Downloaded from orbit.dtu.dk on: Apr 23, 2024

DTU Library

Maiorana-McFarland class: Degree optimization and algebraic properties

Pasalic, Enes

Published in:
I E E E Transactions on Information Theory

Link to article, DOI:
10.1109/TIT.2006.881721

Publication date:
2006

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Pasalic, E. (2006). Maiorana-McFarland class: Degree optimization and algebraic properties. *I E E E Transactions on Information Theory*, *52*(10), 4581-4594. https://doi.org/10.1109/TIT.2006.881721

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Maiorana–McFarland Class: Degree Optimization and Algebraic Properties

Enes Pasalic

***Abstract*—In this paper, we consider a subclass of the Maiorana–McFarland class used in the design of resilient nonlinear Boolean functions. We show that these functions allow a simple modification so that resilient Boolean functions of maximum algebraic degree may be generated instead of suboptimized degree in the original class. Preserving a high-nonlinearity value immanent to the original construction method, together with the degree optimization gives in many cases functions with cryptographic properties superior to all previously known construction methods. This approach is then used to increase the algebraic degree of functions in the extended Maiorana–McFarland (MM) class (nonlinear resilient functions $F : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)^m$ derived from linear codes). We also show that in the Boolean case, the same subclass seems not to have an optimized algebraic immunity, hence not providing a maximum resistance against algebraic attacks. A theoretical analysis of the algebraic properties of extended Maiorana–McFarland class indicates that this class of functions should be avoided as a filtering function in nonlinear combining generators.**

***Index Terms*—Algebraic degree, algebraic immunity, Boolean function, nonlinearity, resiliency, vectorial Boolean function.**

I. Introduction

RESILIENT Boolean functions have important applications in a nonlinear combiner model of stream cipher [26]. Apart from resiliency, the other cryptographic criteria of Boolean functions used in linear feedback shift register (LFSR) based stream ciphers such as nonlinear filtering generator and nonlinear combiner have more or less been identified. A function used in such an application should posses a high algebraic degree to increase the linear complexity of the keystream sequence, and furthermore, to withstand correlation attacks [35], [25], [17], [16] the function should have a modest order of resiliency and a high nonlinearity. In addition, algebraic attacks based on the low-degree annihilation of Boolean functions has recently been introduced in [8], [10].

Not all of these criteria can be satisfied simultaneously and concerning the resiliency order, denoted by t, Siegenthaler [34] proved that $d \leq n - t - 1$ for balanced functions, where d denotes the algebraic degree. Such a function, reaching this bound, is called *degree optimized*. Recently (since 2000), a lot of new results have been published in a very short time which include nontrivial nonlinearity (upper) bounds [32], [36], [39], [2], [4] and construction of resilient functions attaining either those bounds or reaching very close. Considering a Boolean function on n variables with order of resiliency $(t > \frac{n}{2} - 2)$ and attaining maximum possible nonlinearity, generalized construction methods have been proposed in [36], [29]. Construction of highly nonlinear functions with lower order of resiliency has been discussed in [31], [22]. But unfortunately, none of these methods is general in the sense that they would be able to generate a function for any input size n and any order of resiliency t. This is only true for the Maiorana–McFarland (MM) class [13], but this technique in general does not generate degree optimized functions.

The MM class of functions is characterized by having affine functions from smaller variable space as its subfunctions. Denoting by "$\cdot$"a usual dot product, $f : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)$ in this class is defined as $f(y, x) = \phi(y) \cdot x + h(y)$, $x \in \mathbb{F}_2^k$, $y \in \mathbb{F}_2^s$, $n = s+k$, where ϕ is any mapping from $\mathrm{GF}(2)^s$ to $\mathrm{GF}(2)^k$, and h is any Boolean function on $\mathrm{GF}(2)^s$. Note that for fixed y, restriction of f (subfunction of f) is an affine function in x. Then it can easily be shown that the degree of f is upper-bounded by $n - k + 1$. The nonlinearity value for the functions in this class reaches its maximum value for a high resiliency order, whereas in case of low or modest resiliency, the nonlinearity is very high but in most of the cases not reaching the upper bound. However, it is not clear whether there exist classes of functions reaching this bound, especially for large input spaces.

In the remainder of this paper, we confine ourselves to considering only a subclass of the MM class obtained by imposing a restriction on ϕ to be injective. From this subclass we derive a new degree optimized class of resilient Boolean functions. The procedure of obtaining a degree optimized function, starting with a function of relatively low degree from the MM class, may be viewed as a simple adding of the terms of high algebraic order in a particular manner. The functions obtained in such a way will in many cases exhibit the best known cryptographic criteria; more precisely, for a given input space n, order of resiliency t, these functions attain in many cases the highest nonlinearity value for degree optimized functions, that is, for $d = n - t - 1$. Moreover, the new class turns out to cover exactly those cases for which the construction of degree optimized functions through original MM method is not possible.

Resilient nonlinear functions $F : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)^m$ are important cryptographic objects, and several methods were developed to construct cryptographically strong such functions. The use of bent concatenation together with a function composition was proposed in [20]. The technique in [38] uses a linear resilient function, obtained from an error-correcting code, and ap-

Manuscript received January 17,2006; revised May 3, 2006. The material in this paper was presented in part at the Ninth IMA Conference on Cryptography and Coding, Cirencester, U.K., December 2003.

The author is with the Danish Technical University, Matematiktorvet, Building 303, DK-2800 Kgs. Lyngby, Denmark (e-mail: enespasalic@yahoo.se).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2006.881721

0018-9448/$20.00 © 2006 IEEE

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

plies a highly nonlinear permutation on such a function. An application of linearized polynomials in construction of nonlinear resilient functions has been proposed in [7]. However, most of the methods generate functions of relatively low algebraic degree.

The mapping F above can naturally be viewed as a collection of m Boolean mappings, that is, $F = (f_0, \ldots, f_{m-1})$, where $f_i : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)$ $(0 \leq i \leq m-1)$, each f_i specifying the ith output bit of F. In the case of vectorial Boolean functions, all cryptographic criteria are defined with respect to nonzero linear combinations of component functions f_i, thus, the component functions must be carefully selected. Similar ideas used in the degree optimization of Boolean function are applied to class of $F : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)^m$ that uses a single or a set of disjoint linear codes (called extended MM class in the sequel), see Section IV for further details. In this manner, resilient functions of very high algebraic degree are obtained.

Another important issue related to this class of functions is its algebraic properties. These properties in the first place reflect the resistance of functions not to admit a low-degree annihilation. That is, neither for f nor for $1+f$ there should exist a low-degree function g such that $f(x)g(x) = 0$, alternatively $(1+f(x))g(x) = 0$. For the Boolean case, it was proved that any function in n variables (the function or its complement) admits a nontrivial annihilation by degree $\lceil \frac{n}{2} \rceil$ function g [10]. The degree of annihilators for arbitrary f can be significantly lower than $\lceil \frac{n}{2} \rceil$; therefore the functions allowing annihilators of degree $\geq \lceil \frac{n}{2} \rceil$ are said to have maximum *algebraic immunity*. We show that a certain subclass of the MM class does not posses the maximum algebraic immunity, hence not providing a maximum resistance to algebraic attacks. Moreover, a similar technique, when applied to resilient nonlinear functions in the extended MM class, indicates the existence of extremely low degree multivariate equations. This result was not predicted with a general degree bound derived in [9]. It completely compromises the use of resilient functions $F : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)^m$ in the extended MM class as a filtering function in nonlinear combining generators.

The rest of the paper is organized as follows. Section II introduces basic definitions and cryptographic criteria relevant for Boolean mappings. In Section III, a deeper background on the MM class is presented. Then we propose a modification of this class, which results in a new class of degree optimized resilient functions attaining in many cases the highest nonlinearity known. Section IV is an extended framework of the method presented in Section III aimed at construction of nonlinear vectorial resilient functions of very high algebraic degree. Algebraic immunity of a subclass of functions in the MM class is investigated in Section V. The algebraic properties of the extended MM class are treated in Section VI. Finally, some concluding remarks are given in Section VII.

II. Preliminaries

A Boolean function on n variables may be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$. A Boolean function $f(x_1, \ldots, x_n)$ is also interpreted as the output column of its *truth table* f, i.e., a binary string of length 2^n

$$f = [f(0,0,\ldots,0), f(1,0,\ldots,0), \ldots, f(1,1,\ldots,1)].$$

The *Hamming weight* or simply the weight of a binary string S is the number of ones in S. This is denoted by $\mathrm{wt}(S)$. The *Hamming distance* between S_1, S_2 of the same length is denoted by $d(S_1, S_2)$, i.e.,

$$d(S_1, S_2) = \#(S_1 \neq S_2).$$

An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $\mathrm{wt}(f) = 2^{n-1}$).

Addition operator over $\mathrm{GF}(2)$ is denoted by $\oplus$, and if no confusion is to arise we use the usual addition operator $+$. Sometimes, abusing the notation, $''+''$ is also used for a bitwise vector addition and in such cases we emphasize such an ambiguity. The Galois field of order 2^n will be denoted by $\mathbb{F}_{2^n}$ and the corresponding vector space by $\mathbb{F}_2^n$. An n-variable Boolean function $f(x_1, \ldots, x_n)$ can be considered to be a multivariate polynomial over $\mathbb{F}_2$. This polynomial can be expressed as a sum of distinct kth-order products $(0 \leq k \leq n)$ of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i} \right) \tag{1}$$

for $\lambda_u \in \mathbb{F}_2$, $u = (u_1, \ldots, u_n)$.

This representation of f is called the algebraic normal form (ANF) of f. The *algebraic degree* of f, denoted by $\deg(f)$ or sometimes simply d, is the maximal value of the Hamming weight of u such that $\lambda_u \neq 0$. There is a one-to-one correspondence between the truth table and the ANF via the so-called inversion formulas.

The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$. For any $0 \leq b \leq n$ an n-variable function is called nondegenerate on b variables if its ANF contains exactly b distinct input variables. Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. The set of all n-variable affine (respectively, linear) functions is denoted by $\mathcal{A}_n$ (respectively, $\mathcal{L}_n$). The *nonlinearity* of an n-variable function f is

$$\mathcal{N}_f = \min_{g \in \mathcal{A}_n} (d(f,g)). \tag{2}$$

That is, the nonlinearity is the distance from the set of all n-variable affine functions.

For $x, \omega \in \mathbb{F}_2^n$, the dot or inner product is defined as $x \cdot \omega = x_1\omega_1 + \cdots + x_n\omega_n$. The *Walsh transform* of $f \in \mathcal{B}_n$ at point $\omega \in \mathbb{F}_2^n$ is a real valued function defined by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \cdot \omega}. \tag{3}$$

In terms of Walsh spectra, the nonlinearity of f is given by

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|. \tag{4}$$

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

In [37], an important characterization of resilient functions has been provided. A function $f(x_1,\ldots,x_n)$ is *t-resilient* if and only if its Walsh transform satisfies

$$W_f(\omega)=0, \qquad \text{for } 0\le \mathrm{wt}(\omega)\le t.$$

Following the notation used in [31], [32], by an (n,t,d,σ) function we denote an n-variable, t-resilient function with degree d and nonlinearity σ.

III. The MM Class Revisited

Construction of resilient functions by concatenating the truth tables of small affine functions was first described in [1] and revisited in greater details in [33], [6]. The concatenation simply means that the truth tables of the functions are merged. For instance, for $f=f_1\|f_2$, the upper half part of the truth table of f correspond to f_1 and the lower half part to f_2. The concatenation of affine functions together with certain nonlinear function has been used in several works. Independently, Dobbertin [14] and Seberry *et al.* [33] have provided constructions of balanced Boolean functions (n even), which attain the best known nonlinearity values for this class of functions. The improvement upon these results seems to be an extremely difficult task. The basic idea was to utilize all $2^{n/2}-1$ nonconstant distinct linear functions in $n/2$ variables. Then in a recursive manner a specific nonlinear function in $n/2$ variables could be constructed in order to obtain an n-variable function (concatenation of $2^{n/2}-1$ linear function and one nonlinear function) of the highest nonlinearity known for the class of balanced functions and even n.

A more general approach was utilized in [31], where each affine function was used more than once in the form of a composition with nonlinear functions. In such way, highly nonlinear low-order resilient functions could be obtained, the functions having the nonlinearity $2^{n-1}-2^{\frac{n}{2}}+2^{\frac{n}{2}-2}$ for even n. The nonlinearity value was further improved due to the method in [23]. To reach beyond the nonlinearity value $2^{n-1}-2^{\frac{n}{2}}+2^{\frac{n}{2}-2}$ (n is again even) the authors apply the concatenation of $2^{\frac{n}{2}}-2^k$ linear resilient functions in $n/2$ variables together with a highly nonlinear resilient function in $n/2+k$ variables satisfying certain conditions. Furthermore, in [3], the concatenation of affine functions is replaced by concatenation of quadratic functions but neither of these methods produces the degree optimized functions in general.

The difference between the technique to be presented in this paper from the known construction methods is the interplay between the choice of linear functions and the nonlinear function. More precisely, to construct a t-resilient degree optimized n variable function (a high nonlinearity is in particular achieved when n is odd) the $2^{n-k}-1$ in number k-variable t-resilient linear functions are selected with respect to certain covering relation and one nonlinear function in k-variable of particular form. This method generates functions whose nonlinearity attains exactly the same value as the technique that uses concatenation of distinct linear functions. Moreover, due to the choice of a nonlinear function the degree is optimized reaching the Siegenthaler's bound.

We recall the definition of the functions in the original MM class [13] as a concatenation of purely affine functions.

Definition 1: For any positive integers s,k such that $n=s+k$ an MM function is a Boolean function on $\mathbb{F}_2^n$ defined by

$$f(y,x)=\phi(y)\cdot x+h(y), \qquad x\in\mathbb{F}_2^k, y\in\mathbb{F}_2^s. \tag{5}$$

Here, h is any Boolean function on $\mathbb{F}_2^s$ and ϕ is any mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^k$.

Notice that in the definition of the MM class ϕ is an arbitrary function from $\mathbb{F}_2^s$ to $\mathbb{F}_2^k$. By imposing the restriction that ϕ is injective we must have $k\ge s$. A special case of this method is a construction of bent functions. Taking $n=2k$, i.e., $s=k$ and any bijective mapping ϕ (ϕ is a permutation on $\mathbb{F}_2^s$) will result in a bent function. It is also easy to verify that requiring ϕ to be such that $\mathrm{wt}(\phi(y))\ge t+1$ for any $y\in\mathbb{F}_2^s$ correspond to a t-resilient function f.

Let us investigate the consequences of the condition that $\phi:\mathbb{F}_2^s\mapsto\mathbb{F}_2^k$ is injective of weight greater than t, for $t\ge 0$. As already noticed [6], there is a binomial relationship between the parameters involved (note that $n=s+k$)

$$\binom{k}{t+1}+\binom{k}{t+2}+\cdots+\binom{k}{k}\ge 2^{n-k}. \tag{6}$$

Hence, for $n=s+k$ such that (6) holds, then there will exist injective mappings ϕ and, consequently, the function f will be t-resilient functions with nonlinearity $\mathcal{N}_f=2^{n-1}-2^{k-1}$ [6] (see also Theorem 1 below). Obviously, the aim is to minimize the parameter k with respect to (6). Therefore, for fixed integers t and $n=s+k$, $0\le t<k$ we define

$$\boldsymbol{k}=\min_{t<k}\left\{ k \mid \sum_{i=0}^{k-(t+1)}\binom{k}{t+1+i}\ge 2^{n-k}\right\}. \tag{7}$$

The ANF of f, as defined by (5), is more easily comprehend when f is represented as a concatenation of linear functions from $\mathcal{L}_{\boldsymbol{k}}$, that is, $h(y)=0$. For the exact calculation of cryptographic properties it is of relevance to specify the mapping ϕ[1] (or at least to prove the existence of such a mapping). Let for any $0\le t<k$, $\mathcal{L}_{\boldsymbol{k}}^t$ denote the set of all linear functions on $\mathbb{F}_2^{\boldsymbol{k}}$ nondegenerate on at least $t+1$ variables, that is,

$$\mathcal{L}_{\boldsymbol{k}}^t=\{\,\varphi_c(x)=c\cdot x \mid c\in\mathbb{F}_2^{\boldsymbol{k}},\mathrm{wt}(c)>t\,\}. \tag{8}$$

Then, the following properties have been proved in [6].

Theorem 1: [6] For any $0\le t<n$, let $\boldsymbol{k}$ be defined by (7) and $\mathcal{L}_{\boldsymbol{k}}^t$ by (8). Let us choose $2^{n-\boldsymbol{k}}$ distinct linear functions in $\mathcal{L}_{\boldsymbol{k}}^t$, each being labeled by an element of $\mathbb{F}_2^{n-\boldsymbol{k}}$ as follows:

$$\tau\in\mathbb{F}_2^{n-\boldsymbol{k}} \iff \ell_{[\tau]}\in\mathcal{L}_{\boldsymbol{k}}^t, \qquad \text{where } [\tau]=\sum_{i=1}^{n-\boldsymbol{k}}\tau_i 2^{i-1}.$$

Then the Boolean function defined for all $(y,x)\in\mathbb{F}_2^{n-\boldsymbol{k}}\times\mathbb{F}_2^{\boldsymbol{k}}$ by

$$f(y,x)=\sum_{\tau\in\mathbb{F}_2^{n-\boldsymbol{k}}}(y_1+\tau_1+1)\cdots(y_{n-\boldsymbol{k}}+\tau_{n-\boldsymbol{k}}+1)\ell_{[\tau]}(x) \tag{9}$$

[1]It turns out that both the autocorrelation properties as well as the algebraic degree of function f will depend on the choice of ϕ.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

is a t-resilient function with nonlinearity $\mathcal{N}_f = 2^{n-1} - 2^{\boldsymbol{k}-1}$. In general, $\deg(f) \leq n - \boldsymbol{k} + 1$ with equality if there exists a variable $x_i, i = 1, \ldots, \boldsymbol{k}$, which occurs an odd number of times in $\ell_{[\tau]}(x)$ when τ runs through $\mathbb{F}_2^{n-\boldsymbol{k}}$.

Remark 1: The authors in [6] only consider a concatenation of linear functions. A more general approach is to use affine functions instead, that is, to replace $\ell_{[\tau]}(x)$ by $a_{[\tau]}(x)$. If ϕ is injective then none of the cryptographic parameters is affected by this replacement so one can equally well consider only linear functions. Referring to Definition 1 and (9), one can define f to be a concatenation of affine functions, that is,

$$f(y,x) = \sum_{\tau \in \mathbb{F}_2^{n-\boldsymbol{k}}} \prod_{i=1}^{n-\boldsymbol{k}} (y_i + \tau_i + 1) a_{[\tau]}(x) \tag{10}$$

where $a_{[\tau]}(x) = \phi(\tau) \cdot x + h(\tau)$. Then the set $\mathcal{L}_{\boldsymbol{k}}^t$ above is replaced by

$$\mathcal{A}_{\boldsymbol{k}}^t = \{\, a_c(x) = c \cdot x + b_c \mid c \in \mathbb{F}_2^{\boldsymbol{k}},\ b_c \in \mathbb{F}_2, \mathrm{wt}(c) > t \,\}.$$

Thus, according to Theorem 1 the algebraic degree of f is upper-bounded by $\deg(f) \leq n - \boldsymbol{k} + 1$. On the other hand, the degree of any t-resilient function satisfies $\deg(f) \leq n - t - 1$. An obvious consequence is that the functions in the MM class are in general not degree optimized. This is always true for any $t < \boldsymbol{k} - 2$. In particular, when ϕ is injective then $\boldsymbol{k} \geq \lceil \frac{n+1}{2} \rceil$ for any $t > 0$, and therefore functions in the MM class cannot be degree optimized for $t < \lceil \frac{n+1}{2} \rceil - 2$.

A. Degree Optimization of the MM Class

In our method discussed below, to construct an n-variable t-resilient function, we use a set of $2^k - 1$ affine functions (each exactly once) in k-variables and exactly one specific nonlinear t-resilient function on k variables. Here k is the design parameter which can be calculated for any n and t through the formula (12) below. Hence, the function obtained through our method may be represented as a concatenation of the truth tables as $g = a_1 \| \cdots \| a_{i-1} \| \pi \| a_{i+1} \| \cdots \| a_{2^{n-k}}$, where each a_j, $j \neq i$ is affine function in $\mathcal{A}_k$ and π is a nonlinear function in $\mathcal{B}_k$.

In what follows, we look at the restriction of the set $\mathcal{A}_k^t$ but for convenience we consider the elements of $\mathbb{F}_2^k$ that uniquely correspond to linear functions as in Theorem 1. Hence, for $k > t$ and $t \geq 0$, for some fixed

$$\eta = (0, \ldots, 0, \overbrace{1}^{i_1}, \ldots, \overbrace{1}^{i_{t+1}}) \in \mathbb{F}_2^k$$

of weight $t+1$, we define the set $S_k^t(\eta) \subset \mathbb{F}_2^k$ as follows:

$$S_k^t(\eta) = \eta \cup \{\gamma \in \mathbb{F}_2^k \mid \mathrm{wt}(\gamma) > t \ \&\ \exists j \in [1, t+1] : \gamma_{i_j} = 0 \,\}. \tag{11}$$

In other words, $a \in S_k^t(\eta)$ if and only if $\eta \not\preccurlyeq a$, that is, η is not covered by any $a \in S_k^t(\eta) \setminus \{\eta\}$, where the relation $\eta \preccurlyeq a$ means that a *covers* η, i.e., $\eta_i \leq a_i$ for all i in the range $[1, k]$.

Clearly, the cardinality of this set is

$$\#S_k^t(\eta) = \sum_{i=0}^{k-(t+1)} \binom{k}{t+1+i} - 2^{k-t-1} + 1.$$

To verify this, without loss of generality (w.l.o.g.) assume that $\eta = (\overbrace{1, \ldots, 1}^{t+1}, 0, \ldots, 0)$. Keeping the first $t+1$ coordinates fixed there will be exactly $2^{k-t-1} - 1$ vectors in $\mathbb{F}_2^k \setminus \{\eta\}$ which cover η. Therefore, for fixed integers t and $n = s + k$, $0 \leq t < n$ we define

$$\boldsymbol{k} = \min_{t<k} \Big\{\, k \mid \sum_{i=0}^{k-(t+1)} \binom{k}{t+1+i} - 2^{k-t-1} + 1 \geq 2^{n-k} \Big\}. \tag{12}$$

Henceforth, we assume that k is always chosen to be the minimum positive integer satisfying (12), that is, $k = \boldsymbol{k}$.

Construction 1: Let t be a nonnegative integer, and let $n \geq t+3$ be the input variable space. For a positive integer k defined by (12) and for a fixed $\eta \in \mathbb{F}_2^k$ of weight $t+1$ (with $\eta_{i_j} = 1$ if and only if $j \in [1, t+1]$), let the set $S_k^t(\eta)$ be given by (11). Denote by ϕ any injective mapping from $\mathbb{F}_2^{n-k}$ to $S_k^t(\eta)$ satisfying $\phi(\delta) = \eta$ for some $\delta \in \mathbb{F}_2^{n-k}$. Then, for $(y, x) \in \mathbb{F}_2^{n-k} \times \mathbb{F}_2^k$ we construct the function $g : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ as follows:

$$g(y,x) = \begin{cases} \phi(y) \cdot x + h(y), & y \neq \delta \\ \phi(\delta) \cdot x + x_{i_{t+2}} x_{i_{t+3}} \cdots x_{i_k} + h(\delta), & y = \delta \end{cases}$$

where h is any Boolean function on $\mathbb{F}_2^{n-k}$.

Remark 2: The existence of injective ϕ in Construction 1 is assured as k satisfies (12).

To simplify the proofs concerning the main properties of functions proposed by Construction 1 and to emphasize the connection to the MM class, we first derive a result which interlinks Construction 1 with the pure affine concatenation as given in Remark 1.

Proposition 1: Let $f(y,x)$ be a function in the standard MM class, defined by means of Remark 1, that is,

$$f(y,x) = \sum_{\tau \in \mathbb{F}_2^{n-k}} \prod_{i=1}^{n-k} (y_i + \tau_i + 1) a_{[\tau]}(x)$$

where $a_{[\tau]}(x) = \phi(\tau) \cdot x + h(\tau)$ and ϕ, h are the same mappings used to define g in Construction 1. Assume that $t < k - 2$. Then the function $g(y,x)$, as defined in Construction 1, is a degree optimized function whose algebraic normal form is given by

$$g(y,x) = f(y,x) + x_{i_{t+2}} x_{i_{t+3}} \cdots x_{i_k} \prod_{i=1}^{n-k} (y_i + \delta_i + 1). \tag{13}$$

Proof: We first prove that the algebraic normal form of g is given as above. Note that we can write

$$\begin{aligned} f(y,x) &= \sum_{\tau \in \mathbb{F}_2^{n-k}} \left(\prod_{i=1}^{n-k} (y_i + \tau_i + 1) \right) a_{[\tau]}(x) \\ &= \sum_{\tau \in \mathbb{F}_2^{n-k} \setminus \delta} \left[\left(\prod_{i=1}^{n-k} (y_i + \tau_i + 1) \right) a_{[\tau]}(x) \right] \\ &\quad + \left(\prod_{i=1}^{n-k} (y_i + \delta_i + 1) \right) a_{[\delta]}(x). \end{aligned}$$

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

Then clearly

$$g(y,x) = f(y,x) + \left(\prod_{i=1}^{n-k}(y_i+\delta_i+1)\right) \times (\overbrace{a_{[\delta]}(x)+\phi(\delta)\cdot x + h(\delta)}^{=0} + x_{i_{t+2}}x_{i_{t+3}}\cdots x_{i_k})$$

and we obtain (13) as stated.

To prove that g is degree optimized it suffices to notice that any term in the ANF of f is of the form $y_{j_1}\cdots y_{j_s}x_i$, hence containing only one x_i for $i = 1,\ldots,k$. Thus, the terms $x_{i_{t+2}}x_{i_{t+3}}\cdots x_{i_k}\prod_{i=1}^{n-k}(y_i+\delta_i+1)$ cannot be present in the ANF of f assuming that $k-t>2$. The term $x_{i_{t+2}}x_{i_{t+3}}\cdots x_{i_k}y_1\cdots y_{n-k}$ is of degree $k-(t+1)+n-k = n-t-1$, so g is degree optimized. □

Note that the assumption that $t < k-2$ perfectly matches those functions in the MM class which cannot be degree optimized. Furthermore, the function g as described above besides the term of the highest degree order introduces many terms of order $n-t-2$ down to $k-(t+2)$ none of which is present in the ANF of f. This results in a significantly increased linear complexity of g in comparison to f. Another important observation is that the number of terms present in the ANF of g will depend on the value of δ, and the maximum number is obtained for $\delta = (0,\ldots,0)$.

Next we prove that the function g is t-resilient having the same nonlinearity as f.

Theorem 2: The function g proposed by Construction 1 is an $(n,t,n-t-1,2^{n-1}-2^{k-1})$ function. Furthermore, the Walsh spectra of g is seven-valued, and more precisely

$$W_g(w) \in \{0, \pm 2^{t+2}, \pm 2^{k-t}(2^t-1), \pm 2^k\}.$$

Proof: By Proposition 1, g is a degree optimized function. Note that $g(y,x)$ is an affine t-resilient function for any fixed $y \neq \delta$. Hence, to show that g is t-resilient it is enough to show that the function $x_{i_1}+\cdots+x_{i_{t+1}}+x_{i_{t+2}}x_{i_{t+3}}\cdots x_{i_k}$ is a t-resilient function. This is obviously true since this function contains $t+1$ more linear terms from a disjoint variable space than the nonlinear term. Then g can be viewed as a concatenation of t-resilient functions, hence t-resilient itself.

Abusing the notation, we use the addition operator $''+''$ for a componentwise bit addition of vectors and also for a usual integer addition. That is, for $\alpha,\beta \in \mathbb{F}_2^k$ we compute $\alpha+\beta = (\alpha_1+\beta_1,\ldots,\alpha_k+\beta_k)$. It should be clear from the context which operation is performed.

To prove that the nonlinearity value is the same as for f we consider the Walsh transform of g. Then for any $(\beta,\alpha) \in \mathbb{F}_2^{n-k}\times\mathbb{F}_2^k$ we have

$$\begin{aligned} W_g((\beta,\alpha)) &= \sum_{y\in\mathbb{F}_2^{n-k}}\sum_{x\in\mathbb{F}_2^k}(-1)^{g(y,x)\oplus(y,x)\cdot(\beta,\alpha)} \\ &= \sum_{y\in\mathbb{F}_2^{n-k}\setminus\delta}(-1)^{y\cdot\beta\oplus h(y)}\sum_{x\in\mathbb{F}_2^k}(-1)^{(\phi(y)+\alpha)\cdot x} \\ &\quad (-1)^{\delta\cdot\beta\oplus h(\delta)}\sum_{x\in\mathbb{F}_2^k}(-1)^{\phi(\delta)\cdot x\oplus\alpha\cdot x\oplus x_{i_{t+2}}x_{i_{t+3}}\cdots x_{i_k}}. \end{aligned}$$

There are three cases to consider. The first case arises when $\alpha \in \mathbb{F}_2^k$ is such that $\alpha = \phi(y)$ for some $y \neq \delta$, that is, $\alpha \in S_k^t(\eta)\setminus\eta$. Then obviously the first sum in (14) is equal to $\pm 2^k$, where this nonzero contribution is obtained for some $y \neq \delta$. But

$$(-1)^{\delta\cdot\beta\oplus h(\delta)}\sum_{x\in\mathbb{F}_2^k}(-1)^{(\phi(\delta)\oplus\alpha)\cdot x\oplus x_{i_{t+2}}x_{i_{t+3}}\cdots x_{i_k}} = 0,$$

since the exponent is a balanced function in x. To verify this, notice that since ϕ is injective it implies that $\phi(\delta)+\alpha \neq \mathbf{0}$ in the exponent of the second sum. Due to the properties of the set $S_k^t(\eta)$ and since α is an element of this set, α cannot cover $\phi(\delta)$, or equivalently, $(\phi(\delta)+\alpha)\cdot x$ will contain at least one x_j, $j \in \{i_1,\ldots,i_{t+1}\}$.

The second case to consider is the case when $\alpha = \phi(\delta)$. Clearly the first sum in (14) is zero. The second sum is of the form $(-1)^{\delta\cdot\beta\oplus h(\delta)}\sum_{x\in\mathbb{F}_2^k}(-1)^{x_{i_{t+2}}\cdots x_{i_k}}$ implying that

$$|W_g((\beta,\alpha))| = 2^k - 2\cdot 2^{k-(t+1)} = 2^{k-t}(2^t-1).$$

Finally, the third case arises when $\alpha \notin S_k^t(\eta)$. Then the first sum in (14) is obviously zero, whereas the second sum may take three different values depending on the value of α. Indeed, since $(\phi(\delta)+\alpha)\cdot x \neq \mathbf{0}$, the second sum is either 0 or $\pm 2\cdot 2^{t+1} = \pm 2^{t+2}$ depending on whether $(\phi(\delta)+\alpha)\cdot x \oplus x_{i_{t+2}}\cdots x_{i_k}$ is balanced or not. The value 0 corresponds to the case of balancedness, that is, $(\phi(\delta)+\alpha)\cdot x$ contains some x_j such that $j \notin \{i_{t+2},\ldots,i_k\}$. When $(\phi(\delta)+\alpha)\cdot x$ does not contain some x_j such that $j \notin \{i_{t+2},\ldots,i_k\}$ two cases are possible. Then $(\phi(\delta)+\alpha)\cdot x + x_{i_{t+2}}\cdots x_{i_k}$ is either balanced ($W_g((\beta,\alpha)) = 0$), or this function is balanced on all $(t+1)$-dimensional flats except for being constant on exactly one flat of dimension $t+1$ corresponding to the nonlinear term $x_{i_{t+2}}\cdots x_{i_k}$. In the latter case, $W_g((\beta,\alpha)) = \pm 2^{t+2}$. To summarize, when $\alpha \notin S_k^t(\eta)$, $W_g((\beta,\alpha)) \in \{0,\pm 2^{t+2}\}$.

Hence,

$$\mathcal{N}_g = 2^{n-1} - \frac{1}{2}\max_{(\beta,\alpha)\in\mathbb{F}_2^{n-k}\times\mathbb{F}_2^k}|W_g((\beta,\alpha))| = 2^{n-1}-2^{k-1}.$$

Also, from the details of the proof it is clear that

$$W_g(w) \in \{0,\pm 2^{t+2},\pm 2^{k-t}(2^t-1),\pm 2^k\}. \qquad \square$$

Remark 3: The concept of using the nonlinear functions may naturally be extended to include even more nonlinear functions on the subspaces of dimension k. Notice that using more such functions will additionally increase the complexity of the keystream sequence but this feature is traded off against more rigorous conditions on the set $S_k^t(\eta)$. Thus, defining the set $T \subseteq P = \{p \in \mathbb{F}_2^k \mid \mathrm{wt}(p) = t+1\}$, the problem is transformed to finding such $\boldsymbol{k} = \min_{t<k}\{\, k \mid \#S_k^t(T) \geq 2^{n-k}\}$, where

$$S_k^t(T) = \{c \mid c \in \mathbb{F}_2^k, \mathrm{wt}(c) > t \text{ and } p \not\preccurlyeq c \text{ for any } p \in T\}.$$

Now taking any injective mapping ϕ from $\mathbb{F}_2^{n-k}$ to $S_k^t(T)$, the function g^* can be defined in a similar way as above

$$g^*(y,x) = \begin{cases} \phi(y)\cdot x + h(y), & y \mid \phi(y) \in S_k^t(T)\setminus T \\ \phi(y)\cdot x + \prod_{i=1}^k x_i^{\phi(y)_i\oplus 1} + h(y), & y \mid \phi(y) \in T \end{cases}$$

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

where h is any Boolean function on $\mathbb{F}_2^{n-k}$, and $\phi(y)_i$ denotes the ith coordinate of the image of ϕ.

We give two important examples to emphasize the importance of this construction. These examples demonstrate the possibility of constructing degree optimized resilient functions with nonlinearity which has not been achieved previously.

Example 1: A construction of an $(11, 2, 8, \mathcal{N}_f)$ function has been discussed in the literature. Using a recursive procedure called Algorithm B, an $(11, 2, 8, 984)$ function has been obtained in [31], which so far gives the highest nonlinearity for fixed $n = 11$, $t = 2$, $d = 8$.

According to the weight divisibility results

$$W_f(\alpha) \equiv 0 \pmod{2^{t+2+\lfloor \frac{n-t-2}{d} \rfloor}}, \quad \forall\, \alpha \in \mathbb{F}_2^n$$

and for any (n, t, d) function f, see [2], [32]. It can be verified that for $n = 11$, $t = 2$, $d = 8$, that $|\max_{\alpha \in \mathbb{F}_2^n} W_f(\alpha)| = r \cdot 16$, where $r \geq 3$. Note that the standard MM method would require the value $k = 6$ to improve upon the nonlinearity of the above result [31] (for $k = 6$ we would have $\mathcal{N}_f = 2^{n-1} - 2^{k-1} = 992$). But then $t < k - 2$ implying that this method cannot generate a degree optimized function (actually, the maximum degree through this technique is $d = n - k + 1 = 6$). It can be verified that for $n = 11$, $t = 2$ and $k = 6$

$$\#S_k^t(\eta) = \sum_{i=0}^{k-(t+1)} \binom{k}{t+1+i} - 2^{k-t-1} + 1 = 35 \geq 2^{n-k} = 32$$

implying that **for the first time**, using Construction 1, we can construct an $(11, 2, 8, 992)$ function g.

In the following example, we consider the same input parameters but including even more nonlinear terms as remarked above.

Example 2: In order to preserve the same nonlinearity value, we use the same k as in the preceding example. Then for $n = 11$, $t = 2$ and $k = 6$, let $T = \{(1,1,1,0,0,0), (1,1,0,1,0,0)\}$. For such a choice of T we have

$$\begin{aligned} \#S_k^t(T) &= \sum_{i=0}^{k-(t+1)} \binom{k}{t+1+i} - 2^{k-t-1} + 1 - 3 \\ &= 32 \geq 2^{n-k} = 32 \end{aligned}$$

implying that using the extension of Construction 1 as given in the above remark we can construct an $(11, 2, 8, 992)$ function g^* having much more terms of high algebraic degree than the function g in Example 1.

The choice of T in the preceding example is not arbitrary. For some other choices of this set it can happen that $\#S_k^t(T) < 2^{n-k}$ implying a decrease in nonlinearity since a larger k must be used.

It should be noticed that for a fixed k there is a maximum cardinality of the set T for which the nonlinearity value remains the same.

Proposition 2: For given integers n, k let $T \subset \mathbb{F}_2^k$ satisfying, $\#S_k^t(T) \geq 2^{n-k}$. Then, if

$$\#T \leq 2^{k-t-2}$$

the nonlinearity of function f defined by means of extended Construction 1 is $\mathcal{N} = 2^{n-1} - 2^{k-1}$.

Proof: We follow the same steps as in the proof of Theorem 2. There are three cases to consider. When $\alpha \in S_k^t(T) \setminus T$, the values in the Walsh spectra remain the same as in the case with $\#T = 1$. Let $\phi(P) = T$ keeping the same notation as before. Then we consider

$$\begin{aligned} W_g((\beta, \alpha)) &= \sum_{y \in \mathbb{F}_2^{n-k}} \sum_{x \in \mathbb{F}_2^k} (-1)^{g(y,x) \oplus (y,x) \cdot (\beta, \alpha)} \\ &= \sum_{y \in \mathbb{F}_2^{n-k} \setminus P} (-1)^{y \cdot \beta \oplus h(y)} \sum_{x \in \mathbb{F}_2^k} (-1)^{(\phi(y)+\alpha) \cdot x} \\ &\quad + \left(\sum_{y \in P} (-1)^{y \cdot \beta \oplus h(y)} \right) \\ &\quad \times \sum_{x \in \mathbb{F}_2^k} (-1)^{(\phi(y)+\alpha) \cdot x + \prod_{i=1}^k x_i^{\phi(y)_i \oplus 1}}. \end{aligned} \tag{14}$$

Then again the sum in (14) is equal to $\pm 2^k$. Also,

$$\sum_{y \in P} (-1)^{y \cdot \beta \oplus h(y)} \sum_{x \in \mathbb{F}_2^k} (-1)^{(\phi(y)+\alpha) \cdot x + \prod_{i=1}^k x_i^{\phi(y)_i \oplus 1}} = 0$$

due to the properties of $S_k^t(T)$.

The second case to consider is the case when $\alpha \in \phi(P) = T$. Clearly, the first sum in (14) is zero. Since α is fixed, the terms in the second sum are equal to zero unless $\phi(y) = \alpha$. For such a y, say $y = \delta$, we compute the sum

$$(-1)^{\delta \cdot \beta \oplus h(\delta)} \sum_{x \in \mathbb{F}_2^k} (-1)^{x_{i_{t+2}} \cdots x_{i_k}}$$

implying that $|W_g((\beta, \alpha))| = 2^k - 2 \cdot 2^{k-(t+1)} = 2^{k-t}(2^t - 1)$. Notice that the other terms are equal to zero due to the properties of $S_k^t(T)$. That is, when $\phi(y) \neq \alpha$ then $(\phi(y) + \alpha) \cdot x + \prod_{i=1}^k x_i^{\phi(y)_i \oplus 1}$ is a balanced function on x.

The third case arises when $\alpha \notin S_k^t(T)$. Then the first sum in (14) is obviously zero, whereas the second sum may take three different values depending on the value of α. However, it can be verified that the maximum absolute value is upper-bounded, that is,

$$|W_g((\beta, \alpha))| \leq \#T \cdot 2^{t+2}.$$

Thus, provided that $\#T \leq 2^{k-t-2}$ we have $|W_g((\beta, \alpha))| \leq 2^k$, which concludes the proof. □

Open Problem 1: Derive a general explicit formula for the cardinality of $S_k^t(T)$ as a function of k, t, and $|T|$. In particular, for given n, t, and the minimal k satisfying the condition

$$\sum_{i=0}^{k-(t+1)} \binom{k}{t+1+i} - 2^{k-t-1} + 1 \geq 2^{n-k}$$

determine the maximum cardinality of T (where T has more than one element) such that $\#S_k^t(T) \geq 2^{n-k}$.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

IV. Resilient Functions of High Algebraic Degree

When constructing multiple-output Boolean functions one applies similar cryptographic criteria as in the Boolean case. Since this mapping is defined as $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, all the criteria of concern are defined with respect to all nonzero linear combinations of the output functions $f_0, \ldots, f_{m-1}$.

Lemma 1: [38] A function $F = (f_0, \ldots, f_{m-1})$ is an (n, m, t)-resilient function if and only if all nonzero linear combinations of $f_0, \ldots, f_{m-1}$ are $(n, 1, t)$-resilient functions.

The definition of nonlinearity follows in a similar manner, taken from [28].

Definition 2: The nonlinearity of $F = (f_0, \ldots, f_{m-1})$, denoted by $\mathcal{N}_F$, is defined as

$$\mathcal{N}_F = \min_{\alpha \in \mathbb{F}_2^m \setminus \{0\}} \mathcal{N}_{f_\alpha} \tag{15}$$

where $f_\alpha = \sum_{i=0}^{m-1} \alpha_i f_i$, $\alpha_i \in \mathbb{F}_2$.

Similarly, the algebraic degree of F is defined as

$$\deg(F) = \min_{\alpha \in \mathbb{F}_2^m \setminus \{0\}} \deg\Big(\sum_{i=0}^{m-1} \alpha_i f_i\Big). \tag{16}$$

We use the same notation most often found in the literature. An (n, m, t) function will denote an n-input, m-output, t-resilient function. The information about the nonlinearity and degree will be given additionally.

The preceding definitions imply a more subtle design of cryptographically strong functions outputting m bits compared to the Boolean case. Linear codes have been frequently used in many methods (see, for example, [18], [30]) to obtain resilient functions. The concept relies on the fact that the nonzero codewords of a $[u, m, t+1]$ linear code C are strictly of weight greater than t. This gives rise to t-resilient linear functions of the form $l_i(x) = \boldsymbol{\Theta}_i \cdot x$, where $\boldsymbol{\Theta}_i$ is some nonzero codeword of C. Then, denoting by $\boldsymbol{\Theta}_0, \ldots, \boldsymbol{\Theta}_{m-1}$ the basis of C, we obviously have that all nonzero linear combinations of the form $(\sum_{i=0}^{m-1} a_i \boldsymbol{\Theta}_i) \cdot x$ are again t-resilient linear functions. Using codewords of the same code in a certain manner and also the codewords of many disjoint codes (see below for the definition) one may construct highly nonlinear resilient functions $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. Since each component function of F may be viewed as a concatenation of a linear function it makes sense to call this class of functions the extended MM class.

The main result that enables the use of linear codes is given in the following lemma [18].

Lemma 2: [18] Let $\boldsymbol{\Theta}_0, \ldots, \boldsymbol{\Theta}_{m-1}$ be a basis of a binary $[u, m, t+1]$ linear code C. Let β be a primitive element in $\mathbb{F}_{2^m}$ and $(1, \beta, \ldots, \beta^{m-1})$ be a polynomial basis of $\mathbb{F}_{2^m}$. Define a bijection $\rho : \mathbb{F}_{2^m} \mapsto C$ by

$$\rho(a_0 + a_1\beta + \cdots + a_{m-1}\beta^{m-1}) = a_0\boldsymbol{\Theta}_0 + \cdots + a_{m-1}\boldsymbol{\Theta}_{m-1}.$$

Consider the matrix

$$A^* = \begin{pmatrix} \rho(1) & \rho(\beta) & \ldots & \rho(\beta^{m-1}) \\ \rho(\beta) & \rho(\beta^2) & \ldots & \rho(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \rho(\beta^{2^m-2}) & \rho(1) & \ldots & \rho(\beta^{m-2}) \end{pmatrix}$$

of size $(2^m - 1) \times m$, whose entries are elements of $\mathbb{F}_2^u$ (actually the codewords of C). For any linear combination of columns (not all zero) of the matrix A^*, each nonzero codeword of C will appear exactly once in such a nonzero linear combination.

Remark 4: Since the elements of A^* are vectors, we need a triple index set to refer to a specific coordinate of some entry of A^*. Thus, $A^*_{i,j}(k)$ will indicate the kth position of the entry (vector) found in the intersection of the ith row and jth column of A^*. Hence, for A^*, of size $r \times s$ with elements in $\mathbb{F}_2^u$ we let the indices set run as follows: $i = 0, \ldots, r-1$; $j = 0, \ldots, s-1$; $k = 1, \ldots, u$. To refer to the whole vector, we simply write $A^*_{i,j}$. We also keep $'[\ ]'$ to denote the decimal representation of vectors, i.e., for $\alpha \in \mathbb{F}_2^u$, $[\alpha] = \sum_{l=1}^{u} \alpha_l 2^{l-1}$.

This lemma actually shows how to use the codewords of a linear code efficiently when constructing a function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. Then in case that $u > n - m$ one can use any 2^{n-m} rows of A^* to define $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ through the columns of A, where A is obtained by deleting some rows of A^*. The component functions of $F = (f_0, \ldots, f_{m-1})$ are simply defined as follows. For any $y \in \mathbb{F}_2^{n-u}$, we define $f_j(y, x) = A_{[y],j} \cdot x, j = 0, \ldots, m-1$.

When the parameters of C are such that $u \leq n - m$, the alternative is to use a set of disjoint $[u, m, t+1]$ linear codes as originally proposed in [18].

Definition 3: [18] A set of linear $[u, m, t+1]$ codes $\{C_1, C_2, \ldots, C_s\}$ such that

$$C_i \cap C_j = \{0\}, \qquad 1 \leq i < j \leq s$$

is called a set of linear $[u, m, t+1]$ disjoint (nonintersecting) codes.

Then the following result was given in [18], which enables us to construct an (n, m, t) function by using the codewords of several disjoint codes.

Theorem 3: [18] If there exists a set of linear $[u, m, t+1]$ disjoint codes with cardinality $\lceil 2^{n-u}/(2^m - 1) \rceil$ then there exists a t-resilient function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ with nonlinearity

$$\mathcal{N}_F = 2^{n-1} - 2^{u-1}.$$

The problem of finding a set of disjoint codes has been solved [5], [27]. In particular, when the length of the code is of the form $u = 2^m - 1$, the method in [5] gives a certain number of disjoint $[2^m - 1, m, 2^{m-1}]$ simplex-like codes. We call these codes simplex-like since they are all derived from the simplex code. On the other hand, the simplex code is considered to be a unique dual code of the Hamming code.

We combine these results with the construction idea discussed above to obtain nonlinear resilient functions of very high algebraic degree. From now on, we assume that the cardinality of the set of disjoint $[u, m, t+1]$ linear codes is b for some $b \geq 1$.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

We denote this set by $\mathcal{C}$, i.e., $\mathcal{C} = \{C_1, \ldots, C_b\}$. It is easily verified that denoting by $e = \lfloor log_2 b(2^m - 1) \rfloor$, the input space n is given as $n = e + u$, where u is the length of the codes.

Note that a straightforward application of Theorem 3 would result in functions of degree $d \leq e + 1$, which for small e is far from its optimized value $n - t - 1$. Thus, in order to increase the algebraic order, we replace linear functions at certain positions by nonlinear ones. Remark that Construction 2 below utilizes a set of disjoint simplex-like codes for which the exact calculation of resiliency order is very simple. In general, the resiliency order will depend on the properties of the code in a rather complicated way.

Construction 2: Let $\mathcal{C} = \{C_1, \ldots, C_b\}$ be a set of disjoint $[2^m - 1, m, 2^{m-1}]$ simplex-like codes, and associate to each code a mapping $\rho_r : \mathbb{F}_{2^{2^m-1}} \mapsto C_r$, $1 \leq r \leq b$, so that

$$(a_0, a_1\beta, \ldots, a_{m-1}\beta^{m-1}) \xrightarrow{\rho_r} a_0\boldsymbol{\Theta}_0^r + \cdots + a_{m-1}\boldsymbol{\Theta}_{m-1}^r$$

where $\boldsymbol{\Theta}_0^r, \ldots, \boldsymbol{\Theta}_{m-1}^r$ is a basis of C_r, $a_i \in \mathbb{F}_2$, and β is primitive in $\mathbb{F}_{2^m}$. Let A_r be the associated matrix of C_r as in Lemma 2. Let $A = (A_1^T | A_2^T | \cdots | \hat{A}_b^T)^T$ (with A_i^T denoting the transposing operation), where $\hat{A}_b$ denotes that some rows of A_b may be deleted to adjust A to be of size $2^e \times m$, and denote by $e = \lfloor \log_2 b(2^m - 1) \rfloor$. Let $G = (g_0, \ldots, g_{m-1})$ be a function from $\mathbb{F}_2^{e+2^m-1}$ to $\mathbb{F}_2^m$, whose component functions are defined for any $(y, x) \in \mathbb{F}_2^e \times \mathbb{F}_2^{2^m-1}$ as

$$g_j(y,x) = \begin{cases} A_{[y],j} \cdot x, & y \mid [y] \neq j \\ A_{[y],j} \cdot x + \prod_{k=1}^{2^m-1} x_k^{A_{[y],j}(k) \oplus 1}, & y \mid [y] = j \end{cases}$$

where $j = 0, \ldots, m-1$.

To clarify further the structure of G in Construction 2, we associate to G a function matrix A^f of size $2^e \times m$ as shown at the bottom of the page, where $x^{\rho_i(\beta^z)} = \prod_{k=1}^{2^m-1} x_k^{\rho_{i,k}(\beta^z) \oplus 1}$, denoting by $\rho_{i,k}(\beta^z)$ the kth coordinate in the vector $\rho_i(\beta^z)$ of length $2^m - 1$.[2] Note that for any $y \in \mathbb{F}_2^e$, we have $g_j(y, x) = A^f_{[y],j}$, $0 \leq j \leq m-1$.

[2]Remark that only the first m rows of A^f contain the nonlinear term $x^{\rho_1(\beta^i)}$ for $i = 0, \ldots, m-1$. This term is present in each column of matrix A^f.

Theorem 4: Let $\mathcal{C}$ be a given set of disjoint $[2^m - 1, m, 2^{m-1}]$ simplex-like codes with $|\mathcal{C}| = b$, and let $e = \lfloor \log_2 b(2^m - 1) \rfloor$. Then the function $G : \mathbb{F}_2^{2^m-1+e} \mapsto \mathbb{F}_2^m$, constructed by means of Construction 2, is a $(2^{m-2} - 1)$-resilient function, with

$$\mathcal{N}_G \geq 2^{2^m-2+e} - 2^{2^m-2} - m2^{2^{m-1}-1}$$

and $\deg(G) = e + 2^{m-1} - 1$.

Proof: We again abuse the addition operator $''+''$ to perform componentwise bit addition of vectors, bit addition, and the usual integer addition. Which operation is performed should be clear from the context.

Combining the result of Proposition 1 and the particular placement of nonlinear functions, the ANF of g_j can be written as

$$g_j(y,x) = f_j(y,x) + \prod_{k=1}^{2^m-1} x_k^{A_{j,j}(k) \oplus 1} \left(\prod_{l=1}^{e} (y_l + \tau_l^j + 1) \right)$$

for $j = 0, \ldots, m-1$. Here $\tau^j \in \mathbb{F}_2^e$ satisfies $[\tau^j] = j$, and the ANF of f_j is obtained from the jth column of the matrix A. Hence, the ANF of f_j is given by

$$f_j(y,x) = \sum_{\tau \in \mathbb{F}_2^e} \left(\prod_{l=1}^{e} (y_l + \tau_l + 1) \right) A_{[\tau],j} \cdot x.$$

Then for any nonzero $a = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_2^m$ we may write

$$\sum_{j=0}^{m-1} a_j g_j(y,x) = \sum_{j=0}^{m-1} a_j f_j(y,x) + \sum_{j=0}^{m-1} a_j \Big[\prod_{k=1}^{2^m-1} x_k^{A_{j,j}(k) \oplus 1} \Big(\prod_{l=1}^{e} (y_l + \tau_l^j + 1) \Big) \Big].$$

Since for any nonzero a the sum $\sum_{j=0}^{m-1} a_j f_j(y,x)$ is of degree $d \leq e + 1$, we only have to prove that the terms of the form $\prod_{k=1}^{2^m-1} x_k^{A_{j,j}(k) \oplus 1} \big(\prod_{l=1}^{e} (y_l + \tau_l^j + 1) \big)$ are not canceled in the function $\sum_{j=0}^{m-1} a_j g_j(y,x)$.

$$A^f = \begin{pmatrix} \rho_1(1) \cdot x + x^{\rho_1(\beta^0)} & \ldots & \rho_1(\beta^{m-1}) \cdot x \\ \rho_1(\beta) \cdot x & \ldots & \rho_1(\beta^m) \cdot x \\ \vdots & \ddots & \vdots \\ \rho_1(\beta^{m-1}) \cdot x & \ldots & \rho_1(\beta^{2m-2}) \cdot x + x^{\rho_1(\beta^{2m-2})} \\ \rho_1(\beta^m) \cdot x & \ldots & \rho_1(\beta^{2m-1}) \cdot x \\ \vdots & \ddots & \vdots \\ \rho_1(\beta^{2^m-2}) \cdot x & \ldots & \rho_1(\beta^{m-2}) \cdot x \\ \vdots & \ddots & \vdots \\ \rho_b(1) \cdot x & \ldots & \rho_b(\beta^{m-1}) \cdot x \\ \vdots & \ddots & \vdots \\ \rho_b(\beta^{2^m-2}) \cdot x & \ldots & \rho_b(\beta^{m-2}) \cdot x \end{pmatrix}$$

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

This is obviously true as any linear combination of A's columns gives a rise to two-by-two distinct codewords, that is, for any $y' \neq y''$ and nonzero a

$$\sum_{j=0}^{m-1} a_j A_{[y'],j} \neq \sum_{j=0}^{m-1} a_j A_{[y''],j}.$$

Then any term of the form $y_1 \cdots y_e \prod_{k=1}^{2^m-1} x_k^{A_{j,j}(k)\oplus 1}$ is present in $\sum_{j=0}^{m-1} a_j g_j(y,x)$. Note that the number of such terms is exactly the weight of a. Since the disjoint codes are simplex-like codes, all the codewords are of the same weight 2^{m-1}. Then

$$\mathrm{wt}\left(\prod_{k=1}^{2^m-1} x_k^{A_{j,j}(k)\oplus 1}\right) = 2^{m-1} - 1.$$

Hence, $\deg(G) = e + 2^{m-1} - 1$ as stated.

To prove that G is $(2^{m-2}-1)$-resilient, note that for any fixed y, the function G is either a linear function of weight 2^{m-1} (hence, $(2^{m-1}-1)$-resilient) or it is of the form

$$\left(\sum_{\substack{j=0\\ j\neq s}}^{m-1} a_j A_{[y],j}\right)\cdot x + A_{[y],s}\cdot x + \prod_{k=1}^{2^m-1} x_k^{A_{[y],s}(k)\oplus 1}$$

for some $s \in [0, m-1]$. Then the order of resiliency is determined by the nonlinear term above. We use simple coding arguments to prove that $\left(\sum_{j=0|j\neq s}^{m-1} a_j A_{[y],j}\right)\cdot x + A_{[y],s}\cdot x$ has exactly 2^{m-2} variables not contained in $\prod_{k=1}^{2^m-1} x_k^{A_{[y],s}(k)\oplus 1}$. Let $\boldsymbol{u} = A_{[y],s} + (1,\ldots,1)$ and $\boldsymbol{v} = \sum_{j=0|j\neq s}^{m-1} a_j A_{[y],j} + A_{[y],s}$, where $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^{2^m-1}$. Note that $\mathrm{wt}(\boldsymbol{u}) = 2^{m-1}-1$, $\mathrm{wt}(\boldsymbol{v}) = 2^{m-1}$, and $\mathrm{wt}(\boldsymbol{u}+\boldsymbol{v}) = 2^{m-1}-1$.

We simply show that $\mathrm{wt}(\boldsymbol{u}*\boldsymbol{v}) = 2^{m-2}$, where $\boldsymbol{u}*\boldsymbol{v} = (u_1v_1, \ldots, u_{2^m-1}v_{2^m-1})$. We know that [21]

$$\mathrm{wt}(\boldsymbol{u}+\boldsymbol{v}) = \mathrm{wt}(\boldsymbol{u}) + \mathrm{wt}(\boldsymbol{v}) - 2\mathrm{wt}(\boldsymbol{u}*\boldsymbol{v}).$$

Then $\mathrm{wt}(\boldsymbol{u}*\boldsymbol{v}) = \frac{1}{2}(\mathrm{wt}(\boldsymbol{u}) + \mathrm{wt}(\boldsymbol{v}) - \mathrm{wt}(\boldsymbol{u}+\boldsymbol{v}))$, and substituting the weight values $\mathrm{wt}(\boldsymbol{u}*\boldsymbol{v}) = 2^{m-2}$. Hence, G is a $(2^{m-2}-1)$-resilient function.

To prove the nonlinearity assertion, we first note that for any nonzero $a \in \mathbb{F}_2^m$ such that $\mathrm{wt}(a) = s$

$$g(y,x) = \sum_{j=0}^{m-1} a_j g_j(y,x)$$

is nonlinear on exactly s flats of dimension 2^m-1. Let $J = \{j_1,\ldots,j_s\}$, $0 \leq j_1 \neq \cdots \neq j_s \leq m-1$, be a support set of a, i.e., $a_j = 1$ for all $j \in J$. By the construction, $g(y,x)$ is nonlinear for those y satisfying $[y] \in J$, where $[y]$ denotes the decimal representation of y. Then

$$W_g((\beta,\alpha)) = \sum_{y\in\mathbb{F}_2^e}\sum_{x\in\mathbb{F}_2^{2^m-1}} (-1)^{g(y,x)+(y,x)\cdot(\beta,\alpha)} = \sum_{y\in\mathbb{F}_2^e|[y]\notin J} (-1)^{y\cdot\beta}\sum_{x\in\mathbb{F}_2^k}(-1)^{g(y,x)+x\cdot\alpha} + \sum_{y\in\mathbb{F}_2^e|[y]\in J}(-1)^{y\cdot\beta}\sum_{x\in\mathbb{F}_2^{2^m-1}}(-1)^{g(y,x)+x\cdot\alpha}. \quad (17)$$

Note that for those y, such that $[y] \notin J$, we have $g(y,x)+x\cdot\alpha = (\sum_{j\in J} A_{[y],j} + \alpha)\cdot x$ hence, the exponent above is a linear function in x. Also, for a given y such that $[y] \in J$, the exponent above can be written as

$$g(y,x) + x\cdot\alpha = \left(\sum_{j\in J} A_{[y],j} + \alpha\right)\cdot x + \prod_{k=1}^{2^m-1} x_k^{A_{[y],[y]}(k)\oplus 1}.$$

There are two cases to be considered.

First, suppose that $\alpha \in \mathbb{F}_2^{2^m-1}$ is such that $\alpha \neq \sum_{j\in J} A_{[y],j}$ for any y such that $[y] \notin J$. Then the sum of (17) is obviously zero. Computing the second sum, that is,

$$\sum_{y\in\mathbb{F}_2^e|[y]\in J}(-1)^{y\cdot\beta}\sum_{x\in\mathbb{F}_2^{2^m-1}}(-1)^{g(y,x)+x\cdot\alpha}$$

the worst case arises if $\alpha = \sum_{j\in J} A_{[y],j}$ for some y such that $[y] \in J$. But this y is unique due to the properties of the construction. Denote this y by y', and also for convenience let

$$\prod_{k=1}^{2^m-1} x_k^{A_{[y'],[y']}(k)\oplus 1} = x_{u_1}x_{u_2}\cdots x_{u_{2^{m-1}-1}}$$

and $c = \sum_{j\in J} A_{[y],j} + \alpha$. Thus, the second sum can be written as

$$\left|\sum_{y\in\mathbb{F}_2^e|[y]\in J}(-1)^{y\cdot\beta}\sum_{x\in\mathbb{F}_2^{2^m-1}}(-1)^{g(y,x)+x\cdot\alpha}\right| \leq \left|(-1)^{y'\cdot\beta}\underbrace{\sum_{x\in\mathbb{F}_2^{2^m-1}}(-1)^{x_{u_1}x_{u_2}\cdots x_{u_{2^{m-1}-1}}}}_{2^{2^m-1}-2^{2^m-1}}\right| + \left|\sum_{\substack{y\in\mathbb{F}_2^e|[y]\in J\\ y\neq y'}}(-1)^{y\cdot\beta}\underbrace{\sum_{x\in\mathbb{F}_2^{2^m-1}}(-1)^{\overbrace{c\cdot x}^{\neq 0}+x_{i_1}x_{i_2}\cdots x_{i_{2^{m-1}-1}}}}_{0 \text{ or } -2^{2^m-1}}\right| \leq (2^{2^m-1}-2^{2^{m-1}}) + (s-1)2^{2^{m-1}}.$$

Hence, in this case

$$|W_g((\beta,\alpha))| \leq (2^{2^m-1}-2^{2^{m-1}}) + (s-1)2^{2^{m-1}} = 2^{2^m-1} + (s-2)2^{2^{m-1}}.$$

Note that α can be such that $\alpha \neq \sum_{j\in J} A_{[y],j}$ for any y, either $[y] \in J$ or $[y] \notin J$. Then, it is easy to verify that $|W_g((\beta,\alpha))| \leq s2^{2^{m-1}}$, for such an α.

When $\alpha \in \mathbb{F}_2^{2^m-1}$ is such that $\alpha = \sum_{j\in J} A_{[y],j}$ for some y such that $[y] \notin J$, then the sum in (17) is equal to 2^{2^m-1}. Then using a similar calculation as above

$$\left|\sum_{y\in\mathbb{F}_2^e|[y]\in J}(-1)^{y\cdot\beta}\sum_{x\in\mathbb{F}_2^{2^m-1}}(-1)^{g(y,x)+x\cdot\alpha}\right| \leq s2^{2^{m-1}}.$$

Thus, for such an α we have $|W_g((\beta,\alpha))| \leq (2^{2^m-1}) + s2^{2^{m-1}}$.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

Obviously, the maximum value in the Walsh spectra correspond to the latter case and takes the highest value when $\mathrm{wt}(a) = m$

$$\max_{(\beta,\alpha)\in\mathbb{F}_2^e\times\mathbb{F}_2^{2^m-1}} |W_G((\beta,\alpha))| \leq (2^{2^m-1}) + m2^{2^{m-1}},$$

and the statement is proved. □

We utilize the approach in [18], based on a set of disjoint codes, just to illustrate a wider framework in which our method may be applied. We can equally well use the results given in [30] or in [15], where a single $[u, m, t+1]$ linear code has been used to provide nonlinear resilient functions for any $n > u$. When compared to the result given in Theorem 3 we deduce the following. Utilizing the set of simplex-like codes the method in [18] would generate $(2^m-1+e, m, 2^{m-1}-1)$ functions of nonlinearity $\mathcal{N}_F = 2^{2^m-2+e} - 2^{2^m-2}$, and degree $\deg(F) \leq e+1$. Hence, there is a drop of nonlinearity when using Construction 2. It equals $m2^{2^{m-1}-1}$ and can be neglected in comparison to the term 2^{2^m-2}. Therefore, we assume that there is only a tradeoff between the resiliency and algebraic degree. Actually, our method gives a higher algebraic degree, i.e., $\deg(G) = 2^{m-1} - 1 + e$ compared to $\deg(F) \leq e+1$ and the gain is at least $2^{m-1} - 2$. On the other hand, the resiliency order is decreased by the value 2^{m-2}.

A. Comparison of Cryptographic Criteria to Known Constructions

We now give a short comparison to the known construction methods only in terms of algebraic degree and resiliency since a detailed examination involving all cryptographic criteria would be very tedious and dependent on the choice of input parameters n, m, and t. On the other hand, it has been proved that the construction results proposed in [15], [18], [30] in most of the cases are superior in terms of nonlinearity compared to other methods.

In terms of algebraic degree the method of Cheon [7] using linearized polynomials provides functions with highest degree for a sufficiently large input space. Based on the existence of a single $[u, m, t+1]$ linear code, this method generates nonlinear $(n = u + \triangle + 1, m, t)$-resilient functions with degree $d = \triangle$ for any $\triangle \geq 0$. If one starts with the simplex code then nonlinear $(2^m - 1 + \triangle, m, 2^{m-1} - 1)$-resilient functions can be obtained. By Theorem 4, the degree of G (recall that G is a nonlinear $(2^m - 1 + e, m, 2^{m-2} - 1)$-resilient function) is $2^{m-1} - 1 + e$, which for the same input space, that is, $\triangle = e$, is obviously higher than $\triangle$. The nonlinearity of G is much larger compared to Cheon's construction but the resiliency order is smaller compared to the method of Cheon.

When compared to the construction of Zhang and Zheng [38], in the case that the simplex code is utilized, we can deduce the following. Clearly, for a small input space $n = 2^m - 1$, the method of Zhang and Zheng is better than our, since our construction needs to use as many codewords as possible not giving any nonlinearity for $n = u$. Thus, to make a fair comparison we have to investigate the existence of an $[n = 2^m - 1 + e, m', 2^{m-2}]$ linear code, where m' satisfies $m' > 2^{m-1} + e$. This is because in this case the degree of the Zhang and Zheng method, given as $d = m' - 1$, will be larger than $\deg(G) = 2^{m-1} - 1 + e$ in Theorem 4. Recall that $e = \lfloor \log_2 b(2^m - 1) \rfloor \geq m - 1$, where b is the cardinality of the set of disjoint codes. It seems that in general the codes of the parameters above do exist for small e close to $m - 1$ but not for $e \gg m - 1$. Hence, assuming that many disjoint codes are available our construction is better, whereas for a small cardinality of a set of disjoint codes the method of Zhang and Zheng seems to be better.

In [15], a simple modification of the method of Zhang and Zheng was proposed. The authors simply apply the method to a code of the same length and a larger dimension. Hence, to construct a nonlinear (n, m, t) function of degree $d > m - 1$, in [15] a nonlinear permutation is applied to an $[n, d, t+1]$, where $d > m$. This approach seems to be a bit ambiguous since it is quite natural for given n and t to use the code of highest dimension m. If such a code is utilized in the method of Zhang and Zheng there will not exist $d > m$ and the same conclusion as above applies here.

V. Algebraic Immunity Related to Injective MM Class

Algebraic attacks have attracted a lot of attention recently. Although generic in its nature, they are most successfully applied to certain LFSR based stream cipher schemes whenever the existence of low degree *annihilators* is assured. The main idea behind these attacks on additive stream ciphers may be summarized as follows. The filtering Boolean function f is chosen to satisfy standard cryptographic criteria such as high algebraic degree, high nonlinearity, and a certain resiliency order. Nevertheless, it turned out [24], [10] that these criteria do not provide sufficient protection if there is a low degree function g (called annihilator) such that either $fg = 0$ or $(1 + f)g = 0$. Then the minimum degree of nonzero annihilators of either f or $1 + f$ is by definition *algebraic immunity* [24].

The basic ideas behind algebraic attacks are summarized as follows. In case of nonlinear combiners and nonlinear filtering generators, each output bit will give a rise to a multivariate equation of degree $\deg(f) = d$, and consequently, an overdefined system of equations may be set up and solved in time complexity $T = \binom{K}{d}^{\omega}$, where K is the key length (secret initial content of LFSR) and ω is the complexity of Gaussian elimination (usually one takes $\omega = 3$). Then, assuming that g is of degree d' (with $d' < d$) a degree d' system of multivariate equations may be set up which results in the reduced complexity $T' = \binom{K}{d'}^{\omega}$. In [10], the upper bound on the algebraic immunity was given, that is, $\deg(g) \leq \lceil \frac{n}{2} \rceil$ for any Boolean function f in n variables.

Concerning the MM class (both standard and degree optimized class), it was noticed in [24] that this class trivially admits annihilators of degree $n - k + 1$, where k denotes the size of variable space of affine subfunctions. Algebraic properties of the MM class were also discussed in [11], [12]. Nevertheless, none of these works provide a systematic approach for deriving algebraic properties of a whole subclass of the MM class. In what follows, we demonstrate that a certain subclass of the MM class is most likely not to have an optimized algebraic immunity.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

The algebraic normal form of the MM class, as a concatenation of 2^{n-k} affine functions $a_0, \ldots, a_{2^{n-k}-1}$, is given by

$$f(y,x) = \sum_{\tau \in \mathbb{F}_2^{n-k}} \prod_{i=1}^{n-k} (y_i + \tau_i + 1) a_{[\tau]}(x).$$

The general form of any annihilator of f viewed as a concatenation of some functions on $\mathbb{F}_2^k$ was derived in [24]

$$g(y,x) = \sum_{\tau \in \mathbb{F}_2^{n-k}} \Big(\prod_{i=1}^{n-k} (y_i + \tau_i + 1) \Big) g_{[\tau]}(x) \qquad (18)$$

where $g_{[\tau]}$ is any annihilator of $a_{[\tau]}$, i.e., $g_{[\tau]} a_{[\tau]} = 0$. Selecting $g_{[\tau]}(x) = 0$ for $\tau \in \mathbb{F}_2^{n-k} \backslash \tau^*$ and $g_{[\tau^*]}(x) = (1 + a_{[\tau]})$ for some fixed τ^*, we have that $fg = 0$, where the $\deg(g) = n - k + 1$. The same technique can be applied to the degree optimized MM class discussed previously.

The degree of such an annihilator is exactly $n - k + 1$ which does not reduce the degree of the function f for the standard class since $\deg(f) \leq n - k + 1$. On the other hand, this method gives a certain degree reduction in the case of degree optimized class as in this case $\deg(f) = n - t + 1$.

A. Low Degree Annihilators for the MM Class

We keep the notation introduced previously, that is, n will denote the number of input variables and k is the dimension space of affine subfunctions. The purpose of this subsection is to demonstrate that the injective MM class admits annihilators of degree strictly lower than $n-k+1$ when the size of the affine subspace k is chosen so that the nonlinearity is maximized. This also implies that if g is such an annihilator, its degree will be strictly less than $\lceil n/2 \rceil$ since for the resilient functions in this class we have $n - k + 1 \leq \lceil n/2 \rceil$. Note that the next result addresses only a particular subclass of the MM class, and even though a closed formula for computing the algebraic immunity[3] could not be derived.

If we would like to cancel the presence of the term $y_1 y_2 \cdots y_{n-k} s(x)$ in the general algebraic normal form of g given by (18), then the necessary and sufficient condition is that

$$\sum_{\tau \in \mathbb{F}_2^{n-k}} g_{[\tau]}(x) = \sum_{\tau \in \mathbb{F}_2^{n-k}} (1 + a_{[\tau]}(x)) g'_{[\tau]}(x) = 0$$

where $g'_{[\tau]}(x)$ are Boolean functions in k variables of arbitrary degree. However, this technique does not ensure that, depending on the choice of $g'_{[\tau]}$, there will not be some term of even higher degree than $n - k + 1$. Therefore, we constrain the degree of $g'_{[\tau]}(x)$ not to exceed a fixed value r ($r < k$). Then we try to select the functions $g'_{[\tau]}(x)$ in such a way that we cancel the terms in the ANF of g containing $y_{i_1} \cdots y_{i_p}$ for any p in the range $d \leq p \leq n-k$, where d is a fixed integer $1 \leq d \leq n-k$. If there exists such a choice of $g'_{[\tau]}(x)$, then the degree of g will be equal to $d-1+r+1 = d+r$ which can be less than $n-k+1$.

[3]We use the term algebraic immunity although we only investigate the existence of annihilators for f. However, the same algorithm is applicable to function $1 + f$ and, therefore, the use of algebraic immunity is justified.

To cancel all terms in $g(y,x)$ containing $y_{i_1} y_{i_2} \cdots y_{i_\delta}$, $1 \leq i_1 \neq i_2 \cdots \neq i_\delta \leq n-k$, the following sum must be identical to zero:

$$\sum_{\substack{\tau \in \mathbb{F}_2^{n-k} \\ \tau_{i_{\delta+1}} = \cdots = \tau_{i_{n-k}} = 0}} (1 + a_{[\tau]}(x)) g'_{[\tau]}(x) = 0. \qquad (19)$$

Let us introduce the following general form for the functions $g'_{[\tau]}(x)$, that is,

$$g'_{[\tau]}(x) = a_0^\tau + a_1^\tau x_1 + \cdots + a_k^\tau x_k + a_{i_1 \ldots i_r}^\tau x_{i_1} \ldots x_{i_r}, \ \tau \in \mathbb{F}_2^{n-k}. \qquad (20)$$

Thus, restricting the degree of $g'_{[\tau]}(x)$ not to exceed r we obtain in total $2^{n-k} \cdot \sum_{i=0}^{r} \binom{k}{i}$ unknowns $a_0^\tau, \ldots, a_{i_1 \ldots i_r}^\tau$ when τ runs through $\mathbb{F}_2^{n-k}$. On the other hand, to cancel any subproduct $y_{i_1} y_{i_2} \cdots y_{i_\delta}$, the condition that the (19) must be identical to zero will induce $\sum_{j=0}^{r+1} \binom{k}{j}$ equations in unknowns $a_0^\tau, \ldots, a_{i_1 \ldots i_r}^\tau$ that actually must be zero.

Hence, assuming that we want to completely cancel the terms in the ANF of function g which contain at least d distinct y variables we obtain the total number of equations

$$\sum_{j=0}^{n-k-d} \binom{n-k}{n-k-j} \sum_{j=0}^{r+1} \binom{k}{j}.$$

It is obvious that this homogeneous system of equations is always solvable if the number of unknowns is larger than the number of equations. Thus, if we require that

$$2^{n-k} \cdot \sum_{i=0}^{r} \binom{k}{i} > \sum_{j=0}^{n-k-d} \binom{n-k}{n-k-j} \sum_{j=0}^{r+1} \binom{k}{j} \qquad (21)$$

then we can find an annihilator (or many) of degree $d + r$.

The main idea now is to find d, r such that the condition above is satisfied together with the requirement that $d + r < n - k + 1$. In the sequel, we refer to this approach as equation based annihilation.

Example 3: Consider a construction of a function f on $\mathbb{F}_2^{15}$ using the MM method, for instance by concatenating affine functions on $\mathbb{F}_2^8$. This gives $k = 8$ and $n - k = 7$. Then the trivial annihilation will give annihilators of degree $n - k + 1 = 8$. It can be checked that putting $d = 5$, $r = 1$ and $k = 8$ in

$$2^{n-k} \cdot \sum_{i=0}^{r} \binom{k}{i} > \sum_{j=0}^{n-k-d} \binom{n-k}{n-k-j} \sum_{j=0}^{r+1} \binom{k}{j}$$

gives $2^7 \cdot 9 > 29 \cdot 37$. This means that the number of unknowns is larger than the number of equations and there will exist annihilators of degree $d + r = 6$. It can be verified that further reduction of degree by choosing for instance $d = 3$, $r = 2$, or $d = 4$, $r = 1$ is not possible since the condition above is not satisfied.

It seems to be a difficult task to derive an explicit expression for the choice of the parameters r and d. However, the computer simulations suggest that the best choice is to take $r = 1$ in order to minimize $r+d$, where r, d satisfy (21). The optimal choice of the parameters r and d for certain input values is given in Table I.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

TABLE I
DEGREES OF TRIVIAL AND EQUATION BASED ANNIHILATION

$n;k$	13;7	15;8	17;9	19;10	21;11	23;13
n-k+1	7	8	9	10	11	13
d+r	5	6	7	8	9	10

We only consider the case when distinct affine (linear) functions are used (ϕ is injective) and assume that order of resiliency t is small so that it suffices to take $k=(n+1)/2$. This also implies a high nonlinearity of functions, i.e., $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n-1}{2}}$. The degree $n-k+1$ of trivial annihilation, as described previously, is listed for comparison. Note that this degree coincides with $\lceil \frac{n}{2} \rceil$ for $k=(n+1)/2$.

This technique is applied with almost the same success to the degree optimized MM class discussed previously. This design essentially replaces a few (or a single) affine functions with suitably chosen t-resilent functions of maximum degree $k-t-1$. Using a straightforward approach as above would significantly increase the number of equations since these nonlinear subfunctions would involve much more terms when the degree of $g'_{[\tau]}(x)$ is kept fixed. One solution to this problem is to define $g'_{[\tau]}(x)=0$ for all τ for which $a_{[\tau]}(x)$ is nonlinear. This will reduce the number of unknowns and if $|T|$ denotes the number of nonlinear subfunctions then the total number of unknowns becomes $(2^{n-k}-|T|)\cdot\sum_{i=0}^{r}\binom{k}{i}$. Hence, only if the number of nonlinear subfunctions is not quite small this class will be somewhat better protected against algebraic attacks.

VI. MULTIVARIATE EQUATIONS FOR $F:\mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ IN MM CLASS

Let (n,m,t) denote an n-input, m-output, t-resilient function $F:\mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ represented as $F=(f_0,\ldots,f_{m-1})$. One important application of F is as filtering function in a nonlinear combining generator [26], where simply instead of a single bit (Boolean case) m bits of keystream are generated at the time. Because the outputs are known (known plaintext attack), the goal of the attacker is to find a low degree equation of the maximum degree d in the input variables $x_1,\ldots,x_n$ of the form

$$Q(x_1,\ldots,x_n,\ldots,x_{i_1}\cdots x_{i_d},y_0x_1,\ldots,y_0\cdots y_{m-1}x_{i_1}\cdots x_{i_d})=0$$

where we denote by $y_i=f_i(x)$. Then trivially there will exist equation(s) of degree at most d (see [9]) relating the input and output variables whenever

$$\sum_{i=0}^{d}\binom{n}{i} > 2^{n-m}. \tag{22}$$

Thus, the resistance to algebraic attacks decreases (as smaller d will satisfy the above condition) when the number of outputs m increases from $m=1$ (Boolean case) to $m>1$.

If $g_0,\ldots,g_{m-1}$ are annihilators of, respectively, $f_0,\ldots,f_{m-1}$, that is $f_i(x)g_i(x)=0$, then we also have

$$f_0(x)\cdots f_{m-1}(x)(g_0(x)+\cdots+g_{m-1}(x))=0.$$

Then simply observing the all-ones output at time t, that is, $f_0(x^t)=\cdots=f_{m-1}(x^t)=1$, induces the following equation:

$$g_0(x)+\cdots+g_{m-1}(x)=0$$

which might be of low degree. Note that we are not restricted to only consider the m outputs generated at time t. We also get the equations of the same degree by looking at the outputs at different time instances provided that they are all equal to one.

We say that function $F=(f_0,\ldots,f_{m-1})$ belongs to extended MM class if each f_j can be viewed as a concatenation of linear functions $l_{j,i}(x)$

$$f_j(y,x)=\sum_{\tau\in\mathbb{F}_2^{n-k}}\prod_{i=1}^{n-k}(y_i+\tau_i+1)l_{j,\tau}(x),\quad j=0,\ldots,m-1, \tag{23}$$

where $(y,x)\in\mathbb{F}_2^{n-k}\times\mathbb{F}_2^k$. Note that the algorithm proposed in Section V-A may be applied directly to the function $f_0\cdots f_{m-1}$ as this function may be represented as

$$f_0(y,x)\cdots f_{m-1}(y,x)=\sum_{\tau\in\mathbb{F}_2^{n-k}}\prod_{i=1}^{n-k}(y_i+\tau_i+1)\prod_{j=0}^{m-1}l_{j,\tau}(x). \tag{24}$$

But we can actually do more by considering the annihilators of each f_j. Similarly to the MM case for any f_j defined as above, its annihilator g_j may be written as

$$g_j(y,x)=\sum_{\tau\in\mathbb{F}_2^{n-k}}\left(\prod_{i=1}^{n-k}(y_i+\tau_i+1)\right)(1+l_{j,\tau}(x))h_{j,\tau}(x)$$

where for $j=0,\ldots,m-1$ the functions $h_{j,\tau}(x)$ are

$$h_{j,\tau}(x)=a_0^{j,\tau}+a_1^{j,\tau}x_1+\cdots+a_k^{j,\tau}x_k+\cdots+a_{i_1\cdots i_r}^{j,\tau}x_{i_1}\cdots x_{i_r}, \tag{25}$$

for $\tau\in\mathbb{F}_2^{n-k}$, $a_i^{j,\tau}\in\mathbb{F}_2$.

To have more freedom of choice and more unknowns in our system of equations we consider the annihilators of $f_0\cdots f_{m-1}$ in the form $g_0+\cdots+g_{m-1}$. To cancel all terms in $g(y,x)=g_0(y,x)+\cdots+g_{m-1}(y,x)$ containing $y_{i_1}y_{i_2}\cdots y_{i_\delta}$, $1\le i_1\ne i_2\cdots\ne i_\delta\le n-k$, the following sum must be identical to zero:

$$\sum_{\substack{\tau\in\mathbb{F}_2^{n-k}\\ \tau_{i_{\delta+1}}=\cdots=\tau_{i_{n-k}}=0}}\sum_{j=0}^{m-1}(1+l_{j,\tau}(x))h_{j,\tau}(x)=0. \tag{26}$$

Thus, restricting the degree of $h_{j,\tau}(x)$ not to exceed r, for each g_j we obtain $2^{n-k}\cdot\sum_{i=0}^{r}\binom{k}{i}$ unknowns $a_0^{j,\tau},\ldots,a_{i_1\cdots i_r}^{j,\tau}$ when τ runs through $\mathbb{F}_2^{n-k}$. Thus, the total number of unknowns is $m\cdot 2^{n-k}\cdot\sum_{i=0}^{r}\binom{k}{i}$. On the other hand, to cancel any subproduct $y_{i_1}y_{i_2}\cdots y_{i_\delta}$, the condition that (26) must be identical to zero induces $\sum_{j=0}^{r+1}\binom{k}{j}$ equations in unknowns $a_0^{j,\tau},\ldots,a_{i_1\cdots i_r}^{j,\tau}$ that actually must be zero.

Again, assuming that we want to completely cancel the terms in the ANF of function g which contain at least d distinct y variables, we obtain the total number of equations

$$\sum_{j=0}^{n-k-d}\binom{n-k}{n-k-j}\sum_{j=0}^{r+1}\binom{k}{j}.$$

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

TABLE II
DEGREE OF MULTIVARIATE EQUATIONS FOR CERTAIN SIZE OF PARAMETERS FOR FUNCTIONS DERIVED FROM LINEAR CODES

n	18	20	22	24	28	30	32
k	11	12	13	14	16	17	18
$1+r$ (m=4); d^*	3; 6	3; 7	4; 7	4; 8	4; 10	4; 11	5; 12
$1+r$ (m=6); d^*	2; 5	3; 5	3; 6	3; 7	3; 8	3; 9	3; 10
$1+r$ (m=8); d^*	2; 4	2; 4	2; 5	2; 6	3; 7	3; 8	3; 9

Thus, if we require that

$$m \cdot 2^{n-k} \cdot \sum_{i=0}^{r} \binom{k}{i} > \sum_{j=0}^{n-k-d} \binom{n-k}{n-k-j} \sum_{j=0}^{r+1} \binom{k}{j} \quad (27)$$

then we can find an annihilator (or many) of degree at most $d+r$.

Even though there is always a nontrivial solution to the system above this only means that not all the coefficients of $g_0, \ldots, g_{m-1}$ are equal to zero. Still these coefficients might be such that $g_0 + \cdots + g_{m-1} = 0$ which only gives a trivial solution. To ensure that such a system always has a nontrivial solution in the sense that $g_0 + \cdots + g_{m-1} \neq 0$ we remark the following. This system being underdefined leaves some free variables (coefficients in the functions $h_{j,\tau}(x)$) which might be set arbitrary. Then if for certain assignment for these variables the solution of the system is such that $g_0 + \cdots + g_{m-1} = 0$, we select another values that provide $g_0 + \cdots + g_{m-1} \neq 0$.

It is not easy to analyze the behavior of (27) with respect to parameters d, r which are to be optimized such that $d + r$ is minimized. On the other hand, a closer inspection of the condition above results in the quadratic relationship between input and output variables when m is sufficiently large. To see this notice that

$$\sum_{j=0}^{n-k-d} \binom{n-k}{n-k-j} < 2^{n-k}, \quad \forall d \geq 1.$$

This gives a simple condition that for any m such that $m > \sum_{j=0}^{r+1} \binom{k}{j} / \sum_{i=0}^{r} \binom{k}{i}$, the condition in (27) is satisfied and consequently there exist annihilators of degree $d + r$. Now taking $d = 1$ and $r = 1$ gives

$$m > \frac{1 + k + k(k-1)/2}{1+k} \cong 1 + (k-1)/2. \quad (28)$$

Thus, for $m > \lceil k/2 \rceil$, we obtain quadratic equations regardless of the value of n or degree of F.

Computer simulations suggest that the best choice is to take $d = 1$ and then to select the minimum value of r such that (27) is satisfied. The minimum annihilator degree $d + r$ (with $d = 1$) is given in Table II for certain input values. For the sake of comparison to the bound given in (22), we fix the input space n to be slightly less than $2k-1$, which is the maximum value of n in case of injective MM class of Boolean functions. Assume that for $n = 2k - 4$, it is possible to construct a nonlinear t-resilient function F that belongs to the extended MM class. The smallest positive integer d that satisfy the bound in (22) will be denoted by d^*.

The values in Table II indicates that increasing the number of outputs substantially decreases the resistance to algebraic attacks. Indeed, this behavior of extended MM class is not predicted with the classical bound given by (22). There is a significant discrepancy between d^* and actual degree derived through our algorithm for establishing the low degree multivariate equations.

Example 4: Assume that $m = 8$, i.e., we want to output one byte of data. Then for any $F : \mathbb{F}_2^n \to \mathbb{F}_2^8$, which is linear on k-dimensional subspaces, for $2 \leq k \leq 15$ there exist quadratic annihilators. Then the standard state size $K = 256$ induces the time complexity for algebraic attack to be $\{K(K-1)/2\}^3 \cong K^6/8 = 2^{45}$ The most suitable choice of n, m from the implementation point of view is $n = 32$, $m = 8$. Then for $k = 24$ one can verify that $d = 1$, $r = 2$ satisfy the condition in (27). Thus, there are cubic annihilators for $F : \mathbb{F}_2^{32} \to \mathbb{F}_2^8$ (F being linear on subspaces of dimension $k = 24$).

A. Attacking Nonlinear Combiners Based on Nonlinear Permutations

Another method of constructing nonlinear (n, m, t) function uses a linear resilient function G obtained from a linear $[n, m, t+1]$ code together with a highly nonlinear permutation P. In the original paper [38], the authors only consider the inverse function $P(x) = x^{-1}$ which has relatively good cryptographic properties related to the degree and nonlinearity of such a function. Then a nonlinear (n, m, t) function F is obtained as $F(x) = P \circ G(x)$. Let us denote the outputs of G as $z_1, \ldots, z_m$ and the outputs of P as $y_1, \ldots, y_m$. Then for the inverse function $P(z) = z^{-1}$ there exist quadratic equations over GF (2) between its input and output set of variables [10], that is,

$$\sum_i a_i z_i + \sum_i b_i y_i + \sum_{i,j} c_{i,j} y_i z_j + \sum_{i,j} d_{i,j} z_i z_j + \sum_{i,j} e_{i,j} y_i y_j = 0$$

for some a_i, b_i, $c_{i,j}$, $d_{i,j}$, $e_{i,j} \in$ GF (2). Then since each z_i is a linear function in $x_1, \ldots, x_n$ this quadratic equation relates also the input and output variables x and y. This means that the choice of the inverse function is not appropriate for this design method.

In general, for any permutation $P : \mathbb{F}_2^m \to \mathbb{F}_2^m$ there exist equations of degree at most d relating the input and output variables whenever $\sum_{i=0}^{d} \binom{2m}{i} > 2^m$, see [19]. Furthermore, it can be verified (using computer) that the smallest d satisfying the above condition is well approximated by $d \approx \lceil m/4 \rceil + 1$. This means that for instance if $m = 8$ one can always find cubic equations that relate the input and output variables of F whatever is the choice of nonlinear permutation.

VII. CONCLUSION

The basic construction idea common to both Constructions 1 and 2 is to replace exactly one linear subfunction with its nonlinear counterpart for each constituent function $f_1, \ldots, f_m$, $m \geq 1$. In the case of Boolean functions ($m = 1$), the technique proposed is an efficient means of generating degree optimized functions. In the case of multiple output functions, the exact calculation of resiliency order is rather tedious and it depends on the properties of the codes used in the construction. In the case of the simplex code we could derive the exact resiliency order. Actually, the codes with a sparse weight distribution are more suitable for our construction than those having codewords with many different weights.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.

The second part investigates the algebraic properties of certain subclasses of MM class. Our primary goal was to demonstrate that certain instances of the MM class do not posses an optimized algebraic immunity. The method proposed here can be used to consider other instances of this class. More importantly, the method for establishing the existence of low degree annihilators in the Boolean case applies successfully to resilient m-bit output functions whose construction is based on the use of a single or several linear codes. As a conclusion, this class of functions should not be used as a filtering function in nonlinear combiners unless m is sufficiently smaller than n so that there are no low degree multivariate equations.

REFERENCES

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Advances in Cryptology—EUROCRYPT'91 (Lecture Notes in Computer Sceince)*. Berlin, Germany: Springer-Verlag, 1991, vol. 547, pp. 86–100.

[2] C. Carlet, "On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions," in *Special Issue of Discr. Math. Theor. Comp. Sci.*. New York: Springer-Verlag, 2001, pp. 131–144.

[3] ——, "A larger class of cryptographic Boolean functions via a study of the Maiorana-Mcfarland constructions," in *Advances in Cryptology—CRYPTO 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2442, pp. 549–564.

[4] C. Carlet and P. Sarkar, "Spectral domain analysis of correlation immune and resilient Boolean functions," *Finite Fields Their Applic.*, vol. 8, no. 1, pp. 120–130, 2002.

[5] P. Charpin and E. Pasalic, "Highly nonlinear resilient functions through disjoint codes in projective spaces," *Des., Codes, Cryptogr.*, vol. 37, no. 2, pp. 319–346, 2005.

[6] S. Chee, S. Lee, D. Lee, and H. S. Sung, "On the correlation immune functions and their nonlinearity," in *Advances in Cryptology—ASIACRYPT'96 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1996, vol. 1163, pp. 232–243.

[7] J. H. Cheon, "Nonlinear vector resilient functions," in *Advances in Cryptology—CRYPTO 2001 (Lecture Notes in Computer Sceince)*. Berlin, Germany: Springer-Verlag, 2001, vol. 2139, pp. 181–195.

[8] N. Courtois, "Higher order correlation attacks, XL algorithm and cryptoanalysis of Toyocrypt," in *Proc. ICISC 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2587, pp. 182–199.

[9] ——, "Algebraic attacks on combiner with memory and several outputs," in *Proc. ISICS 2004 (Lecture Notes in Computer Sceince)*. Berlin, Germany: Springer-Verlag, 2004.

[10] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—EUROCRYPT 2003*. Berlin, Germany: Springer-Verlag, 2003, vol. 2656, pp. 346–359.

[11] D. K. Dalai, K. C. Gupta, and S. Maitra, *Algebraic Immunity for Cryptographically Significant Boolean Functions (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 3348, pp. 92–106.

[12] ——, "Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity," in *Fast Software Encryption 2005 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2005, vol. 3557, pp. 98–111.

[13] J. F. Dillon, "Elementary Haddamard Difference Sets," Ph.D. dissertation, Univ. Maryland, College Park, MD, 1974.

[14] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption, Cambridge Security Workshop (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 1008, pp. 61–74.

[15] K. C. Gupta and P. Sarkar, "Improved constructions of nonlinear resilient S-boxes," in *Advances in Cryptology—ASIACRYPT 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2501, pp. 466–483.

[16] T. Johansson and F. Jönsson, "Fast correlation attacks based on turbo code techniques," in *Advances in Cryptology—CRYPTO'99 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1666, pp. 181–197.

[17] ——, "Improved fast correlation attacks on stream ciphers via convolutional codes," in *Advances in Cryptology—EUROCRYPT'99 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1592, pp. 347–362.

[18] T. Johansson and E. Pasalic, "A construction of resilient functions with high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 494–501, Feb. 2003.

[19] L. R. Knudsen, Quadratic Relations in Khazad and Whirlpool, Rep.: New European Schemes for Signatures, Integrity and Encryption, NES/DOC/UIB/WP5/017/1 [Online]. Available: http://www.cosic.esat.kuleuven.be/nessie/reports/

[20] K. Kurosawa, T. Satoh, and K. Yamamoto, "Highly nonlinear t-resilient functions," *J. Univ. Comp. Sci.*, vol. 3, no. 6, pp. 721–729, 1997.

[21] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[22] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1825–1834, Jul. 2002.

[23] ——, "A Maiorana-Mcfarland type construction for resilient Boolean functions on n variables n even) with nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$," *Discr. Appl. Math.*, vol. 154, no. 2, pp. 357–369, 2006.

[24] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology—EUROCRYPT 2004 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 3027, pp. 474–491.

[25] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *J. Cryptol.*, vol. 1, pp. 159–176, 1989.

[26] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1997.

[27] H. Niederreiter and C. P. Xing, "Disjoint linear codes from algebraic function fields," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2174–2177, Sep. 2004.

[28] K. Nyberg, "On the construction of highly nonlinear permutations," in *Advances in Cryptology—EUROCRYPT'92 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1992, vol. 658, pp. 92–98.

[29] E. Pasalic, T. Johansson, S. Maitra, and P. Sarkar, "New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity," in *Workshop on Coding and Cryptography Proc.*, Paris, France, Jan. 2001, vol. 6, pp. 425–435.

[30] E. Pasalic and S. Maitra, "Linear codes in generalized construction of resilient functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2182–2191, Aug. 2002.

[31] P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," in *Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 485–506.

[32] ——, "Nonlinearity bounds and constructions of resilient Boolean functions," in *Advances in Cryptology—CRYPTO 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1880, pp. 515–532.

[33] J. Seberry, X. M. Zhang, and Y. Zheng, "On constructions and nonlinearity of correlation immune Boolean functions," in *Advances in Cryptology—EUROCRYPT'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 181–199.

[34] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.

[35] ——, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Trans. Comp.*, vol. C-34, no. 1, pp. 81–85, Jan. 1985.

[36] Y. Tarannikov, "On resilient Boolean functions with maximal possible nonlinearity," in *Proceedings of INDOCRYPT (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1977, pp. 19–30.

[37] G.-Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 569–571, May 1988.

[38] X. M. Zhang and Y. Zheng, "Cryptographically resilient functions," *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1740–1747, Sep. 1997.

[39] Y. Zheng and X. M. Zhang, "Improving upper bound on nonlinearity of high order correlation immune functions," in *Selected Areas in Cryptography–SAC '2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 2012, pp. 264–274.

Authorized licensed use limited to: Danmarks Tekniske Informationscenter. Downloaded on November 18, 2009 at 14:39 from IEEE Xplore. Restrictions apply.