On Various Nonlinearity Measures for Boolean Functions *

Joan Boyar† Magnus Gausdal Find‡ René Peralta§

July 7, 2015

Abstract

A necessary condition for the security of cryptographic functions is to be "sufficiently distant" from linear, and cryptographers have proposed several measures for this distance. In this paper, we show that six common measures, *nonlinearity, algebraic degree, annihilator immunity, algebraic thickness, normality*, and *multiplicative complexity*, are incomparable in the sense that for each pair of measures, μ_1, μ_2, there exist functions f_1, f_2 with f_1 being more nonlinear than f_2 according to μ_1, but less nonlinear according to μ_2. We also present new connections between two of these measures. Additionally, we give a lower bound on the multiplicative complexity of collision-free functions.

1 Preliminaries

The *Hamming weight* of vector $\mathbf{x} \in \mathbb{F}_2^n$ is the number of nonzero entries in $\mathbf{x}$. The Hamming weight $H^{\mathbb{N}}(n)$ of a natural number n is defined as the Hamming weight of the binary representation of n. We let $B_n = \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$ be the set of Boolean functions on n variables.

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented by its *algebraic normal form*, also known as its Zhegalkin polynomial:

$$f(x_1, \ldots, x_n) = \bigoplus_{S \subseteq \{1,2,\ldots,n\}} \alpha_S \prod_{i \in S} x_i$$

*This is a preliminary version of the article with the same title, accepted for publication for the journal *Cryptography and Communications*, Springer in 2015. For the official version of the paper we refer to the publishers website. Parts of this work appeared in [2].

†Department of Mathematics and Computer Science, University of Southern Denmark. Partially supported by the Danish Council for Independent Research, Natural Sciences. Part of this work was done while visiting the University of Waterloo.

‡Information Technology Laboratory, National Institute of Standards and Technology, USA. Most of this work was done while at the Department of Mathematics and Computer Science, University of Southern Denmark. Part of this work was done while visiting the University of Toronto.

§Information Technology Laboratory, National Institute of Standards and Technology, USA

where $\alpha_s \in \{0,1\}$ for all S and we define $\prod_{i\in\emptyset} x_i$ to be 1. If $\alpha_S = 0$ for $|S| > 1$, f is *affine*. An affine function f is *linear* if $\alpha_\emptyset = 0$ or equivalently if $f(\mathbf{0}) = 0$. The function f is *symmetric* if $\alpha_S = \alpha_{S'}$ whenever $|S| = |S'|$. A function is symmetric if and only if it only depends on the Hamming weight of the input. The kth *elementary symmetric Boolean function*, denoted Σ_k^n, is defined as the sum of all terms where $|S| = k$. For example,

$$\Sigma_2^4(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,$$

and

$$\Sigma_4^4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4.$$

For two functions $f, g \in B_n$ the distance d between f and g is defined as the number of inputs where the functions differ, that is

$$d(f, g) = |\{\mathbf{x} \in \mathbb{F}_2^n | f(\mathbf{x}) \neq g(\mathbf{x})\}|.$$

Definition 1. *Let P be a property. We say that* almost every *Boolean function has property P if*

$$\lim_{n\to\infty} \frac{|\{f\colon \mathbb{F}_2^n \to \mathbb{F}_2 | f \text{ does not have } P\}|}{2^{2^n}} = 0.$$

For the rest of this paper, unless otherwise stated, n denotes the number of input variables. We let log denote the logarithm base 2 and ln the natural logarithm.

2 Introduction

Cryptographic applications, such as hashing, block ciphers and stream ciphers, make use of functions that are simple by some criteria (such as circuit implementations) yet hard to invert almost everywhere. A necessary condition for the latter to hold is that the tools of algebra – and in particular linear algebra – be somehow not applicable to the problem of saying something about x given $f(x)$. Towards this goal, cryptographers have proposed several measures for the distance to linearity for Boolean functions.

Our contributions We consider six such measures. For each pair of measures μ_1, μ_2 we exhibit two infinite families of functions f_1, f_2 on n bits such that for sufficiently large n, f_1 is more nonlinear according μ_1 but less nonlinear according to μ_2. This has already been shown to be the case for some choices of μ_1 and μ_2. For example it was shown for algebraic thickness and normality and for algebraic thickness and nonlinearity by Carlet in [10, 9]. We complete this picture and show this is the case for all pairs of measures.

There exist many results relating the measures degree, annihilator immunity, algebraic thickness and normality, to each others and to cryptographic properties. The analogous questions for multiplicative complexity is, however, only little studied. We show that if f is a function on n bits with

- nonlinearity s, it has multiplicative complexity at most

$$\min\left\{s(n-1), (2+o(1))\frac{sn}{\log s}\right\}$$

- multiplicative complexity M, it has nonlinearity at most $2^{n-1} - 2^{n-M-1}$, and this is tight
- algebraic thickness $s > 1$, it has multiplicative complexity at most

$$\min\left\{s(n-1), (1+o(1))\frac{sn}{\log s}\right\}$$

- m bits of output and multiplicative complexity at most $n - m$, it cannot be a collision resistant hash function.

Furthermore, we study the multiplicative complexity of some highly nonlinear, symmetric functions with large degree and provide both upper and lower bounds.

2.1 The measures

The *nonlinearity* of a function is the Hamming distance to the closest affine function.[1] The nonlinearity of a function on n bits is between 0 and $2^{n-1} - \lceil 2^{n/2-1} \rceil$ [38, 11]. Affine functions have nonlinearity 0.

Functions with nonlinearity $2^{n-1} - 2^{n/2-1}$ exist if and only if n is even. These functions are called *bent*, and several constructions for bent functions exist (see [38, 30, 20] or the survey by Carlet [11]). For odd n, the situation is a bit more complicated; for any bent function f on $n-1$ variables, the function $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1})$ will have nonlinearity $2^{n-1} - 2^{(n-1)/2}$. It is known that for odd $n \geq 9$, this is suboptimal [23].

For a Boolean function f, there is a tight connection between the nonlinearity of f and its Fourier coefficients. More precisely the nonlinearity is determined by the largest Fourier coefficient, and for bent functions all the Fourier coefficients have the same magnitude. A general treatment on Fourier analysis can be found in [36].

The *algebraic degree* (which we from now on will refer to as just the *degree*) of a function is the degree of its Zhegalkin polynomial. That is, the largest $|S|$ such that $\alpha_S = 1$. Algebraic degree is sometimes called "algebraic nonlinearity" [35], "nonlinear order" [24], or "nonlinear degree" [26].

The *annihilator immunity* (also known as algebraic immunity[2]) of a function f is the minimum degree of a non-zero function g such that $fg = 0$ or $(f+1)g =$

[1] Unfortunately, this introduces an overloading of the word "nonlinearity" since it also refers to the more general concept of distance to linear functions. The meaning will be clear from context.

[2] In this paper we use the term "annihilator immunity" rather than "algebraic immunity", see the remark in [17].

0. We denote this measure by $AI(f)$. The function g is called an *annihilator*. It is known that $0 \leq AI(f) \leq \lceil \frac{n}{2} \rceil$ for all functions [15, 16]. For all n, specific symmetric functions are known which achieve the upper bound [17, 7].

The *multiplicative complexity* of a function f, denoted $c_\wedge(f)$, is the smallest number of AND gates necessary and sufficient to compute the function using a circuit over the basis (XOR,AND,1) (i.e. using arithmetic over $GF(2)$). The multiplicative complexity of f is 0 if and only if f is affine. It was shown in [6] that almost all Boolean functions on n bits have multiplicative complexity at least $2^{n/2} - O(n)$. Despite this, no specific function has been proven to have multiplicative complexity larger than $n - 1$.[3]

The *algebraic thickness*, denoted $\mathcal{T}(f)$, is defined as the smallest number of terms in the Zhegalkin polynomial of $f \circ A$ where $A \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a bijective affine mapping. Algebraic thickness was first introduced by Carlet in [10]. In contrast to the previous measures, we do not know of any attacks on the cryptographic use of functions that rely on the assumption of low algebraic thickness. However, the issue is implicitly addressed in [31, 24, 26] and in [32, p. 208]. If f is affine, or the product of affine functions, $\mathcal{T}(f) = 1$. On the other hand, *every* function has algebraic thickness at most $\frac{2}{3}2^n$.

As defined by Carlet in [9], generalizing the definition of Dobbertin in [20], we say that a function f is *weakly k-normal* if there exists a k-dimensional affine subspace on which f is affine. If there exists a k-dimensional affine subspace on which f is constant, then f is said to be *k-normal*. To align the terminology with the rest of the measures in this paper, we will say that the *normality* of a function f is the largest k such that f is k-normal. Thus, unlike the other measures in this paper, we generally seek functions with *low* normality. Affine functions have normality at least $n - 1$. Explicit functions are known with normality $n^{o(1)}$ [41]. k-normal functions are also known as *affine dispersers* of dimension k.

Nonlinearity, degree, and multiplicative complexity all capture an intuitive notion of the degree of "nonlinearity" of Boolean functions. Annihilator immunity, normality and algebraic thickness are also related to nonlinearity, albeit less obviously.

The six measures are affine invariants, that is, if $L \colon \{0,1\}^n \to \{0,1\}^n$ is an invertible affine mapping, applying L to the input variables first does not change the value of any of these measures. For multiplicative complexity, it is easy to see that the affine mapping L can be implemented without any AND gates. For the other measures, see [11, 10].

[3] We have experimentally verified that all functions on four bits have multiplicative complexity at most three. This is somewhat surprising, as circuit realization of random functions (e.g. $x_1x_2x_3x_4 + x_1x_2x_3 + x_2x_3x_4 + x_1x_3x_4 + x_1x_3 + x_2x_4 + x_1x_4$) would appear to need more than three AND gates. In [2] we conjectured that some function on five bits should have multiplicative complexity five. It turns out this is false ([42]). We expect that some function on six bits will have multiplicative complexity six.

2.2 Relationships between the measures and cryptographic properties

There is a substantial body of knowledge that relates nonlinearity, annihilator immunity, and algebraic degree to cryptographic properties. However, the analogous question with respect to multiplicative complexity remains little studied. Among the few published results is [14], in which Courtois et al. show (heuristically) that functions with low multiplicative complexity are less resistant against algebraic attacks. Here we present evidence that low multiplicative complexity in hash functions can make them prone to second preimage or collision attacks.

Multiplicative complexity also turns out to be important in cryptographic protocols. Several techniques for secure multi-party computation yield protocols with communication complexity proportional to the multiplicative complexity of the function being evaluated (see, for example, [21, 25, 34]). Several flavors of one-prover non-interactive cryptographically secure proofs (of knowledge of x given $f(x)$) have length proportional to the multiplicative complexity of the underlying function f (see, for example, [1]). Low multiplicative complexity also plays a role in the efficiency of fully homomorphic encryption and related cryptographic tools.

In this paper we show that very low nonlinearity implies low multiplicative complexity and vice-versa.

For nonlinearity, annihilator immunity, and algebraic degree, there exist symmetric Boolean functions achieving the maximal value among all Boolean functions. However, the only symmetric functions which achieve maximum nonlinearity are the quadratic functions, which have low algebraic degree. In [8] Canteaut and Videau characterize the symmetric functions with almost optimal nonlinearity. In this paper we analyze the multiplicative complexity and annihilator immunity of these functions.

2.3 Nonlinearity of random functions

Random Boolean functions are, with probability $1 - o(1)$, highly nonlinear with respect to each of these measures:

- In [19], Didier shows that the annihilator immunity of almost every Boolean function is $(1 - o(1))n/2$;
- In [37], Rodier shows that the nonlinearity of almost every function is very close to $2^{n-1} - 2^{n/2-1}\sqrt{2n \ln 2}$, which is close to maximum;
- A random function can be picked by flipping a coin for each of the coefficients of a Zhegalkin polynomial. Thus, the fraction of functions with degree at least $n - 1$ is $1 - 2^{-(n+1)}$;
- In [33], Nechiporuk shows that almost every Boolean function has multiplicative complexity at least $(1 - o(1))2^{n/2}$, and at most $(1 + o(1))2^{n/2}$ (see also [22]). A more recent (and independent) proof that in fact, almost

every Boolean function has multiplicative complexity at least $2^{n/2} - O(n)$ is given by Boyar and Peralta in [6];

- In [10], Carlet shows that almost every function has algebraic thickness at least $2^{n-1} - cn2^{\frac{n-1}{2}}$ for some constant c, that for every $n \geq 3$, there exists a function f with $\mathcal{T}(f) \geq 2^{n-1} - n2^{\frac{n-1}{2}}$, and that almost every function has normality at most $1.01 \log n$.

We conclude that almost every function is highly nonlinear according to *all* six measures considered in this paper.

2.4 Some known relations between nonlinearity measures

If a function f has algebraic degree d, the multiplicative complexity is at least $d-1$ [40]. This is a very weak bound for most functions. However this technique easily yields lower bounds of $n-1$ for many functions on n variables, and no larger lower bound is known for any specific function.

Additionally, it has been shown that low nonlinearity implies low annihilator immunity [16]. However, there are functions optimal with respect to annihilator immunity that have nonlinearity much worse than that of bent functions. An example of this is the majority function, see [17]. Bent functions have degree at most $\frac{n}{2}$ ([38, 11]).

Since $f \oplus 1$ is an annihilator for f, the annihilator immunity of a function is at most its degree.

Recently it was shown that any function of degree d has normality at least $\Omega(n^{1/(d-1)})$ [13]. It is not hard to show that if a function has multiplicative complexity at most k, then it is weakly c-normal for some $c \geq n-k$. This is implicit in [5], and mentioned explicitly in [18]. The following relation was showed in [44] and an alternative proof was given in [10].

Proposition 1. *If $f \in B_n$ is weakly-k-normal, then the nonlinearity of f is at most $2^{n-1} - 2^{k-1}$.*

3 Incomparability

In this section we show that the six measures are incomparable in the sense that, for each pair of measures μ_1, μ_2, there exist functions f_1, f_2 with f_1 being more nonlinear according to μ_1 but f_2 being more nonlinear according to μ_2. To show this we look at specific functions as well as functions chosen at random from a (large) subspace of all Boolean functions on n-bits. The results are asymptotic and hold for large enough n, though many also hold for relatively small n. The specific functions are the following:

- The elementary symmetric function Σ_2^n:

  For even n, the function Σ_2^n is bent [38]. For odd n it has nonlinearity $2^{n-1} - 2^{(n-1)/2}$, which is maximum among the symmetric functions on an

odd number of variables [29]. But being a quadratic function, both the algebraic degree and the annihilator immunity are 2 which is almost as bad as for linear functions. The multiplicative complexity is $\lfloor n/2 \rfloor$, which is the smallest possible multiplicative complexity for nonlinear symmetric functions [6].

- MAJ_n:

  MAJ_n on n bits is 1 if and only if at least $n/2$ of the n inputs are 1. In [5] it is shown that when n is a power of 2, the degree is n and the multiplicative complexity is at least $n-1$. In [17] it is shown that MAJ_n has annihilator immunity $\lceil \frac{n}{2} \rceil$; they also show that it has nonlinearity $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$, which by Stirling's approximation is $2^{n-1} - (1+o(1))\sqrt{\frac{2}{\pi}}\frac{2^{n-1}}{\sqrt{n-1}}$.

- $FMAJ_n$:

  We define the function

  $$FMAJ_n(x_1, \ldots, x_n) = MAJ_{\lceil \log n \rceil}(x_1, \ldots, x_{\lceil \log n \rceil}) \oplus x_{\lceil \log n \rceil + 1} \oplus \ldots \oplus x_n :$$

  The degree of $FMAJ_n$ is equal to the degree of $MAJ_{\lceil \log n \rceil}$ which is at least $\frac{\lceil \log n \rceil}{2}$, so the multiplicative complexity is at least $\frac{\lceil \log n \rceil}{2} - 1$. Also, its multiplicative complexity is equal to that of $MAJ_{\lceil \log n \rceil}$, which is at most $\lceil \log(n) \rceil - H^{\mathbb{N}}(\lceil \log n \rceil) + \lceil \log(\lceil \log n \rceil + 1) \rceil$ [5]. The annihilator immunity of $FMAJ_n$ is at least $\left\lceil \frac{\log n}{2} \right\rceil - 1$, since $MAJ_{\lceil \log n \rceil}$ has annihilator immunity $\left\lceil \frac{\log n}{2} \right\rceil$, and $FMAJ_n$ is just $MAJ_{\lceil \log n \rceil}$ plus a linear function. This can change the annihilator immunity by at most 1 [12].

- Σ_n^n :

  This function is 1 if and only if all the n input bits are 1. The nonlinearity of Σ_n^n is 1 because it has Hamming distance 1 to the zero function. It has annihilator immunity 1 ($x_1 \oplus 1$ is an annihilator), its algebraic degree is n, and its multiplicative complexity is $n-1$.

We now use probabilistic arguments to show additional separations. We let F be chosen uniformly at random among the 2^{2^n} different Boolean functions on n bits. For each of our measures μ, most of the probability mass for the value of $\mu(F)$ is concentrated in a fairly small interval. We construct the following functions:

- R: Almost every Boolean function has nonlinearity very close to

  $$2^{n-1} - 2^{n/2-1}\sqrt{2n \ln 2}$$

  [37] and has normality at most $1.01 \log n$ [9]. Furthermore, with probability $1-o(1)$, the multiplicative complexity of $R \cdot x_n$ is at least $(1-o(1)) \cdot 2^{\frac{n-1}{2}}$ [33, 6] and the algebraic thickness at least $\frac{1}{3}2^{n-1}$ [10]. We let R be a function satisfying all these conditions.

- $R^{(3)}$: a function chosen uniformly at random among all functions with algebraic degree 3. With high probability, such a function has normality at most $n^{0.51}$ [9]. We let $R^{(3)}$ be one such function.
- RLW: a random function chosen uniformly among all functions with truth table having distance at most $\frac{1}{10}2^n$ to the constant zero function. Such a function has nonlinearity at most $\frac{1}{10}2^n$, and with high probability it has algebraic thickness is at least $\frac{1}{11}2^n$. We let RLW be one such function.

Incomparability examples: In Table 1 we exhibit incomparability examples. That is, for each pair of measures, we show two functions where one function scores better according to one measure and one function scores better according to the other measure.

Table 1: Incomparability examples. For every pair (f_1, f_2) f_1 scores better in the measure for the row and f_2 scores better in the measure for the column. The pairs marked with (C) were suggested by Carlet in [10, 9]

	MC	deg	AI	AT	Norm
NL	Σ_2^n, MAJ_n	Σ_2^n, MAJ_n	Σ_2^n, MAJ_n	Σ_2^n, RLW (C)	Σ_2^n, R
MC	-	$\Sigma_2^n, FMAJ_n$	$\Sigma_2^n, FMAJ_n$	Σ_2^n, Σ_n^n	$FMAJ_n, \Sigma_n^n$
deg	-	-	$\Sigma_n^n, FMAJ_n$	Σ_2^n, Σ_n^n	$R^{(3)}, \Sigma_n^n$
AI	-	-	-	$R \cdot x_n, FMAJ_n$	$R^{(3)}, \Sigma_n^n$
AT	-	-	-	-	$R \cdot x_n, R^{(3)}$ (C)

Remark: Most of these separation examples are constructive in the sense that they provide actual pairs of separating functions rather than just showing their existence.

Among the constructive examples, most are fairly extreme except with respect to multiplicative complexity and algebraic thickness, where the values are small compared to those for random functions. This is because no specific function has yet been proven to have high multiplicative complexity or algebraic thickness. If larger bounds were proven, one could have more extreme separations: Suppose $f\colon \{0,1\}^{n-1} \to \{0,1\}$ has large algebraic thickness, multiplicative complexity, degree, and annihilator immunity. Let $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1}) \cdot x_n$. Then clearly g has high degree and high multiplicative complexity. However, g has annihilator immunity 1 and normality $n-1$. This is an example where both annihilator immunity and normality fail to capture the intuitive notion of nonlinearity.

Table 2: Functions used for incomparability examples with lower and upper bounds for some of the relevant measures. N/A indicates that the value is not used to show incomparability. Values for multiplicative complexity of MAJ_n are only precise when n is a perfect power of 2.

	NL	MC	deg	AI	AT	Norm
Σ_2^n	$2^{n-1} - 2^{n/2-1}$	$\lfloor \frac{n}{2} \rfloor$	2	2	$\lceil \frac{n}{2} \rceil$	$\lfloor \frac{n}{2} \rfloor$
MAJ_n	$2^{n-1} - (1 + o(1))\sqrt{\frac{2}{\pi}}\frac{2^{n-1}}{\sqrt{n-1}}$	$n-1$	n	$\lceil \frac{n}{2} \rceil$	N/A	N/A
$FMAJ_n$	N/A	$\leq \lceil \log n \rceil + 3\lceil \sqrt{\log n} \rceil$	$\geq \lfloor \log n \rfloor - 3$	$\geq \left\lceil \frac{\lfloor \log n \rfloor}{2} \right\rceil$	$\leq 2 + \frac{2n}{3}$	N/A
Σ_n^n	1	$n-1$	n	1	1	$n-1$
R	$< 2^{n-1} - 2^{n/2-1}\sqrt{2n \ln 2}$	$(1 \pm o(1))2^{n/2}$	$\geq n-1$	$\geq (1 - o(1))\frac{n}{2}$	$\geq \frac{1}{3}2^n$	$\leq 1.01 \log n$
$R^{(3)}$	N/A	$O(n^3)$	3	≤ 3	N/A	$\leq n^{0.51}$
$R \cdot x_n$	N/A	$\geq (1 - o(1))2^{(n-1)/2}$	N/A	1	$\frac{1}{3}2^{n-1}$	$n-1$
RLW	$< \frac{1}{10}2^n$	N/A	N/A	N/A	$\geq \frac{1}{11}2^n$	N/A

4 Relationship between nonlinearity and multiplicative complexity

In this section we will show that, despite being incomparable measures, multiplicative complexity and nonlinearity are somehow related.

We will use the following theorem due to Lupanov [28] (see Lemma 1.2 in [22]). Given a Boolean matrix A, a *decomposition* is a set of Boolean matrices $B_1, \ldots, B_k$ each having rank 1, satisfying $A = B_1 + B_2 + \ldots + B_k$ where addition is over the reals. For each B_i its weight is defined as the number of nonzero rows plus the number of nonzero columns. The *weight* of a decomposition is the sum of the weights of the B_i's.

Theorem 1 (Lupanov)**.** *Every Boolean $p \times q$ matrix admits a decomposition of weight*

$$(1 + o(1))\frac{pq}{\log p}.$$

Theorem 2. *A function $f \in B_n$ with nonlinearity $s > 1$ has multiplicative complexity at most* $\min\{s(n-1), (2 + o(1))\frac{sn}{\log s}\}$.

Proof. Let L be an affine function with minimum distance to f. Let

$$\epsilon(\mathbf{x}) = f(\mathbf{x}) \oplus L(\mathbf{x}).$$

Note that ϵ takes the value 1 s times. Let $\epsilon^{-1}(1)$ be the preimage of 1 under ϵ. Suppose $\epsilon^{-1}(1) = \{z^{(1)}, \ldots, z^{(s)}\}$ where each $z^{(i)}$ is an n-bit vector. Let $M_i(\mathbf{x}) = \prod_{j=1}^{n}(x_j \oplus z_j^{(i)} \oplus 1)$ be the minterm associated to $z^{(i)}$, that is the polynomial that is 1 only on $z^{(i)}$. By definition

$$\epsilon(\mathbf{x}) = \bigoplus_{i=1}^{s} M_i(\mathbf{x}) = \bigoplus_{i=1}^{s} \prod_{j=1}^{n}(x_j \oplus z_j^{(i)} \oplus 1)$$

Adding the minterms together can be done using only XOR gates and gives exactly the function ϵ. We will give two constructions for the minterms. Using the one with fewest AND gates proves the result.

The first construction simply computes each of the s minterms directly using $n-1$ AND gates for each. For the second construction, define the $s \times 2n$ matrix A where columns $1, 2, \ldots, n$ correspond to $x_1, x_2, \ldots, x_n$ and columns $n+1, \ldots, 2n$ correspond to $(1 \oplus x_1), \ldots, (1 \oplus x_n)$, and row i corresponds to minterm M_i. Let $A_{ij} = 1$ if and only if the literal corresponding to column j is a factor in the minterm M_i. Now consider the rectangular decomposition guaranteed to exist by Theorem 1. For each B_i, all non-zero columns are equal. AND together the literals corresponding to these variables. Call the result Q_i. Now each row can be seen as a logical AND of Q_i's. AND these together for every row to obtain the s results. The number of AND gates used is at most the weight of the decomposition, that is at most $(1 + o(1))\frac{2sn}{\log s}$ AND gates. □

Thus, functions with low nonlinearity cannot have too large multiplicative complexity. Now we show that conversely, if the multiplicative complexity is low, this gives a bound on the nonlinearity. This gives a somehow simpler (Fourier-free) proof of Proposition 1 for functions with low multiplicative complexity. Also, there is a more algorithmic flavor to our proof that might have independent interest. The idea of the proof has subsequently been extended to the case with more than one bit of output [4].

Lemma 1. *Suppose f has multiplicative complexity $M \leq \frac{n}{2}$. Then there exists an invertible linear mapping $L\colon \{0,1\}^n \to \{0,1\}^n$, a Boolean function $g \in B_D$ for $D \leq 2M$, and a set $T \subseteq \{1, 2, \ldots, n\}$ such that for $\mathbf{t} = L(\mathbf{x})$, f can be written as*

$$f(x_1, \ldots, x_n) = g(t_1, \ldots, t_D) \oplus \bigoplus_{j \in T} t_j$$

Proof. Let $M = c_\wedge(f)$ and consider an XOR-AND circuit C with M AND gates computing f, and let $A_1, \ldots, A_M$ be a topological ordering of the AND gates. Let the inputs to A_1 be I_1, I_2 and inputs to A_2 be I_3, I_4, etc. so A_M has inputs I_{2M-1}, I_{2M}. Now the value of f, the output of C, can be written as a sum of some of the AND gate outputs and some of the inputs to the circuit:

$$f = \bigoplus_{i \in Z_{out}} A_i \oplus \bigoplus_{i \in X_{out}} x_i,$$

for appropriate choices of Z_{out} and X_{out}. Similarly for I_j:

$$I_j = \bigoplus_{i \in Z_j} A_i \oplus \bigoplus_{i \in X_j} x_i.$$

Define g as $g = \bigoplus_{i \in Z_{out}} A_i$. Since X_j is a subset of $\{0,1\}^n$, it can be thought of as a vector y_j in the vector space $\{0,1\}^n$ where the ith coordinate is 1 if and only if $i \in X_j$.

The dimension D of $Y = span(y_1, \ldots y_{2M})$ is at most $2M$. Let $\{y_{j_1}, \ldots y_{j_D}\}$ be a basis of Y. There exists some invertible linear mapping $L\colon \{0,1\}^n \to \{0,1\}^n$ with $L(x_1, \ldots, x_n) = (t_1, \ldots, t_n)$ having $t_j = y_{i_j}$ for $1 \leq j \leq D$. That is, g depends on just $t_1, \ldots t_D$, and each x_j is a sum of t_l's, hence f can be written as a function of $t_1, \ldots, t_n$ as

$$f = g(t_1, \ldots, t_D) \oplus \bigoplus_{j \in T} t_j.$$

□

Corollary 1. *If a function $f \in B_n$ has multiplicative complexity M, it has nonlinearity at most $2^{n-1} - 2^{n-M-1}$. Furthermore for $M \leq \frac{n}{2}$, the function defined as*

$$f(x_1, x_2, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2M-1}x_{2M},$$

has this nonlinearity.

Proof. Since nonlinearity is an affine invariant, we can use Lemma 1 and look at the nonlinearity of

$$f = g(t_1, \ldots, t_{2M}) \oplus \bigoplus_{j \in T_{out}} t_j$$

Now the best affine approximation of g *agrees* on at least $2^{2M-1} + 2^{M-1}$ inputs. Replacing g with its best affine approximation, we obtain a function that agrees with f on at least $2^{n-2M}(2^{2M-1} + 2^{M-1}) = 2^{n-2M}2^{2M-1} + 2^{n-2M}2^{M-1} = 2^{n-1} + 2^{n-M-1}$ proving the upper bound on the nonlinearity. The nonlinearity of the function

$$f(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2M-1}x_{2M},$$

follows from simple calculations. □

Remark: This shows that Σ_2^n is optimal with respect to nonlinearity among functions having multiplicative complexity $\lfloor n/2 \rfloor$.

5 A few new results on algebraic thickness

A counting argument in [10] shows that almost every function has algebraic thickness at least $2^{n-1} - cn2^{\frac{n-1}{2}}$ for some constant $c > 0$. The proposition below states that this is not too far from being tight.

Proposition 2. *The set of functions with $\mathcal{T}(f) \leq 2^{n-1}$ has measure at least $\frac{1}{2}$.*

Proof. Recall that for every function $f \in B_n$ there exists a unique degree $n-1$ function $f' \in B_n$ and $b \in \mathbb{F}_2$ such that

$$f(x_1, \ldots, x_n) = f'(x_1, \ldots, x_n) + b\Sigma_n^n$$

We will for every function f' of degree at most $n-1$ argue that if f' has $\mathcal{T} > 2^{n-1}$ then $\mathcal{T}(f' + \Sigma_n^n) < 2^{n-1}$. Since there are 2^{2^n-1} functions with degree at most $n-1$, this will prove the theorem. Let f' be a function with degree at most $n-1$ with $\mathcal{T}(f') > 2^{n-1}$. By the definition of algebraic thickness, we have that the algebraic normal form of $\tilde{f'}(x_1, \ldots, x_n) := f'(1+x_1, \ldots, 1+x_n)$ has at least $2^{n-1}+1$ terms.

Now consider the algebraic normal form of $f = f' + \Sigma_n^n$ under the simple translation $x_i \to 1 + x_i$

$$\begin{aligned} & f(1 + x_1, \ldots, 1 + x_n) \\ =& f'(1 + x_1, \ldots, 1 + x_n) + \Sigma_n^n(1 + x_1, \ldots, 1 + x_n) \\ =& \tilde{f'}(x_1, \ldots, x_n) + \bigoplus_{i=0}^{n} \Sigma_i^n(x_1, \ldots, x_n) \end{aligned}$$

By assumption this has at most $2^n - (2^{n-1}+1) = 2^{n-1} - 1$ terms in its Zhegalkin polynomial. □

Also it should be mentioned that for some applications, one can rule out the possibility of certain inputs. A simple example of this is when a function is used as a filter function for a linear feedback shift register. In such a case the input to the function should never be $\mathbf{0}$.

That is, if a function f is to be used for a linear feedback shift register, we might as well use the function f' such that $f'(\mathbf{x}) = f(\mathbf{x})$ except when $\mathbf{x} = 0$. This function modification is sometimes called the "algebraic complement" [43]. Expressed in terms of the Zhegalkin polynomial

$$f'(\mathbf{x}) = f(\mathbf{x}) \oplus (x_1 + 1) \cdot \ldots \cdot (x_n + 1)$$

Notice that if the number of terms in the Zhegalkin polynomial of f is larger than 2^{n-1}, the algebraic thickness of f' is at most $2^{n-1} - 1$. That is, if we only care about the values of a function f on non-zero inputs, there is an equivalent function f' with $\mathcal{T}(f') \leq 2^{n-1}$.

Using essentially the same construction as in the proof of Theorem 2, one can obtain a relation between multiplicative complexity and algebraic thickness.

Theorem 3. *A function $f \in B_n$ with algebraic thickness $s > 1$ has multiplicative complexity at most* $\min\{s(n-1), (1+o(1))\frac{sn}{\log s}\}$.

6 Low multiplicative complexity and one-wayness

Consider an XOR-AND circuit C with M gates in total of which μ gates are AND. Consider a topologically minimal AND gate, and let X and b be its two inputs. The circuit computing X consist of XOR gates. Now if we restrict the inputs to satisfy that $X = 0$, the value computed by the AND gate is the constant zero (see Figure 1). Similarly if we restrict the inputs to satisfy $X = 1$, the AND gate computes the value b. In either of the two cases, the number of AND gates decreases by at least 1. After at most μ such restrictions the circuit computes some linear function L.

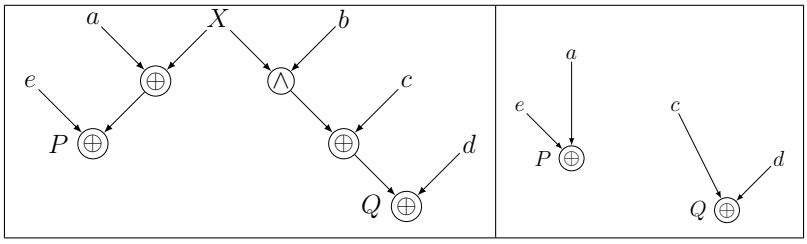

Figure 1: The circuit to the right is the circuit obtained when X in the left circuits is restricted to the value 0. Notice that only the gates P, Q remain nonredundant.

This implies that C can be inverted in time $poly(M)2^{\mu}$: Suppose y has a non-empty preimage under f. Then for each of the 2^{μ} choices, obtain the linear operator L and check if $L(x) = y$ has a solution. If it has a solution report one. The total time complexity is at most $poly(M)2^{\mu}$ since solving linear equations can be done in time polynomial in n and simplifying a circuit under an affine restriction (as in Figure 1) can be done in time polynomial in the size of the circuit.

Thus, one-way functions, if they exist, have superlogarithmic multiplicative complexity.

The one-wayness requirements of hash functions include the much stronger requirement of *collision resistance*: it must be infeasible to find two inputs that map to the same output. We next observe that collision resistance of a function f with n inputs and $m < n$ outputs requires f to have multiplicative complexity at least $n - m$.

Let C be a circuit for f that has μ AND gates. Negations can be "pushed" to the outputs of the circuit without changing the number of AND gates. Once at the outputs, for purposes of finding a collision, negations can be simply removed. Thus, without loss of generality, we can assume the circuit contains no negations and that we seek two distinct inputs which map to $\mathbf{0}$.

Since there are no negations in the circuit, one such input is $\mathbf{0}$. We next show how to obtain a second preimage of $\mathbf{0}$.

Pick a topologically minimal AND gate and set one of its inputs to 0. This generates one homogeneous linear equation on the inputs to f and allows us to

remove the AND gate from the circuit (see Figure 1). Repeating this until no AND gates are left yields a homogeneous system S with at most μ equations, plus a circuit C' which computes a homogeneous linear system with m equations. Since the n inputs correspond to n variables, the system of equations has $2^{n-m-\mu}$ distinct solutions. Thus, if $m + \mu < n$, then standard linear algebra yields non-zero solutions. These are second preimages of $\mathbf{0}$.

We re-state this as a theorem below. The idea of using hyperplane restrictions to eliminate AND gates has been used before, however with different purposes, see e.g. [5, 18].

Theorem 4. *Collision resistance of a function f from n to m bits requires that f have multiplicative complexity at least $n - m$.*

It is worth noting that the bound from Theorem 4 does not take into account the position of the AND gates in the circuit. It is possible that fewer linear equations can be used to remove all AND gates. We have tried this on the reduced-round challenges issued by the Keccak designers (Keccak is the winner of the SHA-3 competition, see `http://keccak.noekeon.org/crunchy_contest.html`). These challenges are described in the notation Keccak$[r, c, nr]$ where r is the rate, c the capacity, and nr the number of rounds. For the collision challenges, the number of outputs is set to 160. Each round of Keccak uses $r + c$ AND gates. However, in the last round of Keccak the number of AND gates that affect the output bits is equal to the number of outputs.

We consider circuits for Keccak with only one block (r bits) of input. The circuit for Keccak$[r$=1440$, c$=160$, nr$=1$]$ contains 160 AND gates, yet 96 linear equations will remove them all. Keccak$[r$=1440$, c$=160$, nr$=2$]$ contains 1760 AND gates, yet 1056 linear equations removes them all. Thus, finding collisions is easy, because 1440 is greater than $160 + 1056$ (in the one-round case, because $1440 > 160 + 96$). These two collision challenges were first solved by Morawiecki (using SAT solvers, see `http://keccak.noekeon.org/crunchy_mails/coll-r2-w1600-20110729.txt`) and, more recently, by Duc et al. (see `http://keccak.noekeon.org/crunchy_mails/coll-r1r2-w1600-20110802.txt`). Our reduction technique easily solves both of these challenges, and yields a large number of multicollisions.

Dinur et al. are able to obtain collisions for Keccak$[r$=1440$, c$=160$, nr$=4$]$ i.e. for four rounds of Keccak (see `http://keccak.noekeon.org/crunchy_mails/coll-r3r4-w1600-20111124.txt`). The technique of Theorem 4 cannot linearize the Keccak circuit for more than two rounds. How to leverage our methods to solve three or more rounds is work in progress.

7 Some symmetric Boolean functions with high nonlinearity

When designing Boolean functions for cryptographic applications, we seek functions with high nonlinearity, simple structure, high annihilator immunity, and

high algebraic degree. Bent functions have high nonlinearity. Symmetric functions have simple structure. However, the multiplicative complexity of a symmetric function on n variables is never larger than $n + 3\sqrt{n}$ [6]. The symmetric functions with highest nonlinearity are quadratic ([39] and [29]). But these functions have low algebraic degree, low annihilator immunity, and multiplicative complexity only $\lfloor \frac{n}{2} \rfloor$.

For $n \geq 3$, let

$$F_n(x_1, x_2, \ldots, x_n) = \bigoplus_{k=3}^{n} \Sigma_k^n(x_1, \ldots, x_n) = \bigoplus_{\substack{S \subseteq [n] \\ |S| \geq 3}} \prod_{i \in S} x_i,$$

and

$$G_n(x_1, \ldots, x_n) = \Sigma_2^n(x_1, \ldots, x_n) \oplus \Sigma_n^n(x_1, \ldots, x_n) = \left(\sum_{1 \leq i < j \leq n} x_i x_j \right) \oplus x_1 x_2 \ldots x_n.$$

It is known that there are exactly 8 symmetric functions with nonlinearity exactly 1 less than the largest achievable value. These are $F_n \oplus \lambda$ and $G_n \oplus \lambda$, where $\lambda \in \{0, 1, \Sigma_1^n, \Sigma_1^n + 1\}$ [8]. These functions have many of the criteria sought after for cryptographic functions: they are symmetric, have optimal degree, and almost optimal nonlinearity. We have exactly calculated or tightly bound the multiplicative complexity of these functions. Precise values are important for applications in secure multiparty computations.

Since the λ can always be computed and added using only XOR operations, we only consider F_n and G_n. In [5] it is shown that the Hamming weight of n bits $x_1, \ldots, x_n$ can be computed using an XOR-AND circuit having $n - H^{\mathbb{N}}(n)$ AND gates, where $H^{\mathbb{N}}(n)$ is the Hamming weight of the binary representation of n. Furthermore, it is noted that the value of the ith least significant bit in the Hamming weight is equal to the function $\Sigma_{2^i}^n(x_1, \ldots, x_n)$ and that for an integer k represented as a sum of distinct powers of 2, if $k = 2^{i_0} + 2^{i_1} + \ldots + 2^{i_j}$, then $\Sigma_k^n = \Sigma_{2^{i_0}}^n \cdot \ldots \cdot \Sigma_{2^{i_j}}^n$.

Lemma 2. *The multiplicative complexity of G_n is $n - 1$.*

Proof. Let $n = u_k, u_{k-1}, ..., u_1, u_0$ be the binary representation of n. To compute $G_n(x)$, one first computes the Hamming weight of x, giving $\{\Sigma_{2^k}^n(x) \mid 0 \leq k \leq \lceil \log_2(n+1) \rceil - 1\}$.

This uses $n - H^{\mathbb{N}}(n)$ AND gates, and gives us Σ_2^n directly. Σ_n^n is the product of $\{\Sigma_{2^i}^n \mid u_i = 1\}$, which requires exactly $H^{\mathbb{N}}(n) - 1$ AND gates to compute. Thus, exactly $n - 1$ AND gates are used. The value of G_n is computed with one additional XOR to add Σ_2^n and Σ_n^n. The multiplicative complexity cannot be lower than this since the degree of G_n is n. □

Proposition 3. *The multiplicative complexity of F_n is at least $n - 1$, since the degree is n.*

Lemma 3. *The multiplicative complexity of F_n is $n-1$ for $3 \leq n \leq 6$.*

Proof. For $n = 3$, $F_n = E_3^3$, which has multiplicative complexity 2. For $n = 4$, $F_n = T_3^4$, which has multiplicative complexity 3. Proofs of the multiplicative complexities of these functions are in [5].

For $n = 5$, compute the Hamming weight of x, giving

$$\{\Sigma_1^5(x), \Sigma_2^5(x), \Sigma_4^5(x)\}.$$

This uses $5 - 2 = 3$ AND gates.

$$\begin{aligned} F_5 &= \Sigma_3^5 \oplus \Sigma_4^5 \oplus \Sigma_5^5 \\ &= (\Sigma_4^5 \oplus \Sigma_2^5) \wedge (\Sigma_4^5 \oplus \Sigma_1^5) \end{aligned}$$

This can be computed using only one additional AND gate.

For $n = 6$, compute the Hamming weight of x, giving

$$\{\Sigma_1^6(x), \Sigma_2^6(x), \Sigma_4^6(x)\}.$$

This uses $6 - 2 = 4$ AND gates.

$$\begin{aligned} F_6 &= \Sigma_3^6 \oplus \Sigma_4^6 \oplus \Sigma_5^6 \oplus \Sigma_6^6 \\ &= (\Sigma_4^6 \oplus \Sigma_2^6) \wedge (\Sigma_4^6 \oplus \Sigma_1^6) \end{aligned}$$

This can be computed using only one additional AND gate. □

Lemma 4. *The multiplicative complexity of F_n is at most $n - H^{\mathbb{N}}(n) + k - 1$, for $k = \lceil \log(n+1) \rceil$.*

Proof. First compute the Hamming weight of the input, that is the functions $\Sigma_{2^i}^n$ for $i = 0, 1, \ldots, k-1$. The function

$$(1 \oplus \Sigma_1^n) \cdot (1 \oplus \Sigma_2^n) \cdot (1 \oplus \Sigma_4^n) \cdot \ldots \cdot (1 \oplus \Sigma_{2^{k-1}}^n)$$

can be computed with $k - 1$ additional AND gates. This function is equal to

$$1 \oplus \bigoplus_{i=1}^{n} \Sigma_i^n = (1 \oplus x_1)(1 \oplus x_2) \cdot \ldots \cdot (1 \oplus x_n),$$

since they are both 1 if and only if all input bits are 0. That is F_n can now be obtained without further multiplications since

$$(1 \oplus \Sigma_1^n) \cdot (1 \oplus \Sigma_2^n) \ldots (1 \oplus \Sigma_{2^{k-1}}^n) \oplus 1 \oplus \Sigma_1^n \oplus \Sigma_2^n = F_n$$

□

Corollary 2. *The multiplicative complexity of F_n is $n-1$ for $n \geq 7$ of the form $2^k - 1$.*

Proof. This follows immediately from the previous lemma, since $H^{\mathbb{N}}(2^k - 1) = k$ □

Proposition 4. $F_n(\mathbf{x}) = x_n \wedge (\Sigma_2^{n-1} \oplus \Sigma_3^{n-1} \oplus ... \oplus \Sigma_{n-1}^{n-1}) \oplus (\Sigma_3^{n-1} \oplus \Sigma_4^{n-1} \oplus ... \oplus \Sigma_{n-1}^{n-1}) = x_n \wedge (F_{n-1}(\mathbf{x}') \oplus \Sigma_2^{n-1}(\mathbf{x}')) \oplus F_{n-1}(\mathbf{x}')$, *where* $\mathbf{x}'$ *denotes* $(x_1, \ldots, x_{n-1})$.

Corollary 3. *The multiplicative complexity of* F_n *is* $n-1$ *for* $n \geq 8$ *of the form* 2^k.

Proof. We use Proposition 4. The previous corollary says that $F_{n-1}(\mathbf{x}')$ can be computed using only $n-2$ AND gates, and the proof of Lemma 4 shows that Σ_2^{n-1} is computed as a by-product of this. □

Corollary 4. *The multiplicative complexity of* F_n *is at least* $n-1$ *and at most* $n + \lceil \log_2 n \rceil - 3$.

Proof. By Lemma 4, the multiplicative complexity of F_n is at most $n - H^{\mathbb{N}}(n) + \lceil \log_2(n+1) \rceil - 1$. By the previous corollary, we know that we can ignore the case where n is a power of 2, so $H^{\mathbb{N}}(n) \geq 2$ and $\lceil \log_2(n+1) \rceil = \lceil \log_2 n \rceil$. □

It turns out that these eight functions have very low annihilator immunity. We consider the variants of F_n first and then the variants of G_n.

Lemma 5. *The function* $f = a \oplus b\Sigma_1^n \oplus \bigoplus_{i=3}^n \Sigma_i^n$ *has annihilator immunity at most* 2.

Proof. Let $\tilde{f} = b\Sigma_1^n \oplus \bigoplus_{i=3}^n \Sigma_i^n$, and let $h = 1 \oplus (1 \oplus b)\Sigma_1^n \oplus \Sigma_2^n$ be the algebraic complement of $\tilde{f}$, [43]. Notice that

$$\tilde{f} \oplus h = \bigoplus_{i=1}^{n} \Sigma_i^n \oplus 1 = (1 \oplus x_1)(1 \oplus x_2) \ldots (1 \oplus x_n)$$

which is 1 if and only if $\mathbf{x} = \mathbf{0}$. That is for $\mathbf{x} \neq \mathbf{0}$, $\tilde{f} = h$, so $1 \oplus h$ clearly annihilates $\tilde{f}$ on all non-zero inputs. Since $\tilde{f}(\mathbf{0}) = 0$, h is an annihilator of $\tilde{f}$ with degree 2. Since $\tilde{f}$ is equal to either f or $f+1$, h is also an annihilator of f. □

Lemma 6. *The function* $f = a \oplus b\Sigma_1^n \oplus \Sigma_2^n \oplus \Sigma_n^n$ *has annihilator immunity at most* 2.

Proof. Let $\mathbf{1}$ denote the all 1 input vector. For any fixed choice of a, and b, either $(a \oplus b\Sigma_1^n \oplus \Sigma_2^n)(\mathbf{1}) = 1$ or $(a \oplus b\Sigma_1^n \oplus \Sigma_2^n)(\mathbf{1}) = 0$. In the first case, the function $h = 1 \oplus a \oplus b\Sigma_1^n \oplus \Sigma_2^n$ is an annihilator of f, and otherwise $h = a \oplus b\Sigma_1^n \oplus \Sigma_2^n$ is an annihilator of $f \oplus 1$. □

8 Conclusion

In this paper, we show that six measures of nonlinearity, *nonlinearity, algebraic degree, annihilator immunity, algebraic thickness, normality*, and *multiplicative complexity*, are incomparable in the sense that for each pair of measures, μ_1, μ_2, there exist functions f_1, f_2 with f_1 being more nonlinear than f_2 according to μ_1, but less nonlinear according to μ_2. We also present new connections between multiplicative complexity and both nonlinearity and algebraic thickness. Further work on connections, such as the recent work of Cohen and Tal [13] and our own work [3], showing that functions with a certain algebraic thickness have a certain normality, as well as the work of Lobanov [27], would be interesting, because they imply that weakness according to one measure can leave a cryptographic system open to an attack defined by a weakness according to another measure.

Additionally, we presented a first lower bound on the multiplicative complexity of functions which are collision-free. Low multiplicative complexity may give rise to other attacks on various cryptographic functions, as could weakness according to the other measures, which like multiplicative complexity, have received less attention.

Finally, we studied some symmetric functions known to have high nonlinearity and considered their multiplicative complexity and annihilator immunity, both of which were found to be relatively low.

Acknowledgements

We are grateful to Meltem Sönmez Turan for many discussions on the subject of this work.

References

[1] Boyar, J., Damgaard, I., Peralta, R.: Short non-interactive cryptographic proofs. Journal of Cryptology **13**, 449–472 (2000)

[2] Boyar, J., Find, M., Peralta, R.: Four measures of nonlinearity. In: P.G. Spirakis, M.J. Serna (eds.) CIAC, *Lecture Notes in Computer Science*, vol. 7878, pp. 61–72. Springer (2013)

[3] Boyar, J., Find, M.G.: Constructive relationships between algebraic thickness and normality. CoRR **abs/1410.1318** (2014). URL `http://arxiv.org/abs/1410.1318`

[4] Boyar, J., Find, M.G.: The relationship between multiplicative complexity and nonlinearity. In: E. Csuhaj-Varjú, M. Dietzfelbinger, Z. Ésik (eds.) Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part II, *Lecture Notes in Computer Science*, vol. 8635,

pp. 130–140. Springer (2014). DOI 10.1007/978-3-662-44465-8_12. URL http://dx.doi.org/10.1007/978-3-662-44465-8_12

[5] Boyar, J., Peralta, R.: Tight bounds for the multiplicative complexity of symmetric functions. Theor. Comput. Sci. **396**(1-3), 223–246 (2008)

[6] Boyar, J., Peralta, R., Pochuev, D.: On the multiplicative complexity of Boolean functions over the basis $(\wedge, \oplus, 1)$. Theor. Comput. Sci. **235**(1), 43–57 (2000)

[7] Braeken, A., Preneel, B.: On the algebraic immunity of symmetric Boolean functions. In: S. Maitra, C.E.V. Madhavan, R. Venkatesan (eds.) INDOCRYPT, *LNCS*, vol. 3797, pp. 35–48. Springer, Heidelberg (2005)

[8] Canteaut, A., Videau, M.: Symmetric Boolean functions. IEEE Transactions on Information Theory **51**(8), 2791–2811 (2005)

[9] Carlet, C.: On cryptographic complexity of Boolean functions. In: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, pp. 53–69. Springer (2002)

[10] Carlet, C.: On the degree, nonlinearity, algebraic thickness, and nonnormality of Boolean functions, with developments on symmetric functions. IEEE Transactions on Information Theory **50**(9), 2178–2185 (2004)

[11] Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Y. Crama, P.L. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, chap. 8, pp. 257–397. Cambridge, UK: Cambridge Univ. Press (2010)

[12] Carlet, C., Dalai, D.K., Gupta, K.C., Maitra, S.: Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction. IEEE Transactions on Information Theory **52**(7), 3105–3121 (2006)

[13] Cohen, G., Tal, A.: Two structural results for low degree polynomials and applications. CoRR **abs/1404.0654** (2014). URL http://arxiv.org/abs/1404.0654

[14] Courtois, N., Hulme, D., Mourouzis, T.: Solving circuit optimisation problems in cryptography and cryptanalysis. E-print can be found at http://eprint.iacr.org/2011/475.pdf

[15] Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: E. Biham (ed.) EUROCRYPT, *LNCS*, vol. 2656, pp. 345–359. Springer, Heidelberg (2003)

[16] Dalai, D.K., Gupta, K.C., Maitra, S.: Results on algebraic immunity for cryptographically significant Boolean functions. In: A. Canteaut, K. Viswanathan (eds.) INDOCRYPT, *LNCS*, vol. 3348, pp. 92–106. Springer, Heidelberg (2004)

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

[18] Demenkov, E., Kulikov, A.S.: An elementary proof of a 3n - o(n) lower bound on the circuit complexity of affine dispersers. In: F. Murlak, P. Sankowski (eds.) MFCS, *LNCS*, vol. 6907, pp. 256–265. Springer, Heidelberg (2011)

[19] Didier, F.: A new upper bound on the block error probability after decoding over the erasure channel. IEEE Transactions on Information Theory **52**(10), 4496–4503 (2006)

[20] Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In: B. Preneel (ed.) FSE, *LNCS*, vol. 1008, pp. 61–74. Springer, Heidelberg (1994)

[21] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: Proceedings of the nineteenth annual ACM symposium on Theory of computing, STOC '87, pp. 218–229. ACM, New York, NY, USA (1987). DOI 10.1145/28395.28420. URL `http://doi.acm.org/10.1145/28395.28420`

[22] Jukna, S.: Boolean Function Complexity: Advances and Frontiers. Springer Berlin Heidelberg (2012)

[23] Kavut, S., Maitra, S., Yücel, M.D.: There exist Boolean functions on n (odd) variables having nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ if and only if n>7. IACR Cryptology ePrint Archive **2006**, 181 (2006)

[24] Knudsen, L.R.: Truncated and higher order differentials. In: Fast Software Encryption, pp. 196–211. Springer (1995)

[25] Kolesnikov, V., Schneider, T.: Improved garbled circuit: Free XOR gates and applications. In: L. Aceto, I. Damgård, L.A. Goldberg, M.M. Halldórsson, A. Ingólfsdóttir, I. Walukiewicz (eds.) ICALP (2), *LNCS*, vol. 5126, pp. 486–498. Springer, Heidelberg (2008)

[26] Lai, X.: Higher order derivatives and differential cryptanalysis. In: Communications and Cryptography, pp. 227–233. Springer (1994)

[27] Lobanov, M.: Exact relations between nonlinearity and algebraic immunity. Journal of Applied and Industrial Mathematics **3**, 367–376 (2009)

[28] Lupanov, O.: On rectifier and switching-and-rectifier schemes. Dokl. Akad. 30 Nauk SSSR 111, 1171-1174. (1965)

[29] Maitra, S., Sarkar, P.: Maximum nonlinearity of symmetric Boolean functions on odd number of variables. IEEE Transactions on Information Theory **48**(9), 2626–2630 (2002)

[30] McFarland, R.L.: Sub-difference sets of Hadamard difference sets. J. Comb. Theory, Ser. A **54**(1), 112–122 (1990)

[31] Meier, W., Staffelbach, O.: Nonlinearity criteria for cryptographic functions. In: J.J. Quisquater, J. Vandewalle (eds.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 434, pp. 549–562. Springer (1989)

[32] Menezes, A., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press (1996)

[33] Nechiporuk, E.I.: On the complexity of schemes in some bases containing nontrivial elements with zero weights (in russian). Problemy Kibernetiki **8**, 123–160 (1962)

[34] Nielsen, J.B., Nordholt, P.S., Orlandi, C., Burra, S.S.: A new approach to practical active-secure two-party computation. In: R. Safavi-Naini, R. Canetti (eds.) CRYPTO, *LNCS*, vol. 7417, pp. 681–700. Springer, Heidelberg (2012)

[35] O'Connor, L., Klapper, A.: Algebraic nonlinearity and its applications to cryptography. Journal of Cryptology **7**(4), 213–227 (1994)

[36] O'Donnell, R.: Analysis of Boolean Functions. Book draft. Available at www.analysisofbooleanfunctions.org (2012)

[37] Rodier, F.: Asymptotic nonlinearity of Boolean functions. Des. Codes Cryptography **40**(1), 59–70 (2006)

[38] Rothaus, O.S.: On "bent" functions. J. Comb. Theory, Ser. A **20**(3), 300–305 (1976)

[39] Savický, P.: On the bent Boolean functions that are symmetric. Eur. J. Comb. **15**(4), 407–410 (1994)

[40] Schnorr, C.P.: The multiplicative complexity of Boolean functions. In: T. Mora (ed.) AAECC, *LNCS*, vol. 357, pp. 45–58. Springer, Heidelberg (1988)

[41] Shaltiel, R.: Dispersers for affine sources with sub-polynomial entropy. In: R. Ostrovsky (ed.) FOCS, pp. 247–256. IEEE (2011)

[42] Turan, M.S., Peralta, R.: The multiplicative complexity of Boolean functions on four and five variables. In: Proceedings of LightSec'14. Springer (2014)

[43] Zhang, X., Pieprzyk, J., Zheng, Y.: On algebraic immunity and annihilators. Information Security and Cryptology–ICISC 2006 pp. 65–80 (2006)

[44] Zheng, Y., Zhang, X.M., Imai, H.: Restriction, terms and nonlinearity of boolean functions. Theor. Comput. Sci. **226**(1-2), 207–223 (1999). DOI 10.1016/S0304-3975(99)00073-0. URL `http://dx.doi.org/10.1016/S0304-3975(99)00073-0`