$, since $a_{2,s_1,s_2,\ldots,s_j} + \cdots + a_{2,s_{i-j},\ldots,s_{i-1}} = \binom{i-2}{j-1}(a_{2,s_1} + \cdots + a_{2,s_{i-1}})$ and $\binom{i-2}{0} + \binom{i-2}{1} + \cdots + \binom{i-2}{i-3} = 2^{i-2} - 1$. In general, let $wt(x) = i > k$, $x_k = x_{s_1} = x_{s_2} = \ldots = x_{s_{i-1}} = 1$, where $i+1 \leq s_1 < s_2 < \ldots < s_{i-1} \leq n$. Then $h(x) = x_i = 0$. Therefore, $g(x) = 0$ and by induction the claim follows.

Claim 2: For $1 \leq k \leq d$ and $d+1 \leq s_1 < s_2 < \ldots < s_{k-1} \leq n$, we have $a_{k,s_1,s_2,\ldots,s_{k-1}} = 0$. That is, $a_1 = a_{2,d+1} = \cdots = a_{2,n} = a_{3,d+1,d+2} = \cdots = a_{d,n-d+2,\ldots,n} = 0$.

Proof: For $k = 1$, consider $x = (1,0,\ldots,0,1\ldots,1)$ such that $wt(x) = d+1$ and $x_{n-d+1} = \ldots = x_n = 1$. Since $d = \lfloor \frac{n}{3} \rfloor$, we have $d+1 < n-d$. Then we have $h(1,0,\ldots,0,1,\ldots,1) = x_{d+1} = 0$ and therefore $g(1,0,\ldots,0,1,\ldots,1) = 0$. That is, $a_1 + a_{1,n-d+1} + \cdots + a_{1n} + a_{1,n-d+1,n-d+2} + \cdots + a_{1,n-d+2,\ldots,n} = 0$. Then by Claim 1, $a_1 = 0$. For $k = 2$, consider the points $(0,1,0,\ldots,0,1,\ldots,1)$ and $(0,1,0,\ldots,0,1,\ldots,1,0)$ with

weight $d+1$. Clearly, $h(x)=0$ at these two points. Then $g(x)=0$, and by Claim 1 we have $a_{2,n-d+1}+\cdots+a_{2,n}=a_{2,n-d}+\cdots+a_{2,n-1}$. That is, $a_{2,n-d}=a_{2,n}$. Similarly, we have $a_{2,d+1}=a_{2,d+2}=\ldots=a_{2,n}$. Let $d<w\leq n$ and $w-1$ be odd. Consider a point $(x_1,x_2,\ldots,x_n)$ of weight w satisfying $x_2=1$, $x_w=0$ and $x_{t_1}=x_{t_2}=\ldots=x_{t_{w-1}}=1$, where $d+1\leq t_1<t_2<\ldots<t_{w-1}\leq n$. Then $g(x_1,\ldots,x_n)=0$ and $a_{2,t_1}=0$. For $2<k\leq d$, consider all those points $(x_1,x_2,\ldots,x_n)$ of weight $d+1$ satisfying $x_k=1$ and $x_{t_1}=x_{t_2}=\ldots=x_{t_d}=1$, where $n-2d+2\leq t_1<t_2<\ldots<t_d\leq n$. Clearly, $h(x)=0$ at all these points, since $d+1<n-2d+2$ (i.e. $3d\leq n$). Therefore, $g(x)=0$ and we get a system of equations. Then by Claim 1 we have $a_{k,n-2d+2,n-2d+3,\ldots,n-2d+k}=\ldots=a_{k,n-k+2,n-k+3,\ldots,n}$ (in fact, we get a system of $\binom{2d-1}{d}$ equations with $\binom{2d-1}{k-1}$ variables; in particular, taking $k=d$, we get a system of $\binom{2d-1}{d}$ equations with $\binom{2d-1}{d-1}$ variables. It is easy to verify that the system has at most two solutions $(0,0,\ldots,0)$ and $(1,1,\ldots,1)$). Then we can deduce easily that $a_{k,d+1,\ldots,d+k-1}=\ldots=a_{k,n-k+2,n-k+3,\ldots,n}$. Let $d\leq w<n$ and $\binom{w-1}{k-1}$ be odd. Consider a point $(x_1,x_2,\ldots,x_n)$ of weight w satisfying $x_k=1$, $x_w=0$ and $x_{t_1}=x_{t_2}=\ldots=x_{t_{w-1}}=1$, where $d+1\leq t_1<t_2<\ldots<t_{w-1}\leq n$. Then $g(x_1,\ldots,x_n)=0$ and $a_{k,t_1,t_2,\ldots,t_{k-1}}=0$, and the claim follows.

Claim 3: For $2\leq k\leq d$ and $r<k$, we have $a_{r,k,s_1,\ldots,s_{k-2}}=a_{r,k}=0$, where $d+1\leq s_1<\ldots<s_{k-2}\leq n$.

Proof: Similar to Claim 1, for $2\leq k\leq d$ and $r<k$, we have

$$a_{r,k,s_1,s_2,\ldots,s_{i-2}}=a_{r,k}+\sum_{\substack{|J|=k-2\\ J\subseteq\{s_1,\ldots,s_{i-2}\}}}a_{r,k,J},$$

where $i>k$ and $i+1\leq s_1<s_2<\ldots<s_{i-1}\leq n$. For $k=2$, consider $x=(1,1,0,\ldots,0,1,\ldots,1)$ such that $wt(x)=d+1$ and $x_{n-d+2}=\ldots=x_n=1$. Then $g(x)=0$ and $a_{12}+a_{1,2,n-d+2}+\cdots+a_{1,2,n}+a_{1,2,n-d+2,n-d+3}+\cdots+a_{1,2,n-d+3,\ldots,n}=a_{12}+a_{12}+\ldots+a_{12}=a_{12}=0$. For $2<k\leq d$, similar to the proof of Claim 2, we can deduce the result.

Claim 4: Let $1\leq u\leq d-1$. By induction, for $u+1\leq k\leq d$ and $0<r_1<\ldots<r_u<k$, we have $a_{r_1,\ldots,r_u,k,s_1,\ldots,s_{k-u-1}}=a_{r_1,\ldots,r_u,k}=0$, where $d+1\leq s_1<s_2<\ldots<s_{k-u-1}\leq n$.

Proof: Similar to Claim 1, we have

$$a_{r_1,\ldots,r_u,k,s_1,s_2,\ldots,s_i}=a_{r_1,\ldots,r_u,k}+\sum_{\substack{|J|=k-u-1\\ J\subseteq\{s_1,\ldots,s_i\}}}a_{r_1,\ldots,r_u,k,J},$$

where $i>k-u-1$ and $d+1\leq s_1<s_2<\ldots<s_{i-1}\leq n$. Consider $x=(x_1,\ldots,x_n)$ such that $wt(x)=d+1$, $x_1=\cdots=x_{u+1}=1$ and $x_{n-d+u+1}=\ldots=x_n=1$. Then $g(x)=0$ and by induction, $a_{1,\ldots,u+1}+a_{1,\ldots,u+1,n-d+u+1}+\cdots+a_{1,\ldots,u+1,n}+a_{1,\ldots,u+1,n-d+u+1,n-d+u+2}+\cdots+a_{1,\ldots,u+1,n-d+u+2,\ldots,n}=a_{1,\ldots,u+1}+a_{1,\ldots,u+1}+\ldots+a_{1,\ldots,u+1}=a_{1,\ldots,u+1}=0$. For $u+1<k\leq d$, similar to the proof of Claim 2, we can deduce the result.

Therefore, for $u+1\leq k\leq d$ and $0<r_1<\ldots<r_u<k$, we have $a_{r_1,\ldots,r_u,k,s_1,\ldots,s_i}=0$, where $i\geq k-u-1$ and $d+1\leq s_1<s_2<\ldots<s_i\leq n$. That is, $g=0$ and $h+1$ has no annihilator of degree at most d.

Now consider $h\cdot g=0$. Let $\tilde{h}(x_1,\ldots,x_n)=h(x_1+1,x_2+1,\ldots,x_n+1)$. It is easy to verify that $\tilde{h}(x_1,\ldots,x_n)=h(x_{n-1},x_{n-2},\ldots,x_1,x_n)+1$. By the above proof,

Table 1: Algebraic Immunity of the HWBF

n	6	7	8	9	10	11	12	13	14	15
$\mathcal{AI}$	3	3	4	4	4	5	5	5	5	6

Table 2: Behavior of the HWBF against Fast Algebraic Attacks

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

$\tilde{h}(x_1,\ldots,x_n)$ has no annihilator of degree at most d. Therefore, $h(x_1,\ldots,x_n)$ has no annihilator of degree at most d, and the result follows. □

In Table 1, we give the exact algebraic immunity of the n-variable HWBF, for $6 \leq n \leq 15$.

Next, we investigate the normality of the HWBF.

Theorem 5. *The HWBF $h \in B_n$ is a $\lfloor \frac{n}{2} \rfloor$-normal function.*

Proof. Let $x \in \mathbb{F}_2^n$ and $x_1 = x_2 = \ldots = x_{\lceil \frac{n}{2} \rceil} = 0$. Then $wt(x) \leq n - \lceil \frac{n}{2} \rceil \leq \lceil \frac{n}{2} \rceil$, and $h(x) = 0$. Let $E_1 = \{(0,\ldots,0,x_{\lceil \frac{n}{2} \rceil+1},\ldots,x_n)\}$. It is a $\lfloor \frac{n}{2} \rfloor$-dimensional subspace of $\mathbb{F}_2^n$. Clearly, $h|_{E_1} = 0$, and h is an $\lfloor \frac{n}{2} \rfloor$-normal function. □

Resistance to fast algebraic attacks.
Let $\deg(g_1) = d < \mathcal{AI}(h)$ and $h \cdot g_1 = g_2$. 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 $\deg(g_1) + \deg(g_2) \geq n$ for any g_1 of degree less than $\mathcal{AI}(h)$. Let $\deg(g_2) = e$. For $6 \leq n \leq 13$, in Table 2, we give the lowest possible values of (d,e), which seems to be quite acceptable.

There are some other variants of algebraic attacks. In [39], the authors introduced the higher order algebraic attack, with applications towards cryptanalysis of Carlet–Feng functions and rotation symmetric Boolean functions. However, those attacks do not work, since in practice the number of variables of the filter function is much less than the length of the LFSR. In [15], algebraic attacks on the augmented function are introduced, which are dependant on low-degree conditional equations. Given a Boolean function with a large number of variables and good algebraic immunity, it is hard to find a low-degree equation. Therefore, higher order algebraic attacks and algebraic attacks on the augmented function can not pose a security threat to the HWBF.

Table 3: Algebraic immunity and nonlinearity of some randomly selected 10-variable Boolean functions

$\mathcal{AI}$	5	5	5	5	5	5	5	5	5	5	5	5
nl	458	452	456	448	452	466	462	456	450	442	462	458

Summary of the features of the function:. While the HWBF is as simple as a symmetric function (in the sense that the complexity of computing the output of HWBF is almost as low as for a symmetric function), its BDD size is considerably higher, which has an interest for cryptography. Symmetric functions are considered dangerous by the cryptographic community, since an attacker could, in theory, use the symmetry property. In fact, an n variable symmetric Boolean function has a BDD of size $O(n^2)$ [19], and therefore is weak against BDD-based attacks. Moreover, many symmetric functions are not balanced and there is no even-variable balanced symmetric function with optimum algebraic immunity for $n \geq 4$. The nonlinearity of the HWBF is similar to that of a symmetric function with optimum algebraic immunity. It does not have the weakness of a symmetric function but it has the same nice quality of being efficiently implementable in hardware, which allows taking n much larger, thus increasing the strength of its cryptographic properties.

Comparing with a randomly selected balanced Boolean function, the algebraic immunity and nonlinearity of this function may be low. In fact, when $n = 10$, $\mathcal{AI}(h) = 4$ and $nl(h) = 372$. We can generate 128 pseudo random different integers between 1 and 256 and get a Boolean function whose truth table has the value 1 in these 128 positions. Using this method, we generated 64 randomly selected balanced Boolean functions. All these functions have the optimum algebraic immunity 5 and their nonlinearities are between 442 and 466. Algebraic immunity and nonlinearity of the first 12 generated functions can be found in Table 3. It is known that most of Boolean functions have almost optimal algebraic immunity and a nonlinearity close to $2^{n-1} - 2^{n/2-1}\sqrt{2n \ln 2}$ [32], for n large enough. As a comparison, the nonlinearity of HWBF is only around $2^{n-1} - 2^{n-1}\sqrt{\frac{2}{\pi n}}$, quite far away from that number.

For the same number of variables n, the algebraic immunity and nonlinearity of the HWBF are certainly lower than for other optimal functions, such as the Carlet–Feng function [7]. However, since the HWBF is very simple and can be implemented efficiently in hardware (which is the most important framework for us, since LFSR are better suited for hardware implementation), we can use the HWBF with many more variables. In fact, the time complexity of computing the output to the Carlet–Feng function is similar to the complexity of computing the discrete log, which requires exponential time when viewed asymptotically, e.g. using the index calculus method [9], the time complexity is $O(\exp((1.587 + O(1))n^{1/3}(\ln n)^{2/3}))$, while the output of the HWBF can be computed only in linear time (in fact, the number of ones can even be counted in logarithmic time using the parallel algorithm [18]). As for the space complexity, using Pohlig–Hellman method, the 20-variable Carlet–Feng function allows computing one output bit per cycle with more than 1000 half-adders and full-adders. In comparison, the 64-variable HWBF allows computing one output bit with only $2^6 - 1 = 63$ half-adders and $2^6 - 6 - 1 = 57$ full-adders [16]. Therefore, by the time and space complexity, we compare the 16-variable Carlet–Feng function with the 256-variable HWBF and give an example as follows.

Example 1: Let $f_c \in B_{16}$ be the Carlet–Feng function discussed by [37]. Then $\deg(f_c) = 15$, $\mathcal{AI}(f_c) = 8$ and $nl(f_c) = 32530$. Let $\widetilde{h} = h_{256} + x_{257}x_{258} + x_{259}x_{260} + x_{261}x_{262} + x_{263}x_{264} + x_{265}x_{266} + x_{267}x_{268} + x_{269}x_{270} + x_{271}x_{272}$ (we take this function $\widetilde{h}$, since its efficiency of the implementation is similar to that of h_{256}, while it has better cryptographic properties). Then $\deg(\widetilde{h}) = 255$, $\mathcal{AI}(\widetilde{h}) \geq \mathcal{AI}(h) \geq 86$ and $nl(\widetilde{h}) = 2^{271} - 2^9\binom{254}{127}$ (it should be noted that the resistance to the fast algebraic attack of $\widetilde{h}$ is also better than that of h since if $\widetilde{h} * g_1 = g_2$, then $h * g_1 = g_2 + (x_{257}x_{258} + x_{259}x_{260} + x_{261}x_{262} + x_{263}x_{264} + x_{265}x_{266} + x_{267}x_{268} + x_{269}x_{270} + x_{271}x_{272}) * g_1)$. 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 [26]. The algebraic attack has an on-line complexity proportional to $N^{\omega \mathcal{AI}(f)}$, where N is the length of the register and $\omega \approx 2.37$ (see e.g. [17]). Therefore, the bias of f_c is $\epsilon = 0.0036$, while the bias of $\widetilde{h}$ is $\epsilon = 0.0001$. As for the algebraic attack, f_c has an on-line complexity proportional to $N^{18.96}$, while the algebraic attack on $\widetilde{h}$ has an on-line complexity proportional to $N^{203.82}$. Moreover, for any ordering of variables, $BDD(\widetilde{h}) > 2^{51}$ [19], while $BDD(f_c) < 2^{15}$. Therefore, the cryptographic properties of $\widetilde{h}$ are much better than those of f_c.

Concerning the resistance to fast algebraic attacks, it is more difficult to make comparisons since the known algorithms do not allow investigating large enough values of n; however, it seems most probable that the HWBF function in a large number of variables allows better resistance than the other known functions with good algebraic immunity.

4. Conclusion

This paper investigates some cryptographic properties of the HWBF. To summarize, the HWBF is balanced, has optimum algebraic degree and satisfies strict avalanche criterion. The algebraic immunity is at least $\lfloor \frac{n}{3} \rfloor + 1$. The function seems to have quite acceptable behavior against fast algebraic attacks, as can be checked for small values of n. It also has a high BDD size. Since the HWBF can be implemented very efficiently, it can be used with a number of variables much larger than the other known functions with good algebraic immunity; this allows reaching very good cryptographic properties implying high resistance of the stream ciphers using it as a filter to the main attacks, and in the same time high speed of these ciphers. The HWBF is therefore a very good candidate for being used in the design of stream ciphers; indeed, very few functions have been found so far which can allow resistance to all the main known attacks, and except this one, none of them is very efficiently implementable.

Acknowledgment

The authors would like to thank Jeremie Detrey and Sylvain Guilley for their help in calculating the number of transistors necessary to implement the HWBF. Work by P.S. started during an enjoyable visit at Temasek Labs at National University of Singapore, while on a sabbatical research leave from his home institution. He would like to thank TL@NUS for the hospitality and great working conditions.

[1] A. Braeken, B. Preneel, On the algebraic immunity of symmetric Boolean functions, in: Progress in Cryptology, Indocrypt 2005, in: LNCS, vol. 3797, 2005, pp. 35–48.

[2] R. E. Bryant, On the Complexity of VLSI Implementations and Graph Representations of Boolean Functions with Application to Integer Multiplication, IEEE Transactions on Computers 40 (2) (1991), 205–213.
[3] C. Carlet, On the higher order nonlinearities of algebraic immune functions, in: Advances in Cryptology, CRYPTO 2006, in: LNCS, vol. 4117, 2006, pp. 584–601.
[4] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, pages 257–397, 2010. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
[5] C. Carlet, Comments on 'Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials, IEEE Transactions on Information Theory 57 (7) (2011), 4852–4853.
[6] C. Carlet, D.K. Dalai, K.C. Gupta, S. Maitra, Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, IEEE Transactions on Information Theory 52 (7) (2006), 3105–3121.
[7] C. Carlet, 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, in: LNCS, vol. 5350, 2008, pp. 425–440.
[8] C. Carlet, K. Feng, An Infinite Class of Balanced Vectorial Boolean Functions with Optimum Algebraic Immunity and Good Nonlinearity, in: IWCC 2009, In: LNCS, vol. 5557, 2009, pp. 1–11.
[9] D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two, IEEE Transactions on Information Theory 30 (4) (1984), 587–594.
[10] N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, in: Advances in Cryptology, CRYPTO 2003, in: LNCS, vol. 2729, 2003, pp. 176–194.
[11] N. Courtois, W. Meier, Algebraic attacks on stream ciphers with linear feedback, in: Advances in Cryptology, EUROCRYPT 2003, in: LNCS, vol. 2656, 2003, pp. 345–359.
[12] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, Elsevier–Academic Press, 2009.
[13] D. K. Dalai, K. C. Maitra, S. Maitra, Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity, in: 12th International Workshop, FSE 2005, in: LNCS, vol. 3557, 2005, pp. 98–111.
[14] D. K. Dalai, S. Maitra, S. Sarkar, Baisc theory in construction of Boolean functions with maximum possible annihilator immunity, Designs, Codes and Cryptography 40 (1) (2006), 41–58.
[15] S. Fischer, W. Meier, Algebraic Immunity of S-Boxes and Augmented Functions, in: 14th International Workshop, FSE 2007, in: LNCS, vol. 4593, 2007, pp. 366–381.
[16] S. Guilley. Hardware cost of a code. Online: http://perso.enst.fr/guilley/code_hw.pdf
[17] P. Hawkes, G. G. Rose, Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers, in: Advances in Cryptology, CRYPTO 2004, in: LNCS, vol. 3152, 2004, pp. 390–406.
[18] F. V. IV, New Algorithms for Computing Gröbner Bases, PhD thesis, Clemson University, 2011.
[19] D. E. Knuth, The Art of Computer Programming Volume 4, Fascicle 1: Bitwise tricks & techniques; Binary Decision Diagrams, Addison–Wesley Professional, 2009.
[20] M. Krause, BDD-Based Cryptanalysis of Keystream Generators, in: Advances in Cryptology, EUROCRYPT 2002, in: LNCS, vol. 1462, 2002, pp. 222–237.
[21] M. Krause and D. Stegemann, Reducing the space complexity of BDD-Based attacks on keystream generators, in: 13th International Workshop, FSE 2006, in: LNCS, vol. 4047, 2006, pp. 163–178.
[22] N. Li, W. F. Qi, Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity, in: Advances in Cryptology, ASIACRYPT 2006, in: LNCS, vol. 4284, 2006, pp. 84–98.
[23] N. Li, L. Qu, W. Qi, G. Feng, C. Li, D. Xie, On the construction of Boolean functions with optimal algebraic immunity, IEEE Transactions on Information Theory 54 (3) (2008), 1330–1334.
[24] M. S. Lobanov, Exact relation between nonlinearity and algebraic immunity, Discrete Mathematics and Applications, 16 (5) (2006), 453–460.
[25] W. Meier, E. Pasalic, C. Carlet, Algebraic attacks and decomposition of Boolean functions, in: Advances in Cryptology, EUROCRYPT 2004, in: LNCS, vol. 3027, 2004, pp. 474–491.
[26] W. Meier, O. Staffelbach, Fast correlation attacks on stream ciphers, in: Advances in Cryptology, EUROCRYPT 1988, in: LNCS 330, 1988, pp. 301-314.
[27] S. Mesnager, Improving the Lower Bound on the Higher Order Nonlinearity of Boolean Functions With Prescribed Algebraic Immunity, IEEE Transactions on Information Theory 54 (8) (2008), 3656–3662.
[28] E. Pasalic, Almost fully optimized infinite classes of Boolean functions resistant to (fast) algebraic

cryptanalysis, in: Information Security and Cryptology-ICISC 2008, in: LNCS, vol. 5461, 2009, pp. 399–414.
[29] J. Peng, Q. Wu, H. Kan, On Symmetric Boolean Functions With High Algebraic Immunity on Even Number of Variables, IEEE Transactions on Information Theory 57 (10) (2011), 7205–7220.
[30] L. Qu, K. Feng, F. Liu, L. Wang, Constructing symmetric Boolean functions with maximum algebraic immunity, IEEE Transactions on Information Theory 55 (5) (2009), 2406–2412.
[31] P. Rizomiliotis, On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation, IEEE Transactions on Information Theory 56 (8) (2010), 4014–4024.
[32] F. Rodier, Asymptotic nonlinearity of Boolean functions, Designs, Codes and Cryptography 40 (1) (2006), 59–70.
[33] O. S. Rothaus, On bent functions, Journal of Combinatorial Theory, Series A 20 (3) (1976), 300–305.
[34] Y. Shaked, A. Wool, Cryptanalysis of the Bluetooth E0 Cipher Using OBDD's, in: ISC 2006, in: LNCS, vol. 4176, 2006, pp. 187–202.
[35] D. Stegemann, Extended BDD-Based Cryptanalysis of Keystream Generators, in: SAC 2007, in: LNCS, vol. 4876, 2007, pp. 17–35.
[36] C. Tan, S. Goh, Several classes of even-variable balanced Boolean functions with optimal algebraic immunity, IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences E94.A (1) (2011), 165–171.
[37] D. Tang, C. Carlet, X. Tang, Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks, IEEE Transactions on Information Theory 59 (1) (2013), 653–664.
[38] Z. Tu, Y. Deng, A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity, Designs, Codes and Cryptography 60 (1) (2011), 1–14.
[39] Q. Wang, T. Johansson, Higher Order Algebraic Attacks on Stream Ciphers, Cryptology ePrint Archive, 2012/013 [Online]. Available: eprint.iacr.org/2012/013.
[40] Q. Wang, T. Johansson, A note on fast algebraic attacks and higher order nonlinearities, in: Information Security and Cryptology-INSCRYPT 2010, in: LNCS, vol. 6584, 2011, pp. 84–98.
[41] Q. Wang, J. Peng, H. Kan, X. Xue, Constructions of cryptographically significant Boolean functions using primitive polynomials, IEEE Transactions on Information Theory 56 (6) (2010), 3048–3053.
[42] Q. Wang, C. H. Tan, Balanced Boolean functions with optimum algebraic degree, optimum algebraic immunity and very high nonlinearity, to appear in Discrete Applied Mathematics, doi: 10.1016/j.dam.2013.11.014.
[43] X. Zeng, C. Carlet, J. Shan, L. Hu, More balanced Boolean functions with optimal algebraic immunity, and good nonlinearity and resistance to fast algebraic attacks, IEEE Transactions on Information Theory 57 (9) (2011), 6310–6320.