Generalized Maiorana-McFarland Construction of Resilient Boolean Functions With High Nonlinearity and Good Algebraic Properties

WeiGuo Zhang (张卫国) and Enes Pasalic

***Abstract*—A new framework concerning the construction of resilient Boolean functions whose nonlinearity is strictly greater than $2^{n-1} - 2^{\lfloor n/2 \rfloor}$ is given. Firstly, a generalized Maiorana-McFarland (GMM) construction technique is described, which extends the current approaches by combining the usage of affine and nonlinear functions in a controllable manner. It is shown that for any given m, this technique can be used to construct a large class of n-variable (n both even and odd) m-resilient degree-optimized Boolean functions with currently best known nonlinearity. This class may also provide functions with excellent algebraic properties, measured through the resistance to (fast) algebraic attacks, if the number of $n/2$-variable affine subfunctions used in the construction is relatively low. The fact that this class might have an efficient hardware implementation, along with overall good cryptographic properties, makes these functions as attractive candidates for the use in certain stream cipher schemes.**

***Index Terms*—Algebraic degree, algebraic immunity, Boolean functions, cryptography, fast algebraic attacks, nonlinearity, resiliency, stream ciphers.**

I. Introduction

Boolean functions play a central role in the design of certain stream cipher schemes, and such schemes may become susceptible to various cryptanalytic attacks utilising possible weaknesses of Boolean functions. Resiliency and high nonlinearity are two of the most important criteria of Boolean functions when they are used as nonlinear filtering functions in certain stream cipher models. Resiliency ensures the cipher is not prone to (fast) correlation attacks [15], [25], while high nonlinearity offers protection against best affine approximation (BAA) attacks [8]. Notice that high nonlinearity is a desirable property in both nonlinear combiners and nonlinear filtering generators [14] (being standard application examples), though for the latter schemes resiliency is not an essential criterion. Since the early 1990s, the construction of resilient functions with high nonlinearity has been an important challenge in cryptography and it was extensively studied, see [4], [24], [5], [1], [17], [20], [21], [11], [12], [28] and the references therein.

It is an open problem how tight the nonlinearity bound of resilient Boolean functions is. Sarkar and Maitra [21] presented that if f is an n-variable, m-resilient function, then the nonlinearity $N_f \equiv 0 \bmod 2^{m+1}$ which gives a nontrivial upper bound on the nonlinearity of resilient functions, i.e.,

$$N_f \le \max\{\kappa \mid \kappa \equiv 0 \bmod 2^{m+1}, \kappa < \mathrm{nlmax}(n)\}, \qquad (1)$$

where $\mathrm{nlmax}(n)$ denotes the maximum nonlinearity of an n-variable Boolean function. This bound can be achieved if m is large enough, which has also been independently proved by Tarannikov [26] and by Zheng and Zhang [30]. However, it is not clear whether this bound is tight for low values of m. We only know that when $m \le n/2 - 2$ there exist strictly almost optimal (SAO) resilient functions on both even and odd number of variables, where an n-variable Boolean function is called SAO if its nonlinearity is strictly greater than $2^{n-1} - 2^{\lfloor n/2 \rfloor}$.

For even n, the major advancements concerning the constructions of SAO resilient functions have been presented in [20], [11], [12], [28]. In particular, Zhang and Xiao [28] proposed a construction method for constructing SAO resilient functions on $\mathbb{F}_2^n$ (n even) with the currently best known nonlinearity.

For odd $n \le 7$, the optimal nonlinearity of n-variable functions is $2^{n-1} - 2^{(n-1)/2}$. Furthermore, for odd $n \ge 9$, the maximum achievable value of N_f is unknown in general, and we only know that it is strictly larger than $2^{n-1} - 2^{(n-1)/2}$ [9]. In addition, Kavut and Yücel (KY) [10] discovered 9-variable Boolean functions with nonlinearity 242. The first attempt in this direction was in [19], where a 15-variable Boolean function with nonlinearity 16276 was constructed by Patterson and Wiedemann (PW) [19] and later it was modified in [13] and [22] to yield a balanced function with nonlinearity 16262 and 16272 respectively. Seberry, Zhang, and Zheng [23] showed how to use the PW functions to construct balanced functions with SAO nonlinearity for odd $n \ge 29$. The challenge is to get resilient functions with SAO nonlinearity. In [20], a method to construct SAO m-resilient functions on odd numbers of variables has been proposed. S. Sarkar and Maitra [22] obtained 15-variable 1-resilient functions with nonlinearity 16264, which implies that a 1-resilient function with nonlinearity $2^{n-1} - 2^{(n-1)/2} + 8 \cdot 2^{(n-15)/2}$ can be constructed for odd $n \ge 17$.

Although the original Maiorana-McFarland (MM) construction technique can provide resilient functions with high nonlinearity, by concatenating the truth tables of “small variable” affine functions [4], [5], in general it cannot generate SAO resilient functions. This is especially true if the concatenation uses distinct affine functions so that the function ϕ (cf. Definition 2) is injective. On the other hand, if the injectivity

W.-G. Zhang is with the ISN Laboratory, Xidian University, Xi’an 710071, China (e-mail: zwg@xidian.edu.cn; http://web.xidian.edu.cn/wgzhang)

E. Pasalic is with the University of Primorska, FAMNIT, Koper, Slovenia (e-mail: enes.pasalic6@gmail.com)

DOI: https://doi.org/10.1109/TIT.2014.2345772

is dropped (thus allowing a repetition of affine functions) it was demonstrated [20] that a careful use of affine functions in less than $n/2$ variables may provide resilient Boolean functions with SAO nonlinearity. In other direction, Carlet [1] introduced a super-class of MM class by concatenating quadratic functions and provided a better upper bound on nonlinearity of resilient functions in the MM class. Nevertheless, this method does not generate resilient functions with SAO nonlinearity. In [2, pp. 63] the author admit that due to rather hard conditions this generalization is rather ineffective (apart from large resiliency order) and that searching for other constructions seems to be necessary.

In this paper, we introduce a generalized Maiorana-McFarland (GMM) construction technique for designing n-variable (n both even and odd) SAO m-resilient Boolean functions of low order of resiliency m. The main idea behind our approach is a different way of decomposing the total variable space so that more subfunctions, which are m-resilient affine functions, can be found through an elaborate design method. In essence, our primary construction does not use a single injective mapping ϕ (which corresponds to the concatenation of affine functions without a repetition) but rather uses several injective mappings defined on different variable spaces and therefore the method can be viewed as a concatenation of affine/linear functions whose variable spaces are not identical. When n is even, our method combines the concatenation of $n/2$-variable resilient affine functions (for even n) together with resilient affine functions on $n/2-k$ variables, for some $k \in [1, n/2-2]$. Therefore, the concatenation of 2^k many $(n/2-k)$-variable affine functions may be viewed as a nonlinear subfunction on an $n/2$-variable space. Consequently, our construction essentially concatenates suitably chosen affine and nonlinear resilient functions, where the latter are not necessarily quadratic (depending on the size of the subspace $n/2-k$). Later, this approach is further generalized yielding Construction 2, and in the last part of this article the idea is generalized for the case when n is odd.

It turns out that the algebraic immunity (AI) is affected by the choice of these linear/affine functions which means that deriving some lower bounds on AI is a rather elusive task. Nevertheless, based on computer simulations, the resistance of these functions to (fast) algebraic attack appears to be better if both linear and affine functions are used without using "too many" $n/2$-variable functions in the concatenation, though it also depends on the space decomposition in a quite complicated manner (cf. Section III-B). Unfortunately, even though we have tried to address the issue of "too many" in a rigorous manner, a better understanding of the impact of the choice of subfunctions and their dimensions is still lacking. Nevertheless, a large class of resilient functions with currently best known nonlinearity is obtained, and our results are superior to any other method for virtually all input instances. This class is characterized by an optimal algebraic degree, extremely high nonlinearity, and it has been confirmed that within this class there are functions with very good AI (either optimal or almost optimal) and good resistance to fast algebraic attack (FAA).

Since the resistance of our functions against FAA is only moderate (not optimal) for resilient functions, we provide different alternative solutions to this problem. In the first place, the desired security margins may be achieved by increasing the number of variables since the complexity of implementation of GMM functions is rather low due to the employment of affine subfunctions.

In other direction, by dropping both resiliency and injectivity of our mappings ϕ_i (allowing a repetition of affine functions in the concatenation), the existence of balanced highly nonlinear Boolean functions within the GMM class with excellent algebraic properties is confirmed. That is, functions with optimal AI, very good nonlinearity and almost optimal resistance to FAA are exhibited and a generic method of their construction is given.

In the last part of this article we generalize the above approach for the case when n is odd. The derived functions also attain the highest known nonlinearity values for (small order) resilient functions, and furthermore the lower bound on nonlinearity is even improved in most of the cases compared to the bound for the above approach. However, since these functions are defined for relatively large input spaces their AI property are infeasible to determine.

The remainder of this paper is organized as follows. In Section II, we present the basic concepts and notions. In Section III, we introduce the GMM construction technique, and construct SAO resilient functions on even number of variables. The usage of GMM functions in the design of S-boxes in block cipher applications along with the design of balanced (1-resilient) functions using GMM method satisfying all the relevant cryptographic criteria is discussed in Section IV. A large class of n-variable (n odd) resilient functions with currently best known nonlinearity are obtained in Section V. Section VI concludes the paper with a conjecture on the upper bound on nonlinearity of resilient Boolean functions.

II. Preliminaries

For the convenience of the reader we repeat the relevant material without proof, thus making our exposition self-contained.

Let $\mathcal{B}_n$ denote the set of Boolean functions of n variables. A *Boolean function* $f(X_n) \in \mathcal{B}_n$ is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, the finite field with two elements, where $X_n = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. The additions of integers in $\mathbb{R}$ is denoted by $+$ and Σ_i, and over $\mathbb{F}_2$ by $\oplus$ and $\bigoplus_i$. For simplicity, we denote by $+$ the addition of vectors of $\mathbb{F}_2^n$. Any Boolean function has a unique representation as a multivariate polynomial over $GF(2)$, called *algebraic normal form* (ANF),

$$f(X_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^{n} x_i^{u_i}), \tag{2}$$

where $\lambda_u \in \mathbb{F}_2,\ u = (u_1, \ldots, u_n)$. The *algebraic degree* of $f(X_n)$, denoted by $deg(f)$, is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$, where $wt(u)$ denotes the Hamming weight of u. A Boolean function with $deg(f) \leq 1$ is said to be *affine* and the set of all n-variable affine functions is denoted by $\mathcal{A}_n$. An affine function with the constant term equal to zero is called a *linear* function. Any linear function on

$\mathbb{F}_2^n$ is denoted by $\omega \cdot X_n = \omega_1 x_1 \oplus \ldots \oplus \omega_n x_n$, where $\omega = (\omega_1, \ldots, \omega_n)$, $X_n = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, and "$\cdot$" denotes the dot (inner) product of two vectors. Also, we say that a linear function $\omega \cdot X_n$ is *nondegenerate* in k variables if $wt(\omega) = k$.

Many properties of Boolean function can be deduced from its Walsh spectra. The *Walsh transform* of $f(x)$ is an integer valued function over $\mathbb{F}_2^n$ defined by

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

A function f is balanced if its output column in the truth table contains equal number of 0's and 1's, i.e., $W_f(0) = 0$. Two Boolean functions $f(X_n), g(X_n) \in \mathcal{B}_n$ are said to be a pair of *disjoint spectra functions* if $W_f(\omega) W_g(\omega) = 0$, for all $\omega \in \mathbb{F}_2^n$. In terms of Walsh spectra, the nonlinearity of f is given by [16]

$$N_f = 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |W_f(w)|. \tag{4}$$

The *concatenation*, denoted by "$||$" simply means that the truth tables of the functions are merged. For instance, for $f_1, f_2 \in \mathcal{B}_n$ one may construct $f = f_1 || f_2 \in \mathcal{B}_{n+1}$, meaning that the upper half part of the truth table of f corresponds to f_1 and the lower part to f_2.

Definition 1. *Given $f(x) \in \mathcal{B}_n$, define*

$$AN(f) = \{g(X_n) \in \mathcal{B}_n \mid f(x)g(X_n) = 0,\ \forall X_n \in \mathbb{F}_2^n\}. \tag{5}$$

Any function $g \in AN(f)$ is called an annihilator *of f. The* AI*, denoted by $AI(f)$, of function $f \in \mathcal{B}_n$ is the minimum degree of all non-zero annihilators of f and $f + 1$.*

In [27], a spectral characterization of resilient functions has been presented. The following fact will be proved useful for our discussion.

Lemma 1. *[27] An n-variable Boolean function is m-*resilient *if and only if its Walsh transform satisfies*

$$W_f(\omega) = 0, \text{ for all } \omega \in \mathbb{F}_2^n \text{ such that } 0 \le wt(\omega) \le m.$$

A method of transforming a balanced Boolean function into a 1-resilient function was presented in [18]. This method is called LT-method (Linear Transformation method) in [11]. Given a balanced function $f \in \mathcal{B}_n$, we define

$$S_f = \{\omega \in \mathbb{F}_2^n \mid W_f(\omega) = 0\}. \tag{6}$$

If there exist n linearly independent vectors in S_f, then one can construct a nonsingular $n \times n$ matrix B_f whose rows are linearly independent vectors from S_f. Let $f'(x) = f(C_f x)$, where $C_f = B_f^{-1}$. Then f' is 1-resilient, and both f' and f have the same nonlinearity and algebraic properties.

III. GMM CONSTRUCTION TECHNIQUE

In this section, we recall the definition of the original MM class Boolean functions and define the GMM family of functions. We then present the GMM construction technique that yields the design of SAO resilient Boolean functions on even number of variables.

Definition 2. *For any positive integers p, q such that $n = p+q$, an* MM *function $f \in \mathcal{B}_n$ is defined by*

$$f(Y_q, X_p) = \phi(Y_q) \cdot X_p \oplus g(Y_q), \quad X_p \in \mathbb{F}_2^p,\ Y_q \in \mathbb{F}_2^q, \tag{7}$$

where ϕ is any mapping from $\mathbb{F}_2^q$ to $\mathbb{F}_2^p$, $g \in \mathcal{B}_q$.

The standard MM construction technique is in nature a construction of nonlinear n-variable Boolean functions by concatenating 2^q p-variable affine functions. This simply means that the truth table of f consists of 2^q truth tables of p-variable affine functions since f is affine in variables $x_1, \ldots, x_p$ for any fixed $Y_q \in \mathbb{F}_2^q$. It is well-known that the nonlinearity of this class of functions entirely depends on the size of p, that is, assuming that ϕ is injective $N_f = 2^{n-1} - 2^{p-1}$. To ensure that ϕ is injective for m-resilient functions, only nondegenerate affine functions in at least $m+1$ variables must be used and therefore p must satisfy the following inequality $\sum_{i=m+1}^{p} \binom{p}{i} \ge 2^{n-p}$. This immediately implies that $p \ge \lceil n/2 \rceil$ for any $m \ge 0$, thus $N_f \le 2^{n-1} - 2^{\lceil \frac{n}{2} \rceil}$. The case when ϕ is not injective has been treated in [1], [20].

For even n, our generalization of this method is based on the observation that it is not necessary to use affine functions in p variables ($p > n/2$) to ensure that ϕ is injective. One may equally well only use the totality of m-resilient affine functions of up to $n/2$ variables that are available (there are $\sum_{i=m+1}^{n/2} \binom{n/2}{i}$ such functions), whereas the remaining $\sum_{i=0}^{m} \binom{n/2}{i}$ functions are suitable nonlinear m-resilient functions. These functions are actually affine on some $(n/2 - i)$-variable space for some suitable $i > 0$, but when viewed as functions on an $n/2$-variable space (a concatenation of 2^i distinct m-resilient linear functions in $n/2 - i$ variables) these functions are nonlinear.

The GMM construction technique is now described in due detail. It uses suitably selected linear (affine) functions for achieving the best known nonlinearity for this class of functions, cf. Example 1 and 2.

Construction 1. *Let for $1 \le i \le n-1$, $E_i \subseteq \mathbb{F}_2^i$ and $E'_i = E_i \times \mathbb{F}_2^{n-i}$ such that*

$$\bigcup_{i=1}^{n-1} E'_i = \mathbb{F}_2^n, \tag{8}$$

and

$$E'_{i_1} \cap E'_{i_2} = \emptyset, \quad 1 \le i_1 < i_2 \le n-1.$$

Let $X_n = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $X'_i = (x_1, \ldots, x_i) \in \mathbb{F}_2^i$ and $X''_{n-i} = (x_{i+1}, \ldots, x_n) \in \mathbb{F}_2^{n-i}$. Let ϕ_i be a mapping from $\mathbb{F}_2^i$ to $\mathbb{F}_2^{n-i}$. A GMM type Boolean function $f \in \mathcal{B}_n$ can be constructed as follows:

$$f(X_n) = \phi_i(X'_i) \cdot X''_{n-i} \oplus g_i(X'_i), \text{ if } X'_i \in E_i,\ i = 1, \ldots, n-1, \tag{9}$$

where $g_i \in \mathcal{B}_i$.

Remark 1. *We formally allow $1 \le i \le n-1$, though from the SAO point of view it only makes sense to use affine functions in at most $n/2$ variables, thus $i \ge n/2$.*

For the convenience of the reader, the following example further clarifies the space decomposition $\bigcup_{i=1}^{n-1} E'_i = \mathbb{F}_2^n$ in Construction 1.

Example 1. *Let us consider the construction of a balanced function on $\mathbb{F}_2^6$, i.e., $n = 6$. Since $m = 0$, the number of nondegenerate linear functions in 3-variables in at least one variable equals to $\sum_{i=1}^{3} \binom{3}{i} = 7$. For instance, f can be partially specified as follows (where for simplicity $g(X_i') = 0$):*

$$\begin{array}{ll} f(0,0,0,X_3'') = x_4 & f(1,0,0,X_3'') = x_5 \\ f(0,1,0,X_3'') = x_6 & f(1,1,0,X_3'') = x_4 \oplus x_5 \\ f(0,0,1,X_3'') = x_4 \oplus x_6 & f(1,0,1,X_3'') = x_5 \oplus x_6 \\ f(0,1,1,X_3'') = x_4 \oplus x_5 \oplus x_6 & f(1,1,1,X_3'') = h(X_3'') \end{array}$$

More formally, we have specified a mapping $\phi_3 : \mathbb{F}_2^3 \setminus \{(1,1,1)\} \to T_3$, where $T_3 = \{a \in \mathbb{F}_2^3 \mid wt(a) \geq 1\}$. For instance, $\phi_3((0,0,0)) = (1,0,0)$, thus $\phi_3((0,0,0)) \cdot X_3'' = (1,0,0) \cdot (x_4, x_5, x_6) = x_4$. Let $E_3 = \mathbb{F}_2^3 \setminus \{(1,1,1)\}$ and $E_3' = E_3 \times \mathbb{F}_2^3$, so that

$$\mathbb{F}_2^6 = E_3' \cup \{(1,1,1)\} \times \mathbb{F}_2^3,$$

which may be rewritten as $\mathbb{F}_2^6 = E_3' \cup \{(1,1,1)\} \times \mathbb{F}_2 \times \mathbb{F}_2^2$. Because f is completely specified on E_3', it remains to specify $h(X_3'')$. This may be done by specifying two functions $h(0,x_5,x_6), h(1,x_5,x_6) \in \mathcal{B}_2$ for the cases $x_4 = 0$ and $x_4 = 1$, respectively. Thus, let

$$\begin{array}{l} f(1,1,1,0,x_5,x_6) = h(0,x_5,x_6) = x_5 \\ f(1,1,1,1,x_5,x_6) = h(1,x_5,x_6) = x_5 \oplus x_6, \end{array}$$

and consequently

$$h(X_3'') = (1 \oplus x_4) h(0,x_5,x_6) \oplus x_4 h(1,x_5,x_6) = x_5 \oplus x_4 x_6$$

is a nonlinear balanced function, and f is now completely specified. It can be verified that $N_f = 26$ which is better compared to the standard MM method providing f with $N_f = 24$.

Remark 2. *It would be of benefit to further decompose the space and use subfuntions in smaller number of variables, but in the above example it is clearly impossible since there are no four distinct linear functions in one variable. Note also that 26 is the maximum possible nonlinearity of balanced functions on $\mathbb{F}_2^6$. This approach is formalised in Theorem 1 by introducing $(a_{n/2}, \ldots, a_{n-m-1}) \in \mathbb{F}_2^{n/2-m}$ which through inequality (10) examines the possibility of using suitable subfunctions in the least number of variables.*

Theorem 1. *With the same notation as in Construction 1, let n be even and $E_i = \emptyset$, for $1 \leq i \leq n/2 - 1$. Let $0 \leq m \leq n/2 - 2$, and $(a_{n/2}, \ldots, a_{n-m-1}) \in \mathbb{F}_2^{n/2-m}$ (where $a_{n/2} = 1$) be the binary vector such that $\sum_{i=n/2}^{n-m-1} a_i 2^i$ is maximal, satisfying at the same time,*

$$\sum_{i=n/2}^{n-m-1} \left(a_i \cdot 2^{n-i} \sum_{j=m+1}^{n-i} \binom{n-i}{j} \right) \geq 2^n. \tag{10}$$

Let $e = \max\{i \mid a_i \neq 0,\ n/2 \leq i \leq n-m-1\}$. For $n/2 \leq i \leq e$, set

$$\begin{cases} |E_i| = 0, & \text{if } a_i = 0 \\ |E_i| \leq \sum_{j=m+1}^{n-i} \binom{n-i}{j}, & \text{if } a_i = 1. \end{cases} \tag{11}$$

For $n/2 \leq i \leq e$ and $a_i = 1$, let ϕ_i be an injective mapping from E_i to T_i, where

$$T_i = \{c \mid wt(c) \geq m+1,\ c \in \mathbb{F}_2^{n-i}\}. \tag{12}$$

Then the function $f \in \mathcal{B}_n$ proposed by Construction 1 is a SAO m-resilient function with nonlinearity

$$N_f \geq 2^{n-1} - 2^{n/2-1} - \sum_{i=n/2+1}^{e} a_i \cdot 2^{n-i-1}. \tag{13}$$

Proof: Obviously, the inequality in (10) ensures that (11) holds. Then $|E_i| \leq |T_i|$ for any $n/2 \leq i \leq e$. Hence, it is possible to build the series of injective mappings ϕ_i from E_i to T_i with $n/2 \leq i \leq e$ and $a_i = 1$. Without loss of generality, we always let $g_i = 0$. For any $\omega = (\omega_1, \ldots, \omega_n) = (\Omega_k', \Omega_{n-k}'') \in \mathbb{F}_2^n$, by (8), we have,

$$\begin{aligned} W_f(\omega) &= \sum_{X_n \in \bigcup_{i=n/2}^{e} E_i'} (-1)^{f(X_n) \oplus \omega \cdot X_n} \\ &= \sum_{i=n/2}^{e} \left(\sum_{X_i' \in E_i} (-1)^{\Omega_i' \cdot X_i'} \right. \\ &\qquad \left. \times \sum_{X_{n-i}'' \in \mathbb{F}_2^{n-i}} (-1)^{\phi_e(X_i') \cdot X_{n-i}'' \oplus \Omega_{n-i}'' \cdot X_{n-i}''} \right) \\ &= \sum_{i=n/2}^{e} a_i S_i(\omega), \end{aligned} \tag{14}$$

where

$$\begin{aligned} S_i(\omega) = & \sum_{X_i' \in E_i} (-1)^{(\omega_1, \ldots, \omega_i) \cdot X_i'} \\ \times & \sum_{X_{n-i}'' \in \mathbb{F}_2^{n-i}} (-1)^{\phi_i(X_i') \cdot X_{n-i}'' + (\omega_{i+1}, \ldots, \omega_n) \cdot X_{n-i}''}. \end{aligned} \tag{15}$$

Obviously, if $\phi_i^{-1}(\omega_{i+1}, \ldots, \omega_n)$ exists,

$$S_i(\omega) = (-1)^{(\omega_1, \ldots, \omega_i) \cdot \phi_i^{-1}(\omega_{i+1}, \ldots, \omega_n)} \cdot 2^{n-i};$$

Otherwise, $S_i(\omega) = 0$. That is,

$$S_i(\omega) = \begin{cases} \pm 2^{n-i}, & \text{if } \phi_i^{-1}(\omega_{i+1}, \ldots, \omega_n) \text{ exists} \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

Therefore,

$$|W_f(\omega)| \leq \sum_{i=n/2}^{e} a_i \cdot 2^{n-i}. \tag{17}$$

Note that inequality in (10) cannot be satisfied if $E_{n/2} = \emptyset$. Thus, we have $E_{n/2} \neq \emptyset$ which implies that $a_{n/2} = 1$. By (4), inequality in (44) holds.

When $0 \leq wt(\omega) \leq m$, we always have $(\omega_{i+1}, \ldots, \omega_n) \notin T_i$ for $n/2 \leq i \leq n-1$. By (16), we have $S_i = 0$. Hence,

$$W_f(\omega) = \sum_{i=n/2}^{n-1} a_i S_i(\omega) = 0. \tag{18}$$

Due to Lemma 1, f is an m-resilient Boolean function. ■

Obviously, the degree of f proposed in Theorem 1 can reach $e+1$. Siegenthaler [25] and Xiao and Massey [27] proved that for an n-variable m-resilient function of degree d it holds that $d \le n-m-1$. Such a resilient function having $d = n-m-1$ is called *degree-optimized.* Notice if $e = n-m-2$, which means that $(m+2)$-variable functions are used in the construction, then it might be the case that $\deg(f) = n-m-1$. The sufficient condition that f is degree-optimized in the case $e = n-m-2$ is,

$$\bigoplus_{X'_e \in E_e} \phi_e(X'_e) \cdot X''_{n-e} \neq 0. \tag{19}$$

Indeed, this implies that the term

$$x_1 x_2 \cdots x_{n-m-2} \left(\bigoplus_{X'_e \in E_e} \phi_e(X'_e) \cdot X''_{n-e} \right) \tag{20}$$

of degree $n-m-1$ is present in the ANF of f.

On the other hand, if $e < n-m-2$ then $n-e > m+2$ and we let $\{i_1, \dots, i_{m+1}\} \cup \{i_{m+2}, \dots, i_{n-e}\} = \{e+1, \dots, n\}$. For a fixed $\delta \in E_e$, let $\phi_e(\delta) = (c_{e+1}, \dots, c_n)$ with $(c_{i_1}, \dots, c_{i_{m+1}}) = (1, \dots, 1)$. The algebraic degree of the function obtained in Theorem 1 can be optimized as below:

$$f'(X_n) = \begin{cases} \phi_i(X'_i) \cdot X''_{n-i} \oplus g_i(X'_i), & \text{if } X'_i \in E_i, \\ & \;\; i = 1, \dots, e-1 \\ \phi'_e(X'_e) \cdot X''_{n-e} \oplus g_e(X'_i), & \text{if } X'_i \in E_e \setminus \{\delta\} \\ c \cdot X''_{n-e} \oplus x_{i_{m+2}} \dots x_{i_{n-e}}, & \text{if } X'_i = \delta. \end{cases} \tag{21}$$

Thus, the nonlinear function

$$h(X''_{n-e}) = c \cdot X''_{n-e} \oplus x_{i_{m+2}} \dots x_{i_{n-e}} \tag{22}$$

of degree $n-e-m-1$ is used instead of one affine function. Moreover, the degree of f' equals to $e + (n-e-m-1) = n-m-1$, that is, f' is degree-optimized (the term $x_1 \dots x_e x_{i_{m+2}} \dots x_{i_{n-e}}$ occurs in the ANF of f'). It is clear that this nonlinear function is m-resilient, therefore f' is an m-resilient function. Next we will show that $N_{f'} \in \{N_f, N_f - 2^{m+1}\}$, where f is the function in Construction 1 given by (8).

Let $f' \in \mathcal{B}_n$ be defined as in (21). Without loss of generality, we always let $g_i = 0$. For any $\omega = (\omega_1, \dots, \omega_n) \in \mathbb{F}_2^n$,

$$W_{f'}(\omega) = \left(\sum_{i=n/2}^{e-1} a_i S_i(\omega) \right) + S'_e(\omega) + S_\delta(\omega), \tag{23}$$

where $S_i(\omega)$, for $i = n/2, \dots, e-1$, are defined in the proof of Theorem 1. Furthermore,

$$\begin{aligned} S'_e(\omega) &= \sum_{X'_e \in E_e \setminus \{\delta\}} (-1)^{(\omega_1, \dots, \omega_e) \cdot X'_e} \\ &\times \sum_{X''_{n-e} \in \mathbb{F}_2^{n-e}} (-1)^{\phi'_e(X'_e) \cdot X''_{n-e} \oplus (\omega_{e+1}, \dots, \omega_n) \cdot X''_{n-e}} \\ &= \begin{cases} (-1)^{(\omega_1, \dots, \omega_e) \cdot \phi_e'^{-1}(\omega_{e+1}, \dots, \omega_n)} \cdot 2^{n-e}, \\ \qquad\qquad \text{if } \phi'^{-1}(\omega_{e+1}, \dots, \omega_n) \text{ exists} \\ 0, \qquad\quad \text{otherwise} \end{cases} \\ &= \begin{cases} \pm 2^{n-e}, & \text{if } \phi'^{-1}(\omega_{e+1}, \dots, \omega_n) \text{ exists} \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

and

$$\begin{aligned} S_\delta(\omega) &= (-1)^{(\omega_1, \dots, \omega_e) \cdot \delta} \\ &\times \sum_{X''_{n-e} \in \mathbb{F}_2^{n-e}} (-1)^{h(X''_{n-e}) \oplus (\omega_{e+1}, \dots, \omega_n) \cdot X''_{n-e}} \\ &= \begin{cases} 0, \quad \text{if } (\omega_{i_1}, \dots, \omega_{i_{m+1}}) \neq (c_{i_1}, \dots, c_{i_{m+1}}) \\ 2^{n-e} - 2^{m+2}, & \text{if } (\omega_{e+1}, \dots, \omega_n) = c \\ \pm 2^{m+2}, & \text{otherwise.} \end{cases} \end{aligned}$$

Then, we always have

$$\max_{\omega \in \mathbb{F}_2^n} |S'_e(\omega) + S_\delta(\omega)| = \begin{cases} 2^{n-e}, & S'_e(\omega) S_\delta(\omega) = 0 \\ 2^{n-e} + 2^{m+2}, & \text{otherwise.} \end{cases}$$

By (23) and (17), we have

$$N_{f'} = \begin{cases} N_f, & S'_e(\omega) S_\delta(\omega) = 0 \\ N_f - 2^{m+1}, & \text{otherwise.} \end{cases}$$

Remark 3. *Let*

$$\begin{aligned} T'_e = \{c \mid c = (c_{e+1}, \dots, c_n) \in \mathbb{F}_2^{n-e}, \\ wt(c) \ge m+1, (c_{i_1}, \dots, c_{i_{m+1}}) \neq (1 \dots 1)\}. \end{aligned} \tag{24}$$

Essentially, we can ensure that

$$S'_e(\omega) S_\delta(\omega) = 0 \tag{25}$$

if $|E_e| - 1 \le |T'_e|$ and ϕ'_e is an injective mapping from $E_e \setminus \{\delta\}$ to T'_e, see [17], [28] for further details.

By an (n, m, d, N_f) function we mean an n-variable, m-resilient Boolean function f with algebraic degree d and nonlinearity N_f.

The following example further explains the particular choice of the subfunctions used in the construction of a $(12, 1, -, 2^{11} - 2^5 - 2^4)$ function. Note that if the standard MM method was used (with injective ϕ) one would be forced to select 32 linear/affine functions (nondegenerate in at least two variables) from $\mathbb{F}_2^7$ and the resulting nonlinearity would be $2^{11} - 2^6 < 2^{11} - 2^5 - 2^4$.

Example 2. *Using the GMM method one can construct a $(12, 1, -, 2^{11} - 2^5 - 2^4)$ function. Note that*

$$2^6 \sum_{j=2}^{6} \binom{6}{j} + 2^5 \sum_{j=2}^{5} \binom{5}{j} \ge 2^{12}.$$

We can set $E_6 \subseteq \mathbb{F}_2^6$ with $|E_6| = \sum_{j=2}^{6} \binom{6}{j} = 57$, and $E_7 = \overline{E_6} \times \mathbb{F}_2$ where $\overline{E_6} = \mathbb{F}_2^6 \setminus E_6$. Obviously, $|E_7| = 2 \cdot \sum_{j=0}^{1} \binom{6}{j} \le \sum_{j=2}^{5} \binom{5}{j}$. This essentially means that the number of 1-resilient functions in five variables suffices for specifying the remaining 7 functions in 6 variables, just as it has been done in Example 1. So it is possible to build two injective mappings $\phi_6 : E_6 \mapsto T_6$ and $\phi_7 : E_7 \mapsto T_7$. From Theorem 1 and its proof, a 12-variable, 1-resilient Boolean function with nonlinearity $2^{11} - 2^5 - 2^4 = 2000$ can be constructed as follows:

$$f(X_{12}) = \begin{cases} \phi_6(X'_6) \cdot X''_6, & \text{if } X'_6 \in E_6 \\ \phi_7(X'_7) \cdot X''_5, & \text{if } X'_7 \in E_7. \end{cases}$$

TABLE I
SUBFUNCTIONS IN THE CONSTRUCTION OF A 12-VARIABLE GMM FUNCTION

$l_0(X_6'') = x_8 \oplus x_9 \oplus x_{11}$	$l_1(X_6'') = x_7 \oplus x_{11} \oplus x_{12}$
$l_2(X_6'') = x_7 \oplus x_9 \oplus x_{11}$	$l_3(X_6'') = x_{11} \oplus x_{12}$
$l_4(X_6'') = x_{10} \oplus x_{11}$	$l_5(X_6'') = x_7 \oplus x_8 \oplus x_{11} \oplus x_{12}$
$l_6(X_6'') = x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12}$	$l_7(X_6'') = x_7 \oplus x_{12}$
$l_8(X_6'') = x_9 \oplus x_{11} \oplus x_{12}$	$l_9(X_6'') = x_7 \oplus x_8 \oplus x_{10}$
$l_{10}(X_6'') = x_7 \oplus x_8 \oplus x_9 \oplus x_{11}$	$l_{11}(X_6'') = x_7 \oplus x_{10}$
$l_{12}(X_6'') = x_7 \oplus x_9 \oplus x_{10} \oplus x_{12}$	$l_{13}(X_6'') = x_8 \oplus x_9 \oplus x_{11} \oplus x_{12}$
$l_{14}(X_6'') = x_7 \oplus x_{10} \oplus x_{11} \oplus x_{12}$	$l_{15}(X_6'') = x_9 \oplus x_{10} \oplus x_{12}$
$l_{16}(X_6'') = x_7 \oplus x_{10} \oplus x_{12}$	$l'_{17}(X_5'')=x_{10}\oplus x_{12}$ * $l''_{17}(X_5'')=x_{10}\oplus x_{11}$ *
$l_{18}(X_6'') = x_7 \oplus x_9 \oplus x_{11} \oplus x_{12}$	$l_{19}(X_6'') = x_7 \oplus x_8 \oplus x_{11}$
$l_{20}(X_6'') = x_8 \oplus x_{11} \oplus x_{12}$	$l_{21}(X_6'') = x_7 \oplus x_8 \oplus x_{10} \oplus x_{11}$
$l_{22}(X_6'') = x_7 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{11}$	$l'_{23}(X_5'')=x_9\oplus x_{10}\oplus x_{11}$ * $l''_{23}(X_5'')=x_9\oplus x_{10}\oplus x_{11}\oplus x_{12}$ *
$l_{24}(X_6'') = x_8 \oplus x_9 \oplus x_{10} \oplus x_{11}$	$l'_{25}(X_5'')=x_{10}\oplus x_{11}\oplus x_{12}$ * $l''_{25}(X_5'')=x_9\oplus x_{12}$ *
$l_{26}(X_6'') = x_7 \oplus x_9 \oplus x_{10}$	$l_{27}(X_6'') = x_8 \oplus x_9 \oplus x_{12}$
$l_{28}(X_6'') = x_9 \oplus x_{10} \oplus x_{11}$	$l_{29}(X_6'') = x_7 \oplus x_8 \oplus x_9$
$l_{30}(X_6'') = x_7 \oplus x_9 \oplus x_{10} \oplus x_{11}$	$l_{31}(X_6'') = x_8 \oplus x_{12}$
$l_{32}(X_6'') = x_{10} \oplus x_{11} \oplus x_{12}$	$l_{33}(X_6'') = x_8 \oplus x_{10} \oplus x_{11}$
$l_{34}(X_6'') = x_8 \oplus x_9$	$l_{35}(X_6'') = x_{10} \oplus x_{12}$
$l_{36}(X_6'') = x_8 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12}$	$l_{37}(X_6'') = x_7 \oplus x_8 \oplus x_{12}$
$l_{38}(X_6'') = x_7 \oplus x_8 \oplus x_9 \oplus x_{11} \oplus x_{12}$	$l'_{39}(X_5'')=x_8\oplus x_{12}$ * $l''_{39}(X_5'')=x_8\oplus x_{11}$ *
$l_{40}(X_6'') = x_9 \oplus x_{10}$	$l_{41}(X_6'') = x_9 \oplus x_{11}$
$l'_{42}(X_5'')=x_9\oplus x_{10}$ * $l''_{42}(X_5'')=x_9\oplus x_{10}\oplus x_{12}$ *	$l_{43}(X_6'') = x_7 \oplus x_9$
$l_{44}(X_6'') = x_7 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12}$	$l_{45}(X_6'') = x_7 \oplus x_8 \oplus x_9 \oplus x_{12}$
$l_{46}(X_6'') = x_9 \oplus x_{12}$	$l_{47}(X_6'') = x_7 \oplus x_{10} \oplus x_{11}$
$l_{48}(X_6'') = x_7 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{12}$	$l_{49}(X_6'') = x_8 \oplus x_{10} \oplus x_{12}$
$l_{50}(X_6'')=x_7\oplus x_8\oplus x_9\oplus x_{10}$ $\oplus x_{11}\oplus x_{12}$	$l_{51}(X_6'') = x_8 \oplus x_9 \oplus x_{10} \oplus x_{12}$
$l_{52}(X_6'') = x_7 \oplus x_8 \oplus x_{10} \oplus x_{11} \oplus x_{12}$	$l_{53}(X_6'') = x_7 \oplus x_8 \oplus x_{10} \oplus x_{12}$
$l_{54}(X_6'') = x_8 \oplus x_{10} \oplus x_{11} \oplus x_{12}$	$l_{55}(X_6'') = x_7 \oplus x_8$
$l_{56}(X_6'') = x_8 \oplus x_{11}$	$l'_{57}(X_5'')=x_9\oplus x_{11}$ * $l''_{57}(X_5'')=x_9\oplus x_{11}\oplus x_{12}$ *
$l_{58}(X_6'') = x_7 \oplus x_{11}$	$l_{59}(X_6'') = x_7 \oplus x_9 \oplus x_{12}$
$l'_{60}(X_5'')=x_8\oplus x_9\oplus x_{10}\oplus x_{11}\oplus x_{12}$ * $l''_{60}(X_5'')=x_{1q}\oplus x_{12}$ *	$l_{61}(X_6'') = x_7 \oplus x_8 \oplus x_9 \oplus x_{10}$
$l_{62}(X_6'') = x_8 \oplus x_{10}$	$l_{63}(X_6'') = x_8 \oplus x_9 \oplus x_{10}$

*Table I lists 57 different 6-variable and 14 different 5-variable 1-resilient linear functions (denoted with *) used as subfunctions of f. E.g. the function $x_8 \oplus x_9 \oplus x_{11}$ is a subfunction of f, more precisely $f(0,0,0,\dots,0,X_6'') = x_8 \oplus x_9 \oplus x_{11}$, where $X_6'' = (x_7,\dots,x_{12})$. In general, in Table I, x_1 are used to identify the column whereas $x_2,\dots,x_6$ enumerates the rows, e.g. $f(1,0,0,\dots,0,X_6'') = x_7 \oplus x_{11} \oplus x_{12}$. Notice that the parameter $e = \max\{i \mid a_i \neq 0,\ n/2 \le i \le n-m-1\}$, as defined in Theorem 1, equals to $n/2+1 = 7$. In other words, it determines the smallest variable space used in the construction, in this case the usage of linear functions in $n-e = 5$ variables.*

Notice that $\deg(f) \le e+1 = 8$ in Example 2, and simply by replacing for instance the 5-variable function $x_8 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12}$ (found in the last row of Table I) with a nonlinear function $x_8 \oplus x_9 \oplus x_{10}x_{11}x_{12}$ one gets a degree-optimized function f'.

The *design procedure*, for achieving the highest nonlinearity using injective ϕ_i, that applies to Construction 1 can be summarised as follows:

a) Select all $\sum_{i=m+1}^{n/2}\binom{n/2}{i}$ linear functions nondegenerate in at least $m+1$ variables.
b) Determine the maximum value of $\sum_{i=n/2}^{n-m-1} a_i 2^i$ satisfying inequality in (10), where $(a_{n/2},\cdots,a_{n-m-1}) \in \mathbb{F}_2^{n/2-m}$ and $a_{n/2} = 1$. Here, $a_i = 1$ indicates the usage of linear functions in $n-i$ variables, for $i = n/2,\dots,n-m-1$. Due to (17), the nonlinearity is larger when affine functions from smaller variable spaces are available, i.e., when i is larger.
c) The injective mappings $\phi_i : E_i \to T_i$ are chosen arbitrary, though the selection of elements from T_i along with the possibility of using either linear or affine functions appear to affect the algebraic properties of the function (cf. Section III-B), hence the functions g_i are nonconstant.
d) If f is not degree-optimized then f' is constructed by replacing one $(n-e)$-variable function with a nonlinear function as described previously. It should be noted that $N_{f'} = N_f$ if the equation in (25) holds.

Using the GMM construction technique, we can provide degree-optimized resilient Boolean functions with currently best known nonlinearity, as illustrated in Table II.

A. A formal comparison to the method in [28]

The main reason why the GMM technique performs better than the method proposed in [28] is that the number of subfunctions available using the GMM method appears to be, in general, larger than the number of partially linear disjoint spectra functions used in [28]. This is formally confirmed by comparing these numbers when the term 2^{k-1} ($\lceil \frac{n}{4} \rceil \le k < t$) appears in the value of nonlinearity (which is always the case for SAO functions), where $t = n/2$. The number of subfunctions available in [28] is,

$$\sum_{i=m+1}^{2k-t}\binom{2k-t}{i}. \tag{26}$$

On the other hand, this count for the GMM construction is given by,

$$\left\lfloor \frac{\sum_{i=m+1}^{k}\binom{k}{i}}{2^{t-k}} \right\rfloor. \tag{27}$$

Lemma 2. *Let $u > v > m$ and let*

$$A_u = \sum_{i=m+1}^{u}\binom{u}{i}, \quad A_v = \sum_{i=m+1}^{v}\binom{v}{i}.$$

Then,

$$A_u = 2^{u-v}A_v + \sum_{i=1}^{u-v} 2^{i-1}\binom{u-i}{m}. \tag{28}$$

Proof: Using $\binom{u}{i} = \binom{u-1}{i} + \binom{u-1}{i-1}$, we have

$$\begin{aligned} A_u &= \sum_{i=m+1}^{u-1}\left(\binom{u-1}{i} + \binom{u-1}{i-1}\right) + 1 \\ &= \sum_{i=m+1}^{u-1}\binom{u-1}{i} + \sum_{i=m+1}^{u-1}\binom{u-1}{i-1} + 1 \\ &= 2\sum_{i=m+1}^{u-1}\binom{u-1}{i} + \binom{u-1}{m} \\ &= 2A_{u-1} + \binom{u-1}{m} \\ &= 2^{u-v}A_v + \sum_{i=1}^{u-v} 2^{i-1}\binom{u-i}{m}. \end{aligned}$$

TABLE II
NONLINEARITY COMPARISON OF THE DEGREE-OPTIMIZED GMM FUNCTIONS TO THE WORK IN [28] (n EVEN)

m	n	GMM construction	Ref. [28]
1	12	$2^{11}-2^{5}-2^{4}$	$2^{11}-2^{5}-2^{4}-2^{2}$
	14	$2^{13}-2^{6}-2^{4}-2^{3}-2^{2}$	$2^{13}-2^{6}-2^{5}-2^{2}$
	16	$2^{15}-2^{7}-2^{5}$	$2^{15}-2^{7}-2^{5}-2^{2}$
	18	$2^{17}-2^{8}-2^{6}$	$2^{17}-2^{8}-2^{6}-2^{2}$
	20	$2^{19}-2^{9}-2^{6}$	$2^{19}-2^{9}-2^{6}-2^{2}$
	24	$2^{23}-2^{11}-2^{7}-2^{2}$	$2^{23}-2^{11}-2^{8}-2^{2}$
	26	$2^{25}-2^{12}-2^{8}$	$2^{25}-2^{12}-2^{8}-2^{2}$
	28	$2^{27}-2^{13}-2^{8}-2^{2}$	$2^{27}-2^{13}-2^{9}-2^{2}$
	30	$2^{29}-2^{14}-2^{9}$	$2^{29}-2^{14}-2^{9}-2^{2}$
	36	$2^{35}-2^{17}-2^{10}-2^{9}-2^{2}$	$2^{35}-2^{17}-2^{11}-2^{2}$
	54	$2^{53}-2^{26}-2^{15}-2^{2}$	$2^{53}-2^{26}-2^{15}-2^{14}-2^{2}$
	58	$2^{57}-2^{28}-2^{16}-2^{2}$	$2^{57}-2^{28}-2^{16}-2^{15}-2^{2}$
2	16	$2^{15}-2^{7}-2^{6}$	$2^{15}-2^{7}-2^{6}-2^{3}$
	18	$2^{17}-2^{8}-2^{7}$	$2^{17}-2^{8}-2^{7}-2^{3}$
	20	$2^{19}-2^{9}-2^{7}-2^{5}$	$2^{19}-2^{9}-2^{8}$
	22	$2^{21}-2^{10}-2^{8}$	$2^{21}-2^{10}-2^{8}-2^{3}$
	26	$2^{25}-2^{12}-2^{9}$	$2^{25}-2^{12}-2^{9}-2^{3}$
	30	$2^{29}-2^{14}-2^{10}-2^{3}$	$2^{29}-2^{14}-2^{11}-2^{3}$
	34	$2^{33}-2^{16}-2^{11}-2^{10}-2^{3}$	$2^{33}-2^{16}-2^{12}-2^{3}$
	44	$2^{43}-2^{21}-2^{14}-2^{3}$	$2^{43}-2^{21}-2^{14}-2^{13}-2^{3}$
	48	$2^{47}-2^{23}-2^{15}-2^{14}$	$2^{47}-2^{23}-2^{16}-2^{3}$
	62	$2^{61}-2^{30}-2^{19}-2^{3}$	$2^{61}-2^{30}-2^{19}-2^{18}-2^{3}$
	70	$2^{69}-2^{34}-2^{21}-2^{20}-2^{3}$	$2^{69}-2^{34}-2^{22}-2^{3}$
	88	$2^{87}-2^{43}-2^{26}-2^{3}$	$2^{87}-2^{43}-2^{26}-2^{24}-2^{3}$
3	20	$2^{19}-2^{9}-2^{8}-2^{4}$	$2^{19}-2^{9}-2^{8}-2^{7}-2^{4}$
	30	$2^{29}-2^{14}-2^{11}-2^{10}$	$2^{29}-2^{14}-2^{12}-2^{4}$
	36	$2^{35}-2^{17}-2^{13}-2^{4}$	$2^{35}-2^{17}-2^{13}-2^{12}-2^{4}$
	46	$2^{45}-2^{22}-2^{16}-2^{13}$	$2^{45}-2^{22}-2^{16}-2^{15}-2^{4}$
4	30	$2^{29}-2^{14}-2^{12}-2^{11}$	$2^{29}-2^{14}-2^{13}$
	36	$2^{35}-2^{17}-2^{14}-2^{12}$	$2^{35}-2^{17}-2^{15}-2^{5}$
5	42	$2^{41}-2^{20}-2^{17}$	$2^{41}-2^{20}-2^{17}-2^{14}-2^{6}$
	74	$2^{73}-2^{36}-2^{27}$	$2^{73}-2^{36}-2^{27}-2^{24}-2^{6}$
6	40	$2^{39}-2^{19}-2^{17}-2^{15}$	$2^{39}-2^{19}-2^{17}-2^{16}-2^{7}$
	46	$2^{45}-2^{22}-2^{19}-2^{18}$	$2^{45}-2^{22}-2^{20}-2^{7}$
7	44	$2^{43}-2^{21}-2^{19}-2^{18}$	$2^{43}-2^{21}-2^{20}-2^{8}$
	52	$2^{51}-2^{25}-2^{22}$	$2^{51}-2^{25}-2^{22}-2^{21}-2^{8}$
8	56	$2^{55}-2^{27}-2^{24}-2^{23}$	$2^{55}-2^{27}-2^{25}$
	70	$2^{69}-2^{34}-2^{29}$	$2^{69}-2^{34}-2^{29}-2^{27}-2^{9}$
9	54	$2^{53}-2^{26}-2^{24}-2^{23}$	$2^{53}-2^{26}-2^{24}-2^{23}-2^{22}$
	62	$2^{61}-2^{30}-2^{27}$	$2^{61}-2^{30}-2^{27}-2^{26}$

$\blacksquare$

Theorem 2. *Construction 1 always achieves either the same or better nonlinearity compared to the method in [28].*

Proof: Using Lemma 3.1, we have

$$A_k = 2^{t-k} A_{2k-t} + \sum_{i=1}^{t-k} 2^{i-1} \binom{k-i}{m}.$$

Obviously, $\lfloor \frac{A_k}{2^{t-k}} \rfloor > A_{2k-t}$, i.e.,

$$\left\lfloor \frac{\sum_{i=m+1}^{k} \binom{k}{i}}{2^{t-k}} \right\rfloor > \sum_{i=m+1}^{2k-t} \binom{2k-t}{i}.$$

$\blacksquare$

B. Algebraic immunity of the GMM construction

The AI of the GMM method is hard to analyze due to the dependency of the degree of the annihilators on the choice of the subfunctions. Indeed, computer simulations confirm that the choice of subfunctions does affect the AI, and furthermore the usage of both affine and linear functions has an positive impact on the AI. In other words, the arbitrary functions g_i used in (21) should be nonconstant functions. For instance, in most of the cases the AI of a 12-variable function f is rather poor, $AI(f) = 3$ if $g_i = 0$. Instead, by replacing some linear subfunctions with affine subfunctions, which also applies to item 3) in the design procedure of Construction 1, the AI reaches its suboptimal value 5.

However, the use of nonconstant g_i is not sufficient for ensuring a large AI and we show below that for $n \geq 16$ the functions obtained using Theorem 1 cannot have optimal AI. This is primarily due to the use of many $n/2$-variable functions which in turn gives rise to a large number of unknowns and thereby to solvable system of equations as discussed below. Therefore, in Section IV-B we investigate the case when not too many $n/2$-variable functions are used and demonstrate improved resistance to both fast and classical algebraic attacks.

It was shown [17] that in general algebraic properties of the standard MM class may not be optimal. Using an equivalent form of (7), a function f in the MM class can be represented as a concatenation of affine functions and written as,

$$f(Y_{n-k}, X_k) = \bigoplus_{\tau \in \mathbb{F}_2^{n-k}} \prod_{i=1}^{n-k} (y_i \oplus \tau_i \oplus 1) a_{[\tau]}(x), \tag{29}$$

where $a_{[\tau]}(x) = \phi(\tau) \cdot x \oplus h(\tau)$ and $\phi : \mathbf{F}_2^{n-k} \to \mathbf{F}_2^k$, $h : \mathbf{F}_2^{n-k} \to \mathbf{F}_2$. Then, any annihilator of f can be represented as,

$$g(Y_{n-k}, X_k) = \bigoplus_{\tau \in \mathbb{F}_2^{n-k}} \Big(\prod_{i=1}^{n-k} (y_i \oplus \tau_i \oplus 1) \Big) g_{[\tau]}(x), \tag{30}$$

where $g_{[\tau]}$ is any annihilator of $a_{[\tau]}$, i.e., $g_{[\tau]} a_{[\tau]} = 0$.

Let us introduce a formula similar to (29) but referring to the GMM class:

$$\begin{aligned} f(Y_{n/2}, X_{n/2}) = & \bigoplus_{\tau \in \mathbb{F}_2^{n/2} \setminus E'} \prod_{i=1}^{n/2} (y_i \oplus \tau_i \oplus 1) a_{[\tau]}(x) \\ \oplus & \bigoplus_{\tau \in E'} \prod_{i=1}^{n/2} (y_i \oplus \tau_i \oplus 1) u_{[\tau]}(x), \end{aligned} \tag{31}$$

where $u_{[\tau]}$ are (say) quadratic functions.

Then, any annihilator of f can be represented as,

$$\begin{aligned} g(Y_{n/2}, X_{n/2}) = & \bigoplus_{\tau \in \mathbb{F}_2^{n/2} \setminus E'} \Big(\prod_{i=1}^{n/2} (y_i \oplus \tau_i \oplus 1) \Big) g_{[\tau]}(x) \\ \oplus & \bigoplus_{\tau \in E'} \Big(\prod_{i=1}^{n/2} (y_i \oplus \tau_i \oplus 1) \Big) g'_{[\tau]}(x), \end{aligned} \tag{32}$$

where $g_{[\tau]}$ is any annihilator of $a_{[\tau]}$, i.e., $g_{[\tau]} a_{[\tau]} = 0$ and $g'_{[\tau]}$ is any annihilator of $u_{[\tau]}$, i.e., $g'_{[\tau]} u_{[\tau]} = 0$. If we would like to cancel the presence of the term $y_1 y_2 \cdots y_{n/2} s(x)$ in the general algebraic normal form of g given by (32), then the necessary and sufficient condition is that,

$$\begin{aligned} & \bigoplus_{\tau \in \mathbb{F}_2^{n/2} \setminus E'} g_{[\tau]}(x) \oplus \bigoplus_{\tau \in E'} g'_{[\tau]}(x) \\ = & \bigoplus_{\tau \in \mathbb{F}_2^{n/2} \setminus E'} (1 \oplus a_{[\tau]}(x)) h_{[\tau]}(x) \oplus \bigoplus_{\tau \in E'} (1 \oplus u_{[\tau]}(x)) h'_{[\tau]}(x) \\ = & \, 0, \end{aligned} \tag{33}$$

where $h_{[\tau]}(x)$ and $h'_{[\tau]}(x)$ are Boolean functions in $n/2$ and k' $(k' \leq n/2)$ variables of arbitrary degree, respectively.

However, this technique does not ensure that, depending on the choice of $h_{[\tau]}$ and $h'_{[\tau]}$, there will not be some term of even higher degree than $n-n/2+1$. Therefore, we constrain the degrees of $h_{[\tau]}(x)$ and $h'_{[\tau]}(x)$ not to exceed fixed values r $(r<n/2)$ and $r-1$, respectively. Then we try to select the functions $h_{[\tau]}(x)$ and $h'_{[\tau]}$ 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 $d\le p\le n-n/2$, where d is a fixed integer $1\le d\le n-n/2$. If there exists such a choice of $h_{[\tau]}(x)$ and $h'_{[\tau]}$ then the degree of g will be equal to $d-1+r+1=d+r$ which can be less than $n-n/2+1$.

To cancel all terms in $g(y,x)$ containing $y_{i_1}y_{i_2}\cdots y_{i_\delta}$, $1\le i_1\ne i_2\cdots\ne i_\delta\le n-n/2$, the following two sum must be identical to zero,

$$\bigoplus_{\substack{\tau\in\mathbb{F}_2^{n/2}\setminus E'\\ \tau_{i_{\delta\oplus 1}}=\cdots=\tau_{i_{n/2}}=0}}(1\oplus a_{[\tau]}(x))h_{[\tau]}(x)=0, \tag{34}$$

$$\bigoplus_{\substack{\tau\in E'\\ \tau_{i_{\delta\oplus 1}}=\cdots=\tau_{i_{n/2}}=0}}(1\oplus u_{[\tau]}(x))h'_{[\tau]}(x)=0. \tag{35}$$

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

$$\begin{aligned} h_{[\tau]}(x)=a_0^\tau &\oplus a_1^\tau x_1\oplus\ldots\oplus a_{n/2}^\tau x_{n/2}\\ &\oplus a_{i_1\cdots i_r}^\tau x_{i_1\cdots i_r},\ \ \tau\in\mathbb{F}_2^{n/2}\setminus E' \qquad (36)\\ h'_{[\tau]}(x)=b_0^\tau &\oplus b_1^\tau x_1\oplus\ldots\oplus b_{k'}^\tau x_{k'}\\ &\oplus b_{i_1\cdots i_{r-1}}^\tau x_{i_1\cdots i_{r-1}},\ \ \tau\in E'. \qquad (37)\end{aligned}$$

Thus, restricting the degree of $h_{[\tau]}(x)$ not to exceed r and $r-1$ we obtain in total $(2^{n/2}-|E'|)\cdot\sum_{i=0}^{r}\binom{n/2}{i}$ unknowns $a_0^\tau,\ldots,a_{i_1\cdots i_r}^\tau$, when τ runs through $\mathbb{F}_2^{n/2}\setminus E'$. Similarly, by restricting the degree $h'_{[\tau]}(x)$ not to exceed $r-1$ we obtain $|E'|\cdot\sum_{i=0}^{r-1}\binom{k'}{i}$ unknowns $b_0^\tau,\ldots,b_{i_1\cdots i_{r-1}}^\tau$, when τ runs through E'. On the other hand, to cancel any subproduct $y_{i_1}y_{i_2}\cdots y_{i_\delta}$, the condition that (34) and (35) must be identical to zero will induce $\sum_{j=0}^{r+1}\binom{n/2}{j}+\sum_{j=0}^{r}\binom{k'}{j}$ equations in unknowns $a_0^\tau,\ldots,a_{i_1\cdots i_r}^\tau$ and $b_0^\tau,\ldots,b_{i_1\cdots i_{r-1}}^\tau$ 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,

$$\sum_{j=0}^{n/2-d}\binom{n/2}{n/2-j}\left[\sum_{j=0}^{r+1}\binom{n/2}{j}+\sum_{j=0}^{r}\binom{k'}{j}\right]. \tag{38}$$

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,

$$\begin{aligned}&(2^{n/2}-|E'|)\cdot\sum_{i=0}^{r}\binom{n/2}{i}+|E'|\cdot\sum_{i=0}^{r-1}\binom{k'}{i}\\ &>\sum_{j=0}^{n/2-d}\binom{n/2}{n/2-j}\left[\sum_{j=0}^{r+1}\binom{n/2}{j}+\sum_{j=0}^{r}\binom{k'}{j}\right],\end{aligned} \tag{39}$$

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 $d+r<n-n/2+1$. In the sequel we refer to this approach as *equation based annihilation.*

Example 3. *Consider a construction of a function $(12,1,10,2000)$ on $\mathbb{F}_2^{12}$ using the GMM method given in Example 2, thus $k'=5$ and $|E'|=14$. Then, a trivial annihilation, obtained by defining g to be $1+a_{[\tau]}$ for a 6-dimensional subspace given by τ and zero otherwise, will give annihilators of degree $n-n/2+1=7$. It can be checked that putting $d=5,r=1$ and $k'=5$ in*

$$\begin{aligned}&(2^{n/2}-|E'|)\cdot\sum_{i=0}^{r}\binom{n/2}{i}+|E'|\cdot\sum_{i=0}^{r-1}\binom{k'}{i}\\ &>\sum_{j=0}^{n/2-d}\binom{n/2}{n/2-j}\left[\sum_{j=0}^{r+1}\binom{n/2}{j}+\sum_{j=0}^{r}\binom{k'}{j}\right]\end{aligned} \tag{40}$$

gives $(2^6-14)\cdot 7+14>7\cdot 28$. 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 in (39) is not satisfied.

Remark 4. *Note that the set E' can contain subfunctions of degree 2 or more. For instance, in Example 2 14 different 5-variable 1-resilient linear functions can be simply viewed as 7 different 1-resilient quadratic functions with disjoint spectra on $\mathbb{F}_2^6$. Furthermore, the functions $u_{[\tau]}(x)$ do not have to be quadratic functions. It is easily verified that for the function $(16,1,14,2^{15}-2^7-2^5)$, the functions $u_{[\tau]}(x)$ have degree 3.*

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 minimise $r+d$, for r,d satisfying (39). The optimal choice of the parameters r and d for certain input values is given in Table III, where $E'=2n/2-\sum_{i=0}^{m+1}\binom{n/2}{i}$, that is, all m-resilient affine functions in $n/2$ variables are used. For $n\ge 16$ it is apparent that Construction 1 does not provide functions with maximum AI. The degree $n-n/2+1$ of trivial annihilation, as described previously, is listed for comparison. Also, the results concerning AI of functions obtained using Theorem 1, based on computer simulations, are listed. Note once again that the AI depends on the choice of subfunctions, and both AI and resistance to FAA can be improved if a proper proportion of functions with large and small number of variables is chosen, see Section IV-B. The results of simulations for $n=16,18$ are empty due to infeasibility of computing AI for $n>16$.

This technique is almost with the same success applied to the degree-optimized GMM class discussed previously.

The resistance against FAA is measured by considering the sum of the degrees of functions g and h in the relation of the form $f(x)g(x)=h(x)$. Set $e=deg(g)$, $d=deg(h)$.The cryptanalyst seeks for nonzero $g,h\in\mathcal{B}_n$ so that $e+d$ in the above relation is minimized. The tuple (e,d) completely determines the complexity of the associated FAA. The resistance

TABLE III
COMPARISON OF SIMULATED AI VALUES TO TWO DIFFERENT UPPER BOUNDS ON AI

$n;n/2$	12;6	14;7	16;8	18;9	20;10
$n-n/2+1$	7	8	9	10	11
$d+r$	6	7	7	8	9
AI of Th. 1 (comp. simul.)	5	6	7	-	-

to FAA is optimal if $e+d \geq n$ for any $e \in [1, \lceil n/2 \rceil - 1]$. It is well-known [6] that there always exist functions $g, h \in \mathcal{B}_n$ satisfying that $e+d=n$, but finding f satisfying $e+d \geq n$ for any nonzero g, h appears to be very difficult. One such function in $n=9$ variables was found in [3], therefore the main attempt in this direction is to design functions satisfying $e+d \geq n-1$, which are then called suboptimal with respect to FAA.

Unfortunately, for the standard GMM method the existence of functions $f, g \in \mathcal{B}_n$ of degree 2 and $n/2$, respectively, was observed for all choices (non-exhaustive) of subfunctions that optimize the nonlinearity. Therefore, the resistance to FAA turns out not to be particularly good. It appears that the reason for this behaviour is the usage of many $n/2$-variable affine functions in the design. This can be circumvented by allowing a repetition of functions from smaller variable spaces while only using“a few” affine functions in $n/2$-variables. This results in balanced Boolean functions with excellent algebraic properties which we discuss in the next section, cf. Example 4 and the subsequent discussion.

IV. DESIGNING BALANCED GMM FUNCTIONS

In this section we demonstrate the possibility of designing highly nonlinear balanced (or 1-resilient) Boolean functions with good resistance to FAA. To achieve our goal we firstly provide the existence evidence of functions within the GMM class satisfying all relevant cryptographic criteria. These functions are firstly found by performing a simple computer search for optimal choice of affine subfunctions, their number for different dimensions and their placement. Therefore, we also give a deterministic approach of constructing balanced functions with slightly decreased resistance to FAA compared to the computer based search; hence providing a further evidence of the richness and the possibilities of further optimization and refinement of the cryptographic criteria within the GMM class.

A. Balanced GMM functions with overall good properties

As previously mentioned the only problem of the GMM class, generated by means of Construction 1, is its relatively bad resistance to FAA and slightly suboptimal AI $n/2-1$. The conducted simulations and the analysis in Section III-B indicate that the usage of "too many" $n/2$-variable affine functions in the concatenation has a negative impact on algebraic properties. Here, "too many" means that the usage of almost all available $n/2$-variable functions always implies a bad resistance against FAA, whereas functions with good algebraic properties but just slightly lower nonlinearity can be easily found if only a small portion of affine $n/2$-variable functions is used. More generally, based on extensive computer simulations, the smaller number of functions in large number of variables and consequently a larger number of "small" functions then the better is the resistance against FAA while the nonlinearity is slightly decreased at the same time. Here, "small" functions means k-variable affine functions with $k \ll n/2$. In this case, the functions ϕ_i, $i > n/2$, defined previously may not be injective any longer, thus the repetition of affine functions in $(n-i)$-variables is also allowed. Since it is very tedious to describe the choices of the subfunctions in an exact mathematical manner, we only give a few examples that confirm the existence of functions satisfying all relevant cryptographic criteria and leave the search for optimal functions as an interesting design problem.

Example 4. *Let us consider the construction of $f : \mathbb{F}_2^8 \to \mathbb{F}_2$. Using the standard GMM approach and 4-variable affine functions along with 3-variable functions we would be able to construct $(8,0,6,116)$ functions with $AI(f)=3$ but it turns out that $(e,d)=(2,4)$ would always exist (for certain choices of subfunctions even $(e,d)=(1,3)$ may exist). Now using a single 4-variable function, twenty 3-variable and twenty 2-variable functions, one can construct*

$$\begin{aligned} f \;\; = \;\; & 00110011001110011001011010101100101010100011 \\ & 10010110011011111111000011111010110000111001 \\ & 11001100101011000011110001010101110001101111 \\ & 00001001011010011001101010101100001110100101 \\ & 11000110001100110011110001010011111100000000 \\ & 000000111001001111001001100110011001 \end{aligned}$$

which has $AI(f)=4$, its nonlinearity is $N_f=112$, $\deg(f)=6$, and in addition it turns out that $e+d \geq n-1=7$ for any choice of the nonzero functions g and h. Furthermore, by LT-method, this function has 8 linearly independent vectors ω for which $W_f(\omega)=0$ thus it can be transformed into 1-resilient function preserving all other parameters. This 1-resilient function f' has the following truth table:

$$\begin{aligned} f' \;\; = \;\; & 01011110010010011011110111111000000010101100 \\ & 01111010001011111000000011000000011100101001 \\ & 00010110111110010010001111101000101011010010 \\ & 00010011011110110001001110001011100101011000 \\ & 00001101101101000111011111011100110110011001 \\ & 001010001110110101010010110101100001 \end{aligned}$$

Another example of a function satisfying all relevant cryptographic criteria including excellent algebraic properties is the following $f \in B_{10}$ whose truth table is given in a hexadecimal format.

5fa509faac3a56aac69336a696ffc369
60a395006c565f39a563c53fc33a0fc3
6f69c3c6aaa5f3666aa095a9a6f95563
53995f3963f50f5fa66953056c9a3a50
fc90a5f635309faaffcc303563956c96
ff3c05365350c99f3305963a3359f0f3
36f5635560cf5cfa0a6009caa030a033
cf06930a30fa3093c0f0663c5aa05c65

This $(10,0,8,472)$ function with optimal AI and suboptimal resistance to FAA, i.e., $e+d \geq n-1=9$, can be easily transformed into 1-resilient function f' having exactly the

TABLE IV
BALANCED GMM FUNCTIONS WITH EXCELLENT ALGEBRAIC PROPERTIES

n	$\deg(f)$	resiliency	$\deg g + \deg h$	AI	N_f
8	6	1	$\geq n-1=7$	4	112
10	8	1	$\geq n-1=9$	5	472
12	11	0	$\geq n-1=11$	6	1960
12	10	1	$\geq n-1=11$	6	1960
14	13	0	$\geq n-1=13$	7	7994

same parameters as f. The truth table of f' which is a $(10,1,8,472)$ function is given by,

47f2f5cb420466d65885742c141374e0
3ff35343874bfa7c2e53f2378646bf2b
6c391afa726d6026901d17d1397ae42f
4330584156067f99e5c9a5f39da99c9a
78f5b40843ab53eedfcdc34de060dcbd
839b7504cd5a4c9c3282e0506bb88a57
527db3abc26ab928dfde4626a2aed0c6
48342a9babdbac8b9f6d58090f698596

Remark 5. *Notice that the above* $(10,1,8,472)$ *function is not a SAO function since its nonlinearity is not larger than* $2^{n-1}-2^{n/2}=480$. *On the other hand, the function has excellent algebraic properties.*

In Table IV we list a few balanced/resilient functions obtained by using a small portion of $n/2$-variable functions, thus trading off the nonlinearity of the functions against (almost) optimal algebraic properties. The truth tables of the (12,0,11,1960), (14,0,13,7994), (12,1,10,1960) functions with good algebraic properities can be found in Appendix A.

B. GMM functions with good algebraic properties and nonlinearity

The use of many $n/2$-variable functions in Theorem 1 is a direct consequence of the fact that optimizing the vector $(a_{n/2},\ldots,a_{n-m-1}) \in \mathbb{F}_2^{n/2-m}$, such that $\sum_{i=n/2}^{n-m-1} a_i 2^i$ is maximal and satisfying at the same time $\sum_{i=n/2}^{n-m-1}\left(a_i \cdot 2^{n-i}\sum_{j=m+1}^{n-i}\binom{n-i}{j}\right) \geq 2^n$, implies the usage of a large number of $n/2$-variable functions. In what follows, we propose a deterministic method for constructing highly nonlinear GMM functions with good algebraic properties which only uses a moderate number of $n/2$-variable functions, more precisely $2^{n/2-1}$ such functions without repetition are used. As a consequence, we are forced to drop the injective property of the mappings ϕ_i defined in Construction 1 and Theorem 1, for $i > n/2$. Thus, ϕ_i is λ_i-to-1 for some positive integer $\lambda_i \geq 1$.

One possibility of selecting suitable λ_i is to take $\lambda_{n/2+1}=2$ and $\lambda_{n/2+2}=4$, which gives $2^{n/2-1}\times 2^{n/2}+2\times 2^{n/2-2}\times 2^{n/2-1}+4\times 2^{n/2-2}\times 2^{n/2-2}=2^n$. Notice that the existence of $2^{n/2-1}$ many $(n/2)$-variable and $2^{n/2-2}$ many $(n/2-1)$-variable linear subfunctions is always guaranteed. On the other hand, all the available $(n/2-2)$-variable linear functions are used, including the all zero function. Notice that the design below provides a very good lower bound on nonlinearity by cancelling the contribution of $(n/2+1)$-variable subfunctions in the computation of spectral values (when the contribution of $n/2$-variable functions is nonzero, cf. (51) in the proof of Theorem 3.

Construction 2. *Let* $n \geq 8$ *be even and* $V_0 \subset \mathbb{F}_2^{n/2-1} \setminus \{\boldsymbol{0}_{n/2-1}\}$ *with* $|V_0| = 2^{n/2-2}$, *where* $\boldsymbol{0}_i$ *denote the all zero vector in* $\mathbb{F}_2^i$. *Let* $U_{n/2} = \mathbb{F}_2 \times V_0$, $U_{n/2+1} = \mathbb{F}_2^{n/2-1} \setminus V_0$ *and* $U_{n/2+2} = \mathbb{F}_2^{n/2-2}$. *For* $n/2 \leq i \leq n-1$, *let* E_i *be defined as in Construction 1, and*

$$|E_i| = \begin{cases} 2^{n/2-1}, & if\ i \in \{n/2, n/2+1\} \\ 2^{n/2}, & if\ i = n/2+2 \\ 0, & if\ n/2+2 < i < n. \end{cases} \tag{41}$$

For $n/2 \leq i \leq n/2+2$, *let* ϕ_i *be a* λ_i *to 1 mapping from* E_i *to* U_i, *where* $\lambda_{n/2}=1$, $\lambda_{n/2+1}=2$, *and* $\lambda_{n/2+2}=4$. *Let* $X_n = (x_1,\ldots,x_n) \in \mathbb{F}_2^n$, $X'_i = (x_1,\ldots,x_i) \in \mathbb{F}_2^i$ *and* $X''_{n-i} = (x_{i+1},\ldots,x_n) \in \mathbb{F}_2^{n-i}$. *A GMM type Boolean function* $f \in \mathcal{B}_n$ *can be constructed as follows:*

$$f(X_n) = \phi_i(X'_i)\cdot X''_{n-i} \oplus g_i(X'_i), \text{ for } X'_i \in E_i, \\ i \in \{n/2, n/2+1, n/2+2\}, \tag{42}$$

where $g_i \in \mathcal{B}_i$ *are say randomly chosen balanced functions, in particular satisfying*

$$\left|\{g_i(X'_i)=0 \mid X'_i \in \phi_i^{-1}(\boldsymbol{0}_{n-i})\}\right| = \lambda_i/2. \tag{43}$$

Theorem 3. *The function* $f \in \mathcal{B}_n$, *proposed by Construction 2, is a balanced function with nonlinearity*

$$N_f \geq 2^{n-1} - 2^{n/2}. \tag{44}$$

Proof: For $i \in \{n/2, n/2+1, n/2+2\}$, let $\omega = (\Omega'_i, \Omega''_{n-i}) = (\omega_1,\cdots,\omega_n) \in \mathbb{F}_2^n$, where $\Omega'_i = (\omega_1,\cdots,\omega_i)$ and $\Omega''_{n-i} = (\omega_{i+1},\cdots,\omega_n)$. We have,

$$W_f(\omega) = \sum_{X_n \in \mathbb{F}_2^n} (-1)^{f(X_n)\oplus\omega\cdot X_n} = \sum_{i=n/2}^{n/2+2} S_i(\omega), \tag{45}$$

where

$$\begin{aligned} S_i(\omega) &= \sum_{X'_i \in E_i} (-1)^{\Omega'_i\cdot X'_i \oplus g_i(X'_i)} \\ &\times \sum_{X''_{n-i}\in\mathbb{F}_2^{n-i}} (-1)^{\phi_i(X'_i)\cdot X''_{n-i}\oplus\Omega''_{n-i}\cdot X''_{n-i}}. \end{aligned} \tag{46}$$

Note that

$$\begin{aligned} &\sum_{X''_{n-i}\in\mathbb{F}_2^{n-i}} (-1)^{\phi_i(X'_i)\cdot X''_{n-i}\oplus\Omega''_{n-i}\cdot X''_{n-i}} \\ &= \begin{cases} 2^{n-i}, & if\ \phi_i^{-1}(\Omega''_{n-i}) = X'_i \\ 0 & if\ \phi_i^{-1}(\Omega''_{n-i}) \neq X'_i. \end{cases} \end{aligned} \tag{47}$$

Since ϕ_i is a λ_i to 1 mapping from E_i to U_i, we have $|\phi_i^{-1}(\Omega''_{n-i})| = \lambda_i$, thus

$$S_i(\omega) = 2^{n-i} \sum_{X'_i\in\phi_i^{-1}(\Omega''_{n-i})} (-1)^{\Omega'_i\cdot X'_i\oplus g_i(X'_i)}. \tag{48}$$

Furthermore,

$$\begin{aligned} |S_i(\omega)| &= \big|2^{n-i} \sum_{X'_i \in \phi_i^{-1}(\Omega''_{n-i})} (-1)^{\Omega'_i \cdot X'_i \oplus g_i(X'_i)}\big| \\ &\leq \lambda_i \cdot 2^{n-i} \\ &= \begin{cases} 2^{n/2}, & if\ i = n/2, n/2+1, \\ 2^{n/2+1}, & if\ i = n/2+2 \end{cases} \end{aligned} \tag{49}$$

Combining (46) and (47) for $i = n/2$, we have

$$S_{n/2}(\omega) = \begin{cases} 0, & if\ \Omega''_{n/2} \in U_{n/2+1} \\ \pm 2^{n/2}, & if\ \Omega''_{n/2} \notin U_{n/2+1}. \end{cases} \tag{50}$$

When $\Omega''_{n/2} \notin U_{n/2+1}$, then $S_{n/2+1}(\omega) = 0$. Therefore,

$$|S_{n/2}(\omega)| + |S_{n/2+1}(\omega)| = 2^{n/2}. \tag{51}$$

Obviously, using (51) and (49), we get

$$|W_f(\omega)| = \sum_{i=n/2}^{n/2+2} |S_i(\omega)| \leq 2^{n/2} + 4 \cdot 2^{n/2-2} = 2^{n/2+1},$$

which by (4) implies that $N_f \geq 2^{n-1} - 2^{n/2}$, as claimed. Notice that f is mainly a concatenation of affine nonconstant functions apart from a possible sporadic usage of $(n-i)$-variable constant functions. However, by (43), these constant functions are used in a balanced manner, implying that f is balanced. ■

Instead of describing the design procedure, we illustrate the choice of subfunctions in the example below, which can be easily generalized to larger n. The space decomposition should be clear from the examples accompanying Construction 1.

Example 5. *Using Construction 2 one can design an 8-variable function by selecting eight 4-variable, eight 3-variable, and sixteen 2-variable affine functions as subfunctions, see Table V for its properties. The nonlinearity bound gives that $N_f \geq 2^{n-1} - 2^{n/2}$, which gives $N_f = 112$. For simplicity X''_{n-i} is replaced by $Y = (y_1, \ldots, y_{n-i})$ and the design procedure is as follows:*

a) *Select $2^{n/2-1} = 8$ different 4-variable linear functions of the form $h = a_4y_4 + a_3y_3 + a_2y_2 + a_1y_1 + a_0$, where the vectors $(a_4, \ldots, a_1)$, with $a_0 = 0$, are given as,*

$$(0,1,1,1);\ (0,1,1,0);\ (0,0,1,1);\ (0,0,0,1),$$

$$(1,1,1,1);\ (1,1,1,0);\ (1,0,1,1);\ (1,0,0,1).$$

b) *Select $2^{n/2-1} = 8$ many 3-variable linear (affine) functions of the form $r = b_3y_3 + b_2y_2 + b_1y_1 + b_0$ by repeating each function below, specified by (b_3, b_2, b_1), twice:*

$$(0,0,0);\ (0,1,0);\ (1,0,1);\ (1,0,0).$$

Notice that g_5 (see 42) in this case must ensure that the repetition of the all-zero function corresponds to the use of all-one function. Also, the fact that (a_3, a_2, a_1) is never equal to (b_3, b_2, b_1) for any of the chosen functions ensures that these functions are disjoint spectra functions.

TABLE V
DETERMINISTIC GMM FUNCTIONS WITH OVERALL GOOD PROPERTIES

n	$\deg(f)$	resiliency	$\deg g + \deg h$	AI	N_f	N_f in Table II
8	6	1	$\geq n-1=7$	4	112	-
10	8	1	$\geq n-2=8$	5	480	-
12	10	1	$\geq n-2=10$	6	1960	2000
14	11	1	$\geq n-3=11$	7	8040	8100

c) *We select sixteen 2-variable functions of the form $s = c_2y_2 \oplus c_1y_1 \oplus c_0$ by repeating 4 times the functions specified by (c_2, c_1) below,*

$$(0,0);\ (0,1);\ (1,0);\ (1,1).$$

Once again, the all-zero function is repeated twice as well as its complement through a suitably chosen g_6.

Remark 6. *The deterministic approach described above is only one way of specifying repetition of small linear functions, which may not be suitable for obtaining good algebraic properties for large n. There exist other approaches that give better algebraic properties such as the following one. Instead of fixing the variable spaces of the subfunctions to be $n/2, n/2+1$ and $n/2+2$ one may introduce a parameter s, with $n/2+1 < s < n-1$, and define*

$$|E_i| = \begin{cases} 2^{n/2-1}, & if\ n/2 \leq i < s \\ 2^{n/2}, & if\ i = s \\ 0, & if\ s < i < n. \end{cases} \tag{52}$$

and

$$\lambda_i = \begin{cases} 1, & if\ i = n/2 \\ 2, & if\ i = n/2+1 \\ 2^{i-n/2-1}, & if\ n/2+2 \leq i \leq s-1 \\ 2^{n-s}, & if\ i = s. \end{cases} \tag{53}$$

which gives better algebraic properties since more "small" subfunctions are used.

The properties of a few functions constructed using this approach are given in Table V, whereas the truth tables of these functions can be found in Appendix B. The last row in Table V lists the nonlinearities of functions obtained by means of Theorem 1, whose algebraic properties are not very good. Even though $N_f \geq 2^{n-1} - 2^{n/2}$ for Construction 2, to slightly improve the algebraic properties for $n = 14$ and $n = 16$ we utilize the ideas in Remark 6, for which it can be shown that $N_f \geq 2^{n-1} - 2^{n/2} - (s-2) \cdot 2^{n/2-2}$. This is strictly less than SAO nonlinearity, but the actual nonlinearity values are much higher. For all the functions in Table V we were able to find n linearly independent zero values in their Walsh spectra, hence all the functions could be transformed into 1-resilient functions using the LT-method. See examples in Appendix B.

V. CONSTRUCTION OF SAO m-RESILIENT FUNCTIONS ON ODD NUMBER OF VARIABLES

In this section, we show that for any positive integer m, it is possible to construct n-variable (n odd) SAO m-resilient functions with currently best known nonlinearity either by a straightforward generalization of the even n case or, alternatively, by using PW functions (or KY functions) as the input instance for our construction methods.

A. Construction of SAO functions using direct sum

A straightforward approach for constructing a SAO resilient Boolean function for odd n is to use the direct sum of a GMM function on even number of variables and a KY (or PW) function[1].

From here on, a balanced function is regarded as a 0-resilient function, and a function that is neither balanced nor 1-resilient is regarded as a (-1)-resilient function. Note that a KY function and a PW function are both (-1)-resilient functions.

Lemma 3. *Let $f(y,x) = g(y) \oplus h(x)$, where g is an m_1-resilient function and h is an m_2-resilient function. Then f is an (m_1+m_2+1)-resilient function.*

Note that the truth table of f in Lemma 3 is the concatenation of the truth tables of h or $h+1$ in some order which depends on g.

Construction 3. *Let $n = n_1 + n_2$ where n_1 is even and n_2 is odd. Let $g(y) \in \mathcal{B}_{n_1}$ be an m_1-resilient function obtained by Construction 1 and $h(x) \in \mathcal{B}_{n_2}$ be a known m_2-resilient function with SAO nonlinearity. The function $f \in \mathcal{B}_n$ is then defined by $f(y,x) = g(y) \oplus h(x)$. Then, by Lemma 3, f is an (m_1+m_2+1)-resilient function.*

Under certain conditions, related to the variable space of g above, f in Construction 3 has SAO nonlinearity. To determine these conditions explicitly we assume that h belongs to some of the following cases.

- $h \in \mathcal{B}_9$ is a KY function;
- $h \in \mathcal{B}_{15}$ is a PW function;
- $h \in \mathcal{B}_{15}$ is a PW0 function, where "PW0" means a 15-variable balanced function with nonlinearity 16272 [22].

Take the direct sum of a GMM function and a KY function as an illustration. Let

$$\begin{aligned} &f(x_1,\dots,x_{n_1},x_{n_1+1},\dots,x_{n_1+9}) \\ &= g(x_1,\dots,x_{n_1}) \oplus h(x_{n_1+1},\dots,x_{n_1+9}), \end{aligned} \quad (54)$$

where n_1 is an even number, $g \in \mathcal{B}_{n_1}$ is a GMM function and $h \in \mathcal{B}_9$ is a KY function. Let $\alpha \in \mathbb{F}_2^{n_1}$ and $\beta \in \mathbb{F}_2^9$, and note that $W_f(\alpha,\beta) = W_g(\alpha)W_h(\beta)$. To ensure that

$$N_f > 2^{n-1} - 2^{(n-1)/2},$$

where $n = n_1 + 9$, we require

$$28 \cdot (2^{n_1} - 2N_g) < 2^{(n_1+10)/2},$$

i.e.,

$$N_g > 2^{n_1-1} - \frac{4}{7} \cdot 2^{n_1/2}. \quad (55)$$

Let $n(m)$ be the minimum n such that the nonlinearity of the m-resilient function $f \in \mathcal{B}_n$ constructed above is strictly greater than $2^{n-1} - 2^{(n-1)/2}$. Then we have the following dependency between n and m :

m	1	2	3	4	5	6	7	8	9	10
$n(m)$	29	35	41	47	51	57	61	67	71	77

Similarly, when $f \in \mathcal{B}_n$ is obtained by using direct sum of a GMM function and a PW function, we require $N_g > 2^{n_1-1} - \frac{16}{27} \cdot 2^{n_1/2}$, and then we have

m	1	2	3	4	5	6	7	8	9	10
$n(m)$	35	41	47	53	57	63	67	73	77	83

Example 6. *It is possible to construct a 51-variable 5-resilient functions with SAO nonlinearity. Note that a 42-variable 5-resilient function g with nonlinearity $2^{41} - 2^{20} - 2^{17}$ can be constructed by Construction 1. Let $f(x,y) = g(x) \oplus h(y)$, where $h \in \mathcal{B}_9$ is a KY function. Obviously, $N_f = 2^{50} - \frac{1}{2}(2^{21} + 2^{18}) \cdot 28 = 2^{50} - 2^{25} + 512 \cdot 2^{10}$.*

More examples can be found in Table VI, where also a comparison to Construction 4 is given. Clearly, cryptographically stronger functions are mostly obtained through Construction 4, whereas only in certain cases depicted by * in superscript better functions arise from Construction 3.

B. Extension of the GMM method for odd n

Nevertheless, the results given in the previous section can be significantly improved if the GMM method is applied directly, though the direct sum is again used implicitly, but this time within the GMM method.

Construction 4. *Let $n = 2k + t$, where $t \geq 9$ is odd. Let for $k \leq i \leq n-1$, $E_i \subseteq \mathbb{F}_2^i$ and $E'_i = E_i \times \mathbb{F}_2^{n-i}$ such that*

$$\bigcup_{i=k}^{n-1} E'_i = \mathbb{F}_2^n, \quad (56)$$

and

$$E'_{i_1} \cap E'_{i_2} = \emptyset,\ k \leq i_1 < i_2 \leq n-1.$$

Let m be a nonnegative integer, and $(a_k,\dots,a_{n-m-1})$ be the binary vector such that $\sum_{i=k}^{n-m-1} a_i 2^i$ is maximal, satisfying at the same time,

$$\sum_{i=k}^{n-m-1} \left(a_i \cdot 2^{n-i} \sum_{j=m+1}^{n-i} \binom{n-i}{j} \right) \geq 2^n. \quad (57)$$

Let

$$e = \max\{i \mid a_i \neq 0,\ k+1 \leq i \leq n-1\}. \quad (58)$$

For $k+1 \leq i \leq e-1$, set

$$|E_i| = \begin{cases} 0, & \textit{if } a_i = 0 \\ \sum_{j=m+1}^{n-i} \binom{n-i}{j}, & \textit{if } a_i = 1. \end{cases} \quad (59)$$

For $k+1 \leq i \leq e$ and $a_i = 1$, let ϕ_i be an injective mapping from E_i to T_i, where

$$T_i = \{c \mid wt(c) \geq m+1,\ c \in \mathbb{F}_2^{n-i}\}. \quad (60)$$

Let $\{i_1,\dots,i_{m+1}\} \cup \{i_{m+2},\dots,i_{n-e}\} = \{e+1,\dots,n\}$ and $c = (c_{e+1},\dots,c_n) \in \mathbb{F}_2^{n-e}$ with $(c_{i_1},\dots,c_{i_{m+1}}) = (1,\dots,1)$. Let

$$\begin{aligned} T'_e = \{c \mid c = (c_{e+1},\dots,c_n) \in \mathbb{F}_2^{n-e}, \\ wt(c) \geq m+1, (c_{i_1},\dots,c_{i_{m+1}}) \neq (1\dots1)\}. \end{aligned} \quad (61)$$

[1] It has already been noted by Dillon [7] that the direct sum method (decomposable functions) may have severe cryptographic weaknesses. Thus, this construction serves more as the existence evidence of functions with large SAO nonlinearity.

TABLE VI
NONLINEARITY COMPARISON FOR SAO m-RESILIENT FUNCTIONS ON $\mathbb{F}_2^n$ (n ODD)

h	Construction 4	h	Construction 3
PW0	$(31, 1, 29, 2^{30} - 2^{15} + 4 \cdot 512)$	KY	$(31, 1, -, 2^{30} - 2^{15} + 512)$
PW0	$(33, 1, 31, 2^{32} - 2^{16} + 5 \cdot 2^{10} + 896)$	KY	$(33, 1, -, 2^{32} - 2^{16} + 4 \cdot 2^{10} + 512)$
PW0	$(35, 1, 33, 2^{34} - 2^{17} + 12 \cdot 2^{10})$	KY	$(35, 1, -, 2^{34} - 2^{17} + 9 \cdot 2^{10})$
PW0	$(37, 1, 35, 2^{36} - 2^{18} + 27 \cdot 2^{10} + 768)$	KY	$(37, 1, -, 2^{36} - 2^{18} + 25 \cdot 2^{10})$
PW0	$(39, 1, 37, 2^{38} - 2^{19} + 56 \cdot 2^{10})$	PW	$(39, 1, -, 2^{38} - 2^{19} + 53 \cdot 2^{10})$
PW	$(41, 1, 39, 2^{40} - 2^{20} + 127 \cdot 2^{10} + 1020)$	KY	$(41, 1, -, 2^{40} - 2^{20} + 108 \cdot 2^{10} + 768)$
PW	$(43, 1, 41, 2^{42} - 2^{21} + 256 \cdot 2^{10})$	PW	$(43, 1, -, 2^{42} - 2^{21} + 266 \cdot 2^{10})$ $\star$
PW	$(45, 1, 43, 2^{44} - 2^{22} + 575 \cdot 2^{10})$	PW	$(45, 1, -, 2^{44} - 2^{22} + 532 \cdot 2^{10})$
PW	$(47, 1, 45, 2^{46} - 2^{23} + 2^{20} + 128 \cdot 2^{10})$	PW	$(47, 1, -, 2^{46} - 2^{23} + 2^{20} + 107 \cdot 2^{10} + 512)$
PW	$(49, 1, 47, 2^{48} - 2^{24} + 2 \cdot 2^{20} + 320 \cdot 2^{10})$	PW	$(49, 1, -, 2^{48} - 2^{24} + 2 \cdot 2^{20} + 296 \cdot 2^{10})$
PW	$(51, 1, 49, 2^{50} - 2^{25} + 4 \cdot 2^{20} + 768 \cdot 2^{10})$	PW	$(51, 1, -, 2^{50} - 2^{25} + 4 \cdot 2^{20} + 700 \cdot 2^{10})$
PW	$(53, 1, 51, 2^{52} - 2^{26} + 9 \cdot 2^{20} + 637 \cdot 2^{10} + 1020)$	PW	$(53, 1, -, 2^{52} - 2^{26} + 9 \cdot 2^{20} + 592 \cdot 2^{10})$
PW	$(55, 1, 53, 2^{54} - 2^{27} + 19 \cdot 2^{20} + 512 \cdot 2^{10})$	PW	$(55, 1, -, 2^{54} - 2^{27} + 19 \cdot 2^{20} + 160 \cdot 2^{10})$
PW	$(57, 1, 55, 2^{56} - 2^{28} + 39 \cdot 2^{20})$	PW	$(57, 1, -, 2^{56} - 2^{28} + 39 \cdot 2^{20} + 160 \cdot 2^{10})$ $\star$
PW	$(59, 1, 57, 2^{58} - 2^{29} + 79 \cdot 2^{20})$	PW	$(59, 1, -, 2^{58} - 2^{29} + 78 \cdot 2^{20} + 320 \cdot 2^{10})$
PW	$(61, 1, 59, 2^{60} - 2^{30} + 158 \cdot 2^{20})$	PW	$(61, 1, -, 2^{60} - 2^{30} + 158 \cdot 2^{20} + 320 \cdot 2^{10})$ $\star$
–	–	KY,PW0	$(35, 2, -, 2^{34} - 2^{17} + 2 \cdot 2^{10})$ $\star$
KY,PW0	$(37, 2, 34, 2^{36} - 2^{18} + 16 \cdot 2^{10})$	KY,PW0	$(37, 2, -, 2^{36} - 2^{18} + 4 \cdot 2^{10})$
KY,PW0	$(39, 2, 36, 2^{38} - 2^{19} + 32 \cdot 2^{10})$	KY,PW0	$(39, 2, -, 2^{38} - 2^{19} + 36 \cdot 2^{10})$
PW0	$(41, 2, 38, 2^{40} - 2^{20} + 95 \cdot 2^{10} + 1016)$	KY,PW0	$(41, 2, -, 2^{40} - 2^{20} + 72 \cdot 2^{10})$
KY,PW,PW0	$(43, 2, 40, 2^{42} - 2^{21} + 192 \cdot 2^{10})$	PW0	$(43, 2, -, 2^{42} - 2^{21} + 200 \cdot 2^{10})$ $\star$
PW0	$(45, 2, 42, 2^{44} - 2^{22} + 444 \cdot 2^{10} + 1016)$	PW	$(45, 2, -, 2^{44} - 2^{22} + 424 \cdot 2^{10})$
PW	$(47, 2, 44, 2^{46} - 2^{23} + 928 \cdot 2^{10})$	PW0	$(47, 2, -, 2^{46} - 2^{23} + 870 \cdot 2^{10})$
PW	$(49, 2, 46, 2^{48} - 2^{24} + 2 \cdot 2^{20})$	PW	$(49, 2, -, 2^{48} - 2^{24} + 2^{20} + 888 \cdot 2^{10})$
PW	$(51, 2, 48, 2^{50} - 2^{25} + 4 \cdot 2^{20})$	PW	$(51, 2, -, 2^{50} - 2^{25} + 4 \cdot 2^{20} + 160 \cdot 2^{10})$ $\star$
PW	$(53, 2, 50, 2^{52} - 2^{26} + 9 \cdot 2^{20})$	PW	$(53, 2, -, 2^{52} - 2^{26} + 8 \cdot 2^{20} + 320 \cdot 2^{10})$ $\star$
PW	$(55, 2, 52, 2^{54} - 2^{27} + 18 \cdot 2^{20})$	PW	$(55, 2, -, 2^{54} - 2^{27} + 18 \cdot 2^{20} + 320 \cdot 2^{10})$
PW	$(57, 2, 54, 2^{56} - 2^{28} + 37 \cdot 2^{20} + 1023 \cdot 2^{10} + 1016)$	PW	$(57, 2, -, 2^{56} - 2^{28} + 36 \cdot 2^{20} + 640 \cdot 2^{10})$
PW	$(59, 2, 56, 2^{58} - 2^{29} + 76 \cdot 2^{20})$	PW	$(59, 2, -, 2^{58} - 2^{29} + 76 \cdot 2^{20} + 640 \cdot 2^{10})$ $\star$
PW	$(61, 2, 58, 2^{60} - 2^{30} + 154 \cdot 2^{20})$	PW	$(61, 2, -, 2^{60} - 2^{30} + 153 \cdot 2^{20} + 256 \cdot 2^{10})$
PW	$(63, 2, 60, 2^{62} - 2^{31} + 312 \cdot 2^{20})$	PW	$(63, 2, -, 2^{62} - 2^{31} + 309 \cdot 2^{20} + 896 \cdot 2^{10})$
PW	$(65, 2, 62, 2^{64} - 2^{32} + 626 \cdot 2^{20})$	PW	$(65, 2, -, 2^{64} - 2^{32} + 626 \cdot 2^{20} + 512 \cdot 2^{10})$ $\star$
PW	$(67, 2, 64, 2^{66} - 2^{33} + 2^{30} + 240 \cdot 2^{20})$	PW	$(67, 2, -, 2^{66} - 2^{33} + 2^{30} + 229 \cdot 2^{20})$
–	–	KY,PW0	$(41, 3, -, 2^{40} - 2^{20} + 16 \cdot 2^{10})$ $\star$
KY,PW0	$(43, 3, 39, 2^{42} - 2^{21} + 128 \cdot 2^{10})$	KY,PW0	$(43, 3, -, 2^{42} - 2^{21} + 32 \cdot 2^{10})$
KY,PW0	$(45, 3, 41, 2^{44} - 2^{22} + 256 \cdot 2^{10})$	KY,PW0	$(45, 3, -, 2^{44} - 2^{22} + 288 \cdot 2^{10})$ $\star$
PW0	$(47, 3, 43, 2^{46} - 2^{23} + 672 \cdot 2^{10})$	KY,PW0	$(47, 3, -, 2^{46} - 2^{23} + 576 \cdot 2^{10})$
KY,PW,PW0	$(49, 3, 45, 2^{48} - 2^{24} + 2^{20} + 512 \cdot 2^{10})$	PW0	$(49, 3, -, 2^{48} - 2^{24} + 2^{20} + 352 \cdot 2^{10})$
KY,PW,PW0	$(51, 3, 47, 2^{50} - 2^{25} + 3 \cdot 2^{20})$	PW	$(51, 3, -, 2^{50} - 2^{25} + 3 \cdot 2^{20} + 320 \cdot 2^{10})$ $\star$
KY,PW,PW0	$(53, 3, 49, 2^{52} - 2^{26} + 7 \cdot 2^{20})$	PW	$(53, 3, -, 2^{52} - 2^{26} + 7 \cdot 2^{20} + 640 \cdot 2^{10})$ $\star$
PW	$(55, 3, 51, 2^{54} - 2^{27} + 16 \cdot 2^{20})$	PW	$(55, 3, -, 2^{54} - 2^{27} + 14 \cdot 2^{20} + 32 \cdot 2^{10})$
PW	$(57, 3, 53, 2^{56} - 2^{28} + 32 \cdot 2^{20})$	PW	$(57, 3, -, 2^{56} - 2^{28} + 33 \cdot 2^{20} + 256 \cdot 2^{10})$ $\star$
PW	$(59, 3, 55, 2^{58} - 2^{29} + 72 \cdot 2^{20})$	PW	$(59, 3, -, 2^{58} - 2^{29} + 66 \cdot 2^{20} + 512 \cdot 2^{10})$
PW	$(61, 3, 57, 2^{60} - 2^{30} + 144 \cdot 2^{20})$	PW	$(61, 3, -, 2^{60} - 2^{30} + 144 \cdot 2^{20} + 832 \cdot 2^{10})$ $\star$
PW	$(63, 3, 59, 2^{62} - 2^{31} + 296 \cdot 2^{20})$	PW	$(63, 3, -, 2^{62} - 2^{31} + 293 \cdot 2^{20})$
PW	$(65, 3, 61, 2^{64} - 2^{32} + 608 \cdot 2^{20})$	PW	$(65, 3, -, 2^{64} - 2^{32} + 586 \cdot 2^{20})$
PW	$(67, 3, 63, 2^{66} - 2^{33} + 2^{30} + 192 \cdot 2^{20})$	PW	$(67, 3, -, 2^{66} - 2^{33} + 2^{30} + 202 \cdot 2^{20})$ $\star$
–	–	KY,PW0	$(47, 4, -, 2^{46} - 2^{23} + 128 \cdot 2^{10})$ $\star$
KY	$(49, 4, 44, 2^{48} - 2^{24} + 2^{20})$	KY,PW0	$(49, 4, -, 2^{48} - 2^{24} + 256 \cdot 2^{10})$
KY,PW0	$(51, 4, 46, 2^{50} - 2^{25} + 2 \cdot 2^{20})$	KY,PW0	$(51, 4, -, 2^{50} - 2^{25} + 2 \cdot 2^{20} + 256 \cdot 2^{10})$ $\star$
KY,PW0	$(53, 4, 48, 2^{52} - 2^{26} + 5 \cdot 2^{20})$	KY,PW0	$(53, 4, -, 2^{52} - 2^{26} + 4 \cdot 2^{20} + 512)$
KY,PW,PW0	$(55, 4, 50, 2^{54} - 2^{27} + 12 \cdot 2^{20})$	KY,PW0	$(55, 4, -, 2^{54} - 2^{27} + 9 \cdot 2^{20})$
KY,PW,PW0	$(57, 4, 52, 2^{56} - 2^{28} + 24 \cdot 2^{20})$	PW	$(57, 4, -, 2^{56} - 2^{28} + 26 \cdot 2^{20} + 512 \cdot 2^{10})$ $\star$
KY,PW,PW0	$(59, 4, 54, 2^{58} - 2^{29} + 56 \cdot 2^{20})$	PW	$(59, 4, -, 2^{58} - 2^{29} + 53 \cdot 2^{20})$
PW	$(61, 4, 56, 2^{60} - 2^{30} + 128 \cdot 2^{20})$	PW0	$(61, 4, -, 2^{60} - 2^{30} + 112 \cdot 2^{20} + 256 \cdot 2^{10})$
PW	$(63, 4, 58, 2^{62} - 2^{31} + 256 \cdot 2^{20})$	PW	$(63, 4, -, 2^{62} - 2^{31} + 266 \cdot 2^{20})$ $\star$
PW	$(65, 4, 60, 2^{64} - 2^{32} + 576 \cdot 2^{20})$	PW	$(65, 4, -, 2^{64} - 2^{32} + 532 \cdot 2^{20})$
PW	$(67, 4, 62, 2^{66} - 2^{33} + 2^{30} + 128 \cdot 2^{20})$	PW	$(67, 4, -, 2^{66} - 2^{33} + 2^{30} + 94 \cdot 2^{20})$
–	–	KY	$(51, 5, -, 2^{50} - 2^{25} + 512 \cdot 2^{10})$ $\star$
PW0	$(53, 5, 47, 2^{52} - 2^{26} + 2 \cdot 2^{20})$	KY	$(53, 5, -, 2^{52} - 2^{26} + 2^{20})$
KY,PW0	$(55, 5, 49, 2^{54} - 2^{27} + 8 \cdot 2^{20})$	KY	$(55, 5, -, 2^{54} - 2^{27} + 2 \cdot 2^{20})$
KY,PW0	$(57, 5, 51, 2^{56} - 2^{28} + 16 \cdot 2^{20})$	KY,PW0	$(57, 5, -, 2^{56} - 2^{28} + 18 \cdot 2^{20})$ $\star$
PW0	$(59, 5, 53, 2^{58} - 2^{29} + 40 \cdot 2^{20})$	KY,PW0	$(59, 5, -, 2^{58} - 2^{29} + 36 \cdot 2^{20})$
KY,PW,PW0	$(61, 5, 55, 2^{60} - 2^{30} + 96 \cdot 2^{20})$	KY,PW0	$(61, 5, -, 2^{60} - 2^{30} + 72 \cdot 2^{20})$
KY,PW,PW0	$(63, 5, 57, 2^{62} - 2^{31} + 192 \cdot 2^{20})$	PW	$(63, 5, -, 2^{62} - 2^{31} + 212 \cdot 2^{20})$ $\star$
PW	$(65, 5, 59, 2^{64} - 2^{32} + 480 \cdot 2^{20})$	PW	$(65, 5, -, 2^{64} - 2^{32} + 424 \cdot 2^{20})$
PW	$(67, 5, 61, 2^{66} - 2^{33} + 2^{30})$	PW0	$(67, 5, -, 2^{66} - 2^{33} + 856 \cdot 2^{20})$

If $|E_e| - 1 \leq |T'_e|$, then let ϕ'_e be an injective mapping from $E_e \setminus \{\delta\}$ to T'_e. Let $E_k \subset F_2^k$ with $|E_k| = |T_k|$ where

$$T_k = \{c \mid wt(c) \geq m - m_0,\ c \in \mathbb{F}_2^k\}. \tag{62}$$

Let $h \in \mathcal{B}_t$ be a known SAO m_0-resilient function. Let $X_n = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $X'_i = (x_1, \ldots, x_i) \in \mathbb{F}_2^i$ and $X''_{n-i} = (x_{i+1}, \ldots, x_n) \in \mathbb{F}_2^{n-i}$. Then we construct a function $f \in \mathcal{B}_n$ as follows:

$$f(X_n) = \begin{cases} \phi_k(X'_k) \cdot X''_k \oplus h(X''_t), & \textit{if } X'_k \in E_k \\ \phi_i(X'_i) \cdot X''_{n-i}, & \textit{if } X'_i \in E_i, \\ & \quad k+1 \leq i \leq e-1 \\ \psi(X'_e) \cdot X''_{n-e}, & \textit{if } X'_i \in E_e \setminus \{\delta\} \\ c \cdot X''_{n-e} \oplus x_{i_{m+2}} \ldots x_{i_{n-e}}, & \textit{if } X'_i = \delta, \end{cases} \tag{63}$$

where

$$\psi = \begin{cases} \phi'_e, & \textit{if } |E_e| - 1 \leq |T'_e| \\ \phi_e, & \textit{otherwise.} \end{cases} \tag{64}$$

The major difference compared to Construction 3, described in the previous section, is that a t-variable SAO function is "embedded" within the GMM construction. In most of the cases the attained nonlinearity is slightly better than the one achieved by Construction 3 (see Table VI). The algebraic properties depend on the choice of $h \in \mathcal{B}_t$ (an m_0-resilient SAO function with t odd), and in general these are infeasible to check due to the size of variable space.

Theorem 4. *Let $f \in \mathcal{B}_n$ be as proposed in Construction 4. Then f can be a degree-optimized m-resilient function with nonlinearity*

$$N_f \geq \begin{cases} 2^{n-1} - 2^k(2^{t-1} - N_h) - \sum_{i=k+1}^{n-1} a_i \cdot 2^{n-i-1}, \\ \qquad\qquad |E_e| - 1 \leq |T'_e| \\ 2^{n-1} - 2^k(2^{t-1} - N_h) - \sum_{i=k+1}^{n-1} a_i \cdot 2^{n-i-1} - 2^{m+1}, \\ \qquad\qquad \textit{otherwise.} \end{cases} \tag{65}$$

Proof: For any $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{F}_2^n$,

$$W_f(\omega) = \sum_{i=k}^{n-1} a_i S_i(\omega),$$

where

$$S_i(\omega) = \sum_{X_n \in E'_i} (-1)^{f(X_n) + \omega \cdot X_n}.$$

Note that

$$S_k(\omega) = \begin{cases} \pm 2^k \cdot W_h(\omega_{2k+1}, \ldots, \omega_n), \\ \qquad\qquad \text{if } \phi_k^{-1}(\omega_{k+1}, \ldots, \omega_{2k}) \text{ exists} \\ 0, \qquad\qquad \text{otherwise,} \end{cases}$$

and for $i = k+1, \ldots, e-1$,

$$S_i(\omega) = \begin{cases} \pm 2^{n-i}, & \text{if } \phi_i^{-1}(\omega_{i+1}, \ldots, \omega_n) \text{ exists} \\ 0, & \text{otherwise.} \end{cases}$$

Then,

$$\max_{\omega \in \mathbb{F}_2^n} |S_e(\omega)| = \begin{cases} 2^{n-e}, & \text{if } |E_e| \leq |T'_e| + 1 \\ 2^{n-e} + 2^{m+2}, & \text{otherwise.} \end{cases} \tag{66}$$

By (4), inequality in (65) holds. The results concerning the resiliency and algebraic degree follow from Lemma 3 and Theorem 1, and the details are omitted here. ■

Remark 7. *To be more precise, we have*

$$N_f \geq \begin{cases} 2^{n-1} - 2^{(n-1)/2} - \sum_{i=k+1}^{n-1} a_i \cdot 2^{n-i-1} + \xi, \\ \qquad\qquad \textit{if } |E_e| - 1 \leq |T'_e| \\ 2^{n-1} - 2^{(n-1)/2} - \sum_{i=k+1}^{n-1} a_i \cdot 2^{n-i-1} + \xi - 2^{m+1}, \\ \qquad\qquad \textit{otherwise.} \end{cases}$$

where

$$\xi = \begin{cases} 2^{k+1}, & \textit{if } h \textit{ is a KY function} \\ 2^{k+4}, & \textit{if } h \textit{ is a PW function} \\ 2^{k+4} + 2^{k+1}, & \textit{if } h \textit{ is a PW0 function.} \end{cases}$$

Example 7. *Let $n = 41$, $k = 13$, and h be a PW function with $N_h = 16276$, thus $t = 15$. A 1-resilient function $f \in \mathcal{B}_{41}$ can be constructed as follows:*

$$f(X_{41}) = \begin{cases} \phi_{13}(x_1 \ldots, x_{13}) \cdot (x_{14}, \ldots, x_{26}) \oplus h(x_{27}, \ldots, x_{41}), \\ \qquad\qquad \textit{if } (x_1 \ldots, x_{13}) \in E_{13} \\ \phi_{25}(x_1 \ldots, x_{25}) \cdot (x_{26} \ldots, x_{41}), \\ \qquad\qquad \textit{if } (x_1 \ldots, x_{25}) \in E_{25}, \end{cases}$$

where $E_{25} = \overline{E_{13}} \times \mathbb{F}_2^{12}$. Note that

$$\begin{aligned} |E_{25}| &= \left(\binom{13}{0} + \binom{13}{1}\right) \cdot 2^{12} \\ &< |\{c \mid wt(c) \geq 2,\ c \in \mathbb{F}_2^{16}\}| + 1. \end{aligned}$$

Thus, it is possible to construct a 41-variable 1-resilient function with nonlinearity $2^{40} - 2^{20} + 2^{17}$ which is greater than $2^{40} - 2^{20} + 2^{16}$ [22].

VI. Concluding remarks

In this paper, we have presented a GMM construction method to obtain SAO resilient functions with a nonlinearity higher than that attainable by any previously known construction method. The following conjecture appears to be quite natural with respect to all the design improvements that seem to slowly approach this bound.

Conjecture 1. *Let $n \geq 8$ and $m < \lfloor n/4 \rfloor$. For any m-resilient function $f \in \mathcal{B}_n$,*

$$N_f \leq 2^{n-1} - \lfloor 2^{n/2-1} \rfloor - 2^{\lfloor n/4 \rfloor + m - 1}.$$

The original class proposed here can be slightly modified (by avoiding the use of too many $n/2$-variable affine functions) to provide functions with excellent algebraic properties. By using GMM construction technique, we can obtain cryptographic Boolean functions having good tradeoff among the parameters important to resist the known cryptanalytic techniques. Additionally, a low hardware implementation cost further makes GMM functions as attractive candidates for the use in certain stream cipher schemes. An analysis of hardware implementation of the GMM class is left unanswered due to space constraints.

GMM construction technique can also be used to get resilient S-boxes with SAO nonlinearity by means of disjoint linear codes. Details on this work can be found in [29].

Appendix A

This appendix list two functions in the GMM class, an "optimal" choice of subfunctions and their placement was found by computer search. The truth table of the (12,0,11,1960) function with optimal AI and good resistance to FAA ($e + d \geq 11$) is given below:

```
503f afa3 69f5 5a95 f5cf 3655 c3a0 f0a0 c3a6 f3a9 c00a 93aa 3cf9
6c6f 3c6c c65a 99cc 9f63 055f c966 30a5 3665 f93c 3c33 6af6 0093 5390
0399 3c05 06c5 39cc 3a95 9096 ff63 aaff 993a 5fcf c6ff 6a5c 3c60 3390 f506
0533 9906 9f6c ccc5 cfc3 6933 9c90 c90c 3f66 9c55 6039 a395 f0c9 a6f3
9f0a 593c 6533 5069 3a50 5a0c 930f 5fa6 3939 c990 a0fc f39f 363c 9350
f5ac c536 9a9a 9966 6f55 c39c 3ff0 03aa 3055 9a96 050a 60ca acf0 a00a
f595 55ac 6cf6 cf9c 95fa 0c60 f0aa 050f 3065 65ca 33f3 0665 3fc6 56fa aff0
0af9 0fa0 5a09 0cf6 fa65 00a9 6f9f 69a0 606f 5596 09cc aafc c655 cf93 afac
0a0f cafa 5665 9595 969f f9f6 6c5a 9c6a 5a30 0f6c 3033 0530 5fa6 6a3c
956f f695 c330 9366 9636 c6a6 c3f3 53cc ac56 a699 06ac aa65 95f3 6500
ff90 6afa 509a f300 0055 f936 0f69 5f63 365a 33a9 c3aa f369 6cf9 0acf 0933
ca5a 0fc0 5f9a 05f5 a355 f5ac f356 960a 5c69 9a3f c055 fa96 6606 90a5
60aa ca9c 0f95 36af fa53 c0f6 39c5 96c9 695f 6359 906f 0656 9a00 3c6c
003f 5363 c6f3 6fca a566 3599 6965 9069 6a39 cca3 f9aa 0c9c a063 093c
6faf cfa0 39cc f390 56aa 399f 69a0 f30f 35a5 3939 560f 03af a95c 39c6
556c 53af 336f a0aa 5f6c 656a cf30 0c3c 93c6 355a a96f 5099 3a9a 0660
a5c6 ff3f 300a accc 6300 6cac 6500 a099 39ca 9f56 6509 3cf5 cc33 c906
36af 6f56 f90c 560f accf 6f6f a0f9 90af 9056 a00a ca3a 5a33 9f33 3665 faac
```

The truth table of the (14,0,13,7994) function with optimal AI and good resistance to FAA ($e + d \geq 13$) is given below:

```
09c3 630a 3930 a055 a066 a5a5 0aaa a536 c636 5a93 63ff 0af5
9a35 9355 a336 f06f cccf 5359 3fc5 6c39 3aaa faf5 c900 c363 c00a f369
c5c0 aca3 066a 030a 6a35 ccc0 39fc ac0a ff5a 9500 fa5f 0936 ca03 5a96
cac3 ac6c 03f5 9350 636f 5f6a 3355 cffa 53af 9933 6339 c60a 00f5 9065
a6ca 5605 636a aa3f 9a0f a396 96aa f9af 9665 fc6f a095 553a f656 696f
c96f c60f 33a3 0f99 5f5f 0aaa 663f a605 c3f9 ac5c a099 9699 fcaf f95a
96a9 6f5a 0936 99ff aa93 3cfa 5f0c 653c 90f3 6593 3a6c 0a66 3afa 3c90
3c05 3ca6 536c 5353 56a3 6a6a 90f6 599f aa66 fa3f f59f 5533 6063 95fc
353a f665 09c5 9a90 c060 fa95 3faa aa0a f036 a69a 0330 369f 590c 30ff
ffca 0305 0356 0fa3 0959 a53f f395 69f5 3a55 ff33 f5f0 06a0 69ff 6c6a
acc9 c9c6 63ac f593 309c 5ff9 6a9c 5f39 06c0 accf 5055 033f 0055 cfa9
065c 35a5 390c 3ac0 509f 9cf3 660f 0c90 63cc 3666 6669 55a0 063f 53f5
5069 0505 af50 9c66 6959 95ca 0695 fc55 f96a cf93 56f6 0ac5 399c c6fa
9393 c656 f90a acca 9fc6 aa30 a09a 366c 9aaf a9f6 fa0c 0f9f 0c36 305a
a553 5fcf 0a3a ac00 035f a050 36ac 6f0f f6f0 53cf c600 c5a6 f355 5a6c
9003 93af ac0c c5c6 66c6 f003 9009 66aa afcc 3599 3506 6396 5afc 66c0
59c9 a56c 6959 c653 ffc9 3035 a0f3 09fa 3003 33f0 c9c0 af6c 3f93 f503
69fc 36cf 5f56 39f9 0c63 0560 5ac6 399f 3f03 9aac c3fa 0f59 53aa 0fc3
cc53 fa9f f993 5ffa 9036 5a66 f990 93c5 c3ff facc 3c6f 3966 3565 f6f5
3363 f6a5 ca30 35a6 60fa 6f69 035a fc63 5659 0f35 33a5 c995 9639 f309
6a35 6ca9 cf3f f55f 5cf9 50fc 0963 6690 3a96 c606 55c0 6699 9633 f00c
93f9 9655 3fcf 5369 6c99 63ff 05cf 950a 5333 faa9 c653 0009 5c65 a5ac
a630 cc09 636c 05ca 59f5 c5c9 5ac0 fc39 fcc9 09a0 a055 63f9 655c fafa
56f3 afaf f69f 603c f5fc 0995 0903 cccc 6965 c09c c903 faf6 aa6f f506 56ff
0ff9 6069 c960 60aa a096 500c c660 3fca 005f 006c 6063 690c 3cff ca56
6669 6039 553c a500 aac3 5a50 5aa6 69cf f0af 9335 9355 a9a6 55f3 a309
50c0 5a56 a0ca 59af 30c9 f306 95f5 66a5 36fc 935a 3a36 5a66 cccc 0059
6faf 9695 56a0 0330 9a3f 0a5a 053c caf6 a93a 9a03 c9c0 55c6 653a f560
af9f 9356 5a9a 605a ccff 6950 05c6 3550 5af0 c3aa 5399 096c c5a6 95c9
a69f 5933 5955 6ca6 9a99 9936 9099 3fa3 3f0a c66a 3993 c3f3 55c0 5990
f339 c53f 5650 a50f 60c9 f930 f563 f9ff 099f 5659 a99f 96f3 fcf9 006f
a69f 6669 a93f 956f 93f9 3af9 3339 0f9f 0969 3aca 6c59 3aa0 6ca3 3055
9f95 9cf0 365a a5c0 9563 c965 0550 3a9f f309 906a c63a 309f a500 f593
6f3a 5500 3560 5596 0950 0353 3c96 c633 06ca a33a 596a 0309 6950 9506
0a9c a5c5 c965 3cc5 f63c ca53 5503 c00a 693a c905 609c c663 c9a3 60a6
9036 c5af 6306 0500 30ca 0c55 c56f 9539 9990 9960 f3ff cf09 96c6 f05a
cacc c3a0 353f 3305 6f66 559c 0aa9 00a0 63c5 ca03 0ac0 3055 c65f 6565
50f5 33f3 069c 0005 3065 3fff 9906 cac0 5ffc c95f 9999 09aa fc03 995c
9ccf 9595 36f3 f953 66f5 a005 a566 a5ff aa9f 995a 0f99 a956 96f3 66fc
65cc c5fa 5c35 f6af 0fc6 9f6a 93af f069 cc9a f65f 3aa9 6c56 c993 c365
5695 9596 66ca 003f 9c6c 6903 ffaa f530 a6cc 5053 6f55 9caf 3c39 5ca3
f55f af50 f3f9 5360 ca5a ff63 fffa fa50 06fc c9c3 0af5 3353 59c0 555c a3a0
6ca9 fa06 0f39 305c 035a 59ca c53a c5aa f5c3 5ca5 ca50 5ff3 5cc6 a303
0356 96fc afc6 f6c9 c9a0 3af3 ac55 a5cc 590f 9f3a 6ff9 cf39 965f 3f9a
0f06 6033 39cf aa66 9a5f c0f3 9f90 3cfc c66a 36f5 c53c c690 3393 9059
933c 9fa0 f3f0 99ac 6c5f 059a 09c0 c5f3 99f0 5395 9aa9 539c 9cff 6390
5ca3 3550 036f 9003 3335 09fa 6596 0aaf 3655 a300 cf9c f5f3 350f 5996
fc3c 3655 0a9c cca5 0c00 369a a3c9 a00f f3f3 0053 39f9 0cc3 fa36 0a03
09ac 0365 5c6a 09c9 5550 c5f0 9365 6009 650f 05ac 996f 06fc a69f f3c3
90a0 3a0c 0f5c a3a9 f30c cfff 3a0a 0ff9 a900 a003 0393 3f63 6c3c 360c
5533 f590 0af3 a555 9a6a 0336 9c9c 5950 cc06 5a5c a0c0 6fc0 fcaa 0303
3c0c 35f0 950a 59aa fc95 6f03 5f56 f963 aaf0 33f3 f9f3 5965 f6af 3369
af65 6355 f99f 39a6 0c6a 0660 f903 a953 9c63 3905 acc9 c305 a5cc 35f9
f093 a0f0 a9f3 ca96 a560 f6f5 ffc9 66cf ac60 93f9 f350 aacc f0aa f035 0f59
5566 9566 5966 c3a9 f965 566a 65fa 9faa 00cc 3633 0c0c 9faf c933 96c5
6c3c 0cc5 faaa 0ca3 a00a 3caf 6c55 09af 5a33 fac3 c05f 6f9a 5f39 069f
9669 9535 99cc 5c60 5f5f 96cf 0a9f 0f39 5563 9965 0cf5 f669 fc03 09a0
53f9 6f0c a0af c0a5 fa9c c59c 3ca9 956a 56f6 090c f0c0 aa06 f3c0 ff9c 00ff
5500 3350 ac36 c505 969c a3c3 59c3 6a5c 050a c093 60a9 96f9 366c 53a5
a59c 09f3 50f5 93c9 c5f6 cc96 6c3a a3ff 3a60 3093 a9fc f56c 3ca6 c660
3c6a a663 c959 a999 f35c fa09 aaf5 03c6 0509 696a 0953 09a6 f90a ff3f
c05f c63c fa05 0caa 3af0 53af a63f 503c 5055 69ac 05f6 f956 55ca 9f95
0a6a c359 0c09 f5c0 3aff 09f3 aa5f 09c5 0acc 3cf9 f3c9 3395 5a0c 9360
9530 955f f5f9 3f3f c50f 5930 99f3 03c9 f60a 39a9 6af5 aa99 636a 3fc0
966c 95ca cff6 a633 5906 609a 9f30 a030 f053 ffa0 c90a 6afc 30c3 f509
690c 9fcf 56f0 c0a9 90af 6336 95fc 5ff6 0603 9ccc 903a 63a0 f60a f650
cc00 cc63 f959 cafa 565f 03c9 3990 fa30 3056 605f c63a 3f60 5365 036c
c6a0 30c5 9536 965c 9093 0f56 cf30 a9a3 63c9 9595 59ff 639a 69a0 3969
5aa5 959c 03c9 f3a0 aa0f 939c f66f 0363 3039 6906 9a63 c00c 6aaf 0059
59a6 0caa 5a95 6ff3 f6cf 9af3 3995 ccc5 3690 6300 5a3f 6335 36f6 3ca6
9a33 3350 39f3 65c6 3a05 c9f0 5c55 333f 63f5 5653 c355 cf99 56ac 9c5f
365a f955 a665 f3c6 afc3 fc05 633c 5055 c939 cca9 093f fcc9 af36 33c5
a65c 3359 f535 5959 f3f9 5acc 9365 3039 ca53 a9c3 a05c 0af5 f6a3 53ca
```

A $(12, 0, 10, 1960)$ function with optimal AI and suboptimal resistance to FAA, i.e., $e + d \geq n - 1 = 11$ is given below:

```
503f afa3 69f5 5a95 f5cf 3655 c3a0 f0a0 c3a6 f3a9 c00a 93aa 3cf9
6c6f 3c6c c65a 99cc 9f63 055f c966 30a5 3665 f93c 3c33 6af6 0093 5390
0399 3c05 06c5 39cc 3a95 9096 ff63 aaff 993a 5fcf c6ff 6a5c 3c60 3390
f506 0533 9906 9f6c ccc5 cfc3 6933 9c90 c90c 3f66 9c55 6039 a395 f0c9
a6f3 9f0a 593c 6533 5069 3a50 5a0c 930f 5fa6 3939 c990 a0fc f39f 363c
9350 f5ac c536 9a9a 9966 6f55 c39c 3ff0 03aa 3055 9a96 050a 60ca acf0
a00a f595 55ac 6cf6 cf9c 95fa 0c60 f0aa 050f 3065 65ca 33f3 0665 3fc6
56fa aff0 0af9 0fa0 5a09 0cf6 fa65 00a9 6f9f 69a0 606f 5596 09cc aafc
c655 cf93 afac 0a0f cafa 5665 9595 969f f9f6 6c5a 9c6a 5a30 0f6c 3033
0530 5fa6 6a3c 956f f695 c330 9366 9636 c6a6 c3f3 53cc ac56 a699 06ac
aa65 95f3 6500 ff90 6afa 509a f300 0055 f936 0f69 5f63 365a 33a9 c3aa
f369 6cf9 0acf 0933 ca5a 0fc0 5f9a 05f5 a355 f5ac f356 960a 5c69 9a3f
c055 fa96 6606 90a5 60aa ca9c 0f95 36af fa53 c0f6 39c5 96c9 695f 6359
```

906f 0656 9a00 3c6c 003f 5363 c6f3 6fca a566 3599 6965 9069 6a39 cca3
f9aa 0c9c a063 093c 6faf cfa0 39cc f390 56aa 399f 69a0 f30f 35a5 3939
560f 03af a95c 39c6 556c 53af 336f a0aa 5f6c 656a cf30 0c3c 93c6 355a
a96f 5099 3a9a 0660 a5c6 ff3f 300a accc 6300 6cac 6500 a099 39ca 9f56
6509 3cf5 cc33 c906 36af 6f56 f90c 560f accf 6f6f a0f9 90af 9056 a00a
ca3a 5a33 9f33 3665 faa9

This function can be transformed to a $(12,1,10,1960)$ function with the same algebraic properties: $AI(f) = 6$, $e+d \geq 11$.

2190 7278 1abb 3578 6037 ded4 04b2 caa9 f852 d6fa 25c7 758c
d11e 2c5d 0ada 3314 cb4a 3dd2 a9eb 1295 916c 9596 727f 847a 3b21 2699
369d c11f eb76 a962 87ea cf3d c640 0ae9 a55d a223 8174 43a2 873c 919b
b187 2928 7df4 cb1c ed44 a86a 3b3f 8155 b53e 3571 923f 69a7 2e6e 5410
95df acbf 7d70 78d5 7d30 cb7e 3e0a 395a b391 28a0 777d 6c99 a71e 97b9
2746 403b ecef eef5 2bdf 56ad 8a90 99b9 20ab da16 0be1 ff4c 388d 1264
049f f6ea c34c 9852 9506 28ca 4347 366f e928 0011 8ab2 e609 a5b0 a87d
105d 8db4 4b08 ced3 b1ca 706b d929 0e89 d9b2 352d d708 f2a2 75ed aef9
036a 262b f76c 794f 9a6a e5c3 03d4 f9ad 9265 dc73 5b32 70d2 5d08 e88d
458b 357b 5d87 2278 f7e3 6f87 5ec6 fe04 198c 9b3c d530 d2bb 934b 670a
ea06 8e0d e116 52dc abea 9c64 3c5e 3d57 3b07 8a54 a4d9 11f4 98b2 70b1
8185 4b14 9409 b6fc e3ef a123 0fd7 c7f4 37e0 7d04 f3c4 3c3a f926 037d
4bb3 0c94 7e5a 6f8b 843c 953e 8402 ccbc 218a 590d b87c 3b43 3249 61c0
b476 5d21 f89d 0f9f a0e6 6c21 e475 cb63 bca6 cfa0 1cbc f997 bd71 4783
2ccd 4cd0 1ca3 4340 99cb c848 b927 ee8f 9f8c 6ee0 fcc6 7dcb 19bf c90c
1a1d 6c20 077c 35f3 8794 19d1 6398 fbd6 5092 5c5e 780e 24a3 7afc 43ec
2c63 ed0c 58a9 f659 f093 050f 686c 8f21 4f37 18da 1dc3 9de6 98b3 c2a7
9774 6f72 fcd2 a460 c456 bdf9 b568 7136 22c3 95f1 a59a 5ff5 2c45 17ce
17ad 0870 8e1a 78ec 94ae 15e0

Appendix B

This appendix relates to Section IV-B, namely Construction 2 and Theorem 3, where a deterministic design method of functions with controllable nonlinearity and good resistance to FAA is given.

By using eight 4-variable, eight 3-variable, sixteen 2-variable affine functions as subfunctions, we obtain an (8,0,6,112) function with $AI(f) = 4$ and $e + d \geq n - 1 = 7$. Its truth table is given by:

$$\begin{gathered} 5a5aaaca00095aa5c35c0f0f33cc9f3c \\ 0ff0660333336aff6996696999653f55 \end{gathered}$$

This function can be transformed into an (8,1,6,112) function whose truth table is then given by:

$$\begin{gathered} 487ac8a7ae07e842b3cdb4f98361e995 \\ 336b451d76e38b6e2451f64466cb3e41 \end{gathered}$$

The truth table of a (10,0,8,480) function with $AI(f) = 5$ and good resistance to FAA ($e{+}d \geq n{-}2 = 8$) is given below:

3cc3 3cc3 6033 3c3c 5a5a 5a5a 00ff ff00 0ff0 f00f 0063 33cc 5aa5
6569 0ff0 0ff0 6969 6969 5aa5 6635 0000 ffff 0f0f 0f0f 3c55 33cc 3333
cccc 00ff 00ff 555a 0f05 5555 6666 6969 9696 ffff ffff 6996 3365 6699
9966 55aa aa55 3cc3 c33c 5a3c 5555 55aa 55aa 0f0f f0f0 6666 0366 6699
6699 300f 6996 3333 3333 6900 3c3c 5a5a a5a5

This function can be transformed into a (10,1,8,480) function with the same algebraic properties. Its truth table is then given by:

3944 8c86 e55d 405b d4fa 31ac 942c 051e 0bf0 9ce3 dbe2 8bb9
923d 9234 2160 917f c5fa 49f5 bb24 1eab adf2 2ba1 9d89 7659 f0f3 8f0c
cdb8 53ea cf2b 6b32 89ea 086c 1467 1df6 50da f37f 3485 c3f2 dec6 623b
2144 eb18 ef6b 55e0 7d20 af79 5607 f89b 482e 4a05 55a4 4a33 3a29 8f9d
9798 4bcb f743 434e 5495 8988 df74 e1a5 03d1 f881

The truth table of a (12,0,10,1960) function with optimal AI, also satisfying $e + d \geq n - 2 = 10$, is given below:

a5a5 5a5a 5569 5a5a 00ff ff00 00ff ff00 a5ff c3f0 6666 9999 5aa5
5aa5 f00f f00f 9655 5555 ffff 9633 f0f0 f0f0 5a69 00f0 6969 6969 9696
9696 5a96 3ca5 9669 6996 6955 ffff 9633 55aa 6969 9696 6969 9696 f0cc
3cc3 9900 a566 9966 9966 5a5a a5a5 0fc3 00ff 6699 33cc 3cc3 5a5a ccc3
553c 5a5a 5a5a a5a5 a5a5 5555 9600 3c3c c3c3 aac3 6699 55aa 6933 00ff
00ff 00ff 00ff Cccc 3333 990f 33cc 99a5 ff5a ffff 6996 00ff ff00 ff00 00ff
0f0f 3cc3 ccf0 00ff 0000 99ff 0f0f 0f0f 0ff0 0ff0 5566 33cc 6699 5555 0faa
cc3c 6666 6666 9999 9999 6699 6699 6996 9669 5a5a 6996 33cc c333
6969 6969 6969 6969 005a 0000 9999 6666 aac3 5555 3c55 3333 6969
9696 9696 6969 f066 0f0f 00ff 000f 9669 9669 cc99 5aa5 6996 55aa 33cc
3333 ffaa 3c66 cccc cccc 55aa a555 c33c 3cc3 0096 0000 0f33 0f0f 6969
0000 0ff0 cc5a 5a5a 5a5a 5a5a 5a5a 69ff 3c3c c3c3 c3c3 aa99 55aa c3c3
3c3c f055 5555 6969 665a 0f0f f0f0 3333 cc0f 5aa5 a55a 5aa5 a55a a5ff
55aa 3333 cccc 0ff0 f00f 5aa5 3333 00ff 00ff ff00 ff00 aac3 3c3c 6666 005a
6996 6996 6696 33cc 6666 6666 6666 6666 0ff0 99f0 c33c c33c 3333 3333
0f96 aa69 5aa5 5555 33cc 66a5 3cc3 c33c 3c3c 3ccc 5aa5 a55a a55a 5aa5
3cc3 3cc3 a55a a55a f0f0 0f0f 0ff0 ff69 33c3 55aa 6666 aa0f 6699 9966
9966 6699 6999 5aff 3c3c 3c3c f00f 0ff0 5555 3c99 6699 9966 6699 9966
6969 33a5 f0ff 6666

This function can be transformed into a (12,1,10,1960) function with the same algebraic properties. Its truth table is then given by:

f473 eab5 9c01 aa7d 0cdb b7c6 a706 cbb2 07d8 5ed0 170d 0921
1ff9 730f 4b4c dd55 8844 e417 b2e3 e53e bf84 9bd8 3077 a21c 9752 ebb3
bea4 2398 8959 f0ad 2a4e b727 35b1 9830 5b6e 8551 27e4 1f9e daeb 3bba
3b8e b485 90c4 9c08 678a 1fec 9cc3 7d1a 4b1f 6cab 901e 9958 2043 fda8
e8f8 cccc 15e2 addb 394d cce0 e854 a535 3639 30b6 4ec2 b470 d9e5 3360
eeb8 1b04 a26e 38fd c613 60a8 74d7 50b2 6b54 75b7 0c37 8097 f9f5 14cd
a9c9 f353 811e 2425 f6a2 41b2 e8c2 a906 2d54 b48d 1ce3 e688 e804 385e
7cb6 a4bb 80ba 933e b250 baef d69e 2718 17db 4399 1da7 fb53 1c2a 159a
df7c 0153 f0b2 7f48 e180 5a60 bed1 4651 a0cf 8118 15fb 5155 95df da59
f2c6 8ff1 cfec c8bc ca77 21de 1f0e 5cc5 b515 8d8c 1978 495f da00 e1a8
f4c8 51ee 8f04 b10b 2e32 55c1 54ac 34bc 7f79 0cd6 cc84 918d c6c7 6e50
132b 5f0f 792f 1941 246c baeb bdd3 0cdd 3197 42ad 1b5e 4a77 bcda e2a7
6de2 30a9 d140 9b05 e507 d0f6 b9ba d049 b6ef 46ca b172 72ae 0a57 98aa
8b6b 2a29 d37a 9212 c01f cbcc c907 2585 1361 2ff7 fe01 e5c6 8716 57cb
dcd faae 117f 27fa 8d10 0d30 a5ab 2a90 3727 6c9d 8242 2b3a e6da 25c2
1872 ea65 7ccc 5707 f2fe b9c5 fe2e 74ec 7941 c8f9 155b 32fb 6d5e 1e87
fa37 642c 8892 7198 007d 83f5 e56d 39a2 51c1 ac32 f87d 3b7f 92f2 ee65
9792 1327 60b1 2639 9870 8f5c 0c15 990b 756a 1128 b30a 0f8c c525 acf3
76ef 2e3c 506c e091 246c fcf63

Below is the truth table of a $(14, 1, 11, 8040)$ function with $AI(f) = 7$ and $e + d \geq n - 3 = 11$. This function is transformed from the truth table of a GMM $(14, 0, 11, 8040)$ function (Due to space constraints we do not provide the truth table of this balanced function).

```
1cd0 dd1c b011 d65a cc71 5735 fecb 20e5 2c5d 506e 514d bd2e
52e1 c798 161e 8851 a8bd bfb1 5c06 7bd1 87b5 7629 cc8a 71f8 aacd 3441
f8df 27c9 6a26 e5c8 70cd 478c d2c2 bd99 731e d40a 8995 2928 075e 8429
f9fd 832c 48b3 4d35 e3a0 e8c9 2309 dc58 6257 9ef0 a234 fd71 0181 194c
eab8 9f4b d74c 5cab 6e3d 59c2 9f48 288f f90b 6f69 3d00 b7e8 0e97 25b8
2dc4 4786 0c7a fc84 3113 223e 75d6 3203 0c18 e4c6 0276 81e0 2a93 1d9d
3b2e fa86 f6de 2e7d c86a 103d e9cb 94f6 b724 1091 95ad 8452 c6c7 eaec
1a6c 1e3d 17f5 d266 3569 9c78 1875 7c10 98c8 863c b339 2e56 db07 bbd0
f15f d6b6 cb6e 741b 8346 9eb6 6f39 ce50 1406 aed8 2211 ca37 95de 1920
b384 3c95 2db4 a228 3d82 9e4f 22e9 2417 e7b4 8f7f beb6 a0b6 c899 630e
012f ae13 830b 6100 52bc e252 1c75 c439 1a5c 46b7 700a 8f12 bb7f c9dc
2628 1dfd 2cdf 6974 0300 df7c a433 5033 5c36 86ab 59d0 7b2d 02cb 831b
f028 d890 ad12 e40d 2b72 5a2b ac8a f12a 73f5 7484 ecca 5b7b e236 817c
4366 e959 8aa4 9a6a 5768 bf3f 04cc 417f 7b0a fcbb ff4b 466e f983 59b0
fd81 7fbf c392 8de0 e330 18ba e31e e7c5 fd7b cde3 b5e2 19ab 771e bdf5
b9e4 a526 a2ce 4379 4c7a 9d74 d7ef ca97 5dc7 29ff 43cc 72d1 50dd e5c5
5138 4665 7916 1bd1 5405 7590 d7bc 1f49 9d6f e568 fd80 0dc8 79a8 9edd
00b2 7d5a 42c8 a1c3 c411 ed9f d96d da45 72aa 1211 0f18 d895 9f5c 95c5
f19a 0276 cba0 3514 9877 66c0 bd4b caee de8b e27c 0091 059c 9958 fc9b
eb4d a9eb c377 8137 4102 6d1d 2f21 9698 774f 6698 2ac1 1a15 f722 24d7
f10c d1b0 877c 524b b10e 18d8 fa99 f89e dd65 2b86 7e0c feb8 9f51 d98c
2f37 3b21 cd90 4cf2 983a dd33 9cb4 55f8 e939 7bf9 62a6 af9f 02fb 932f
417c 6a12 92e5 5553 901f c76b 0c89 353f 4507 a1b0 4e32 e8f6 f5f0 fd7b
e4d5 0246 0c32 962f 924e 5f83 70c2 dfbf 9c97 a463 acb1 bb45 6d25 4218
8ceb be65 9c88 aaad 6dbe b2b0 27e6 fe45 a9a8 c1bc 0d84 c6e6 ac0b 4d0d
e3cf ae90 009f 2857 4b63 2d68 d548 467b b104 2d52 f8e5 66f0 8046 c917
99cd 8240 b3dc 46f8 b19c 5d22 10ef 2ec6 c33f 817a 31be 3c1b b196 1cce
0d43 6fb0 567c 43d2 66ca 4d88 9036 8d3a f7e9 4b26 e843 19e3 18bb b96d
9b3a 6c9d 1a1d 615a df11 29f6 e704 ca8c 098d 9e0a 0c18 eb87 02b4 7748
06bb 9a0a 9fd8 b67f 90d1 18fc 2114 8501 4059 2a3e 0a05 b7e5 8af6 a317
9e76 87b6 7d61 f5ca 5ba9 170c 1303 babb b083 6cf6 277b d22e 9f15 b134
8c4b 433a 6005 ed00 2fba a339 8092 a3f8 119a 61e3 967e f866 1c9c da32
b4a0 a135 1a61 9b8f c9cb 7358 2e95 6a15 e587 d4c5 5194 f169 4203 6c3c
d56b 1142 0fcb b0af edaa 9652 a1ff 003c 92c0 e9f1 6f0f 8ce9 a36c 73a7
56fd 5548 d114 bdf5 73a5 175f f819 a785 bebe ce30 72ea c60b 6ebe 7d9d
6cbb c131 9bfd e5ef 3a84 862a 1395 372f 1fb5 4468 fc8c a990 cd96 3d37
1e97 3c2b 86ae 1e9b 8f4d 7df6 b14f 3882 5ecc c1ec cd7c fc2c 5221 a0f4
f401 ae4e a318 9d8a 0094 62ae e4e7 70b0 582b 5873 b2f2 3713 a369 9e20
4774 99c5 bd61 fba8 2b7b 35a2 5f92 c24f 7ac3 0255 716c c27d 306d a1ea
f6a7 d499 9c87 52f1 22d0 65d8 41d1 cab5 0da4 cf02 dfd9 016a 40ee 6eb8
30dd 7325 41b2 6896 645a 4e65 db85 2e7f f782 6dd4 0d6b a9df 69ee af67
a89f 76e2 8d21 df74 6882 fa94 1430 c641 3e07 a974 c45c c9d1 6f68 5f9d
9cab fce4 42ad 5d83 2dad 7f6b cbef be36 81a5 982b 3536 7105 a7b0 b441
b820 e9b1 f7af ff05 fdc4 3db1 2b85 c2ab 361e 0510 8a59 c7f1 1558 f75d
9589 7f48 3866 609e 1a16 55f6 22f3 0dcb be65 8a3c 2870 8ba4 c04e c063
f43a 6c36 a963 7d4c a6e8 4cad 8a44 3f0e d091 cf7c d8fd 8655 8993 8cb0
bb09 4c77 821f 12fe c542 270c cf42 8b29 69e6 ac3d d311 011c 17dd d123
c768 4071 7d68 e36e de3e 0802 c34b 348f bcca b62e 7bbb 29d5 a6b7 3f53
141b 7212 1f76 4fbc b789 1e8f 1fcf 03a7 f006 8cfa 4dc1 7218 a860 a5ff
9b8f f32b 2c39 5dd1 abe2 4a43 623f 9b80 d1c3 e20d 1a6d 45e0 c14e 8593
861c 1234 4565 f05e dc5a f630 071f c8fe aa9b bd83 b421 5b5c c8dd 2a7f
2277 5cd4 13ec 2ef6 2ea6 7e5d adce 18a5 2e70 be40 0f99 1d3c 3ad7 011e
a2cb a03b 6eae e6d1 cad1 6ec9 35ed 2369 e1e7 bc91 737c e1b5 6685 1412
09f5 bf18 6c7e 32fc 6ebe f09e 4636 f2f5 5ae1 ca59 c91b b451 7356 1528
5600 b460 37c7 88c4 5326 d184 a317 f08f d9f0 fef0 2be4 f190 11a4 9ff6
22c8 d1f6 89b7 3615 8d87 41aa 2f89 5b1d 9dc1 3f9b 0636 be61 b25f aaf8
e721 249d e8c3 c562 4128 3b53 ec5d 028e 2df5 6814 f753 ab3f 9789 7dee
0333 573f 1c9a 49d0 6ff7 f58a 0b43 0e82 386e e51b 922a 564b 32f1 4e97
e64a 321f 33c1 f8bb 4feb f592 fbda b83d ccff 34a5 fb48 ebe1 2d35 2019
7ddd 6aff 2f08 4a93 6e21 9500 36f0 82e2 ecb1 5e6f a4cd 2b69 402c 2e1e
dfe7 0862 9024 4b57 9bbb 7331 6d4c c80b 66e4 7439 e558 add8 d8e5 02ac
66e9 13a8 7fe9 83d1 77f9 087a 000b 1dc8 72b8 6892 7d3b 8297 3437 bd30
bd22 c22d 58f5 fa9e ea11 2edf 51c8 cd44 fc36 5458 d93b 2bdc 6703 7e75
2d9b c373 54b1 a55a 3aa3 564f 23ec 3718 a85b 244e 3612 4f1b 52d5 53c3
a4b5 f5f7 c669 60f3 e27c fe9b f102 0cbd b7fa 9aac 55c1 40b8 422e 9a86
39ce f481 3ba0 d089 9e47 ec16 3b98 49ae fe1d 0cd9 48f3 dff9 8f44 92ca
45d7 72ea 4a3c be2c dcba 21ef 2d4f 0323 3bab 04c0 9b5a 09c5 0391 9d05
5abb 7ada 61e0 31ec 45d0 639a 26b9 d99d f285 8086 eb1e 70be 7417 e8be
bb8a 09de a0fb 4476 14df aa44 15fd 5c7a 4562 b3e0 1be4 533a 53af 615c
dc21 fa95 e9bf 3a2c 51a3 9f5d e1ac c6c8 48a1 1797 1d54 7a20 5246 34e8
e92f e01f 497a 5a2f 135d 7c74 39a4 a412 cab8 8982 d49c e052 b058 288c
1ba5 cb3d 6493 cc4d 49d4 08b2 1173 6080 353f 9042 392d 25b0 ffaf 149a
3d7f 3920 840c c786 f01c fb54 b7d8 3fc9 b252 70d1 4ba0 4744 b4c0 15f5
2cfd 41a0 1da6 4824
```

References

[1] C. Carlet, "A larger class of cryptographic Boolean functions via a study of the Maiorana-Mcfarland constructions," in Advances in Cryptology—CRYPTO'02, Springer-Verlag, 2002, vol. LNCS 2442, pp. 549-564.

[2] C. Carlet, "On plateaued functions and their constructions," in Fast Software Encryption—FSE 2003, Springer-Verlag, 2003, vol. LNCS 2887, pp. 54-73.

[3] C. Carlet, K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in Advances in Cryptology—ASIACRYPT 2008, Springer-Verlag, 2008, vol. LNCS 5350, pp. 425-440.

[4] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in Advances in Cryptology—CRYPTO'91, Springer-Verlag, 1992, vol. LNCS 547, pp. 86-100.

[5] S. Chee, S. Lee, D. Lee and S. H. Sung, "On the correlation immune functions and their nonlinearity," in Advances in Cryptology—Asiacrypt'96, Springer-Verlag, 1997, vol. LNCS 1163, pp. 232-243.

[6] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in Advances in Cryptology—CRYPTO 2003, Springer-Verlag, 2003, vol. LNCS 2729, pp. 176-194.

[7] J. F. Dillon, Elementary Hadamard Difference Sets. Ph.D. Dissertation, Dept. Comput. Sci., Univ. Maryland, College Park, MD, USA, 1974.

[8] C. Ding, G. Xiao and W. Shan, The Stability Theory of Stream Ciphers. Berlin, Germany: Springer-Verlag, 1991.

[9] S. Kavut, S. Maitra, and M. D. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," IEEE Trans. Inf. Theory, vol. 53, no 5, pp. 1743-1751, 2007.

[10] S. Kavut and M. D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," Information and Computation, vol. 208, no. 4, pp. 341-350, 2010.

[11] 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, 2002.

[12] S. Maitra and E. Pasalic, "A Maiorana-McFarland type construction for resilient functions on variables (n even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$," Discrete Applied Mathematics, vol. 154, pp. 357-369, 2006.

[13] S. Maitra and P. Sarkar, "Modifications of Patterson-Wiedemann functions for cryptographic applications," IEEE Trans. Inf. Theory, vol. 48, no. 1, pp. 278-284, 2002.

[14] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, USA: CRC Press, 1997.

[15] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," Journal of Cryptology, vol. 1, no. 3, pp. 159-176, 1989.

[16] W. Meier and O. Staffelbach, “Nonlinearity criteria for cryptographic functions,” in Advances in Cryptology—EUROCRYPT’89, Springer-Verlag, 1990, vol. LNCS 434, pp. 549-562.

[17] E. Pasalic, “Maiorana-McFarland class: degree optimization and algebraic properties,” IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 4581-4594, 2006.

[18] E. Pasalic and T. Johansson, “Further results on the relation between nonlinearity and resiliency of Boolean functions,” in IMA Conference on Cryptography and Coding, Springer-Verlag, 1999, vol. LNCS 1746, pp. 35-45.

[19] N. J. Patterson and D. H. Wiedemann, “The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276,” IEEE Trans. Inf. Theory, vol. 29, no. 3, pp. 354-356, 1983.

[20] P. Sarkar and S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties. In: Advances in Cryptology—EUROCRYPT’00, Springer-Verlag, 2000, vol. LNCS 1807, pp. 485-506.

[21] P. Sarkar and S. Maitra, “Nonlinearity bounds and constructions of resilient functions,” in Advances in Cryptology—CRYPTO’00, Springer-Verlag, 2000, vol. LNCS 1807, pp. 515—532.

[22] S. Sarkar, S. Maitra, “Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros,” Designs, Codes and Cryptography, vol. 49, no. 1-3, pp. 95-103, 2008.

[23] J. Seberry, X. M. Zhang, and Y. Zheng, Nonlinearly balanced Boolean functions and their propagation characteristics. In: Advances in Cryptology—CRYPTO’93, Springer-Verlag, 1994, vol. LNCS 773, pp. 49-60.

[24] J. Seberry, X. M. Zhang, and Y. Zheng, “On constructions and nonlinearity of correlation immune Boolean functions,” in Advances in Cryptology—EUROCRYPT’93, Springer-Verlag, 1994, vol. LNCS 765, pp. 181—199.

[25] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications,” IEEE Trans. Inf. Theory, vol. 30, no. 5, pp. 776-780, 1984.

[26] Y. V. Tarannikov, “On resilient Boolean functions with maximum possible nonlinearity,” In Progress in Cryptology—INDOCRYPT’00, Springer-Verlag, 2000, vol. LNCS 1977, pp. 19-30.

[27] G. Xiao and J. L. Massey, “A spectral characterization of correlation-immune combining functions,” IEEE Trans. Inf. Theory, vol. 34, no. 3, pp. 569-571, 1988.

[28] W.-G. Zhang and G.-Z. Xiao, “Constructions of almost optimal resilient Boolean functions on large even number of variables,” IEEE Trans. Inf. Theory, vol. 55, no. 12, pp. 5822-5831, 2009.

[29] W.-G. Zhang and E. Pasalic, “Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes,” IEEE Trans. Inf. Theory, vol. 60, no. 3, pp. 1638-1651, 2014.

[30] Y. Zheng and X.-M. Zhang, “Improving upper bound on the nonlinearity of high order correlation immune functions,” in Selected Areas in Cryptography’00, Springer-Verlag, 2001, vol. LNCS 2012, pp. 262-274.

WeiGuo Zhang received the Ph.D. degree in cryptography from Xidian University, Xi’an, China, in 2007. Since July 2007, he joined the State Key Laboratory of Integrated Services Networks at Xidian University. His research interests include symmetric cryptography, sequence design, and algebraic coding theory.

Enes Pasalic received the Ph.D. degree in cryptology from Lund University, Lund, Sweden, in 2003. His main research interest is in cryptology and in particular the design and analysis of symmetric encryption schemes. Since May 2003, he has been doing a postdoctoral research at INRIA (Versaille, France) crypto group, and later in 2005 at the Technical University of Denmark, Lyngby. He is currently with University of Primorska, FAMNIT and IAM, Koper, Slovenia.