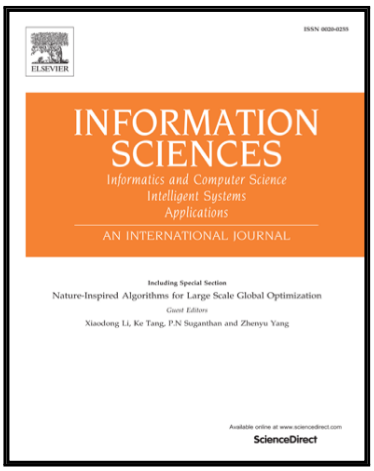
Accepted Manuscript



New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions

Yongzhuang Wei, Enes Pasalic, Fengrong Zhang, Wenling Wu, Chengxiang Wang

PII: S0020-0255(17)30804-6
DOI: 10.1016/j.ins.2017.06.036
Reference: INS 12958

To appear in: *Information Sciences*

Received date: 8 August 2016
Revised date: 12 June 2017
Accepted date: 24 June 2017

Please cite this article as: Yongzhuang Wei, Enes Pasalic, Fengrong Zhang, Wenling Wu, Chengxiang Wang, New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions, *Information Sciences* (2017), doi: 10.1016/j.ins.2017.06.036

New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions

Yongzhuang Wei * Enes Pasalic † Fengrong Zhang ‡ Wenling Wu §
Chengxiang Wang ¶

Abstract

The design of n-variable t-resilient functions with strictly almost optimal (SAO) nonlinearity ($> 2^{n-1} - 2^{\frac{n}{2}}$, n even) appears to be a rather difficult task. The known construction methods commonly use a rather large number (exactly $\sum_{i=t+1}^{n/2} \binom{n/2}{i}$) of affine subfunctions in $\frac{n}{2}$ variables which can induce some algebraic weaknesses, making these functions susceptible to certain types of guess and determine cryptanalysis and dynamic cube attacks. In this paper, the concept of *non-overlap spectra functions* is introduced, which essentially generalizes the idea of disjoint spectra functions on different variable spaces. Two general methods to obtain a large set of non-overlap spectra functions are given and a new framework for designing infinite classes of resilient functions with SAO nonlinearity is developed based on these. Unlike previous construction methods, our approach employs only a few $n/2$-variable affine subfunctions in the design, resulting in a more favourable algebraic structure. It is shown that these new resilient SAO functions properly include all the existing classes of resilient SAO functions as a subclass. Moreover, it is shown that the new class provides a better resistance against (fast) algebraic attacks than the known functions with SAO nonlinearity, and in addition these functions are more robust to guess and determine cryptanalysis and dynamic cube attacks.

Keywords : Stream ciphers, disjoint spectra, non-overlap spectra, resilient functions, nonlinearity.

*Guilin University of Electronic Technology, Guilin, P.R. China, e-mail: walker_wei@msn.com. This work was supported in part by the Natural Science Foundation of China (61572148), in part by the Guangxi Natural Science Found (2015GXNSFGA139007), in part by the project of Outstanding Young Teachers Training in Higher Education Institutions of Guangxi.

†University of Primorska, FAMNIT and IAM, Koper, Slovenia, e-mail: enes.pasalic6@gmail.com. This work is supported in part by the Slovenian Research Agency (research program P3-0384 and research project J1-6720).

‡School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, P.R. China, e-mail: zhfl203@cumt.edu.cn. This work is supported in part by National Science Foundation of China (61303263), and in part by the Fundamental Research Funds for the Central Universities (Grant No. 2015XKMS086).

§Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R. China, e-mail: wwl@is.iscas.ac.cn

¶Institute of Sensors, Signals and Systems, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK, e-mail: cheng-xiang.wang@hw.ac.uk

1 Introduction

During the past three decades, the construction of highly nonlinear resilient Boolean functions has been an interesting research topic [5, 14, 15, 20, 24, 29, 37, 39, 41, 43]. These resilient functions play an important role in the design of certain stream cipher encryption schemes such as nonlinear combiners, for which the output sequences of several linear feedback shift registers (LFSRs) are combined (filtered) via a nonlinear Boolean function to generate the keystream sequence. The security of nonlinear combiners depends almost entirely on the choice of the filtering Boolean function. It is widely accepted that a Boolean function used in nonlinear combiners must fulfill certain cryptographic criteria such as balancedness, high order of resiliency, high nonlinearity and high algebraic degree. These criteria reflect the ability of the cipher to withstand various types of attacks. For instance, the nonlinearity measures the minimum distance between a given Boolean function and the set of affine functions. It indicates the ability of the cipher to withstand various modes of BAA (best affine approximation) and correlation attacks, see [10, 29].

Unfortunately, all the criteria mentioned above cannot be optimized simultaneously and there are certain trade-offs among the criteria. For an n-variable Boolean function whose resiliency order is t, Siegenthaler [29] showed that $d \leq n - t - 1$, where d is the algebraic degree of the function. Apart from the above mentioned criteria, the algebraic properties of Boolean functions are decisive for protecting the cipher against (fast) algebraic attacks [1, 8, 9]. The concept of algebraic immunity (AI) was introduced in [21], indicating the ability of Boolean functions (in relation to the corresponding encryption scheme) to withstand algebraic attacks proposed in 2003 [9]. An optimal resistance of a Boolean function f against algebraic attacks is achieved if AI of $f(x)$ equals to $\lceil n/2 \rceil$. Moreover, the fast algebraic attacks (FAA) on stream ciphers were introduced in [8], thus further extending the mentioned cryptographic criteria. An optimal resistance of Boolean functions (used in certain stream cipher algorithms) against FAA implies that for a given n-variable Boolean function f, there does not exist a pair of functions g and h related through $fg = h$ so that $\deg(g) + \deg(h)$ is less than n. Furthermore, for balanced functions it was shown that there always exist g and h such that $\deg(g) + \deg(h) = n - 1$, hence in this case the degree value $n - 1$ is called optimal, see [19].

The most significant contributions related to the design of highly nonlinear resilient functions, during the past two decades, can be found in [3, 5, 7, 15, 20, 24, 28, 39, 41, 42]. In these works, a well-known method to obtain nonlinear resilient functions relies on the use of Maiorana-McFarland (M-M) techniques or extensions thereof. The basic idea of this approach is to construct nonlinear resilient functions on larger variable spaces by concatenating suitable affine functions on smaller variable spaces. This technique was first introduced by Camion *et al.* in 1992 [3], and it was further used in [7, 27, 28]. At CRYPTO2002, Carlet proposed an extension of the M-M method for obtaining nonlinear resilient functions by concatenating quadratic functions [5]. In 2006, Pasalic presented a method to obtain degree optimized resilient functions by using a slightly modified M-M technique [24]. Later, Maitra *et al.* [20] presented methods to obtain resilient functions of order t with nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{n/2-3} - 2^{n/2-4}$, for all $n \geq 8t + 6$.

Recently, Zhang *et al.* [39, 40] proposed new methods to obtain resilient functions and

resilient S-boxes (multiple-output Boolean functions) with strictly almost optimal nonlinearity $> 2^{n-1} - 2^{n/2}$, for any n even, by concatenating several sets of disjoint spectra functions defined on small variable spaces (the size being $\leq n/2$). However, most of the construction techniques above generally share the same basic idea, that is, the subfunctions of these resilient functions (defined as a restriction of a function when a subset of variables is kept fixed) are affine functions in relatively large number of input variables. More precisely, the number of subfunctions of the t-resilient functions in [40, 41] which are affine in $n/2$ variables is given by $\sum_{i=t+1}^{n/2} \binom{n/2}{i}$. To improve relatively bad algebraic properties, a modified construction that uses only a moderate number of affine subfunctions in $n/2$-variable (the number being $2^{n/2-1}$) has been proposed in [40]. The functions in the modified class then provide relatively good resistance against (fast) algebraic attacks (based on simulations for ($n \leq 14$)), but unfortunately the nonlinearity of these functions in [40] is substantially decreased (the functions do not have SAO nonlinearity any longer).

Intuitively, the use of "too many" large affine subfunctions in $n/2$-variable (namely either $\sum_{i=t+1}^{n/2} \binom{n/2}{i}$ or $2^{n/2-1}$ as in [40]) may induce some algebraic weaknesses in the structure and make a cipher less resistant to various cryptanalytic methods. Indeed, by fixing l variables of an n-variable nonlinear Boolean function, its $(n-l)$-variable subfuntions are either linear or nonlinear which in the former case gives rise to *partial linear relations* with respect to the fixed set of l variables. In fact, there are many attacks on stream ciphers which essentially use these partial linear relations, and the attacks become more efficient for relatively small l.

We recall a few important approaches that efficiently use partial linear relations of nonlinear Boolean functions in the various aspects of cryptanalysis. In 2009, Khoo *et al.* proposed a time-memory-data (TMD) trade-off attack on filtering generators and nonlinear combiners in case the nonlinear filtering function belongs to the Maiorana-McFarland class [16]. These partial linear relations of the nonlinear Boolean functions used in the Grain family of stream ciphers were used to mount related-key chosen IV attacks and internal state recovery attacks on the Grain family of stream ciphers [17, 23]. For the case when the filtering function is a vectorial Boolean function in the M-M class, a guess and determine attack was introduced in [25]. The dynamic cube attacks introduced in [11, 12] also commonly employ some partial linear relations that relate the secret key and IV variables. Finally, at FSE 2013, a new criterion for avoiding the existence of partial linear relations in substitution boxes was proposed in [2].

From the above survey, it appears that cryptographically significant Boolean functions should not give rise to partial linear relations if a relatively small number of inputs is kept fixed. In this direction, our approach efficiently revises the previous construction methods (that can be viewed as a modified M-M class) towards a more favourable algebraic structure of the designed resilient functions with respect to the cardinality of partial linear functions. This is accomplished without degrading the nonlinearity which remains SAO unlike the construction method in [40]. To achieve this goal the concept of *non-overlap spectra functions* is introduced (and employed in the design) and the existence of a large set of functions with this property is proved. The so-called non-overlap spectra functions, which essentially generalizes the idea of disjoint spectra functions, are characterized by the property that for any pair of these functions their nonzero values in the Walsh spectra do not overlap, even though the functions are not defined on the same variable space (which is the case for standard disjoint spectra functions).

The proposed design of resilient functions with SAO nonlinearity is inevitably rather technical and involved, which is also the case with other design methods whose goal is to achieve extremely high nonlinearity values. In difference to previous approaches [39, 40, 41] that use a large set of $n/2$-variable affine subfunctions, our method only uses a few $n/2$-variable affine subfunctions. It is demonstrated (through both theoretical analysis and computer simulations) that these new resilient functions have better algebraic properties, thus improving the resistance to (fast) algebraic attacks compared to the classes in [39, 40, 41]. Furthermore, it is shown that our class properly include the classes of Zhang *et al.* [40, 41] as a subclass. The use of a small number of $n/2$-variable affine subfunctions also implies a better robustness to cryptanalytic methods that employ partial linear relations than the classes in [40, 41]. Most notably, we give a semi-deterministic method which generates algebraically optimal functions (thus providing optimal resistance to (fast) algebraic attacks) with slightly decreased nonlinearity for moderate size of input variables, whereas for large n the algebraic properties are quite acceptable for practical applications though not optimal.

The rest of the paper is organized as follows. In Section 2, some basic notations and definitions related to cryptographic criteria of Boolean functions are introduced. A brief overview of related previous work is given in Section 3. In Section 4, the notion of non-overlap spectra functions is introduced and two methods for finding large sets of non-overlap spectra functions are proposed. The main construction methods of resilient functions with SAO nonlinearity, based on the use of non-overlap spectra functions, are presented in Section 5. In addition, a semi-deterministic method for constructing resilient functions with optimal algebraic properties (for moderate size of the input space) and high nonlinearity is also addressed. Finally, some concluding remarks are given in Section 6.

2 Preliminaries

The binary Galois field is denoted by $GF(2)$ and "$\oplus$" stands for the addition operator over $GF(2)$. An n-dimensional vector space spanned over $GF(2)$ is denoted by $GF(2)^n$. A Boolean function is a mapping $f : GF(2)^n \longrightarrow GF(2)$ and the set of all Boolean functions $f(x_1, \ldots, x_n)$ over $GF(2)^n$ is denoted by $\mathbb{B}_n$. The truth table of a Boolean function $f(x_1, \ldots, x_n)$ is a binary string of length 2^n corresponding to the output values of f when the input values run lexicographically through $GF(2)^n$,

$$(f(0,0,\ldots,0), f(1,0,\ldots,0), f(0,1,\ldots,0), \ldots, f(1,1,\ldots,1)). \tag{1}$$

Especially, if the number of ones is equal to the number of zeros in the truth table of f, then a Boolean function $f(x_1, \ldots, x_n)$ is said to be balanced.

Definition 1 *The algebraic normal form (**ANF**) of an n-variable Boolean function is the multivariate polynomial expression given by,*

$$f(x_1, \ldots, x_n) = \sum_{c \in GF(2)^n} \lambda_c (\prod_{i=1}^{n} x_i^{c_i}), \tag{2}$$

where $c = (c_1, \ldots, c_n) \in GF(2)^n$, $\lambda_c, x_i \in GF(2)$.

The algebraic degree of f, denoted by $\deg(f)$, corresponds to the maximal value of the Hamming weight of c in (2) satisfying the condition $\lambda_c \neq 0$. A Boolean function $f \in \mathbb{B}_n$ is said to be affine if $\deg(f) \leq 1$. In particular, for an affine Boolean function, if its constant term is zero, then such a function is said to be linear.

Definition 2 *For $X = (x_1, \ldots, x_n) \in GF(2)^n$ and $\omega = (\omega_1, \ldots, \omega_n) \in GF(2)^n$ let $\omega \cdot X = \omega_1 \cdot x_1 \oplus \cdots \oplus \omega_n \cdot x_n$ be the inner (dot) product of X and ω . For any $f \in \mathbb{B}_n$, the Walsh transform of $f(x)$ at point ω is defined as*

$$W_f(\omega) = \sum_{X \in GF(2)^n} (-1)^{f(X) \oplus \omega \cdot X}. \tag{3}$$

Definition 3 *[37] A function $f \in \mathbb{B}_n$ is said to be a correlation immune (CI) function of order t if and only if $W_f(\omega) = 0$, for all $\omega \in GF(2)^n$ such that $0 < wt(\omega) \leq t$, where $wt(\omega)$ is the Hamming weight of ω. Moreover, if f is also balanced, that is $W_f(0) = 0$, then f is called a t-resilient function.*

Definition 4 *[22] The nonlinearity of $f \in \mathbb{B}_n$ is defined as*

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in GF(2)^n} |W_f(\omega)|, \tag{4}$$

where $|\cdot|$ denotes absolute value.

Definition 5 *A function $f \in \mathbb{B}_n$, where n is even, is called bent if $W_f(\omega) = \pm 2^{\frac{n}{2}}$, for every $\omega \in GF(2)^n$.*

Definition 6 *A set of Boolean functions $\{f_1, \ldots, f_m\} \subset \mathbb{B}_n$ is called a set of disjoint spectra functions if for all $\omega \in GF(2)^n$,*

$$W_{f_i}(\omega) W_{f_j}(\omega) = 0, \;\; 1 \leq i < j \leq m. \tag{5}$$

To distinguish from the absolute value notation, the cardinality of any set C is denoted by $||C||$. The so-called *disjoint spectra functions* have been extensively used in the design of highly nonlinear resilient functions, see [13, 26, 41].

Lemma 1 *Let m be a positive integer and $X = (X_1, X_2) \in GF(2)^n$, $X_1 \in GF(2)^m$, $X_2 \in GF(2)^{n-m}$. Then, the set of functions*

$$D^* = \{g_c(X) = c \cdot X_1 \oplus h_c(X_2) \mid c \in GF(2)^m, h_c \in \mathbb{B}_{n-m}\},$$

is a set of disjoint spectra functions. In particular, for all $\alpha = (\beta, \theta) \in GF(2)^n$, where $\beta \in GF(2)^m, \theta \in GF(2)^{n-m}$, we have $W_{g_c}(\alpha) \in \{0, 2^m \times W_{h_c}(\theta)\}$.

The set of disjoint spectra functions above has been used as a basic construction primitive for obtaining almost optimal resilient Boolean functions in [41]. Finally, an n-variable, t-resilient Boolean function with algebraic degree d and nonlinearity N_f is denoted by (n, t, d, N_f).

3 An overview of recent works

In this section, we briefly recall the basic construction methods in [40, 41] for designing resilient Boolean functions whose nonlinearity is strictly almost optimal.

The main construction methods proposed in [40, 41] are given below for self-completeness, the reader can refer to [40] and [41] for further details.

Construction A [41]: Let $n \geq 12$ be an even number, t be a positive number, and let $(a_1, \ldots, a_s) \in GF(2)^s$ satisfies

$$\sum_{j=t+1}^{n/2} \binom{n/2}{j} + \sum_{i=1}^{s} \Big(a_i \sum_{j=t+1}^{n/2-2i} \binom{n/2-2i}{j} \Big) \geq 2^{n/2}, \tag{6}$$

where $s = \lfloor (n-2t-2)/4 \rfloor$. Let $X_1 = (x_1, \ldots, x_{n/2}) \in GF(2)^{n/2}$, $X_2 = (x_{n/2+1}, \ldots, x_n) \in GF(2)^{n/2}$, $X'_m = (x_1, \ldots, x_m) \in GF(2)^m$, and $X''_{2i} = (x_{m+1}, \ldots, x_{n/2}) \in GF(2)^{2i}$ with $m + 2i = n/2$. Denote by

$$U_0 = \{c \cdot X_1 \mid c \in GF(2)^{n/2}, wt(c) > t\}, \tag{7}$$

and for $1 \leq i \leq s$ let

$$U_i = \{c \cdot X'_m \oplus h_c(X''_{2i}) \mid h_c \in H_i, c \in GF(2)^m, wt(c) > t\}, \tag{8}$$

where H_i is a nonempty set of $2i$-variable bent functions whose algebraic degree is $\max(2, i)$. Denote by ϕ any injective mapping from $GF(2)^{n/2}$ to $\bigcup_{i=0}^{s} U_i$. Then, one may define a Boolean function $f \in \mathbb{B}_n$ as follows,

$$f(X_1, X_2) = \sum_{\sigma=(\sigma_1,\ldots,\sigma_{n/2}) \in GF(2)^{n/2}} \prod_{i=n/2+1}^{n} (x_i \oplus \sigma_i \oplus 1) \cdot \phi(\sigma), \tag{9}$$

where injectivity of ϕ follows from the inequality (6), see [41].

A more recent construction approach [40], named as Generalized Maiorana-McFarland (GMM) method, which apart from suitable $n/2$-variable affine functions also utilizes small affine functions in a rather involved and sophisticated manner, also generates the functions with SAO nonlinearity.

Construction B [40]: Let $1 \leq i \leq n-1$, $B_i \subseteq GF(2)^i$ and $B'_i = B_i \times GF(2)^{n-i}$ such that $\bigcup_{i=1}^{n-1} B'_i = GF(2)^n$ and $B'_{i_1} \cap B'_{i_2} = \emptyset$, $1 \leq i_1 < i_2 \leq n-1$. Let $X = (x_1, \ldots, x_n) \in GF(2)^n$, $X'_i = (x_1, \ldots, x_i) \in GF(2)^i$, and $X''_{n-i} = (x_{i+1}, \ldots, x_n) \in GF(2)^{n-i}$. A *GMM* type Boolean function $f \in B_n$ is constructed as follows:

$$f(X'_i, X''_{n-i}) = \varphi_i(X'_i) \cdot X''_{n-i} \oplus g_i(X'_i), X'_i \in B_i, 1 \leq i \leq n-1. \tag{10}$$

where φ_i is a mapping from $GF(2)^i$ to $GF(2)^{n-i}$ and $g_i \in \mathbb{B}_i$.

Theorem 1 *[40] With the same notation as in Construction B, let n be even and $B_i = \emptyset$, for $1 \leq i \leq n/2 - 1$. Let $0 \leq t \leq n/2 - 2$ and $(a_{n/2}, \ldots, a_{n-t-1}) \in GF(2)^{n/2-t}$ (where $a_{n/2} = 1$) be a binary vector such that $\sum_{i=n/2}^{n-t-1} a_i 2^i$ is maximal satisfying at the same time the condition*

$$\sum_{i=n/2}^{n-t-1} (a_i 2^{n-i} \sum_{j=t+1}^{n-i} \binom{n-i}{j}) \geq 2^n. \tag{11}$$

Let $r = \max\{i \mid a_i \neq 0, n/2 \leq i \leq n-t-1\}$. For $n/2 \leq i \leq r-1$, set $||B_i|| = 0$, if $a_i = 0$, otherwise set $||B_i|| = \sum_{j=t+1}^{n-i} \binom{n-i}{j}$, if $a_i = 1$. For $n/2 \leq i \leq r$ and $a_i = 1$, let ψ_i be an injective mapping from B_i to D_i, where

$$D_i = \{c \mid wt(c) \geq t+1, c \in GF(2)^{n-i}\}. \tag{12}$$

Then, the function $f \in \mathbb{B}_n$ obtained by Construction B is a t-resilient function with SAO nonlinearity

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

An important observation is that these Boolean functions $f \in \mathbb{B}_n$, obtained by the above constructions, employ a large set of linear functions in $n/2$ variables. For instance, Construction A uses a subset of linear functions in $n/2$ variables $U_0 = \{c \cdot X_1 | c \in GF(2)^{n/2}, X_1 \in GF(2)^{n/2}, wt(c) > t\} \subset \mathbb{B}_{n/2}$. To overcome the potential weaknesses of these functions as mentioned in the introduction, we will propose a new method (based on the use of non-overlap spectra functions introduced below) for constructing highly nonlinear resilient functions with good algebraic properties using less $n/2$-variable affine functions.

4 Constructions of the set of non-overlap spectra functions

In this section, the concept of non-overlap spectra functions is introduced along with an efficient way of generating a large set of such functions. For convenience, throughout the article, we denote by $X_{(i)}^{(j)} = (x_i, x_{i+1}, \ldots, x_j) \in GF(2)^{j-i+1}$ a subset of variables $x_1, \ldots, x_n$, where $1 \leq i < j \leq n$. In particular, when $i = 1$ we simply write $X^{(j)} = (x_1, \ldots, x_j)$. Other letters are used similarly to denote the constants, for instance $\omega^{(n_1)} = (\omega_1, \omega_2, \ldots, \omega_{n_1}) \in GF(2)^{n_1}$. Furthermore, h_c will always denote a bent function from some subset of bent functions H_{2k} defined on a suitable variable subspace of cardinality $2k$.

4.1 A large set of non-overlap spectra functions

Definition 7 *Let $f \in \mathbb{B}_{n_1}, g \in \mathbb{B}_{n_2}, (n_1 > n_2)$, $\omega^{(n_1)} \in GF(2)^{n_1}$ and $\omega^{(n_2)} \in GF(2)^{n_2}$. Let us define a set Γ_f as*

$$\Gamma_f = \{\omega^{(n_2)} \mid \omega^{(n_1)} = (\omega^{(n_2)}, \omega_{n_2+1}, \omega_{n_2+2}, \ldots, \omega_{n_1}) \in \sup(W_f), \omega^{(n_2)} \in GF(2)^{n_2}\},$$

where $\sup(W_f) = \{\omega^{(n_1)} \mid W_f(\omega^{(n_1)}) \neq 0, \omega^{(n_1)} \in GF(2)^{n_1}\}$. *Then,* (f, g) *is called a pair of non-overlap spectra functions if for all* $\omega^{(n_1)} \in \sup(W_f), \omega^{(n_2)} \in \Gamma_f$, *we have* $W_f(\omega^{(n_1)})W_g(\omega^{(n_2)}) = 0$.

Notice that in difference to the standard notion of disjoint spectra functions, the condition $W_f(\omega^{(n_1)})W_g(\omega^{(n_2)}) = 0$ refers to functions that are not defined on the same variable space.

Example 1 *Let* $f(x_1, \ldots, x_7) = x_1 \oplus x_2 \oplus x_3 \oplus x_4x_5 \oplus x_6x_7$ *and* $g(x_1, \ldots, x_5) = x_1 \oplus x_4 \oplus x_5$. *It is easily verified that* $W_f(\omega^{(7)}) \in \{0, \pm 2^5\}$ *and* $W_g(\omega^{(5)}) \in \{0, \pm 2^5\}$. *Furthermore, we know*

$$\sup(W_f) = \{\omega^{(7)} \mid \omega^{(7)} = (1, 1, 1, \beta) \in GF(2)^7, \beta \in GF(2)^4\}.$$

Let

$$\Gamma_f = \{\omega^{(5)} \mid \omega^{(7)} = (\omega^{(5)}, \omega_6, \omega_7) \in \sup(W_f), \omega^{(5)} = (1, 1, 1, \beta_1, \beta_2) \in GF(2)^5\}.$$

Then, for all $\omega^{(7)} \in \sup(W_f), \omega^{(5)} \in \Gamma_f$, *we have* $W_g(\omega^{(5)}) = 0$ *which implies* $W_f(\omega^{(7)}) \cdot W_g(\omega^{(5)}) = 0$. *Therefore,* (f, g) *is a pair of non-overlap spectra functions, where* $\omega^{(7)} \in \sup(W_f), \omega^{(5)} \in \Gamma_f \subset GF(2)^5$.

The concept of a pair of non-overlap spectra functions can be easily extended to a wider framework which we call a large set of non-overlap spectra functions.

Definition 8 *Let* $I_0 = \{\varphi_1, \ldots, \varphi_{m_1}\} \subset \mathbb{B}_{n_1}$ *be a set of mutually disjoint spectra functions, and* $I_1 = \{g_1, \ldots, g_{m_2}\} \subset \mathbb{B}_{n_2}$ *be another set of (mutually) disjoint spectra functions, where* $n_1 > n_2$. *Let also* $\omega^{(n_1)} \in GF(2)^{n_1}$ *and* $\omega^{(n_2)} \in GF(2)^{n_2}$. *Moreover, for* $1 \leq i \leq m_1$, *let*

$$\sup(W_{\varphi_i}) = \{\omega^{(n_1)} \mid W_{\varphi_i}(\omega^{(n_1)}) \neq 0\}$$

and

$$\Gamma_{\varphi_i} = \{\omega^{(n_2)} \mid \omega^{(n_1)} = (\omega^{(n_2)}, \alpha) \in \sup(W_{\varphi_i}), \alpha \in GF(2)^{n_1 - n_2}\}.$$

$I_0 \cup I_1$ *is called a set of non-overlap spectra functions if for all* $\omega^{(n_1)} \in \sup(W_{\varphi_i}), \omega^{(n_2)} \in \Gamma_{\varphi_i}$,

$$W_{\varphi_i}(\omega^{(n_1)}) \cdot W_{g_j}(\omega^{(n_2)}) = 0, \text{ for all } 1 \leq i \leq m_1, 1 \leq j \leq m_2. \tag{14}$$

To obtain a large set of non-overlap spectra functions, suitable in the design of t-resilient functions, we divide the space $GF(2)^{m+k}$ into two subsets $S_0 = \{c \mid c \in GF(2)^{m+k}, wt(c) > t\}$ and $S_1 = \{c \mid c \in GF(2)^{m+k}, wt(c) \leq t\}$. Furthermore, a set of bent functions on a suitable subspace $GF(2)^{2k} \subset GF(2)^n$ is also needed.

Proposition 1 *Let* n, m, k *be three positive integers,* t *be an integer in the range* $[0, m + k - 1]$, *and* $m + 2k = n/2$ *(n even). Let* $X_2 = X_{(m+k+1)}^{(n/2+k)} = (x_{m+k+1}, \ldots, x_{n/2+k}) \in GF(2)^{2k}$, $\deg(h_c) = \max\{2, k\}$ *and define*

$$I_0 = \{\varphi_c(X^{(m+k)}, X_2) = c^{(m+k)} \cdot X^{(m+k)} \oplus h_c(X_2) \mid wt(c^{(m+k)}) > t\} \subset \mathbb{B}_{\frac{n}{2}+k}. \tag{15}$$

Moreover, let $c^{(n/2)} = (c^{(m+k)}, \alpha) \in GF(2)^{n/2}$, *for* $\alpha \in GF(2)^k$, *and define*

$$I_1 = \{g_{c^{(n/2)}}(X^{(n/2)}) = c^{(n/2)} \cdot X^{(n/2)} \mid wt(c^{(m+k)}) \leq t, wt(c^{(n/2)}) > t\} \subset \mathbb{B}_{\frac{n}{2}}. \tag{16}$$

Then, $I_0 \cup I_1$ *is a set of non-overlap spectra functions.*

Proof. From Lemma 1, we know that both I_0 and I_1 are sets of disjoint spectra functions. Let $\omega^{(n/2+k)} = (\theta, \eta) \in GF(2)^{n/2+k}$, where $\theta \in GF(2)^{m+k}$, and $\eta \in GF(2)^{2k}$. Then, for all $\omega^{(n/2+k)} \in GF(2)^{n/2+k}$, we have

$$\begin{aligned} W_{\varphi_c}(\omega^{(n/2+k)}) &= \sum_{(X^{(m+k)},X_2)\in GF(2)^{n/2+k}} (-1)^{c^{(m+k)}\cdot X^{(m+k)} \oplus h_c(X_2) \oplus \omega^{(n/2+k)}\cdot (X^{(m+k)},X_2)} \\ &= \sum_{X_2\in GF(2)^{2k}} (-1)^{h_c(X_2)\oplus \eta\cdot X_2} \left(\sum_{X^{(m+k)}\in GF(2)^{m+k}} (-1)^{(c^{(m+k)}\oplus\theta)\cdot X^{(m+k)}} \right). \end{aligned}$$

Moreover,

$$W_{\varphi_c}(\omega^{(n/2+k)}) = \begin{cases} 0, & (c^{(m+k)} \neq \theta) \\ \pm 2^{m+k} \times 2^k = \pm 2^{n/2}, & (c^{(m+k)} = \theta). \end{cases} \tag{17}$$

On the other hand, for all $\omega^{(n/2)} \in GF(2)^{n/2}$, if $W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) \neq 0$ then $W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) = 2^{n/2}$. Let now $\omega^{(n/2+k)} = (\omega^{(n/2)}, \alpha) \in GF(2)^{n/2+k}$, $\omega^{(n/2)} = (\theta, \beta) \in GF(2)^{n/2}$, where $\alpha, \beta \in GF(2)^k$. From (15) and (17), if $W_{\varphi_\theta}(\omega^{(n/2+k)}) \neq 0$, then we have $wt(\theta) > t$. It directly means that

$$\begin{aligned} W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) &= \sum_{X^{(n/2)}\in GF(2)^{n/2}} (-1)^{c^{(n/2)}\cdot X^{(n/2)} \oplus \omega^{(n/2)}\cdot X^{(n/2)}} \\ &= \sum_{X^{(n/2)}\in GF(2)^{n/2}} (-1)^{(c^{(m+k)},\alpha)\cdot X^{(n/2)} \oplus (\theta,\beta)\cdot X^{(n/2)}} \\ &= \sum_{X^{(m+k)}\in GF(2)^{m+k}} (-1)^{(c^{(m+k)}\oplus\theta)\cdot X^{(m+k)}} \sum_{(x_{m+k+1},\ldots,x_{n/2})\in GF(2)^k} (-1)^{(\alpha\oplus\beta)\cdot(x_{m+k+1},\ldots,x_{n/2})}. \end{aligned}$$

Because $wt(c^{(m+k)}) \leq t$ and $wt(\theta) > t$, thus $c^{(m+k)} \neq \theta$, we always have $W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) = 0$. That is, $W_{\varphi_\theta}(\omega^{(n/2+k)}) \times W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) = 0$ for $\omega^{(n/2)} \in \Gamma_{\varphi_\theta} = \{\omega^{(n/2)} \mid \omega^{(n/2+k)} = (\omega^{(n/2)}, \alpha) \in \sup(W_{\varphi_\theta}), \alpha \in GF(2)^{n_1-n_2}\}$. Therefore, $I_0 \cup I_1$ is a set of non-overlap spectra functions. ∎

The next lemma states that the total number of elements (used to define the support of a function) from the set of affine functions in $n/2$ variables (i.e., U_0) is equal to the total number of elements from the set of non-overlap spectra functions (i.e., $I_0 \cup I_1$). Thus, instead of using purely linear functions we use a small portion of these functions in combination with nonlinear functions from $\mathbb{B}_{\frac{n}{2}+k}$.

Lemma 2 *With the same notations as in Proposition 1, and keeping $m + 2k = n/2$, let*

$$U_0 = \{c^{(n/2)} \cdot X^{(n/2)} \mid wt(c^{(n/2)}) > t\} \subset \mathbb{B}_{\frac{n}{2}},$$

$$I_0 = \{c^{(m+k)} \cdot X^{(m+k)} \oplus h_c(X_2) \mid h_c \in H_{2k}, wt(c^{(m+k)}) > t\} \subset \mathbb{B}_{\frac{n}{2}+k}, \text{ and}$$

$$I_1 = \{c^{(n/2)} \cdot X^{(n/2)} \mid wt(c^{(m+k)}) \leq t, wt(c^{(n/2)}) > t\} \subset \mathbb{B}_{\frac{n}{2}},$$

where $c^{(n/2)} = (c^{(m+k)}, \alpha) \in GF(2)^{n/2}, \alpha \in GF(2)^k$. *Then, the following equation is satisfied*

$$\mu \times 2^{n/2} = \delta_0 \times 2^{n/2+k} + \delta_1 \times 2^{n/2},$$

where $\mu = ||U_0||$, $\delta_0 = ||I_0||$, and $\delta_1 = ||I_1||$.

Proof. It is clear that $\mu = \sum_{i=t+1}^{n/2} \binom{n/2}{i}$ and $\delta_0 = \sum_{i=t+1}^{m+k} \binom{m+k}{i}$. To compute δ_1, we let

$$\delta_0^* = ||\{c^{(n/2)} \mid c^{(n/2)} = (c^{(m+k)}, \alpha) \in GF(2)^{n/2}, wt(c^{(n/2)}) > t\}||,$$

so that $\delta_0^* = 2^k \delta_0$, since α runs over all possible values in $GF(2)^k$. Moreover, we split $\{c^{(n/2)} \mid wt(c^{(n/2)}) > t\}$ into two disjoint sets so that S_0 and S_1, where

$$\begin{aligned} S_0 &= \{c^{(n/2)} \mid c^{(n/2)} = (c^{(m+k)}, \alpha), \alpha \in GF(2)^k, wt(c^{(m+k)}) > t\}, \\ S_1 &= \{c^{(n/2)} \mid c^{(n/2)} = (c^{(m+k)}, \alpha), \alpha \in GF(2)^k, wt(c^{(m+k)}) \leq t, wt(c^{(n/2)}) > t\}. \end{aligned}$$

Then, we have $\mu = 2^k \delta_0 + \delta_1$ and consequently $\mu \times 2^{n/2} = \delta_0 \times 2^{n/2+k} + \delta_1 \times 2^{n/2}$. □

Corollary 1 *Using the same notations as in Proposition 1 and Lemma 2 the following relationship is valid:*

$$\delta_1 = \mu - 2^k \delta_0 = \sum_{i=t+1}^{n/2} \binom{n/2}{i} - 2^k \times \sum_{i=t+1}^{m+k} \binom{m+k}{i}. \tag{18}$$

Example 2 *Let* $n = 16, m = 2, k = 3, t = 1$. *Let* $X_2 = (x_6, \ldots, x_{11}) \in GF(2)^6$ *and*

$$I_0 = \{\varphi_c(X^{(5)}, X_2) = c^{(5)} \cdot X^{(5)} \oplus h_c(X_2) \mid h_c \in H_6, wt(c) > 1\} \subset \mathbb{B}_{11},$$

where H_6 *is a nonempty set of* 6*-variable bent functions with algebraic degree 3. Moreover, let* $c^{(8)} = (c^{(5)}, \alpha) \in GF(2)^8$, *where* $\alpha \in GF(2)^3$, *and define*

$$I_1 = \{g_{c^{(8)}}(X^{(8)}) = c^{(8)} \cdot X^{(8)} \mid wt(c^{(5)}) \leq 1, wt(c^{(8)}) > 1\} \subset \mathbb{B}_8.$$

Then, $I_0 \cup I_1$ *is a set of non-overlap spectra functions, where*

$$||I_0|| = \delta_0 = 26, \qquad ||I_1|| = \delta_1 = 39.$$

Moreover, let $U_0 = \{c^{(8)} \cdot X^{(8)} \mid wt(c^{(8)}) > 1\}$, *thus* $||U_0|| = \mu = 247$. *From Lemma 2, we have* $\mu \times 2^8 = 247 \times 2^8$, *and* $\delta_0 \times 2^{11} + \delta_1 \times 2^8 = 26 \times 2^{11} + 39 \times 2^8 = 247 \times 2^8$. *This means that* $\mu \times 2^8 = \delta_0 \times 2^{11} + \delta_1 \times 2^8$. *In particular,* U_0 *contains* 247 *linear 8-variable Boolean functions, whereas* $I_0 \cup I_1$ *only contains* 39 *linear functions in 8 variables and* 26 *cubic Boolean functions in 11 variables.*

4.2 Further construction of a large set of non-overlap spectra functions with less affine subfunctions

In this section, a construction of the set of non-overlap spectra functions with less affine subfunctions is investigated. In particular, this large set of non-overlap spectra functions includes some nonlinear subfunctions that are defined on different variable spaces which could be helpful for resisting certain kind of attacks such as those discussed in Section 5.5.

Lemma 3 *Let n, m_i, k_i be some positive integers, $(1 \leq i \leq 2, m_1+k_1 < m_2+k_2)$, t be an integer in the range $[0,(m_1+k_1-1)]$, and $m_i+2k_i = n/2$ (n even). Let $m_1+k_1 = d_1$ and with respect to it define*

$$I_0^{(1)} = \{\varphi_{c^{(d_1)}} = c^{(d_1)} \cdot X^{(d_1)} \oplus h_{c^{(d_1)}}(X^{(n/2+k_1)}_{(d_1+1)}) \mid h_{c^{(d_1)}} \in H_{2k_1}, wt(c^{(d_1)}) > t\} \subset \mathbb{B}_{\frac{n}{2}+k_1}. \quad (19)$$

Similarly, for $m_2+k_2 = d_2$, denote by $c^{(d_2)} = (c^{(d_1)}, \alpha) \in GF(2)^{d_2}$ and define

$$I_0^{(2)} = \{\varphi_{c^{(d_2)}} = c^{(d_2)} \cdot X^{(d_2)} \oplus h_{c^{(d_2)}}(X^{(n/2+k_2)}_{(d_2+1)}) \mid h_{c^{(d_2)}} \in H_{2k_2}, wt(c^{(d_1)}) \leq t, wt(c^{(d_2)}) > t\} \subset \mathbb{B}_{\frac{n}{2}+k_2}.$$

Moreover, let $c^{(n/2)} = (c^{(m_2+k_2)}, \alpha^{(k_2)}) \in GF(2)^{n/2}$, and define

$$I_1 = \{g_{c^{(n/2)}}(X^{(n/2)}) = c^{(n/2)} \cdot X^{(n/2)} \mid wt(c^{(m_2+k_2)}) \leq t, wt(c^{(n/2)}) > t\} \subset \mathbb{B}_{\frac{n}{2}}.$$

Then $I_0^{(1)} \cup I_0^{(2)} \cup I_1$ is a set of non-overlap spectra functions.

Proof. From Lemma 1, we know that $I_0^{(1)}, I_0^{(2)}$ and I_1 are all sets of disjoint spectra functions. Let $\omega^{(n/2+k_i)} = (\theta, \eta) \in GF(2)^{n/2+k_i}$, where $\theta \in GF(2)^{m_i+k_i}$, and $\eta \in GF(2)^{2k_i}, (i = 1, 2)$. Then, denoting by $X_1^i = X^{(m_i+k_i)}$ and $X_2^i = X^{(n/2+k_i)}_{(m_i+k_i+1)}$ for all $\omega^{(n/2+k_i)}$, we have

$$\begin{aligned} W_{\varphi_{c^{(m_i+k_i)}}}(\omega^{(n/2+k_i)}) &= \sum_{(X_1^i, X_2^i) \in GF(2)^{n/2+k_i}} (-1)^{c^{(m_i+k_i)} \cdot X_1^i \oplus h_{c^{(m_i+k_i)}}(X_2^i) \oplus \omega^{(n/2+k_i)} \cdot (X_1^i, X_2^i)} \\ &= \sum_{X_1^i \in GF(2)^{m_i+k_i}} (-1)^{(c^{(m_i+k_i)} \oplus \theta) \cdot X_1^i} \sum_{X_2^i \in GF(2)^{2k_i}} (-1)^{h_{c^{(m_i+k_i)}}(X_2^i) \oplus \eta \cdot X_2^i}. \end{aligned}$$

Moreover,

$$W_{\varphi_{c^{(m_i+k_i)}}}(\omega^{(n/2+k_i)}) = \begin{cases} 0, & (c^{(m_i+k_i)} \neq \theta) \\ \pm 2^{m_i+k_i} \times 2^{k_i} = \pm 2^{n/2}, & (c^{(m_i+k_i)} = \theta). \end{cases} \quad (20)$$

On the other hand, for the functions in I_1, for all $\omega^{(n/2)} \in GF(2)^{n/2}$, if $W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) \neq 0$ then $W_{g_{c^{n/2}}}(\omega^{(n/2)}) = 2^{n/2}$.

Let now $\omega^{(n/2+k_i)} = (\omega^{(n/2)}, \alpha) \in GF(2)^{n/2+k_i}$, $\omega^{(n/2)} = (\theta, \beta) \in GF(2)^{n/2}$, $\alpha \in GF(2)^{k_i}$, and $\beta \in GF(2)^{k_i}$. From (15) and (17), if $W_{\varphi_\theta}(\omega^{(n/2+k_i)}) \neq 0$, then we have $wt(\theta) > t$. It directly

means that

$$\begin{aligned} W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) &= \sum_{X^{(n/2)}\in GF(2)^{n/2}} (-1)^{c^{(n/2)}\cdot X^{(n/2)}\oplus \omega^{(n/2)}\cdot X^{(n/2)}} \\ &= \sum_{X^{(n/2)}\in GF(2)^{n/2}} (-1)^{(c^{(m_i+k_i)},\alpha)\cdot X^{(n/2)}\oplus(\theta,\beta)\cdot X^{(n/2)}} \\ &= \sum_{X^{(m_i+k_i)}\in GF(2)^{m_i+k_i}} (-1)^{(c^{(m_i+k_i)}\oplus\theta)\cdot X^{(m_i+k_i)}} \sum_{X^{(n/2)}_{(m_i+k_i+1)}\in GF(2)^k} (-1)^{(\alpha\oplus\beta)\cdot X^{(n/2)}_{(m_i+k_i+1)}}. \end{aligned}$$

Because $wt(c^{(m_i+k_i)}) \le t$ and $wt(\theta) > t$, thus $c^{(m_i+k_i)} \neq \theta$, we always have $W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) = 0$, i.e., $W_{\varphi_\theta}(\omega^{(n/2+k_i)}) \times W_{g_{c^{(n/2)}}}(\omega^{(n/2)}) = 0$. Therefore, $I_0^{(1)} \cup I_0^{(2)} \cup I_1$ is a set of non-overlap spectra functions. □

Lemma 4 *With the same notations as in Lemma 3, let*

$$U_0 = \{c^{(n/2)} \cdot X^{(n/2)} \mid c^{(n/2)} \in GF(2)^{n/2}, wt(c^{(n/2)}) > t\} \subset \mathbb{B}_{\frac{n}{2}}.$$

Then, the following equation is satisfied

$$\mu \times 2^{n/2} = \delta_0^{(1)} \times 2^{n/2+k_1} + \delta_0^{(2)} \times 2^{n/2+k_2} + \delta_1 \times 2^{n/2}, \tag{21}$$

where $\mu = ||U_0||$, $\delta_0^{(i)} = ||I_0^{(i)}||, i = (1,2)$, *and* $\delta_1 = ||I_1||$.

Proof. Using a similar method as in Lemma 2 the result easily follows. □

Example 3 *Let* $n = 16, m_1 = 2, k_1 = 3, m_2 = 4, k_2 = 2, t = 1$. *Denoting* $X_2^1 = (x_6, \ldots, x_{11}) \in GF(2)^6$ *and* $X_2^2 = (x_7, \ldots, x_{10}) \in GF(2)^4$ *we define*

$$I_0^{(1)} = \{\varphi_{c^{(5)}}(X^{(5)}, X_2^1) = c^{(5)} \cdot X^{(5)} \oplus h_{c^{(5)}}(X_2^1) \mid h_{c^{(5)}} \in H_6, wt(c^{(5)}) > 1\} \subset \mathbb{B}_{11},$$

where H_6 *is a nonempty set of* 6*-variable bent functions with algebraic degree 3.*
Moreover, let $c^{(6)} = (c^{(5)}, \alpha_1) \in GF(2)^6, \alpha_1 \in GF(2)$, *and define*

$$I_0^{(2)} = \{\varphi_{c^{(6)}}(X^{(6)}, X_2^2) = c^{(6)} \cdot X^{(6)} \oplus h_{c^{(6)}}(X_2^2) \mid h_{c^{(6)}} \in H_4, wt(c^{(5)}) \le 1, wt(c^{(6)}) > 1\} \subset \mathbb{B}_{10}.$$

Let $c^{(8)} = (c^{(6)}, \alpha^{(2)}) \in GF(2)^8, \alpha^{(2)} \in GF(2)^2$, *and define*

$$I_1 = \{g_{c^{(8)}}(X^{(8)}) = c^{(8)} \cdot X^{(8)} \mid wt(c^{(6)}) \le 1, wt(c^{(8)}) > 1\} \subset \mathbb{B}_8.$$

Then, $I_0^{(1)} \cup I_0^{(2)} \cup I_1$ *is a set of non-overlap spectra functions, where*

$$||I_0^{(1)}|| = \delta_0^{(1)} = 26, ||I_0^{(2)}|| = \delta_0^{(2)} = 5, ||I_1|| = \delta_1 = 19.$$

Moreover, consider $U_0 = \{c^{(8)} \cdot X^{(8)} \mid c^{(8)} \in GF(2)^8, wt(c^{(8)}) > 1\}$ *for which* $||U_0|| = \mu = 247$. *From Lemma 4, we have* $\mu \times 2^8 = 247 \times 2^8$, *and* $\delta_0^{(1)} \times 2^{11} + \delta_0^{(2)} \times 2^{10} + \delta_1 \times 2^8 = 26 \times 2^{11} + 5 \times 2^{10} + 19 \times 2^8 = 247 \times 2^8$. *This means that* $\mu \times 2^8 = \delta_0^{(1)} \times 2^{11} + \delta_0^{(2)} \times 2^{10} + \delta_1 \times 2^8$. *Note that the set* $I_0 \cup I_1$ *in Example 2 contains 39 linear 8-variable Boolean functions, whereas* $I_0^{(1)} \cup I_0^{(2)} \cup I_1$ *only contains* 19 *linear functions in 8 variables. In particular,* $I_0^{(1)} \cup I_0^{(2)} \cup I_1$ *includes two types of nonlinear functions, i.e., 26 nonlinear 11-variable functions and 5 nonlinear 10-variable functions.*

Remark 1 *Using a similar design of the set of non-overlap spectra functions* $I_0^{(1)} \cup I_0^{(2)} \cup I_1$, *we may further obtain a general set of non-overlap spectra functions* $\bigcup_{i=0}^{\ell} I_0^{(i)} \cup I_1$ *if there are some integers* $m_i, k_i, (i = 1, \ldots, \ell)$ *satisfying the conditions below.*

(1) $m_i + 2k_i = n/2, (i = 1, \ldots, \ell)$.

(2) $m_1 + k_1 < m_2 + k_2 < \cdots < m_\ell + k_\ell$.

5 Design methods based on non-overlap spectra functions

In this section, we propose new construction methods for obtaining resilient functions with strictly almost optimal nonlinearity based on the set of non-overlap spectra functions.

The first construction method uses a similar strategy as Construction A, where the main distinction between the two classes is in terms of quite a different structure of the subfunctions. More precisely, in this new construction, the set of functions U_0 used in Construction A is replaced by the set $I_0 \cup I_1$ of non-overlap spectra functions whereas the other subfunctions remain the same. Due to the limited space, we only provide the following example which illustrates the differences between the structure of their subfunctions.

Example 4 *Let us construct an* $(n = 16, t = 1, d = 10, N_f = 2^{15} - 2^7 - 2^5)$ *function* f, *which is not equivalent (in terms of its constituent subfunctions) to any function obtained by means of Construction A.*

With the same notation as in Example 2, let $n = 16, m = 2, k = 3, t = 1$. *Let* $s = \lfloor (n - 2t - 2)/4 \rfloor = 3$, $X_2 = (x_6, \ldots, x_{11}) \in GF(2)^6$, *and define*

$$I_0 = \{\varphi_c(X^{(5)}, X_2) = c^{(5)} \cdot X^{(5)} \oplus h_c(X_2) \mid h_c \in H_6, wt(c^{(5)}) > 1\} \subset \mathbb{B}_{11}.$$

Let $c^{(8)} = (c^{(5)}, \alpha^{(3)}) \in GF(2)^8, \alpha^{(3)} \in GF(2)^3$, *and define*

$$I_1 = \{g_{c^{(8)}}(X^{(8)}) = c^{(8)} \cdot X^{(8)} \mid wt(c^{(5)}) \leq 1, wt(c^{(8)}) > 1\} \subset \mathbb{B}_8.$$

Finally, we define a set of quadratic functions which are partially bent as

$$U_2 = \{c^{(4)} \cdot X^{(4)} \oplus h_c(x_5, \ldots, x_8) \mid h_c \in H_4, wt(c^{(4)}) > 1\}.$$

One can easily verify that $||I_0|| = \delta_0 = 26$, $||I_1|| = \delta_1 = 39$, $||U_2|| = 11$. *These functions suffice to specify the truth table of* f *since* $26 \times 2^3 + 39 + 11 = 258 > 2^{16/2}$, *where we treat the functions from* I_0 *as concatenation of* 2^3 *functions in* $n/2 = 8$ *variables which explains the factor* 2^3. *The design procedure is quite similar to Construction A and for self-completeness we briefly*

Table 1: The subfunctions of h_1 obtained by fixing the variables (x_9, x_{10}, x_{11})

(x_9, x_{10}, x_{11})	Subfunctions
(0,0,0)	$x_6x_7x_8 \oplus x_6x_8$
(1,0,0)	$x_6x_7x_8 \oplus x_6x_8 \oplus x_6$
(0,1,0)	$x_6x_7x_8 \oplus x_6x_8 \oplus x_7$
(0,0,1)	$x_6x_7x_8 \oplus x_6x_8 \oplus x_8$
(1,1,0)	$x_6x_7x_8 \oplus x_6x_8 \oplus x_6 \oplus x_7$
(1,0,1)	$x_6x_7x_8 \oplus x_6x_8 \oplus x_6 \oplus x_8$
(0,1,1)	$x_6x_7x_8 \oplus x_6x_8 \oplus x_7 \oplus x_8$
(1,1,1)	$x_6x_7x_8 \oplus x_6x_8 \oplus x_6 \oplus x_7 \oplus x_8$

discuss the structure of f. Since the variables $x_1, \ldots, x_{11}$ are used to define functions in I_0, the remaining (addressing) variables $x_{12}, \ldots, x_{16}$ are used to specify 26 functions in $x_1, \ldots, x_{11}$ from I_0. Formally, we can take $D_0 = \{d_1, \ldots, d_{26}\}$ to be any subset of $GF(2)^5$ and some one-to-one mapping $\phi : D_0 \to I_0$, meaning that to each of 26 fixed values of $x_{12}, \ldots, x_{16}$ we assign a single function from I_0. However, there are 6 entries that remain to be specified, i.e., we need to specify 6 functions in 11 variables to fully specify the truth table of f. This is equivalent to specifying 48 functions in 8 variables and since $||I_1|| + ||U_2|| = 50$, we can assign some arbitrary subset of cardinality 48. Therefore, there exists an injective mapping ψ from D_1 to $I^* \subset I_1 \cup U_2$, where $D_1 = \{\zeta_1, \ldots, \zeta_{48}\}$ is any subset of $\overline{D_0} \times GF(2)^3$, and $\overline{D_0} = GF(2)^5 \backslash \{D_0\}$, $||I^*|| = 48$. Similarly to Construction A, we obtain an $(n = 16, t = 1, d = 10, N_f = 2^{15} - 2^7 - 2^5)$ resilient function $f \in \mathbb{B}_{16}$ whose ANF is given as,

$$f(X) = \sum_{\sigma \in D_0} \prod_{i=12}^{16} (x_i \oplus \sigma_i \oplus 1) \cdot \phi(\sigma)(x_1, \ldots, x_{11}) \oplus \sum_{\tau \in D_1} \prod_{i=9}^{16} (x_i \oplus \tau_i \oplus 1) \cdot \psi(\tau)(x_1, \ldots, x_8).$$

In particular, let the bent function h_1 in I_0 be given as $h_1 = x_6x_9 \oplus x_7x_{10} \oplus x_8x_{11} \oplus x_6x_7x_8 \oplus x_6x_8$ and let the bent function in U_2 be $h_2 = x_5x_6 \oplus x_7x_8$. Then, we can easily verify that this resilient function differs substantially from any function obtained by Construction A. More precisely, if variables (x_9, x_{10}, x_{11}) are fixed, then h_1 gives rise to different non-affine subfunctions , as described in Table 1. It implies that we necessarily have that $U_0 \neq I_0 \cup I_1$ once we fix the variables (x_9, x_{10}, x_{11}), where $U_0 = \{c^{(8)} \cdot X^{(8)} \mid wt(c^{(8)}) > 1\}$. Therefore, this resilient function cannot be obtained by Construction A and in addition it has a more favorable algebraic structure.

Remark 2 *Using a similar idea as in [24, 41], the functions above can be turned into degree optimized resilient functions (providing a more favorable algebraic structure) with SAO nonlinearity by adding suitable monomials to some subfunctions in I_0. In addition, our method can be extended to employ $I_0^{(1)} \cup I_0^{(2)} \cup I_1$ in Lemma 3 instead of $I_0 \cup I_1$, thus further extending this class of SAO resilient functions.*

5.1 Towards better algebraic properties - using less $n/2$-variable affine functions

In [40], it was noticed that the GMM design method described by means of Construction B suffers from rather poor resistance against (fast) algebraic attacks. The main reason is the use

of "too many" affine functions in $n/2$ variables for the purpose of attaining the best nonlinearity currently known. Consequently, Construction B was slightly modified in [40] not to include "too many" affine functions in $n/2$ variables and it could be demonstrated that the modified class was more resistant to (fast) algebraic attacks at the price of slightly decreased nonlinearity. To increase the resistance to (fast) algebraic attacks we replace a subset of $n/2$-variable affine subfunctions in Theorem 1 by a set of non-overlap spectra functions in less variables, thus again achieving a more desirable nonlinear structure of the corresponding subfunctions. For convenience of the reader, the details of this approach are illustrated in the example below. The enumerated list of design steps is also used in Theorem 2, though in a more general context.

Example 5 *We illustrate the design of an* $(n = 14, t = 1, d = 12, N_f = 2^{13} - 2^6 - 2^4 - 2^3 - 2^2)$ *degree optimized resilient function* f*, which is completely different from the class in [40], [41].*

(1) Let $m = 1, k = 3$*,* $X^{(4)} \in GF(2)^{m+k} = GF(2)^4, X_2 = (x_5, \ldots, x_{10}) \in GF(2)^{2k} = GF(2)^6$ *and define*

$$I_0 = \{\varphi_c(X^{(4)}, X_2) = c^{(4)} \cdot X^{(4)} \oplus h_c(X_2) \mid h_c \in H_6, wt(c^{(4)}) > 1\} \subset \mathbb{B}_{10}.$$

Clearly, $||I_0|| = \delta_0 = 11$ *and these functions cover* 11×2^{10} *entries of the truth table of* f *of length* 2^{14}*. We now select available 1-resilient linear functions from* $\mathbb{B}_7$ *of the following form. Namely, for* $c^{(7)} = (c^{(4)}, \alpha^{(3)}) \in GF(2)^7$ *we define*

$$I_1 = \{c^{(7)} \cdot X^{(7)} \mid wt(c^{(4)}) \leq 1, wt(c^{(7)}) > 1\} \subset \mathbb{B}_7,$$

which is of cardinality 32.
(2) The two sets I_0 *and* I_1 *cover* $11 \times 2^{10} + 32 \times 2^7 = 15 \times 2^{10}$ *positions of the truth table. Thus, the remaining* 2^{10} *positions need to be specified through a selection of suitable linear functions in smaller number of variables. The use of 1-resilient linear functions from smaller variable spaces is governed formally by equation (24) in Theorem 2. The remaining* 2^{10} *positions in the truth table of* f *can be (optimally) specified using the following sets of functions:*

$$\begin{aligned} D_9^* &= \{c^{(5)} \cdot X^{(5)} \mid wt(c^{(5)}) > 1\} \subset \mathbb{B}_5, \quad ||D_9^*|| = 26. \\ D_{10}^* &= \{c^{(4)} \cdot X^{(4)} \mid wt(c^{(4)}) > 1\} \subset \mathbb{B}_4, \quad ||D_{10}^*|| = 11. \\ D_{11}^* &= \{c^{(3)} \cdot X^{(3)} \mid wt(c^{(3)}) > 1\} \subset \mathbb{B}_3, \quad ||D_{11}^*|| = 2. \end{aligned}$$

It is readily verified that $26 \times 2^5 + 11 \times 2^4 + 2 \times 2^3 = 2^{10}$.
(3) Let $B_i \subseteq GF(2)^i$ *and* $B_i' = B_i \times GF(2)^{14-i}$*, for* $i \in \{4, 7, 9, 10, 11\}$*, such that* $\bigcup_{i=1}^{n-1} B_i' = GF(2)^n$ *and* $B_{i_1}' \cap B_{i_2}' = \emptyset$*,* $i_1, i_2 \in \{4, 7, 9, 10, 11\}$*, with* $i_1 \neq i_2$*. Thus,*

$$||B_i|| = \begin{cases} 11, & i = 4, \\ 32, & i = 7, \\ 26, & i = 9, \\ 11, & i = 10, \\ 2, & i = 11. \end{cases} \tag{22}$$

(4) Let ψ_i be injective mappings from B_i to T_i, where

$$T_i = \begin{cases} I_0, & i = 4, \\ I_1, & i = 7. \\ D_9^*, & i = 9, \\ D_{10}^*, & i = 10, \\ D_{11}^{**}, & i = 11. \end{cases} \quad (23)$$

These mappings simply specify which functions from T_i are used when a suitable subset of input variables is fixed. By Theorem 2, the Boolean functions

$$f(X^{(14-i)}, X^{(14)}_{(14-i+1)}) = \psi_i(X^{(14)}_{(14-i+1)}) \oplus g_i(X^{(14)}_{(14-i+1)}) = \psi_i^*(X^{(14-i)}) \oplus g_i(X^{(14)}_{(14-i+1)}),$$

are $(n = 14, t = 1, d = 12, N_f = 2^{13} - 2^6 - 2^4 - 2^3 - 2^2 = 8100)$ that are all degree optimized resilient functions, where $\psi_i(X^{(14)}_{(14-i+1)}) = \psi_i^*(X^{(14-i)}) \in T_i$, $X^{(14)}_{(14-i+1)} \in B_i, X^{(14)}_{(14-i+1)} = (x_{14-i+1}, \ldots, x_{14}) \in GF(2)^i, g_i \in \mathbb{B}_i$, $i \in \{4, 7, 9, 10, 11\}$. In particular, if the bent function in I_0 is $h_0 = (x_6 \oplus x_5x_7)x_8 \oplus (x_7 \oplus x_5x_6 \oplus x_5x_7)x_9 \oplus (x_5 \oplus x_5x_6 \oplus x_6x_7)x_{10}$, then (as previously discussed) we easily find that such a resilient function is substantially different compared to the class in [40], [41] since the subfunctions of I_0 are different from the subfunctions of U_0, where $U_0 = \{c^{(7)} \cdot X^{(7)} \mid wt(c^{(7)}) > 1\}$.

Remark 3 *Notice that the use of t-resilient linear functions in $n/2$ variables and those found on smaller variable spaces are in accordance with the non-overlap spectra property. The use of 6-variable linear functions is avoided due to their negative impact on the nonlinearity of f.*

Theorem 2 *With the same notation as in Construction B and Proposition 1, let n be even and $B_i \neq \emptyset$, $(1 \leq i \leq n/2 - k - 1)$. The design consists of the following steps:*

(1) Let $X^{(m+k)} \in GF(2)^{m+k}, X_2 = (x_{m+k+1}, \ldots, x_{n/2+k})) \in GF(2)^{2k}$, where $m + 2k = n/2$, and define

$$I_0 = \{\varphi_c(X^{(m+k)}, X_2) = c^{(m+k)} \cdot X^{(m+k)} \oplus h_c(X_2) \mid h_c \in H_{2k}, wt(c^{(m+k)}) > t\} \subset \mathbb{B}_{\frac{n}{2}+k}.$$

Moreover, let $c^{(n/2)} = (c^{(m+k)}, \alpha^{(k)}) \in GF(2)^{n/2}, \alpha \in GF(2)^k$, and define

$$I_1 = \{g_{c^{(n/2)}}(X^{(n/2)}) = c^{(n/2)} \cdot X^{(n/2)} \mid wt(c^{(m+k)}) \leq t, wt(c^{(n/2)}) > t\} \subset \mathbb{B}_{\frac{n}{2}}.$$

(2) Let $0 \leq t \leq n/2 - 2$ and $(a_{n/2}, \ldots, a_{n-t-1}) \in GF(2)^{n/2-t}$ (where $a_{n/2} = 1$) be the binary vector such that $\sum_{i=n/2}^{n-t-1} a_i 2^i$ is maximal, and

$$\delta_0 \times 2^{n/2+k} + \delta_1 \times 2^{n/2} + \sum_{i=n/2+1}^{n-t-1} \left(a_i 2^{n-i} \sum_{j=t+1}^{n-i} \binom{n-i}{j} \right) \geq 2^n, \quad (24)$$

where $\delta_i = ||I_i||, i = 0, 1$.

(3) Let $r = \max\{i \mid a_i \neq 0, n/2-k \leq i \leq n-t-1\}$. *For* $n/2-k \leq i < r-1$, *set*

$$||B_i|| = \begin{cases} 0 & (a_i = 0, n/2 < i < r-1), \\ \sum_{j=t+1}^{n-i} \binom{n-i}{j} & (a_i = 1, n/2 < i < r-1). \\ \delta_0 & (a_i = 1, i = n/2-k), \\ \delta_1 & (a_i = 1, i = n/2). \end{cases} \tag{25}$$

(4) For $n/2-k \leq i \leq r$ *and* $a_i = 1$, *let* ψ_i *be an injective mapping from* B_i *to* T_i,

$$T_i = \begin{cases} 0 & (a_i = 0, n/2 < i < r-1), \\ D_i^* & (a_i = 1, n/2 < i < r-1), \\ I_0 & (a_i = 1, i = n/2-k), \\ I_1 & (a_i = 1, i = n/2), \end{cases} \tag{26}$$

where

$$D_i^* = \{c^{(n-i)} \cdot X^{(n-i)} \mid wt(c) > t\}. \tag{27}$$

Then the Boolean function

$$f(X^{(n-i)}, X^{(n)}_{(n-i+1)}) = \psi_i(X^{(n)}_{(n-i+1)}) \oplus g_i(X^{(n)}_{(n-i+1)}) = \psi_i^*(X^{(n-i)}) \oplus g_i(X^{(n)}_{(n-i+1)}),$$

where $\psi_i(X^{(n)}_{(n-i+1)}) = \psi_i^*(X^{(n-i)}) \in T_i, X^{(n)}_{(n-i+1)} \in B_i, g_i \in \mathbb{B}_i$, $X^{(n-i)} = (x_1, \ldots x_{n-i}) \in GF(2)^{n-i}$, $X^{(n)}_{(n-i+1)} = (x_{n-i+1}, \ldots x_n) \in GF(2)^i$, *for* $n/2-k \leq i \leq r$, *is a SAO t-resilient function with nonlinearity*

$$N_f \geq 2^{n-1} - 2^{n/2-1} - \sum_{i=n/2+1}^{r} a_i 2^{n-i-1}. \tag{28}$$

Proof. For any $n/2-k \leq i \leq r$, if (24) is satisfied, then $||B_i|| \leq ||T_i||$. It means that there is a set of injective mappings ψ_i from B_i to T_i, with $n/2-k \leq i \leq r$ and $a_i = 1$. W.l.o.g, we assume $g_i = 0$. For any $w = (w_1, \ldots, w_n) = (w^{(n-i)}, w^{(n)}_{(n-i+1)}) \in GF(2)^n, w^{(n)}_{(n-i+1)} = (w_{n-i+1}, \ldots w_n) \in GF(2)^i$, we have

$$
\begin{aligned}
W_f(w) &= \sum_{X^{(n)} \in \bigcup_{i=n/2-k}^{r} B'_i} (-1)^{f(X^{(n)}) \oplus w \cdot X^{(n)}} \\
&= \sum_{X^{(n)} \in B'_{n/2-k}} (-1)^{f(X^{(n)}) \oplus w \cdot X^{(n)}} \oplus \sum_{X^{(n)} \in B'_{n/2}} (-1)^{f(X^{(n)}) \oplus w \cdot X^{(n)}} \oplus \cdots \oplus \sum_{X^{(n)} \in B'_{r}} (-1)^{f(X^{(n)}) \oplus w \cdot X^{(n)}} \\
&= \sum_{X^{(n)}_{(n/2+k+1)} \in B_{n/2-k}} (-1)^{w^{(n)}_{(n/2+k+1)} \cdot X^{(n)}_{(n/2+k+1)}} \sum_{X^{(n/2+k)} \in GF(2)^{n/2+k}} (-1)^{\psi^*_{n/2-k}(X^{(n/2+k)}) \oplus w^{(n/2+k)} \cdot X^{(n/2+k)}} \\
&\oplus \sum_{X^{(n)}_{(n/2+1)} \in B_{n/2}} (-1)^{w^{(n)}_{(n/2+1)} \cdot X^{(n)}_{(n/2+1)}} \sum_{X^{(n/2)} \in GF(2)^{n/2}} (-1)^{\psi^*_{n/2}(X^{(n/2)}) \oplus w^{(n/2)} \cdot X^{(n/2)}} \oplus \cdots \\
&\oplus \sum_{X^{(n)}_{(n-r+1)} \in B_r} (-1)^{w^{(n)}_{(n-r+1)} \cdot X^{(n)}_{(n-r+1)}} \sum_{X^{(n-r)} \in GF(2)^{n-r}} (-1)^{\psi^*_r(X^{(n-r)}) \oplus w^{(n-r)} \cdot X^{(n-r)}} \\
&= W_{f_{n/2-k}}(w) + \sum_{i=n/2}^{r} a_i \cdot W_{f_i}(w),
\end{aligned}
$$

where

$$
\begin{aligned}
W_{f_{n/2-k}}(w) = & \sum_{X^{(n)}_{(n/2+k+1)} \in B_{n/2-k}} (-1)^{w^{(n)}_{(n/2+k+1)} \cdot X^{(n)}_{(n/2+k+1)}} \\
& \times \sum_{X^{(n/2+k)} \in GF(2)^{n/2+k}} (-1)^{\psi^*_{n/2-k}(X^{(n/2+k)}) \oplus w^{(n/2+k)} \cdot X^{(n/2+k)}},
\end{aligned}
$$

and for $n/2-k \le i < r-1$, we have

$$
\begin{aligned}
W_{f_i}(w) &= \sum_{X^{(n)}_{(n-i+1)} \in B_i} (-1)^{w^{(n)}_{(n-i+1)} \cdot X^{(n)}_{(n-i+1)}} \sum_{X^{(n-i)} \in GF(2)^{n-i}} (-1)^{\psi^*_i(X^{(n-i)}) \oplus w^{(n-i)} \cdot X^{(n-i)}} \\
&= \begin{cases} (-1)^{w^{(n)}_{(n-i+1)} \cdot \psi_i^{*-1}(w^{(n-i)})} \cdot 2^{n-i} & \text{if } \exists \psi_i^{*-1}(w^{(n-i)}), \\ 0 & \text{otherwise.} \end{cases} \\
&= \begin{cases} \pm 2^{n-i} & \text{if } \exists \psi_i^{*-1}(w^{(n-i)}), \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}
$$

From Proposition 1, we have $W_{f_{n/2-k}}(w) + W_{f_{n/2}}(w) \in \{0, \pm 2^{n/2}\}$. Therefore, we have

$$
W_f(w) \le 2^{n/2} + \sum_{i=n/2+1}^{r} a_i 2^{n-i},
$$

and consequently $N_f \ge 2^{n-1} - 2^{n/2-1} - \sum_{i=n/2+1}^{r} a_i 2^{n-i-1}$. Note that any constituent function in $I_0 \cup I_1 \cup \bigcup_{l=n/2+1}^{r} D_i^*$ is always a t-resilient function, thus f is t-resilient as well. □

Corollary 2 *The functions $f \in \mathbb{B}_n$ obtained by Theorem 2 share the same nonlinearity as the functions obtained by Theorem 1.*

Proof. Let $U_0 = \{c^{(n/2)} \cdot X^{(n/2)} \mid wt(c^{(n/2)}) > 1\}$. From Lemma 2, we know that the number of elements contained in U_0 (cf. Theorem 1) is equal to the number of elements in $I_0 \cup I_1$ in Theorem 2. Moreover, the number of elements contained in D_i^* is equal to the number of elements contained in $U_i = \{c^{(n-i)} \cdot X^{(n-i)} \mid c^{(n-i)} \in D_i\}$, for $n/2 < i < r-1$. Therefore, the resilient functions in both Theorem 1 and 2 share the same parameter $(a_{n/2}, \ldots, a_{n-t-1}) \in GF(2)^{n/2-t}$. □

Remark 4 *One can easily verify that the functions obtained by Theorem 2 include the functions obtained by Theorem 1 as a subclass and the methods coincide only if h_c in I_0 is a Maiorana-McFarland type bent function. In addition, instead of using $I_0 \cup I_1$ we can alternatively use the set $I_0^{(1)} \cup I_0^{(2)} \cup I_1$ in Theorem 2, given in Lemma 3.*

5.2 Comparisons regarding the resistance against (fast) algebraic attacks

In Appendix A, the resistance of our functions against (fast) algebraic attacks is discussed. In general, it is shown that the new functions have a better resistance against (fast) algebraic attacks than the class of functions in [40, 41], see Appendix A for further details.

In Table 2, we compare the resistance against (fast) algebraic attacks between our class and the functions in [40, 41] for 12-variable and 14-variable functions. Once again, we emphasize that our class of functions uses a large set of non-overlap spectra functions $I_0 \cup I_1$ rather than a large set of $\frac{n}{2}$-variable affine subfunctions $U_0 = \{c^{(n/2)} \cdot X^{(n/2)} \mid wt(c^{(n/2)}) > 1\}$ as in [40, 41]. Notice also that except for the subfunctions derived from the set $I_0 \cup I_1$, our functions share the same subfunctions and injective methods as the functions in [40, 41]. Due to space constraints, the truth tables of these functions in Table 2 are omitted. Table 2 shows that the new functions provide a better resistance against algebraic attacks than the functions in [40, 41], whereas the nonlinearity and the other parameters of interest remain the same.

Table 2: Comparisons (simulation) regarding the resistance against (fast) algebraic attacks.

n	Resiliency	$\deg(f)$	N_f	AI	$\deg g + \deg h$	Constructions
12	1	8	2000	4	≥ 6	[40],[41]
12	1	8	2000	5	≥ 7	*new*
14	1	12	8100	4	≥ 6	[40]
14	1	12	8100	6	≥ 8	*new*

For instance, an 14-variable function f from [40] only have $AI = 4$ whereas our function attains $AI = 6$. Moreover, when the fast algebraic cryptanalysis is considered, there exist Boolean functions g and h such that $fg = h$ with $\deg(g) + \deg(h) = e + d \geq 6$, for a function f constructed using the method of [40]. However, our method generates a function f' in 14 variables which has $AI = 6$ and there exist Boolean functions g' and h' such that $f'g' = h'$ with $\deg(g') + \deg(h') = e + d \geq 8$, implying that our functions have better resistance against (fast) algebraic attacks even though no modification towards better algebraic properties has been

done. Also, the resistance to various cryptanalytic methods that take advantage of linearity of subfunctions is increased by avoiding the usage of $\frac{n}{2}$-variable affine functions due to the availability of a large set of non-overlap spectra functions, see Section 5.5.

5.3 Balanced (or 1-resilient) functions with good algebraic properties

In this section we demonstrate the possibility of constructing highly nonlinear balanced (or 1-resilient) Boolean functions with good algebraic properties by using nonlinear subfunctions whose number of variables is $\leq \frac{n}{2}$. We firstly provide some existence examples of functions with overall good properties, which are found using computer search for optimal choice of nonlinear subfunctions ($\leq \frac{n}{2}$ -variable), affine subfunctions ($\leq \frac{n}{2}$-variable), and their number for different dimensions. Moreover, we later discuss a semi-deterministic method for designing balanced (or 1-resilient) Boolean functions satisfying all relevant cryptographic criteria.

A. Some new 8-variable and 10-variable 1-resilient functions with overall good properties

In Table 3 we give an example of a balanced 8-variable function (using Theorem 2 thus without the marked terms $\underbrace{*****}$), which consists of three 6-variable nonlinear subfunctions that strictly belong to the set of non-overlap spectra functions, two 4-variable linear subfunctions, and four 3-variable linear subfunctions, i.e., the space decomposition satisfies $3\times 2^6+2\times 2^4+4\times 2^3=2^8$. This function has $AI=4$, $\deg(f)=6$, its nonlinearity is $N_f=112$. Moreover, for any given nonzero Boolean functions h and g such that $f(x)g(x)=h(x)$ we have $\deg(g)+\deg(h)\geq 6$, which implies that f has almost optimal resistance to fast algebraic cryptanalysis.

Table 3: A balanced 8-variable function with overall good properties.

$(x_1,\cdots,x_6)$	(x_7,x_8)
$x_1\oplus x_3x_4\oplus x_3x_5\oplus x_5x_6\underbrace{\oplus x_2x_3x_4\oplus x_3x_4x_5}$	(0, 0)
$x_2\oplus x_4\oplus x_6\oplus x_3x_4\oplus x_5x_6\underbrace{\oplus x_1x_4x_5\oplus x_1x_3x_5x_6}$	(1, 0)
$x_1\oplus x_2\oplus x_3x_4\oplus x_5x_6\oplus x_4x_6\underbrace{\oplus x_4x_5x_6\oplus x_3x_4x_5x_6}$	(0, 1)
$(x_1,\cdots,x_4)$	(x_5,x_6,x_7,x_8)
$x_3\oplus x_4$	(0, 1, 1, 1)
$x_1\oplus x_2\oplus x_3\oplus x_4$	(1, 1, 1, 1)
(x_1,x_2,x_3)	(x_4,x_5,x_6,x_7,x_8)
$x_1\oplus x_2$	(0, 0, 0, 1, 1)
$x_1\oplus x_3$	(1, 0, 0, 1, 1)
$x_2\oplus x_3$	(0, 1, 0, 1, 1)
$x_1\oplus x_3$	(1, 1, 0, 1, 1)

To further improve the resistance of this function against fast algebraic attacks, we add the marked terms $\underbrace{*****}$, see Table 3, and denote this new function by f^*. It can be verified that f^* has $AI=4$, $\deg(f^*)=6$, its nonlinearity is $N_{f^*}=108$ and $\deg(g)+\deg(h)=e+d\geq n-1=7$ for any given nonconstant Boolean functions g and h such that $f(x)g(x)=h(x)$. Moreover, this function f^* can be linearly transformed into a 1-resilient function f^{**} (since there are eight linearly independent vectors ω such that $W_f(\omega)=0$) that preserves all the properties above.

Table 4: A new 1-resilient 8-variable function with overall good cryptographic properties.

(x_1, x_2, x_3, x_4)	(x_5, x_6, x_7, x_8)
$1 \oplus x_1 \oplus x_2 \oplus x_4 \oplus x_1x_3 \oplus$ $x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_2x_3x_4$	(0, 0 , 0 ,0)
$1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus$ $x_3x_4 \oplus x_2x_3x_4$	(0, 0 , 0 , 1)
$1 \oplus x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_4 \oplus$ $x_2x_4 \oplus x_3x_4 \oplus x_1x_3x_4$	(0, 0 , 1 , 0)
$x_1 \oplus x_2 \oplus x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus$ $x_1x_3x_4 \oplus x_2x_3x_4$	(0, 0 , 1 , 1)
$x_1 \oplus x_3 \oplus x_1x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_4 \oplus$ $x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	(0, 1 , 0 , 0)
$x_1 \oplus x_1x_2 \oplus x_4 \oplus x_1x_4 \oplus$ $x_1x_2x_4 \oplus x_3x_4$	(0, 1 , 0 , 1)
$1 \oplus x_1 \oplus x_1x_2 \oplus x_3 \oplus x_1x_3 \oplus x_1x_2x_3 \oplus$ $x_1x_4 \oplus x_2x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	(0, 1 , 1 , 0)
$1 \oplus x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus$ $x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$	(0, 1 , 1 , 1)
$1 \oplus x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus$ $x_1x_2x_4 \oplus x_3x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$	(1, 0 , 0 , 0)
$x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_2x_3 \oplus x_1x_4 \oplus$ $x_2x_4 \oplus x_3x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$	(1, 0 , 0 , 1)
$1 \oplus x_2 \oplus x_3 \oplus x_1x_3 \oplus x_4 \oplus x_3x_4 \oplus$ $x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	(1, 0 , 1 , 0)
$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_3 \oplus x_1x_3 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus$ $x_1x_2x_4 \oplus x_3x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	(1, 0 , 1 , 1)
$x_1 \oplus x_2 \oplus x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus x_4 \oplus x_1x_4 \oplus$ $x_2x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_1x_2x_3x_4$	(1, 1 , 0 , 0)
$1 \oplus x_2 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_4 \oplus x_1x_4 \oplus$ $x_2x_4 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$	(1, 1 , 0 , 1)
$x_2 \oplus x_1x_2 \oplus x_1x_2x_4$	(1, 1 , 1 , 0)
$x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus$ $x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	(1, 1 , 1 , 1)

The truth table of f^{**} is given below:
0011 1001 1100 0011 0110 1001 1001 0011 0011 1001 1100 0011 1001 0110 0110 1100 0101 0000 1010 1111 0101 1100 1010 1100 1010 1111 0101 0000 0100 1000 1110 1101 0110 0011 0110 0011 0110 0011 0110 0011 0110 1100 0110 1100 1001 1001 1001 1001 0110 0110 1001 0110 0110 1111 1001 0000 0101 1010 0101 1010 0011 1100 0011 1100

Nevertheless, further improvements are possible as indicated in Table 4, where another example of a 1-resilient 8-variable function is given. This function has $AI = 4$, $\deg(f) = 6$, its nonlinearity is $N_f = 116$, and $\deg(g)+\deg(h) = e+d \geq n-1 = 7$ for any given nonzero Boolean functions h and g such that $f(x)g(x) = h(x)$. The truth table of this 1-resilient function f^* is given below:
1001 1111 0010 1000 1001 0110 0110 0101 1100 1011 1010 0111 0110 1110 0110 1000 0101 1011 0001 1000 0100 0100 1111 0000 1011 0000 1101 0100 1011 1100 1010 1011 1000 1011 1100 0110 0100 0000 0010 1111 1100 0110 0011 0001 0111 1100 0101 0110 0110 1011 1110 1101 1101 1011 0101 0101 0010 0010 0011 0011 0000 0101 0111 1010

We also provide an example of a 1-resilient 10-variable function with excellent algebraic properties (whose truth table is given in the hexadecimal format):
0cc3 c0f6 2354 dced 0565 307c 1d4d f792 fbab 67c4 257c 3213 4640 d49a b604 953d 5dfd a5c6 9ad4 cbbb 887f 2751 bc21 2876 4819 dcfe db14 920c 992a 2c8a e37f a6f8 1524 e757 eb0f a0d8 96ae 8308 f34b 5a5f 3148 99e8 1f12 0f84 f69b f31f 3eae c77a b851 d671 57c9 ae89 98cf 1c1a 670b 003a 217d 7ad9 70c9 7a08 f0a7 daa9 a276 6138.

This 1-resilient function has $AI = 5$, $\deg(f) = 8$, its nonlinearity is $N_f = 484$, and $\deg(g) + \deg(h) = e + d \geq n - 1 = 9$ for any given nonconstant h and g such that $f(x)g(x) = h(x)$.

Table 5: A comparison related to 1-resilient functions with overall good properties.

n	Resiliency	$deg(f)$	N_f	AI	deg g + deg h	$\frac{n}{2}$-variable subfunctions	Resource
8	1	6	112	4	$\geq n-1=7$	linear	[40]
8	1	6	112	4	–	–	[32]
8	1	6	116	4	$\geq n-1=7$	–	[38]
8	1	6	116	4	$\geq n-1=7$	nonlinear	*new*
10	1	8	472	5	$\geq n-1=9$	linear	[40]
10	1	8	484	5	–	–	[32]
10	1	8	484	5	$\geq n-1=9$	–	[38]
10	1	8	484	5	$\geq n-1=9$	nonlinear	*new*

Remark 5 *In difference to the class of 8-variable and 10-variable functions in [40], these new functions use many nonlinear subfunctions in $n/2$ variables rather than affine $n/2$-variable subfunctions, see Table 5. It is worthy of noticing that, based on our simulations, the placement order of these subfunctions does not impact the algebraic properties of designed functions. The resistance to fast algebraic attacks for the method in [32, 33] is most likely quite bad given by $\deg(g) + \deg(h) = n/2 + 1$, as remarked in [4] for a similar class of functions derived from bent functions in the partial spread class.*

B. A semi-deterministic method for designing balanced (or 1-resilient) Boolean functions with good algebraic properties

The construction of balanced highly nonlinear Boolean functions with good algebraic properties has been addressed in many works [6, 18, 30, 31, 34, 35, 44]). To achieve relatively good resistance against (fast) algebraic attacks, Zhang *et al.* [40] proposed a modified construction of the original approach which uses $2^{\frac{n}{2}-1}$ affine subfunctions in $n/2$ variables from U_0. More precisely, the space decomposition satisfies $2^{\frac{n}{2}-1} \times 2^{\frac{n}{2}} + 2^{\frac{n}{2}-1} \times 2^{\frac{n}{2}-1} + 2^{\frac{n}{2}} \times 2^{\frac{n}{2}-2} = 2^n$ which implies that "only" $2^{\frac{n}{2}-1}$ many affine functions in $n/2$ variables are used in the design. However, using the algorithm for testing the algebraic properties proposed in [36], we can demonstrate that this class of functions does not have an optimal resistance against fast algebraic attacks. For instance, if $n = 20$ and f is constructed by means of the method in [40], using this algorithm we find that there exist nonzero Boolean functions g and h satisfying $\deg(g) + \deg(h) = e + d = 15$ (where $fg = h$). This discrepancy (between the optimal value $n-1$ and the actual value $e+d$) is even larger for the increased input space n and therefore the resistance of the class of functions in [40] against fast algebraic attacks is far from being optimal.

Similarly, a trade-off between the nonlinearity and the resistance against (fast) algebraic attacks of our initial SAO functions has been confirmed by simulations, as in the case of the GMM construction [40]. To achieve good algebraic properties, we need to slightly decrease the nonlinearity of our initial constructions. The main idea is to look for a suitable/optimal space decomposition whose choice usually affects both the algebraic properties and nonlinearity of the designed functions. In fact, the Condition 0, Condition 1, and Condition 2 in [36] essentially provide an approach to estimate the algebraic properties of designed functions. Therefore, to achieve an optimal resistance against (fast) algebraic attacks and high nonlinearity, our design strategy includes two phases. In the first phase, we need to search for a suitable space decomposition that ensures optimal algebraic properties by using the Condition 0, Condition 1, and Condition 2 given in [36]. In the second phase, we employ the ideas of Construction 2 to specify the corresponding functions. The details of this approach are given below.

Construction C: (With the same notation as in Construction B and Theorem 2).

The first phase:
Step 1 For a given integer n, $n \geq 12$ even, solve the equation $\sum_{i=\frac{n}{2}+1}^{n-1} ||B_i|| \times 2^{n-i} = 2^n$ to obtain all solutions $B^{(j)} = \{B^{(j)}_{\frac{n}{2}+1}, \ldots, B^{(j)}_{n-1}\}$.
Step 2 For each solution $B^{(j)}$, calculate $r+d$ and $r+s+e$ (related to AA and FAA) by using the Condition 0, Condition 1, and Condition 2 in [36]. If $r+d = \lceil n/2 \rceil$ and $r+s+e \geq n-1$, then record the solution $B^{(j)} = \{B^{(j)}_{\frac{n}{2}+1}, \ldots, B^{(j)}_{n-1}\}$.
Step 3 Call these solutions $B^{(1)}, B^{(2)}, \ldots, B^{(u)}$.

Remark that the relations $r+d = \lceil n/2 \rceil$ and $r+s+e \geq n-1$ in Step 2 ensure the optimal resistance against (fast) algebraic attacks.

The second phase:
(1) Select an optimal solution w.r.t. the highest nonlinearity given by (30), say $B^{(\lambda)}$, $1 \leq \lambda \leq u$. Let $a_i = 1$, if $B_i^{(\lambda)} \neq 0$, or else $a_i = 0$, for $i = \frac{n}{2}+1, \ldots, n-1$.
(2) For $\frac{n}{2} < i \leq n-1$ and $a_i = 1$, let ψ_i be a mapping from B_i to T_i, where

$$T_i = \{c^{(n-i)} \cdot X^{(n-i)} \mid wt(c^{(n-i)}) > 0\}. \tag{29}$$

Then the Boolean function

$$f(X^{(n-i)}, X^{(n)}_{(n-i+1)}) = \psi_i(X^{(n)}_{(n-i+1)}) \oplus g_i(X^{(n)}_{(n-i+1)}) = \psi_i^*(X^{(n-i)}) \oplus g_i(X^{(n)}_{(n-i+1)}),$$

where $X^{(n)}_{(n-i+1)} \in B_i, X^{(n)}_{(n-i+1)} = (x_{n-i+1}, \ldots x_n) \in GF(2)^i$, $g_i \in \mathbb{B}_i$ are arbitrary for $\frac{n}{2} < i \leq n-1$, is a balanced function with nonlinearity

$$N_f \geq 2^{n-1} - \sum_{l=n/2+1}^{n-1} a_l \times \mu_l \times 2^{n-l-1}, \tag{30}$$

where $\mu_l = \max_{y \in T_l} ||\{\psi_l^{-1}(y)\}||$, $(l = \frac{n}{2} + 1, \ldots, n-1)$.

The result on nonlinearity can be easily derived using a similar method as in Theorem 2.

Remark 6 *To achieve high nonlinearity, we need to select an optimal solution $B^{(\lambda)}$ so that the value $\sum_{l=n/2+1}^{n-1} a_l \times \mu_l \times 2^{n-l-1}$ is as small as possible. On the other hand, it is impossible to provide the exact nonlinearity bound in advance since it depends on suitable decompositions for which the algebraic properties are simultaneously optimized (due to the selection in Step 2 in the first phase).*

The method given in Construction C allows us to design balanced Boolean functions having optimal algebraic properties and very high nonlinearity. To demonstrate the efficiency and quality of our approach we provide two examples (among many others) of one 12-variable and one 14-variable 1-resilient functions with overall good cryptographic properties, see Table 6. We only provide the truth table of this 12-variable function in Appendix. Notice that the space decomposition of this 12-variable 1-resilient function satisfies $31 \times 2^3 + 466 \times 2^2 + 992 \times 2 = 2^{12}$, that is, $||B_9|| = 31, ||B_{10}|| = 466, ||B_{11}|| = 992$, and $||B_i|| = 0$ for $i \neq 9, 10, 11$. The space decomposition of the 14-variable 1-resilient function satisfies $1 \times 2^4 + 140 \times 2^3 + 1784 \times 2^2 + 4056 \times 2 = 2^{14}$, that is, $||B_{10}|| = 1, ||B_{11}|| = 140, ||B_{12}|| = 1784, ||B_{13}|| = 4056$, and $||B_i|| = 0$ for $i \neq 10, 11, 12, 13$.

Table 6: A comparison of 1-resilient functions satisfying all relevant cryptographic criteria.

n	Resiliency	$deg(f)$	N_f	AI	$\deg g + \deg h$	$\frac{n}{2}$-variable subfunctions	Resource
12	1	10	1960	6	$\geq n-2=10$	linear	[40]
12	1	10	1996	6	–	–	[32]
12	1	10	1988	6	$\geq n-1=11$	–	[38]
12	1	10	1988	6	$\geq n-1=11$	nonlinear	*new*
14	1	11	8040	7	$\geq n-3=11$	linear	[40]
14	1	12	8100	7	–	–	[32]
14	1	12	8072	7	$\geq n-1=13$	–	[38]
14	1	12	8072	7	$\geq n-1=13$	nonlinear	*new*

Remark 7 *In difference to the class of 12-variable and 14-variable functions in [40], these new functions use many nonlinear $n/2$-variable subfunctions. This also implies that these new functions have better resistance against (fast) algebraic attacks than the functions in [40]. On the other hand, the functions in [38] are obtained by using a search algorithm based on simulated annealing which quite likely becomes inefficient for larger n. The space decomposition of these functions and the type of subfunctions used there was not discussed in [38]. Nevertheless, the design of resilient functions with SAO nonlinearity and optimal (or suboptimal) resistance against (fast) algebraic attacks still remains an open problem.*

5.4 A comparison regarding the number of $n/2$-variable affine subfunctions

Table 7 below gives the exact value of the number of $n/2$-variable affine subfunctions used in our constructions and their number used in [40, 41], for $k \geq 2$. Notice that by letting $k = 1$

(recall that k is related to the set H_k of $2k$-variable bent functions, cf. Theorem 2), the number of $n/2$-variable affine subfunctions is minimal for both our methods since the effect of increasing k is that m decreases due to the relation $m + 2k = \frac{n}{2}$. In particular, when $k = 1$, the employed bent functions only have two variables (which are then essentially linear functions) so that our method coincides with the approach taken in [40]. Thus, we necessarily have that $k \geq 2$ in order to distinguish the two approaches.

Table 7: The cardinality of affine subfunctions in $n/2$ variables

Number of affine $n/2$-variable subfunctions	Construction
$\sum_{i=t+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{i}$ or $2^{\frac{n}{2}-1}$	[40]
$\sum_{i=t+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{i}$	[41]
$\sum_{i=t+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{i} - 2^k \times \sum_{i=t+1}^{m+k} \binom{m+k}{i}$	*new*

Note that the constructions in [40, 41], for the case $n = 28, t = 1$, require 16369 affine subfunctions in 14 variables, whereas our new construction requires at most 561 affine subfunctions in 14 variables if we consider $m = 2$ (and consequently $k = 6$). Moreover, taking $k = 2$, this number is further reduced and only 37 affine 14-variable subfunctions are needed. In other words, the number of $\frac{n}{2}$-dimensional subspaces/flats on which our functions are weakly normal (being affine on such a subspace/flat) is substantially reduced which potentially gives a better resistance to various cryptanalytic methods.

5.5 Comparisons regarding the resistance against both guess and determine cryptanalysis and (dynamic) cube attacks

Note that the attack complexity of both guess and determine cryptanalysis and (dynamic) cube attacks largely depends on the number of input variables that are kept fixed, say l, and the cardinality of induced partial linear relations ($n - l$ variables) which we denote by Δ. If l is relatively small and the cardinality of these partial linear relations is large enough, then these attacks generally become more efficient. To estimate the resistance against both guess and determine cryptanalysis and (dynamic) cube attacks, we introduce the concept of probability distribution of partial linear relations, which takes into account the above mentioned parameters l and Δ.

Definition 9 *For $f \in \mathbb{B}_n$, let the set of fixed input variables be $(x_{i_1}, \ldots, x_{i_l}), \{i_1, \ldots, i_l\} \subset \{1, \ldots, n\}$, and let the total cardinality of induced partial linear relations be Δ, when $(x_{i_1}, \ldots, x_{i_l})$ runs through $GF(2)^l$. The probability distribution of partial linear relations of $f(x)$ with respect to $(x_{i_1}, \ldots, x_{i_l})$ is defined as*

$$P(l) = \frac{\Delta}{2^l}. \tag{31}$$

In fact, the quantity $P(l)$ measures the probability of getting a partial linear relation of $f(x)$ by randomly fixing the value of $(x_{i_1}, \ldots, x_{i_l})$. In general, the smaller $P(l)$ is the better is the resistance of a Boolean function against both guess and determine cryptanalysis and

(dynamic) cube attacks. In Table 8, we list the exact values of $P(l = \frac{n}{2})$ for our constructions and the methods in [40, 41], for $12 \leq n \leq 40$, $0 \leq t \leq 2$, and $m + 2k = \frac{n}{2}$, where $m = 1$ or $m = 2$. For instance, when $n = 36$ then 1-resilient functions (thus $t = 1$) in [40, 41] have $P(l = 18) = 0.999928 \approx 1$, whereas our new functions only have $P(l = 18) = 0.010670$ if we consider $m = 2$, see Table 8.

Table 8: The value of $P(l = \frac{n}{2})$ for $12 \leq n \leq 40, 0 \leq t \leq 2$.

t	n	[40]	[41]	*New (maximum)*	*New (minimum)*
0	12	0.984375	0.984375	$0.046875, (m = 2)$	$0.046875, (k = 2)$
	14	0.992188	0.992188	$0.054688, (m = 1)$	$0.023438, (k = 2)$
	16	0.996094	0.996094	$0.027344, (m = 2)$	$0.011719, (k = 2)$
	18	0.998047	0.998047	$0.029297, (m = 1)$	$0.005859, (k = 2)$
	20	0.999023	0.999023	$0.014648, (m = 2)$	$0.002930, (k = 2)$
	22	0.999512	0.999512	$0.015137, (m = 1)$	$0.001465, (k = 2)$
	24	0.999756	0.999756	$0.007568, (m = 2)$	$7.324 \times 10^{-4}, (k = 2)$
	26	0.999878	0.999878	$0.007690, (m = 1)$	$3.662 \times 10^{-4}, (k = 2)$
	28	0.999939	0.999939	$0.003845, (m = 2)$	$1.831 \times 10^{-4}, (k = 2)$
	30	0.999969	0.999969	$0.003876, (m = 1)$	$9.155 \times 10^{-5}, (k = 2)$
1	12	0.890625	0.890625	$0.203125, (m = 2)$	$0.203125, (k = 2)$
	14	0.937500	0.937500	$0.250000, (m = 1)$	$0.125000, (k = 2)$
	16	0.964844	0.964844	$0.152344, (m = 2)$	$0.074219, (k = 2)$
	18	0.980469	0.980469	$0.167969, (m = 1)$	$0.042969, (k = 2)$
	20	0.989258	0.989258	$0.098633, (m = 2)$	$0.024414, (k = 2)$
	22	0.994141	0.994141	$0.103516, (m = 1)$	$0.013672, (k = 2)$
	24	0.996826	0.996826	$0.059326, (m = 2)$	$0.007568, (k = 2)$
	26	0.998291	0.998291	$0.060791, (m = 1)$	$0.004150, (k = 2)$
	28	0.999084	0.999084	$0.034241, (m = 2)$	$0.002258, (k = 2)$
	30	0.999512	0.999512	$0.034668, (m = 1)$	$0.001221, (k = 2)$
2	12	0.656250	0.656250	$0.343750, (m = 2)$	$0.343750, (k = 2)$
	14	0.773438	0.773438	$0.460938, (m = 1)$	$0.273438, (k = 2)$
	16	0.855469	0.855469	$0.355469, (m = 2)$	$0.199219, (k = 2)$
	18	0.910156	0.910156	$0.410156, (m = 1)$	$0.136719, (k = 2)$
	20	0.945313	0.945313	$0.289063, (m = 2)$	$0.089844, (k = 2)$
	22	0.967285	0.967285	$0.311035, (m = 1)$	$0.057129, (k = 2)$
	24	0.980713	0.980713	$0.207275, (m = 2)$	$0.035400, (k = 2)$
	26	0.988770	0.988770	$0.215332, (m = 1)$	$0.021484, (k = 2)$
	28	0.993530	0.993530	$0.138062, (m = 2)$	$0.012817, (k = 2)$
	30	0.996307	0.996307	$0.140839, (m = 1)$	$0.007538, (k = 2)$

Moreover, taking $k = 2$, we find that $P(l = 18)$ for our functions is extremely low, i.e., $P(l = 18) = 1.869 \times 10^{-4}$. In other words, for the former methods [40, 41] the adversary finds a partial linear relation by fixing almost any value of $(x_{i_1}, \ldots, x_{i_{18}})$, whereas the probability of getting such relations for our method is negligibly small. Therefore, our new functions potentially provide much better resistance to both guess and determine cryptanalysis and (dynamic) cube attacks than the functions in [40, 41].

Remark 8 *For the modified construction proposed in [40], which uses $2^{\frac{n}{2}-1}$ many $n/2$-variable affine subfunctions, one obtains $P(l = \frac{n}{2}) = \frac{2^{\frac{n}{2}-1}}{2^{\frac{n}{2}}} = \frac{1}{2}$. This implies the existence of a large set of partial linear relations and in average fixing two values of $(x_{i_1}, \ldots, x_{i_l})$ would result in one*

partial linear relation.

6 Conclusions

In this paper, the concept of non-overlap spectra functions, referring to a set of mutually disjoint spectra functions on different variable subspaces, has been introduced. Two general methods for designing a large set of non-overlap spectra functions have been proposed and their use in the construction of resilient functions with SAO nonlinearity has been addressed. In difference to the best known construction methods proposed by Zhang *et al.* (2009, 2014) that employ "too many" $\frac{n}{2}$-variable affine subfunctions, our construction methods only use a few $\frac{n}{2}$-variable affine subfunctions which results in a more favourable algebraic structure. Moreover, these new functions have better resistance against guess and determine cryptanalysis (or dynamic cube attacks that use partial linear relations) than the functions provided by Zhang *et al.* (2009, 2014). The trade-off between optimal algebraic properties and the so-called SAO nonlinearity is still unsettled. The question whether there exist functions with SAO nonlinearity that have an optimal resistance to (fast) algebraic cryptanalysis remains to be answered.

References

[1] F. Armknecht, "Improving fast algebraic attacks," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 3017. Berlin, Germany: Springer-Verlag, 2004, pp. 65–82.

[2] C. Boura and A. Canteaut, "A new criterion for avoiding the propagation of linear relations through an sbox," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 8424. Berlin, Germany: Springer-Verlag, 2014, pp. 585–604.

[3] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Advances in Cryptology–CRYPTO'91* (Lecture Notes in Computer Science), vol. 576. Berlin, Germany: Springer-Verlag, 1992, pp. 86–100.

[4] C. Carlet, "On a weakness of the Tu-Deng function and its repair," *Cryptology ePrint Archive*, report 2009/606, 2009.

[5] C. Carlet, "A larger class of cryptographic boolean functions via a study of the Maiorana-McFarland construction," in *Advances in Cryptology–CRYPTO 2002* (Lecture Notes in Computer Science), vol. 2442. Berlin, Germany: Springer-Verlag, 2002, pp. 549–564.

[6] C. Carlet and 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* (Lecture Notes in Computer Science), vol. 5350. Berlin, Germany: Springer-Verlag, 2008, pp. 425–440.

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

[8] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology–CRYPTO 2003* (Lecture Notes in Computer Science), vol. 2729. Berlin, Germany: Springer-Verlag, 2003, pp. 176–194.

[9] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology–CRYPTO 2003* (Lecture Notes in Computer Science), vol. 2656. Berlin, Germany: Springer-Verlag, 2003, pp. 345–359.

[10] C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers," (Lecture Notes in Computer Science), vol. 561. Berlin, Germany: Springer-Verlag, 1991, pp. 13–28.

[11] I. Dinur and A. Shamir, "Cube attacks on tweakable black box polynomials," in *Advances in Cryptology-CRYPTO 2009* (Lecture Notes in Computer Science), vol. 5479. Berlin, Germany: Springer-Verlag, 2009, pp. 278–299.

[12] I. Dinur and A. Shamir, "Breaking Grain-128 with dynamic cube attacks," in *Fast Software Encryption 2011* (Lecture Notes in Computer Science), vol. 6733. Berlin, Germany: Springer-Verlag, 2011, pp. 167–187.

[13] M. Fedorova and Y. Tarannikov, "On the constructing of highly nonlinear resilient Boolean functions by means of special matrices," in *Progress in Cryptology–INDOCRYPT 2001* (Lecture Notes in Computer Science), vol. 2247. Berlin, Germany: Springer-Verlag, 2001, pp. 254–266.

[14] S. Fu, C. Li, and L. Qu, "A recursive construction of highly nonlinear resilient vectorial functions," *Information Sciences*, vol. 269, pp. 388–396, 2014.

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

[16] K. Khoo, G. Chew, G. Gong, and H. Lee, "Time-memory-data trade-off attack on stream ciphers based on Maiorana-McFarland functions," *IEICE Trans. Funda. Elec. Commu. Comput. Scien.*, vol. 92, no. 1, pp. 11–21, Jan. 2009.

[17] Y. Lee, K. Jeong, J. Sung, and S. Hong, "Related-key chosen IV attacks on Grain-v1 and Grain-128," in *Information Security and Privacy* (Lecture Notes in Computer Science, Springer), vol. 5107. Berlin, Germany: Springer-Verlag, 2008, pp. 321-335.

[18] J. Li, C. Carlet, X. Zeng, C. Li, L. Hu, and J. Shan, "Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks," *Des., Codes and Cryptogr.*, vol. 76, no. 2, pp. 279–305, August 2015.

[19] M. Liu, Y. Zhang, and D. Lin, "Perfect algebraic immune functions," in *Advances in Cryptology–ASIACRYPT'2012* (Lecture Notes in Computer Science), vol. 7658. Berlin, Germany: Springer-Verlag, pp. 172–189, 2012.

[20] S. Maitra and E. Pasalic, "A Maiorana-McFarland type construction for resilient Boolean functions on n variables (n even) with nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$," *Disc. Appl. Math.*, vol. 154, no. 2, pp. 357–369, 2006.

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

[22] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Advances in Cryptology–EUROCRYPT'89* (Lecture Notes in Computer Science), vol. 434. Berlin, Germany: Springer-Verlag, 1990, pp. 549–562.

[23] M. Mihaljevic, S. Gangopadhyay, G. Paul, and H. Imai, "Internal state recovery of Grain-v1 employing normality order of the filter function," *IET Inf. Secur.*, vol. 6, no. 2, pp. 55–64, June 2012.

[24] E. Pasalic, "Maiorana-McFarland class: degree optimization and algebraic properties," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4581–4594, Oct. 2006.

[25] E. Pasalic, "On guess and determine cryptanalysis of LFSR-based stream ciphers," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3398–3406, Oct. 2009.

[26] E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar, "New constructions of resilient and correlation immune boolean functions achieving upper bound on nonlinearity," *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 158–167, April 2001.

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

[28] J. Seberry, X. Zhang, and Y. Zheng, "On constructions and nonlinearity of correlation immune functions," in *Advances in Cryptology–EUROCRYPT'93* (Lecture Notes in Computer Science), vol. 765. Berlin, Germany: Springer-Verlag, 1994, pp. 181–199.

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

[30] D. Tang, C. Carlet, and X. Tang, "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 653–664, Jan. 2013.

[31] Z. Tu and Y. Deng, "A class of 1-resilient function with high nonlinearity and algebraic Immunity," available at http://eprint.iacr.org/2010/179.

[32] Z. Tu and Y. Deng, "Boolean functions optimizing most of the cryptographic criteria," *Discrete Applied Mathematics*, vol. 160, no. 4-5, pp. 427–435, 2012.

[33] Z. Tu and Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity ," *Designs, Codes and Cryptography*, vol. 60, no. 1, pp. 1–14, 2011.

[34] T. Wang, M. Liu, and D. Lin, "Construction of resilient and nonlinear Boolean functions with almost perfect immunity to algebraic and fast algebraic attacks," in *8th International Conference–Inscrypt 2012* (Lecture Notes in Computer Science), vol. 7763. Berlin, Germany: Springer-Verlag, 2013, pp. 276–293.

[35] Q. Wang, J. Peng, H. Kan, and X. Xue, "Constructions of cryptographically significant Boolean functions using primitive polynomials," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 3048–3053, Jun. 2010.

[36] Y. Wei, E. Pasalic, F. Zhang, and S. Hodžić, "Efficient probabilistic algorithm for estimating the algebraic properties of Boolean functions for large n," available at http://eprint.iacr.org/2016/671.

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

[38] J. Yang and W. Zhang, "Generating highly nonlinear resilient Boolean functions resistance against algebraic and fast algebraic attacks," *Security and Communication Networks*, vol. 8, no. 7, pp. 1256–1264, May 2015.

[39] W. 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, March 2014.

[40] W. Zhang and E. Pasalic, "Generalized Maiorana-McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6681–6695, Oct. 2014.

[41] W. Zhang and G. 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, Dec. 2009.

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

[43] F. Zhang, C. Carlet, Y. Hu, and T. Cao, "Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions," *Information Sciences*, vol. 283, pp. 94–106, 2014.

[44] X. Zeng, C. Carlet, J. Shan, and L. Hu, "More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks ," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6310–6320, Sep. 2011.

Appendix A - Evaluating the resistance against (fast) algebraic attacks

In this section, the resistance of our functions against (fast) algebraic attacks is discussed.

Theorem 3 *Let $1 \le i \le n-1$, $B_i \subseteq GF(2)^i$ and $B_i' = B_i \times GF(2)^{n-i}$ such that $\bigcup_{i=1}^{n-1} B_i' = GF(2)^n$ and $B_{i_1}' \cap B_{i_2}' = \emptyset$, $1 \le i_1 < i_2 \le n-1$. Let $X = (x_1, \ldots x_n) \in GF(2)^n$, $X_i' = (x_{j_1}, \ldots x_{j_i}) \in GF(2)^i$, $X_{n-i}'' = (x_{j_{i+1}}, \ldots x_{j_n}) \in GF(2)^{n-i}$, where $\{j_1, \cdots, j_i\} \subset \{1, \cdots, n\}$, $\{j_{i+1}, \cdots, j_n\} \subset \{1, \cdots, n\}$ and $\{j_1, \cdots, j_i\} \cap \{j_{i+1}, \cdots, j_n\} = \emptyset$. Then any t-resilient function in Theorem 2 can be represented as given below,*

$$f(X) = f(X_i', X_{n-i}'') = \sum_{i=1}^{n-1} \{ \sum_{\sigma=(\sigma_{j_1}, \ldots \sigma_{j_i}) \in B_i} \prod_{l=j_1}^{j_i} (x_l \oplus \sigma_l \oplus 1) \cdot (\varphi_{i,[\sigma]}(X_i') \oplus g_i(X_i'))\}, \tag{32}$$

where $\varphi_{i,[\sigma]}(X_i')$ is an injective mapping from B_i to T_i, (the elements of T_i are defined on variable space $GF(2)^{n-i}$, i.e., $X_{n-i}'' \in GF(2)^{n-i}$), $g_i \in \mathbb{B}_i$, and $||B_i|| \neq 0$.

Proof. For any t-resilient function f in Theorem 2, we assume

$$X_{n/2-k}' = (x_{j_1}, \ldots, x_{j_{(n/2-k)}}) = X_{(n/2-k+1)}^{(n)} = (x_{n/2-k+1}, \ldots, x_n) \in GF(2)^{n/2-k},$$

$$X_{n/2}' = (x_{j_1}, \ldots x_{j_{n/2}}) = X_{(n/2+1)}^{(n)} = (x_{n/2+1}, \ldots, x_n) \in GF(2)^{n/2},$$

and let ψ_i be an injective mapping from B_i to T_i (see Theorem 2). Then, f defined by means of Theorem 2 always has the algebraic representation as in (32). □

From Theorem 3, we know that the problem of evaluating the resistance of functions in Theorem 2 against (fast) algebraic attacks is equivalent to the estimation related to the form in (32).

Note that the existence of low degree multipliers (or annihilators) of the Maiorana-McFarland class was originally considered by Pasalic in [24]. Nevertheless, a general technique to estimate the resistance of a random Boolean function (having relatively large input of input variables n, say $n \ge 30$) against (fast) algebraic attacks has been proposed recently in [36]. Based on the evaluation methods in [36], the algebraic properties of our functions are estimated and the results are given in Table 9 and Table 10, for $12 \le n \le 36$.

In Table 9, we compare the theoretical upper bounds on AI of our 1-resilient functions to those in [40, 41] and deduce that the upper bound is always larger for our class (the difference between the actual values has also been confirmed by simulations). In Table 10, based on the possibility of computing both the upper and lower bound on the degree relation $\deg(g) + \deg(h)$ using the method in [36], it is shown that our functions have a very good resistance against FAA. In particular, their resistance to FAA is much better than the resistance of functions in [40, 41]. For instance, if $n = 36$ then the resilient functions obtained by Construction A (or Construction B) in [40, 41] only satisfy the relation $r + s + e = 17 < 36$, whereas our functions achieve $21 \le r + s + e \le 33$.

Table 9: Theoretical upper bound on AI of 1-resilient functions, $(12 \leq n \leq 36)$.

n	$n/2$	$deg(g) = r + d$	Resource
12	6	$r + d = 5$	[40, 41]
		$r + d = 6$	***new***
14	7	$r + d = 5$	[40, 41]
		$r + d = 7$	***new***
16	8	$r + d = 6$	[40, 41]
		$r + d = 7$	***new***
18	9	$r + d = 7$	[40, 41]
		$r + d = 8$	***new***
20	10	$r + d = 7$	[40, 41]
		$r + d = 9$	***new***
22	11	$r + d = 8$	[40, 41]
		$r + d = 10$	***new***
24	12	$r + d = 9$	[40, 41]
		$r + d = 10$	***new***
26	13	$r + d = 9$	[40, 41]
		$r + d = 11$	***new***
28	14	$r + d = 10$	[40, 41]
		$r + d = 12$	***new***
30	15	$r + d = 11$	[40, 41]
		$r + d = 13$	***new***
32	16	$r + d = 11$	[40, 41]
		$r + d = 14$	***new***
34	17	$r + d = 12$	[40, 41]
		$r + d = 15$	***new***
36	18	$r + d = 13$	[40, 41]
		$r + d = 16$	***new***

Appendix

The truth table of an $(n = 12, t = 1, \deg(f) = 10, N_f = 1988)$ function (whose $AI = 6$ and the resistance to FAA $(e + d \geq 11)$ is given in the hexadecimal format below using the convention that the most significant bit is the leftmost bit, e.g. $(0001) = 1$.

83ce 72cb 00cc 75e0 9f11 6883 93f8 422f b691 a895 bd5b db89 4ad2 85fc 4799 6e0f 906d a7e3 ac40 d6f6 bef9 70b6 1006 bcea 2420 7145 6ee5 c2cf 1779 a0a6 9454 fde8 d846 3f94 de6a 4e81 4770 d135 fda8 3ba8 3ac5 63f5 fe33 b9be 7fd9 cb51 44a6 ad9d 5e7e 03ad ef82 7116 d3e9 4847 a4cf 84e4 edc3 688e 5180 c3a3 7d57 9009 61f4 251d 8e95 265e 8c7a cb88 7b34 26f2 bb15 1073 abee 00f4 7712 8a41 51ec f7f3 5203 e12e f8f1 32c7 29ad e529 6a24 12c6 0e76 a203 6947 f496 ac50 3679 db3e e1d2 c567 914a 6b42 17c7 3f4a 7751 a2e6 fc14 3a92 2940 a295 228f 6ec9 1fcd cf7c 0972 19ca 4ad5 dd0e 27f4 03fc 8766 71d4 52b9 8fd1 639a 1edd 5702 074d 4512 2636 5ef1 94c9 8acf dd11 889e 5644 b613 0903 a867 fb83 021e d4f1 7773 e047 873d 3da8 7b54 b18f 6690 2753 39e7 6ccc f5da 6d54 30f4 268b e3b9 8f4f 8bcc 475a e6d7 c552 27dc ecdd 1ee7 a6d3 e434 b11b a5be 6c11 85e4 582c 4b3c 94ab 5a18 3415 638a 8e9e 3966 2058 e135 107b d0c1 4a39 2831 4d6a

Table 10: Upper and lower bound related to FAA for 1-resilient functions with $\deg(f) \geq n-2$.

n	$deg(g') + deg(h) = r + s + e$	Resource
12	$r+s+e=9$	[40, 41]
	$10 \leq r+s+e \leq 11$	***new***
14	$r+s+e=9$	[40, 41]
	$11 \leq r+s+e \leq 13$	***new***
16	$r+s+e=10$	[40, 41]
	$12 \leq r+s+e \leq 14$	***new***
18	$r+s+e=11$	[40, 41]
	$13 \leq r+s+e \leq 17$	***new***
20	$r+s+e=11$	[40, 41]
	$13 \leq r+s+e \leq 19$	***new***
22	$r+s+e=12$	[40, 41]
	$14 \leq r+s+e \leq 21$	***new***
24	$r+s+e=13$	[40, 41]
	$15 \leq r+s+e \leq 22$	***new***
26	$r+s+e=13$	[40, 41]
	$16 \leq r+s+e \leq 25$	***new***
28	$r+s+e=14$	[40, 41]
	$17 \leq r+s+e \leq 26$	***new***
30	$r+s+e=15$	[40, 41]
	$18 \leq r+s+e \leq 28$	***new***
32	$r+s+e=15$	[40, 41]
	$19 \leq r+s+e \leq 29$	***new***
34	$r+s+e=16$	[40, 41]
	$20 \leq r+s+e \leq 31$	***new***
36	$r+s+e=17$	[40, 41]
	$21 \leq r+s+e \leq 33$	***new***

229e 8b35 d2f7 0c06 388d dcbe bd4a 7d80 5da9 01ba b2ec 22f9 f268 957a 40d7 3ada d423 1f77 ce0e 12e9 3084 681a 829b 921a fcac e3a8 bb81 2989 5f1f ba0f b237 2c3a 28de 7b40 e1da 95d1 5313 4560 5ba1 abe1 37ea dd05 eca1 86ea 2006 b7dd 9fb8 affd 8ef2 d4bf e762 ed4a 5b7e 62f1 c12c 1d0d f1ac 7c08 9bb1 8d05 e358 913f fa0d 6bcd 6b83 a473 8d93 4b9b 830d e072 ed6f d205 6468 0397 4e6c