A construction of Boolean functions with good cryptographic properties

Jong H. Chung[1], Pantelimon Stănică[1], Chik-How Tan[2], and Qichun Wang[2]

[1] Department of Applied Mathematics, Naval Postgraduate School,
Monterey, CA 93943–5216, USA [**]
{jhchung,pstanica}@nps.edu
[2] Temasek Laboratories, National University of Singapore, 117411, Singapore
{tslwq,tsltch}@nus.edu.sg

Abstract.
The two important qualities of a cipher is security and speed. Frequently, to satisfy the security of a Boolean function primitive, speed may be traded-off. In this paper we present a general construction that addresses both qualities. The idea of our construction is to manipulate a cryptographically strong base function and one of its affine equivalent functions, using concatenation and negation. We achieve security from the inherent qualities of the base function, which are preserved (or increased) and obtain speed by the simple Boolean operations. We present two applications of the construction to demonstrate the flexibility and efficiency of the construction.

1   Introduction

A stream cipher typically employs at least one Linear Feedback Shift Register (LFSR) to generate a secret key stream. Due to the linear nature of LFSR, the raw bits from LFSRs can not be used to encrypt a message, since the encrypted message is vulnerable to linear cryptanalysis and other forms of attacks. Therefore, the stream cipher filters an LFSR or combines multiple LFSRs to generate stronger secret key stream bits, via a Boolean function as a nonlinear filter or combiner, respectively. Two key factors in designing cryptographic Boolean functions are security and speed. We achieve security by having good measures in as many cryptographic properties as possible for the Boolean function in a cipher, such as balancedness to resist statistical attacks, high nonlinearity to address linear cryptanalysis on block ciphers (or correlation attacks on stream ciphers), high algebraic degree against algebraic attacks (although, this is not sufficient), high correlation immunity and resilience to deal with correlation attacks, and

---

[**] Current address for J.H. Chung: Department of Mathematical Sciences, United States Military Academy, West Point, NY

Report Documentation Page

1. REPORT DATE **2014**	2. REPORT TYPE	3. DATES COVERED **00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE **A construction of Boolean functions with good cryptographic properties**	5a. CONTRACT NUMBER
	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
International Journal Computer Mathematics (2014), 1-12.

14. ABSTRACT
The two important qualities of a cipher is security and speed. Frequently to satisfy the security of a Boolean function primitive, speed may be traded-o . In this paper we present a general construction that addresses both qualities. The idea of our construction is to manipulate a crypto- graphically strong base function and one of its a ne equivalent functions using concatenation and negation. We achieve security from the inher- ent qualities of the base function, which are preserved (or increased) and obtain speed by the simple Boolean operations. We present two applica- tions of the construction to demonstrate the exibility and e ciency of the construction.

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**	

high algebraic immunity to resist (fast) algebraic attacks. Speed is another important aspect in a cipher, since we desire fast encryption and decryption. For example, the Carlet-Feng function has good cryptographic properties, but it is not simple to generate, which may affect certain ciphers to underperform. Here we present some ideas to construct good cryptographic Boolean functions using a cryptographically strong base function, and three simple Boolean operations, namely concatenation, affine transformation, and negation. One of the significant benefits from this construction is the flexibility to choose an appropriate base function with known cryptographic properties (and we propose several such). This means we can customize our function, focusing on certain cryptographic properties. The other benefit is that our function is easy to construct due to the three previously mentioned basic operations.

The paper is organized as follows. In Section 2, the necessary background is established. We then present a construction of functions based on concatenation, affine transformation, and negation in Section 3. In Section 4, we give applications for our construction.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the binary field $\mathbb{F}_2$, and $\mathcal{B}_n$ the set of all n-variable Boolean functions defined on $\mathbb{F}_2^n$.

Any Boolean function $f \in \mathcal{B}_n$ 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, denoted by $\deg(f)$, is the number of variables in the highest order term with nonzero coefficients.

A Boolean function is *affine* if there exists no term of degree strictly greater than 1 in the ANF and the set of all affine functions is denoted by A_n. Let $f \in \mathcal{B}_n$ and E be any flat (that is, a coset of a vector subspace). If the restriction $f|_E$ of f to E is constant (respectively affine), then E is called a constant (respectively affine) flat for f.

Let

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

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 $f \in \mathcal{B}_n$. The *nonlinearity* of f is its distance from the set of all n-variable affine functions, i.e.,

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

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 $\frac{n}{2}$ [13].

A Boolean function $f \in \mathcal{B}_n$ 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 $g \in \mathcal{B}_n$ is called an *annihilator* of f if fg 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 $\lceil \frac{n}{2} \rceil$ [12].

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 [23]:

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

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 [11, 17]. The higher order nonlinearities of functions with high (fast) algebraic immunity is also not very low [6, 26, 37].

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

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

where $\mathbf{u} \in \mathbb{F}_2^n$ and $\mathbf{u} \cdot \mathbf{x}$ is an inner product, for instance, $\mathbf{u} \cdot \mathbf{x} = u_1 x_1 + u_2 x_3 + \cdots + u_n x_n$, where $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{x} = (x_1, \ldots, x_n)$. A function f is said to be resilient of order r if $W_f(\mathbf{u}) = 0$, for $0 \leq wt(\mathbf{u}) \leq r$. 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

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

The autocorrelation function of $f \in \mathcal{B}_n$ is defined by

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

Also, f satisfies the strict avalanche criterion (SAC) if $C_f(\mathbf{a}) = 0$, for $wt(\mathbf{a}) = 1$.

We say that $f, g \in \mathcal{B}_n$ are affine equivalent if there exists an $n \times n$ invertible matrix A over the finite field $\mathbb{F}_2$ and vectors $\mathbf{b}, \mathbf{c} \in \mathbb{F}_2^n$ such that $g(\mathbf{x}) = f(A\mathbf{x} + \mathbf{b}) + \mathbf{c} \cdot \mathbf{x}$. If f is a Boolean function in n variables and H is a flat (a coset of some vector subspace) in $\mathbb{F}_2^n$, we let $f|_H$ to be the (*restriction*) function $f|_H : H \to \mathbb{F}_2$ by $f|_H(\mathbf{x}) = f(\mathbf{x})$, for $\mathbf{x} \in H$.

3 The construction and its cryptographic properties

We next introduce a construction based on balanced functions $f_i \in \mathcal{B}_{n-2}$, $i = 1, 2$ (|| denotes concatenation).

Construction 1. For $\{i, j\} = \{1, 2\}$, we define the functions f on $\mathbb{F}_2^n$:

$$f = f_i || f_j || f_i || \bar{f}_j = x_{n-1} x_n + x_{n-1}(f_i + f_j) + f_i,$$

which is affine equivalent to $f_i || f_j || \bar{f}_i || f_j; \ f_i || \bar{f}_j || f_i || f_j; \ \bar{f}_i || f_j || f_i || f_j;$

$$f = f_i || f_j || f_j || \bar{f}_i = x_{n-1} x_n + x_{n-1}(f_i + f_j) + x_n(f_i + f_j) + f_i,$$

which is affine equivalent to $f_i || f_j || \bar{f}_j || f_i; \ f_i || \bar{f}_j || f_j || f_i; \ \bar{f}_i || f_j || f_j || f_i.$

We could have defined $f = f_i || f_j || \bar{f}_i || \bar{f}_j = x_{n-1}(f_i + f_j) + x_n + f_i$ to also fulfil resiliency, but, unfortunately, a few of the other properties get slightly weaker. Some of the cryptographic properties, like algebraic immunity, or strict avalanche criterion are not (fully) affine invariants, so we prefer to list all concatenations for completeness, but we shall prove our results motivating whenever necessary, the relevant differences between the various classes of functions.

Variations of this construction have appeared in literature and some of their properties have been investigated. Most notably, bent, resiliency and the normality properties of a concatenation (based upon bent functions) were looked at in [5, 8, ?], and the normality of $f_1 || f_2 || f_2 || \bar{f}_1$ for arbitrary f_i with $i = 1, 2$ is addressed in [16] (see also [29] for other properties). We will also prove the normality result later on for *all* these classes. We mention also the paper of Pasalic [27], which introduces the notion of *high degree product* ($\mathcal{HDP}$) to measure the ability of Boolean functions to be resistant to fast algebraic attacks: $f \in \mathcal{B}_n$ satisfies the $\mathcal{HDP}$ of order n if for any non-annihilating function g of degree e with $1 \leq e \leq \lceil n/2 \rceil - 1$, the degree $d = \deg(gf)$ satisfies $e + d \geq n$. Unfortunately, the construction of [27] based upon a four function concatenation does not always produce almost optimal $\mathcal{HDP}$ functions, and this was observed in [39].

We next generalize a known lemma that relates the Walsh–Hadamard coefficients of g (in some dimension) to the Walsh–Hadamard coefficients of its 2^r ($r \geq 1$) concatenation parts.

Lemma 1 *If* $g(\mathbf{x}, x_{n+1}, \ldots, x_{n+r}) = f_1(\mathbf{x}) || f_2(\mathbf{x}) || \cdots || f_{2^r}(\mathbf{x}) = \overset{2^r}{\underset{i=1}{||}} f_i(\mathbf{x})$, *then*

$$W_g(\mathbf{u}, u_{n+1}, \ldots, u_{n+r})$$
$$= W_{f_1}(\mathbf{u}) + (-1)^{u_{n+1}} W_{f_2}(\mathbf{u}) + \cdots + (-1)^{u_{n+1} + \cdots + u_{n+r}} W_{f_{2^r}}(\mathbf{u})$$
$$= \sum_{k=1}^{2^r} (-1)^{\mathbf{a}(k) \cdot \mathbf{u}'} W_{f_k}(\mathbf{u}),$$

where $r \in \mathbb{N}$, $\mathbf{a}(k)$ *is the kth lexicographically ordered vector in* $\mathbb{F}_2^r$, *and* $\mathbf{u}' = (u_{n+1}, \ldots, u_{n+r})$.

Proof. We show our result by induction on r. If $r = 1$, we compute

$$W_g(\mathbf{u}, u_{n+1}) = \sum_{(\mathbf{x}, x_{n+1}) \in \mathbb{F}_2^{n+1}} (-1)^{g(\mathbf{x}, x_{n+1}) + \mathbf{u} \cdot \mathbf{x} + u_{n+1} x_{n+1}}$$

$$= \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g_1(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}} + (-1)^{u_{n+1}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g_2(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}}$$

$$= W_{g_1}(\mathbf{u}) + (-1)^{u_{n+1}} W_{g_2}(\mathbf{u}).$$

In general, assuming that $W_g(\mathbf{u}, u_{n+1}, \ldots, u_{n+r}) = \sum_{k=1}^{2^r} (-1)^{\mathbf{a}(k) \cdot \mathbf{u}'} W_{f_k}(\mathbf{u})$,

then for $g''(\mathbf{x}, x_{n+1}, \ldots, x_{n+r+1}) = f_1(\mathbf{x}) \| f_2(\mathbf{x}) \| \cdots \| f_{2^{r+1}}(\mathbf{x}) = g \| g' = \overset{2^{r+1}}{\underset{i=1}{\|}} f_i(\mathbf{x})$,

where $g' = f_{2^r+1}(\mathbf{x}) \| f_{2^r+2}(\mathbf{x}) \| \cdots \| f_{2^{r+1}}(\mathbf{x})$, we have

$$W_{g''}(\mathbf{u}, u_{n+1}, \ldots, u_{n+r+1})$$

$$= W_g(\mathbf{u}, u_{n+1}, \ldots, u_{n+r}) + (-1)^{u_{n+r+1}} W_{g'}(\mathbf{u}, u_{n+1}, \ldots, u_{n+r})$$

$$= W_{f_1}(\mathbf{u}) + (-1)^{u_{n+1}} W_{f_2}(\mathbf{u}) + \cdots + (-1)^{u_{n+1} + \cdots + u_{n+r+1}} W_{f_{2^{r+1}}}(\mathbf{u})$$

$$= \sum_{k=1}^{2^{r+1}} (-1)^{\mathbf{a}(k) \cdot \mathbf{u}'} W_{f_k}(\mathbf{u}),$$

which shows our claim. $\qquad\square$

Lemma 2 (Proposition 1 of [7]) *Let g_1, g_2 be two Boolean functions in the variables $x_1, \ldots, x_n$ with $\mathcal{AI}(g_1) = d_1, \mathcal{AI}(g_2) = d_2$, and let $g = (1 + x_{n+1})g_1 + x_{n+1}g_2 \in \mathcal{B}_{n+1}$. Then, the following hold:*

1. *If $d_1 \neq d_2$, then $\mathcal{AI}(g) = \min\{d_1, d_2\} + 1$.*
2. *If $d_1 = d_2 (=: d)$, then $d \leq \mathcal{AI}(g) \leq d + 1$. Further, $\mathcal{AI}(g) = d$ if and only if there exists $f_1, f_2 \in \mathcal{B}_n$ of algebraic degrees d that either both annihilate g_1, g_2, or both annihilate $\bar{g}_1, \bar{g}_2$, and $\deg(f_1 + f_2) \leq d - 1$.*

For our next result, we let $f_1 \in \mathcal{B}_{n-2}$ in Construction 1 be any balanced function and $f_2(\mathbf{x}) = f_1(A\mathbf{x} + \mathbf{b})$, where A is an $(n - 2)$ by $(n - 2)$ invertible matrix over the finite field $\mathbb{F}_2$ and $\mathbf{b}$ is an $(n - 2)$ dimensional vector over $\mathbb{F}_2$. Clearly, f_1 and f_2 are affine equivalent, $\deg(f_1) = \deg(f_2)$, $\mathcal{AI}(f_1) = \mathcal{AI}(f_2)$ and $nl(f_1) = nl(f_2)$.

Theorem 3 *Let f be given by Construction 1, with f_1, f_2 nonconstant and affine equivalent. Then f is balanced, $\deg(f) = \max\{\deg(f_1), \deg(f_1 + f_2) + 1\}$, $\mathcal{AI}(f_1) + 2 \geq \mathcal{AI}(f) \geq \min\{\mathcal{AI}(f_1\|f_2), \mathcal{AI}(f_1\|\bar{f}_2)\} \geq \mathcal{AI}(f_1)$. Moreover, $nl(f) = 2^{n-2} + 2nl(f_1)$.*

Proof. We take $f = f_1 \| f_2 \| f_1 \| \bar{f}_2$ as an example (the other cases equivalent to this one in Construction 1 are similar). Clearly, $\deg(f) = \deg(f_1 \| f_2) = \max\{\deg(f_1), \deg(f_1 + f_2) + 1\}$. Since $f_1 \| f_2$ is affine equivalent to $f_1 \| \bar{f}_2$ (precisely, $(f_1 \| \bar{f}_2)(\mathbf{x}) = (f_1 \| f_2)(\mathbf{x}) + x_n$) we have $|\mathcal{AI}(f_1 \| f_2) - \mathcal{AI}(f_1 \| \bar{f}_2)| \leq 1$ (by

[7, Lemma 1]). If $\mathcal{AI}(f_1||f_2) = \mathcal{AI}(f_1||\bar{f}_2)$, by Lemma 2, $\mathcal{AI}(f) \geq \mathcal{AI}(f_1||f_2) \geq \mathcal{AI}(f_1)$. If $|\mathcal{AI}(f_1||f_2) - \mathcal{AI}(f_1||\bar{f}_2)| = 1$, then Lemma 2 shows that $\mathcal{AI}(f) = \min\{d, d+1\} + 1 = d + 1$, where $\min\{\mathcal{AI}(f_1||f_2), \mathcal{AI}(f_1||\bar{f}_2)\} = d$.

If $f = f_1||f_2||f_2||\bar{f}_1$ (the other cases equivalent to this one in Construction 1 are similar), then $\deg(f) = \max\{\deg(f_1||f_2), \deg((f_1 + \bar{f}_2)||(f_2 + \bar{f}_1)) + 1\}$, and since $\deg((f_1 + \bar{f}_2)||(f_2 + \bar{f}_1)) = \max\{\deg(f_1 + \bar{f}_2), \deg(f_1 + \bar{f}_2 + f_2 + \bar{f}_1) + 1\} = \max\{\deg(f_1 + \bar{f}_2), 1\} \leq \deg(f_1)$, we get that $\deg(f) = \deg(f_1||f_2) = \max\{\deg(f_1), \deg(f_1 + f_2) + 1\}$, in this case, as well. The algebraic immunity computation does not change in this case.

To find the nonlinearity, we first consider $f = f_1||f_2||f_1||\bar{f}_2$ of Construction 1 (the others are similar). Using Lemma 1, we obtain

$$\begin{aligned}
W_f(\mathbf{u}, u_{n-1}, u_n) &= W_{f_1}(\mathbf{u}) + (-1)^{u_{n-1}} W_{f_2}(\mathbf{u}) \\
&\quad + (-1)^{u_n} W_{f_1}(\mathbf{u}) + (-1)^{u_{n-1}+u_n} W_{\bar{f}_2}(\mathbf{u}) \\
&= (1 + (-1)^{u_n}) W_{f_1}(\mathbf{u}) + (-1)^{u_{n-1}} (1 - (-1)^{u_n}) W_{f_2}(\mathbf{u}).
\end{aligned}$$

Thus, $W_f(\mathbf{u}, u_{n-1}, 0) = 2W_{f_1}(\mathbf{u})$ and $W_f(\mathbf{u}, u_{n-1}, 1) = 2(-1)^{u_{n-1}} W_{f_2}(\mathbf{u})$. It follows that

$$\max_{(\mathbf{u}, u_{n-1}, u_n) \in \mathbb{F}_2^n} |W_f(\mathbf{u}, u_{n-1}, u_n)| = 2 \max_{\mathbf{u} \in \mathbb{F}_2^{n-2}} |W_{f_1}(\mathbf{u})| = 2^{n-1} - 4nl(f_1)).$$

Therefore, $nl(f) = 2^{n-2} + 2nl(f_1)$. $\qquad \square$

Remark 4 *In most cases,* $\deg(f_1(A\mathbf{x} + \mathbf{b}) + f_1) = \deg(f_1)$*. That is,* $\deg(f) = \deg(f_1)+1$*. As can be seen from Proposition 1 of [7], in many cases,* $\mathcal{AI}(f_1||f_2) = \mathcal{AI}(f_1)+1$*, and so,* $\mathcal{AI}(f) \geq \mathcal{AI}(f_1)+1$*. Further,* $nl(f)$ *is obviously higher than* $nl(f_1)$*. In fact, the fast correlation attack on* f *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 [24]. We have*

$$\frac{1}{2} - \frac{nl(f)}{2^n} = \frac{1}{2} - \frac{1}{4} - \frac{nl(f_1)}{2^{n-1}} = \frac{1}{2}\left(\frac{1}{2} - \frac{nl(f_1)}{2^{n-2}}\right),$$

that is, the bias of f *is half of the bias of* f_1*.*

Remark 5 *Using Proposition 1 of [27], we infer that if one takes* $f_1, f_2 \in \mathcal{B}_n$ *(n even) of maximum* $\mathcal{AI}$*, with the property that for any function* g *of algebraic degree* $1 \leq e \leq \lceil n/2 \rceil - 1$*, we have* $\deg(f_1 g) = d \geq \mathcal{AI}(f_1)$ *and* $e + d \geq n$*, then* $f = f_1||f_2||\bar{f}_1||f_2$ *has maximum* $\mathcal{AI}$*. Such functions* f_1 *are called* perfect *algebraic immune* $(\mathcal{PAI})$*. The authors of [22] showed (in their Theorem 7) that if* f_1 *is a balanced* $\mathcal{PAI}$ *then* $n = 2^k + 1$*, for some* k*; if* f_1 *is unbalanced, then* $n = 2^k$*, for some* k*.*

Next, we are concerned with normality issues of our construction. References [8, 16] contain secondary constructions of normal, or non-normal functions based upon some of the functions of Construction 1, namely $f_1||f_2||f_2||\bar{f}_1$, where f_i are bent or have some normality properties.

Theorem 6 *Let f_i, $f_j \in \mathcal{B}_{n-2}$. If f_i or f_j, whichever is not complemented in Construction 1, is k-normal, then the functions f of Construction 1 are at least $(k+1)$-normal.*

Proof. Due to the affine equivalence to f_i, f_j is k-normal. If f_i is invariant, say 0 on a k-dimensional flat, then $\bar{f}_i$ is constant and equal to 1 on the same flat, which shows that $\bar{f}_i$ is k-normal. We prove the case $f = f_i \| f_j \| f_i \| \bar{f}_j$ only, since other cases can be shown by similar arguments. We show the existence of a $(k+1)$-dimensional affine subspace where $f(\mathbf{x})$ is a constant. Let $\mathbf{z}_1, \ldots \mathbf{z}_k \in$ be k distinct, linearly independent vectors in $\mathbb{F}_2^{n-2}$, $\mathbf{d} = (d_1, d_2, \ldots, d_{n-2})$ be a vector in $\mathbb{F}_2^{n-2}$, and $a_i \in \mathbb{F}_2$ be for $1 \leq i \leq k$. We define a k-dimensional flat $G = \{\mathbf{x} \in \mathbb{F}_2^{n-2} \mid \mathbf{x} = a_1 \mathbf{z}_1 + a_2 \mathbf{z}_2 + \cdots + a_k \mathbf{z}_k + \mathbf{d}, \ a_i = \mathbb{F}_2, \ 1 \leq i \leq k\}$ such that $f_i|_G = 0$. We now construct a $(k+1)$-dimensional flat in the following way. Let $\mathbf{z}_l = (z_{l1}, z_{l2}, \ldots, z_{l(n-2)})$ where $1 \leq l \leq k$. We set $\mathbf{z}'_l = (z_{l1}, z_{l2}, \ldots, z_{l(n-2)}, 0, 0)$, $\mathbf{z}'_{k+1} = (0, \ldots, 0, 1)$, and $\mathbf{d}' = (d_1, d_2, \ldots, d_{n-2}, 0, 0)$ where $\mathbf{z}'_{k+1}$, $\mathbf{d}' \in \mathbb{F}_2^n$. Then $G' = \{\mathbf{x}' \in \mathbb{F}_2^n \mid \mathbf{x}' = a_1 \mathbf{z}'_1 + a_2 \mathbf{z}'_2 + \cdots + a_{k+1} \mathbf{z}'_{k+1} + \mathbf{d}', \ a_i = \mathbb{F}_2, \ 1 \leq i \leq k+1\}$. If a vector $\mathbf{x}' \in G'$ with $a_{k+1} = 0$, then f equals the first f_i in the construction. If a vector $\mathbf{x}' \in G'$ with $a_{k+1} = 1$, then f has the same value as the third f_i in the construction. Therefore, G' is a $(k+1)$-dimensional flat such that $f|_{G'} = 0$. $\square$

Generally, it is difficult to establish a proper limit to the normality of a function. Let f_i or f_j, whichever is not complemented in Construction 1, be k-normal but not $(k+1)$-normal, and we show that the function f of Construction 1 cannot have a constant function value on the $k+2$-dimensional flat $H = \{a_1 \mathbf{e}_{i_1} \oplus \cdots \oplus a_{k+2} \mathbf{e}_{i_{k+2}} \oplus \mathbf{d}\}$, where $\mathbf{d} = (y_1, \ldots y_n)$ is a fixed vector in $\mathbb{F}_2^n$ and $\mathbf{e}_{i_m} = (x_1, \ldots, x_n)$ is an elementary vector such that $x_j = 1$ if and only if $j = i_m$ with $1 \leq i_m \leq n$. We assume $f = f_i \| f_j \| f_i \| \bar{f}_j$, since the other cases can be shown by similar arguments. Let us also assume that H exists such that $f|_H$ is constant. We observe that y_{i_m} is irrelevant (whether it is 0 or 1) due to $\mathbf{e}_{i_m}$, so we set $\mathbf{d}$ with $y_{i_1} = \ldots = y_{i_{k+2}} = 0$. To illustrate better, we rewrite the restriction of our function to H as follows:

$$
\begin{aligned}
f(\mathbf{x})|_H &= (\bar{x}_{n-1} f_i \oplus x_{n-1} f_j) \| (\bar{x}_{n-1} f_i \oplus x_{n-1} \bar{f}_j) |_H \\
&= \bar{x}_n (\bar{x}_{n-1} f_i \oplus x_{n-1} f_j) \oplus x_n (\bar{x}_{n-1} f_i \oplus x_{n-1} \bar{f}_j) |_H \\
&= \bar{x}_{n-1} (\bar{x}_n f_i \oplus x_n f_i) \oplus x_{n-1} (\bar{x}_n f_j \oplus x_n \bar{f}_j) |_H \\
&= f_i \oplus x_{n-1} f_i \oplus x_{n-1} f_j \oplus x_{n-1} x_n |_H.
\end{aligned}
$$

Without loss of generality, we assume $f(\mathbf{x}) = 0$ for all $\mathbf{x} = (x_1, \ldots, x_n) \in H$, and we examine the following cases, depending upon the values of x_{n-1} and x_n.
Case 1: $n-1, n \notin \{i_1, i_2, \ldots, i_{k+2}\}$. Then $x_{n-1} = d_{n-1}$, and $d_n = x_n$. We observe that for all possible values for x_{n-1} and x_n, $f|_H$ is one of the functions, f_i, f_j, or $\bar{f}_j$. Since each function is only k-normal, there exists at least one $\mathbf{x} \in H$ such that $f(\mathbf{x})|_H = 1$, which is a contradiction.
Case 2: $n-1 \notin \{i_1, i_2, \ldots, i_{k+2}\}$ and $x_n \in \{i_1, i_2, \ldots, i_{k+2}\}$. Then $x_{n-1} = d_{n-1}$. If $x_{n-1} = 0$, then regardless of the value of x_n, $f|_H$ equals the function f_i. We note that we can only increase the normality to $k+1$ using x_n, since f_i is k-normal. Therefore, there exists at least one $\mathbf{x} \in H$ such that $f(\mathbf{x})|_H = 1$, which

is a contradiction. If $x_{n-1} = 1$, $f|_H$ equals the function f_j with $x_n = 0$ or $\bar{f}_j$ with $x_n = 1$. Clearly, $f|_H$ is at most k-normal, since $\bar{f}_j = f_j \oplus 1$. So, there exists at least one $\mathbf{x} \in H$ such that $f(\mathbf{x})|_H = 1$, which is a contradiction.

Case 3: $n \notin \{i_1, i_2, \ldots, i_{k+2}\}$ and $x_{n-1} \in \{i_1, i_2, \ldots, i_{k+2}\}$. Then $d_n = x_n$. If $x_n = 0$, then $f|_H$ equals the function, $f_i \| f_j$. Also, if $x_n = 1$, then $f|_H$ equals the function $f_i \| \bar{f}_j$. In both instances, we can only increase the normality to $k+1$, since f_i, f_j and $\bar{f}_j$ are k-normal.

Case 4: $x_{n-1}, x_n \in \{i_1, i_2, \ldots, i_{k+2}\}$. In this case $f|_H$ equals $f_i \| f_j \| f_i \| \bar{f}_j |_H$, and any two vectors $\mathbf{x}', \mathbf{x}'' \in H$ in the forms of $\mathbf{x}' = (a_1, \ldots, a_{n-2}, 1, 0)$ and $\mathbf{x}'' = (b_1, \ldots, b_{n-2}, 1, 1)$ with $a_i, b_i \in \mathbb{F}_2$, $1 \leq i \leq n-2$ have opposite function values. Therefore, we have a contradiction.

Under what conditions the functions of Construction 1 is exactly $(k+2)$-normal remains an open problem.

Theorem 7 *If the base functions f_1 and f_2 in Construction 1 satisfy the strict avalanche criterion, then f satisfies the strict avalanche criterion.*

Proof. For every vector $y \in \mathbb{F}_2^n$, write $\mathbf{y} = (\mathbf{y}', y_{n-1}, y_n)$ with $y' \in \mathbb{F}_2^{n-2}$. We shall show the claim in the case $f = f_1 \| f_2 \| f_1 \| \bar{f}_2$, as all the other possibilities are similar. Let $\mathbf{a} \in \mathbb{F}_2^n$ of weight $wt(\mathbf{a}) = 1$. We consider three cases.

Case 1. Take $\mathbf{a} = (0, \ldots, 0, 1)$. Then

$$
\begin{aligned}
f(\mathbf{x}) + f(\mathbf{x} + \mathbf{a}) &= (f_1 \| f_2)(\mathbf{x}', x_{n-1})\bar{x}_n + (f_1 \| \bar{f}_2)(\mathbf{x}', x_{n-1})x_n \\
&\quad + (f_1 \| f_2)(\mathbf{x}', x_{n-1})x_n + (f_1 \| \bar{f}_2)(\mathbf{x}', x_{n-1})\bar{x}_n \\
&= (f_1 \| f_2)(\mathbf{x}', x_{n-1}) + (f_1 \| \bar{f}_2)(\mathbf{x}', x_{n-1}) = 0_{2^{n-1}} \| 1_{2^{n-1}},
\end{aligned}
$$

hence balanced.

Case 2. Take $\mathbf{a} = (0, \ldots, 1, 0)$. Then

$$
\begin{aligned}
&f(\mathbf{x}) + f(\mathbf{x} + \mathbf{a}) \\
&= (f_1 \| f_2)(\mathbf{x}', \bar{x}_{n-1})\bar{x}_n + (f_1 \| \bar{f}_2)(\mathbf{x}', \bar{x}_{n-1})x_n \\
&\quad + (f_1 \| f_2)(\mathbf{x}', x_{n-1})\bar{x}_n + (f_1 \| \bar{f}_2)(\mathbf{x}', x_{n-1})x_n \\
&= f_1(\mathbf{x}')x_{n-1}\bar{x}_n + f_2(\mathbf{x}')\bar{x}_{n-1}\bar{x}_n + f_1(\mathbf{x}')x_{n-1}x_n + \bar{f}_2(\mathbf{x}')\bar{x}_{n-1}x_n \\
&\quad + f_1(\mathbf{x}')\bar{x}_{n-1}\bar{x}_n + f_2(\mathbf{x}')x_{n-1}\bar{x}_n + f_1(\mathbf{x}')\bar{x}_{n-1}x_n + \bar{f}_2(\mathbf{x}')x_{n-1}x_n \\
&= f_1(\mathbf{x}')\bar{x}_n + f_2(\mathbf{x}')\bar{x}_n + f_1(\mathbf{x}')x_n + \bar{f}_2(\mathbf{x}')x_n = f_1(\mathbf{x}') + f_2(\mathbf{x}') + x_n,
\end{aligned}
$$

which is balanced (regardless of whether $f_1 + f_2$ is balanced).

Case 3. Take $\mathbf{a} = (\mathbf{a}', 0, 0)$, with $wt(\mathbf{a}') = 1$. Write $\mathbf{x}' + \mathbf{a}' = \mathbf{x}''$. Then,

$$
\begin{aligned}
&f(\mathbf{x}) + f(\mathbf{x} + \mathbf{a}) \\
&= (f_1 || f_2)(\mathbf{x}', x_{n-1})\bar{x}_n + (f_1 || \bar{f}_2)(\mathbf{x}', x_{n-1})x_n \\
&\quad + (f_1 || f_2)(\mathbf{x}'', x_{n-1})\bar{x}_n + (f_1 || \bar{f}_2)(\mathbf{x}'', x_{n-1})x_n \\
&= f_1(\mathbf{x}')\bar{x}_{n-1}\bar{x}_n + f_2(\mathbf{x}')x_{n-1}\bar{x}_n + f_1(\mathbf{x}')\bar{x}_{n-1}x_n + \bar{f}_2(\mathbf{x}')x_{n-1}x_n \\
&\quad + f_1(\mathbf{x}'')\bar{x}_{n-1}\bar{x}_n + f_2(\mathbf{x}'')x_{n-1}\bar{x}_n + f_1(\mathbf{x}'')\bar{x}_{n-1}x_n + \bar{f}_2(\mathbf{x}'')x_{n-1}x_n \\
&= (f_1(\mathbf{x}') + f_1(\mathbf{x}''))\bar{x}_{n-1}\bar{x}_n + (f_2(\mathbf{x}') + f_2(\mathbf{x}''))x_{n-1}\bar{x}_n \\
&\quad + (f_1(\mathbf{x}') + f_1(\mathbf{x}''))\bar{x}_{n-1}x_n + (\bar{f}_2(\mathbf{x}') + \bar{f}_2(\mathbf{x}''))x_{n-1}x_n \\
&= (f_1(\mathbf{x}') + f_1(\mathbf{x}''))\bar{x}_{n-1} + (f_2(\mathbf{x}') + f_2(\mathbf{x}''))x_{n-1},
\end{aligned}
$$

which is balanced, since f_1, f_2 satisfy the strict avalanche criterion, and so, both $f_1(\mathbf{x}') + f_1(\mathbf{x}' + \mathbf{a}')$ and $f_2(\mathbf{x}') + f_2(\mathbf{x}' + \mathbf{a}')$ are balanced.

4 Two particular cases, based on the HWBF and Carlet-Feng function

In 2002, Krause [18] introduced another attack using Binary Decision Diagram (BDD). Later research [19, 33] showed the effectiveness of BDD-based attacks on stream ciphers (albeit, they generally require a large amount of memory). Krause notes that one of the effective ways to disrupt BDD-based attacks is for the Boolean function combiner of the stream cipher is to have a robust BDD. There are many constructions of Boolean functions with high algebraic immunity [1, 7, 9, 10, 14, 15, 20, 21, 28, 30–32, 34–36, 38, 40]. However, none of these papers (except for [38]) took BDD-based attacks into consideration. Interestingly, Bryant (see [2, 3]) showed that the Hidden Weighted Bit Function (HWBF) has exponential size BDD.

Below, we give more exact results on the cryptographic properties of functions in our construction if the base functions are variations of the hidden weighted bit function (HWBF), which is defined by

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

It is known [38] that $h_n \in \mathcal{B}_n$ is balanced, with the optimum algebraic degree, satisfying the strict avalanche criterion, $\max_{\mathbf{u} \in \mathbb{F}_2^n} |W_{h_n}(\mathbf{u})| = 4\binom{n-2}{\lceil \frac{n-2}{2} \rceil}$ and algebraic immunity $\mathcal{AI}(h_n) \geq \lfloor \frac{n}{3} \rfloor + 1$.

Let ϕ be the left-rotation symmetric operation on vectors of arbitrary dimension, say $\phi(x_1, x_2, \ldots, x_n) = (x_2, \ldots, x_n, x_1)$. It was shown previously in [38] that the hidden weighted bit (HWBF) function is a concatenation which can be iterated (write $\mathbf{x} = (x_2, \ldots, x_{n-2}) \in \mathbb{F}_2^{n-3}$), as shown in the next formula

$$
\begin{aligned}
h_n(x_1, \mathbf{x}, x_{n-1}, x_n) &= h_{n-1}(x_1, \mathbf{x}, x_{n-1}) || (h_{n-1} \circ \phi)(x_1, \mathbf{x}, x_{n-1}) \\
&= h_{n-2}(x_1, \mathbf{x}) || (h_{n-2} \circ \phi)(x_1, \mathbf{x}) || h_{n-2}(\mathbf{x}, x_{n-1}) || (h_{n-2} \circ \phi)(\mathbf{x}, x_{n-1}) \cdots .
\end{aligned} \tag{1}
$$

Theorem 8 *Let $n \geq 3$ and $f_1 || f_2 = h_{n-1}$ be an $(n-1)$–variables HWBF. Then, all of the functions f from Construction 1 are balanced of degree $\max\{n-2, 2\}$, have nonlinearity $nl(f) = 2^{n-1} - 4\binom{n-4}{\lceil(n-4)/2\rceil}$, and have algebraic immunity $\geq \lfloor \frac{n+2}{3} \rfloor$.*

Proof. Certainly, all functions in Construction 1 are balanced. Furthermore, for any concatenation $g_1 || g_2$, the degree $\deg(g_1 || g_2) = \max\{\deg(g_1), \deg(g_1 + g_2) + 1\}$. Thus, since $\deg(f_1 || f_2) = \deg(h_{n-1}) = n - 2$, we obtain

$$\deg(f_1 || f_2 || f_1 || \bar{f}_2) = \max\{\deg(f_1 || f_2), \deg((f_1 || f_2) + (f_1 || \bar{f}_2)) + 1\}$$
$$= \max\{n - 2, \deg(0_{2^{n-2}} 1_{2^{n-2}}) + 1\}$$
$$= \max\{n - 2, 2\}$$

(we write 0_s, or 1_s, for the corresponding bit repeated s times).

Next, we will do the computation for only one case, say $f = f_1 || f_2 || f_1 || \bar{f}_2$. We will show that $\max\limits_{\mathbf{w} \in \mathbb{F}_2^{n+2}} |W_f(\mathbf{w})| = 8\binom{n-4}{\lceil \frac{n-4}{2} \rceil}$.

Using Lemma 1, with $g_1 = h_{n-1} = f_1 || f_2$, $g_2 = f_1 || \bar{f}_2$, $f_1 = h_{n-2}$, and $f_2 = h_{n-2} \circ \phi$, as in the proof of Theorem 3 we obtain

$$W_f(\mathbf{u}, u_{n-1}, u_n) = (1 + (-1)^{u_n}) W_{f_1}(\mathbf{u}) + (-1)^{u_{n-1}} (1 - (-1)^{u_n}) W_{f_2}(\mathbf{u}).$$

Thus, $W_f(\mathbf{u}, u_{n-1}, 0) = 2W_{f_1}(\mathbf{u})$ and $W_f(\mathbf{u}, u_{n-1}, 1) = 2(-1)^{u_{n-1}} W_{f_2}(\mathbf{u})$. Since $f_1(\mathbf{u}) = h_{n-2}(\mathbf{u})$ and $f_2(\mathbf{u}) = h_{n-2}(\phi(\mathbf{u}))$ and $\max_{\mathbf{u} \in \mathbb{F}_2^n} |W_{h_n}(\mathbf{u})| = 4\binom{n-4}{\lceil \frac{n-4}{2} \rceil}$, it follows that

$$\max\limits_{(\mathbf{u}, u_{n-1}, u_n) \in \mathbb{F}_2^n} |W_f(\mathbf{u}, u_{n-1}, u_n)|$$

$$= 2 \max \left\{ \max\limits_{\mathbf{u} \in \mathbb{F}_2^{n-2}} |W_{h_{n-2}}(\mathbf{u})|, \max\limits_{\mathbf{u} \in \mathbb{F}_2^{n-2}} |W_{h_{n-2}}(\phi(\mathbf{u}))| \right\} = 8\binom{n-4}{\lceil \frac{n-4}{2} \rceil}.$$

We obtain that the nonlinearity of the functions in Construction 1 is $nl(f) = 2^{n-1} - 4\binom{n-4}{\lceil \frac{n-4}{2} \rceil}$.

We now deal with the computation of the algebraic immunity for the considered functions. By Theorem 4 of [38], $\mathcal{AI}(h_n) =: d_n \geq \lfloor \frac{n}{3} \rfloor + 1$. We observe that $h'_n(x_1, x_2, \ldots, x_n) = h_n(x_2, x_3, \ldots, x_n, x_1)$, and certainly $\mathcal{AI}(h_n) = \mathcal{AI}(h'_n)$. By the definition of algebraic immunity, we observe that $\mathcal{AI}(g) = \mathcal{AI}(\bar{g})$ for any Boolean function g, and also, that $\mathcal{AI}(f_i || f_j) = \mathcal{AI}(f_j || f_i)$, and $\mathcal{AI}(f_i || \bar{f}_j) = \mathcal{AI}(\bar{f}_i || f_j)$, $i = 1, 2$. So without loss of generality, we will only consider the case of $f = f_1 || f_2 || f_1 || \bar{f}_2$.

Let $g = g_1 || g_2 || k_1 || k_2 \neq \mathbf{0}$ be an annihilator of f. Thus, g_1, k_1 are both annihilators of f_1; and, g_2, respectively, k_2 are annihilators of f_2, respectively, $\bar{f}_2$, *not all* zero.

First, since $g_1 || g_2$ is an annihilator of $f_1 || f_2 = h_{n-1}$, it follows that $\deg(g_1 || g_2) = 0$, if both $g_1 = g_2 = 0$, or $\deg(g_1 || g_2) \geq d_{n-1}$. Also, observe that $\deg(g_1 + k_1)$ is

Table 1. Algebraic immunity and nonlinearity of the HWBF-based f and the HWBF h

n	$\mathcal{AI}(f)$	$\mathcal{AI}(h)$	$nl(f)$	$nl(h)$
7	3	3	52	44
8	4	4	104	88
9	4	4	216	186
10	5	4	432	372
11	5	5	884	772
12	5	5	1768	1544
13	6	5	3592	3172
14	6	5	7184	6344
15	6	6	14536	12952

Table 2. Behavior of the HWBF-based function f against Fast Algebraic Attacks

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

either 0, if $g_1 = k_1$, or $\geq d_{n-1}$ (since $g_1 + k_1$ is an annihilator of f_1). Now, the degree of the concatenation $g = g_1||g_2||k_1||k_2$ is

$$\deg(g) = \max\{\deg(g_1||g_2), \deg((g_1 + k_1)||(g_2 + k_2)) + 1\}.$$

Next, $\deg(g_1||g_2) = \max\{\deg(g_1), \deg(g_1+g_2)+1\}$, and $\deg((g_1+k_1)||(g_2+k_2)) = \max\{\deg(g_1 + k_1), \deg(g_1 + g_2 + k_1 + k_2) + 1\}$.

It is rather obvious that the worst case is when $g_1 = k_1, g_2 = \bar{k}_2$. Then, $\deg(g) = \max\{\deg(g_1||g_2), 1\} \geq \lfloor \frac{n-1}{3} \rfloor + 1 = \lfloor \frac{n+2}{3} \rfloor$, which proves the first claims. $\qquad\square$

Let $f = f_1||f_2||f_1||\bar{f}_2$ with $f_1 f_2 = h_{n-1}$, the HWBF. In Table 1, one can find the algebraic immunity and nonlinearity of f, compared to the same parameters for the HWBF h. Let $fg = h$, $\deg(g) = d$ and $\deg(h) = e$. In Table 2, we give the lowest possible values of (d,e), as needed for the fast algebraic attack.

There are other cases where our construction is quite strong, improving upon the parameters of other existing constructions. Let $CF \in B_n$ be the Carlet–Feng function whose support is $\{0, 1, \alpha, \ldots, \alpha^{2^{n-1}-2}\}$, where α is a primitive element of the field $\mathbb{F}_{2^n}$. We now consider our construction with the base functions that are variations of CF, and give some experimental results.

Let $f_1 \in \mathcal{B}_{10}$ be the Carlet–Feng function with the primitive polynomial

$$x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$$

Table 3. Algebraic immunity and nonlinearity of the CF-based function f and the function TCT introduced by [35]

n	$\mathcal{AI}(f)$	$\mathcal{AI}(TCT)$	$nl(f)$	$nl(TCT)$
8	4	4	112	108
10	5	5	480	476
12	6	6	1992	1982
14	7	7	8076	8028
16	8	8	32532	32508

and $f_2(\mathbf{x}) = f_1(A\mathbf{x})$, where

$$A = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \mathbf{e}_5, \mathbf{e}_{10}, \mathbf{e}_6, \mathbf{e}_7, \mathbf{e}_8, \mathbf{e}_9)$$

and $\mathbf{e}_i \in \mathbb{F}_2^{10}$ is the unit column vector with 1 on the i-th position. Let $f = f_1||f_2||f_1||\tilde{f}_2 \in \mathcal{B}_{12}$. Then $\mathcal{AI}(f) = 6$ and $nl(f) = 1992$. The nonlinearity of the 12-variable Carlet-Feng function discussed by [35, 36] is only 1970. Also, the balanced function $TCT : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ constructed by [35] which is based on the Carlet–Feng function has the nonlinearity 1982, when $2k = 12$. Clearly, our function f has optimum algebraic immunity and the nonlinearity of our function is also higher than the ones mentioned, in addition to satisfying other cryptographic properties. Let $f_1 \in \mathcal{B}_{n-2}$ be the Carlet–Feng function and $f_2(\mathbf{x}) = f_1(A\mathbf{x})$. For $n = 8, 10, 12, 14, 16$, in Table 3, we give the algebraic immunity and nonlinearity of f, compared to the same parameters for the function TCT introduced by [35].

As it was also motivated in [38] for the HWBF, for the same number of variables, the algebraic immunity and nonlinearity of our construction may be lower than the ones of the Carlet-Feng function. However, since our functions can be implemented very efficiently in hardware (LFRSs are better suited for hardware), we can use more variables, thus increasing the cryptographic properties of the combiner.

References

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

[2] R.E. Bryant, "On the complexity of VLSI implementation and graph representations of Boolean functions with application to integer multiplication," *IEEE Trans. Comput.* 40:2 (1991), 205–213.

[3] R.E. Bryant, "Symbolic Manipulation with Ordered Binary Decision Diagrams," *ACM Computing Surveys* 24:3 (1992), 293–318.

[4] C. Carlet, Comment on "Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials", *IEEE Trans. Inf. Theory* **57:7** (2011), 4852–4853.

[5] C. Carlet, "On secondary constructions of resilient and bent functions," *Coding, Cryptography and Combinatorics*, Progress in Comp. Sci. and Applied Logic, Birkhauser– Verlag, Basel **23** (2004), 3–28.

[6] C. Carlet, "On the higher order nonlinearities of algebraic immune functions," *Adv. in Crypt. – CRYPTO* 2006, LNCS 4117, Springer–Verlag, 2006, pp. 584–601.

[7] 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* 52:7 (2006), 3105–3121.

[8] C. Carlet, H. Dobbertin, G. Leander, "Normal extensions of bent functions," *IEEE Trans. Inf. Theory* 50:11 (2004), 2880–2885.

[9] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," *Adv. in Crypt. – ASIACRYPT* 2008, LNCS 5350, Springer–Verlag, 2008, pp. 425–440.

[10] C. Carlet and K. Feng, "An Infinite Class of Balanced Vectorial Boolean Functions with Optimum Algebraic Immunity and Good Nonlinearity," *IWCC 2009*, LNCS 5557, Springer–Verlag, 2009, pp. 1–11.

[11] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," *Adv. in Crypt. – CRYPTO* 2003, LNCS 2729, Springer–Verlag, 2003, pp. 176–194.

[12] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," *Adv. in Crypt. – EUROCRYPT* 2003, LNCS 2656, Springer–Verlag, 2003, pp. 345–359.

[13] T.W. Cusick, P. Stănică, "Cryptographic Boolean Functions and Applications", Elsevier–Academic Press, 2009.

[14] D.K. Dalai, K.C. Maitra and S. Maitra, "Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity," *Proceedings of FSE 2005*, LNCS 3557, Springer–Verlag, 2005, pp. 98–111.

[15] D. K. Dalai, S. Maitra and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," *Designs, Codes and Cryptography* 40:1 (2006), 41–58.

[16] S. Gangopadhyay and D. Sharma, "On construction of non-normal Boolean functions," *Australasian J. Combinatorics* 38 (2007), 267–272.

[17] P. Hawkes and G.G. Rose, "Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers," *Adv. in Crypt. – CRYPTO* 2004, LNCS 3152, Springer–Verlag, 2004, pp. 390–406.

[18] M. Krause, "BDD–Based Cryptanalysis of Keystream Generators," *Adv. in Crypt. – EUROCRYPT* 2002, LNCS 2332 (2002), pp. 222–237.

[19] M. Krause, D. Stegemann, "Reducing the Space Complexity of BDD–based Attacks on Keystream Generators", *Fast Software Encryption*, 13th International Workshop, FSE 2006, Graz, Austria, March 15–17, 2006, LNCS 4047, pp. 163–178, Springer, 2006.

[20] N. Li and W.F. Qi, "Construction and analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity," *Adv. in Crypt. – ASIACRYPT* 2006, LNCS 4284, Springer–Verlag, 2006, pp. 84–98.

[21] N. Li, L. Qu, W. Qi, G. Feng, C. Li and DuanQiang Xie, "On the Construction of Boolean Functions With Optimal Algebraic Immunity," *IEEE Trans. Inf. Theory* 54:3 (2008), 1330–1334.

[22] M. Liu, Y. Zhang, D. Lin, "Perfect Algebraic Immune Functions," *Adv. in Crypt. – ASIACRYPT* 2012, LNCS 7658, 2012, pp. 172–189.

[23] M. Lobanov, "Tight bound between nonlinearity and algebraic immunity," Cryptology ePrint Archive, 2005/441. Available: eprint.iacr.org/2005/441.

[24] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers," *Adv. in Crypt. – EUROCRYPT* 1988 , LNCS 330, Springer–Verlag, 1988, pp. 301–314.

[25] W. Meier, E. Pasalic and C. Carlet, "Algebraic Attacks and Decomposition of Boolean Functions," *Adv. in Crypt. – EUROCRYPT* 2004, LNCS 3027, Springer–Verlag, 2004, pp. 474–491.

[26] S. Mesnager, "Improving the Lower Bound on the Higher Order Nonlinearity of Boolean Functions With Prescribed Algebraic Immunity," *IEEE Trans. Inf. Theory* 54:8 (2008), 3656–3662.

[27] E. Pasalic, "A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation," *Cryptography and Communications* 4:1 (2012), 25–45.

[28] E. Pasalic, "Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis," *Proceedings of ICISC 2008*, LNCS 5461, Springer–Verlag, 2009, pp. 399–414.

[29] E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar, "New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity," in Workshop on Coding and Cryptography – WCC2001, Paris, France, Jan. 8–12, 2001. Published in Electronic Notes in Discrete Mathematics, Amsterdam, The Netherlands: Elsevier Science, vol. 6, 2001.

[30] E. Pasalic and Y. Wei, "On the Construction of Cryptographically Significant Boolean Functions Using Objects in Projective Geometry Spaces," *IEEE Trans. Inf. Theory* 58:10 (2012), 6681–6693.

[31] L. Qu, K. Feng, F. Liu, and L. Wang, "Constructing symmetric Boolean functions with maximum algebraic immunity," *IEEE Trans. Inf. Theory* 55:5 (2009), 2406–2412.

[32] P. Rizomiliotis, "On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation," *IEEE Trans. Inf. Theory* 56:8 (2010), 4014–4024.

[33] D. Stegemann, "Extended BDD–based Cryptanalysis of Keystream Generators", 14th International Workshop on Selected Areas in Cryptography, SAC 2007, August 16–17, 2007, Ottawa, Canada, LNCS 4876, pp. 17–35, Springer, 2007.

[34] C. Tan and S. Goh, "Several Classes of Even-Variable Balanced Boolean Functions with Optimal Algebraic Immunity," *IEICE Trans.* E94.A:1 (2011), 165–171.

[35] 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* 59:1 (2013) 653–664.

[36] Z. Tu and 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.

[37] Q. Wang, T. Johansson and H. Kan, "Some results on fast algebraic attacks and higher-order non-linearities," *IET Information Security* 6:1 (2012), 41–46.

[38] Q. Wang, C. Carlet, P. Stănică, C.-H. Tan, "Cryptographic Properties of the Hidden Weighted Bit Function," to appear in *Discrete Apppl. Math.*; http://dx.doi.org/10.1016/j.dam.2014.01.010.

[39] W. Wang, M. Liu, Y. Zhang, "Comments on 'A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation'," *Cryptography and Communications* 5:1 (2013), 1–6.

[40] 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* 57:9 (2011), 6310–6320.