On Boolean Functions with Generalized Cryptographic Properties

An Braeken[1], Ventzislav Nikov[2], Svetla Nikova[1], and Bart Preneel[1]

[1] Department Electrical Engineering, ESAT/COSIC,
Katholieke Universiteit Leuven, Kasteelpark Arenberg 10,
B-3001 Heverlee-Leuven, Belgium
an.braeken,svetla.nikova,bart.preneel@esat.kuleuven.ac.be
[2] Department of Mathematics and Computing Science,
Eindhoven University of Technology
P.O. Box 513, 5600 MB, Eindhoven, the Netherlands
v.nikov@tue.nl

Abstract. By considering a new metric, we generalize cryptographic properties of Boolean functions such as resiliency and propagation characteristics. These new definitions result in a better understanding of the properties of Boolean functions and provide a better insight in the space defined by this metric. This approach leads to the construction of "handmade" Boolean functions, i.e., functions for which the security with respect to some specific monotone sets of inputs is considered, instead of the security with respect to all possible monotone sets with the same cardinality, as in the usual definitions. This approach has the advantage that some trade-offs between important properties of Boolean functions can be relaxed.

Keywords: Boolean functions, resiliency, propagation characteristics, monotone sets

1 Introduction

For any two binary vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_2^n$, define the sets $\delta(x, y) = \{i : x_i \neq y_i\}$ and $\sup(x) = \{i : x_i \neq 0\}$. Denote the size of a set A with $|A|$. Then the Hamming distance between the binary vectors x and y is equal to $d(x, y) = |\delta(x, y)|$ and the Hamming weight of x is $\mathrm{wt}(x) = |\sup(x)|$. It was noted that $\delta(x, y)$ has properties similar to metric and $\sup(x)$ has properties similar to norm [FM02,NN03].

Our goal is to use $\delta(x, y)$ instead of the Hamming distance and $\sup(x)$ instead of the Hamming weight and to explore the properties of this new space. For this purpose we consider monotone increasing and monotone decreasing sets. A set Δ is called monotone decreasing if for each set in Δ, its subsets belong to Δ. Similarly, a set Γ is said to be monotone increasing if for each set in Γ its supersets belong to Γ.

As it has already been shown in [NN03], this new space with monotone sets can be used to generalize notions such as codes, minimum distance of a code, minimal codewords, generator and parity check matrices of a code, packing and covering, error-correcting capabilities, etc. In addition, monotone sets are widely used in Secret Sharing Schemes (SSS) to describe the sets of players which are allowed (disallowed) to reconstruct a secret. It has been recently pointed out [FM02,NN03] that the security of (verifiable) SSS can be derived from the properties of this space.

This paper focuses on Boolean functions. In particular, we generalize the definition of *t-resilient* functions to functions which are resilient with respect to a monotone decreasing set Δ. Analogously, the parameters for defining the *propagation characteristics* (PC) of functions are replaced by monotone decreasing sets. Our aim is to provide a new insight to the previous results and to give a better understanding of which structural properties contribute in which way to known results.

1.1 Motivation

Very often the properties of resiliency and PC imply strong requirements to the rest of the parameters of a Boolean function. This leads to some trade-offs between them, since all relevant properties cannot be satisfied simultaneously. For example, Siegenthaler's inequality [S84] states that $d \leq n - t - 1$, where d is the algebraic degree, n is the dimension and t is the order of resiliency. By exactly defining which components need to satisfy a certain order of resiliency or PC, we can strengthen the weaker components by using other constructions and achieve in this way an optimal design.

By means of example, we present a modified version of the combination generator (see Section 3.6 for concrete examples). Let Δ be the set consisting of all subsets of LFSRs for which the sum of the lengths is shorter than the security parameter for the (fast) correlation attack [S85,MS92,JJ99]. It is known that the feedback polynomials of the combining LFSRs should be primitive with distinct degrees, not necessary co-prime, in order to obtain maximum linear complexity [RS87]. Using t-resilient functions the degrees of LFSRs' polynomials are uniformly chosen. But considering Δ-resilient functions instead, allows us to choose the degrees non-uniformly as well as to relax the requirements to the rest of the function parameters like nonlinearity, algebraic degree, etc. Using a Δ-resilient function as combiner f, the (fast) correlation attack can be avoided. Moreover, the degree of the function f should be high in order to counter the linear synthesis by Berlekamp-Massey [M69] and algebraic attacks [CM03]. Note that in this model the trade-off defined by the Siegenthaler's inequality can be relaxed to another form as shown in Section 3.2.

In order to preclude more recent algebraic attacks, we should also require that the function has no low degree multiples [CM03]. To get even better security, but a small trade-off in speed, one can replace some linear feedback shift registers by nonlinear feedback shift registers or clock controlled linear feedback shift registers, since the algebraic attacks of [CM03] do not apply on this model. The

set Δ for defining the resiliency contains again the subsets of LFSRs for which the sum of the lengths is smaller than the security parameter for the (fast) correlation attack.

1.2 Previous Work

The first steps in considering generalizations of classical t-resiliency and functions satisfying PC properties has been made in [CCCF00]. The authors extended the properties of resiliency and propagation characteristics with respect to subspaces. So, our definitions can be seen as natural extensions of the definitions by Canteaut et al., instead of subspaces, to collections of subspaces.

We also refer to the research on almost resilient functions and functions satisfying almost PC properties [KJS01,K99,DSS01]. There, the concept is different and is based on probabilities but it is also introduced for relaxing the parameters and for avoiding (or relaxing) the trade-offs.

1.3 Organization of the Paper

The paper is organized as follows. In Sect. 2, we give some background and preliminaries. Sect. 3 deals with Δ-resilient functions. We first investigate the notions algebraic and numerical degree, nonlinearity and divisibility results for the Walsh coefficients. Then different constructions are identified amongst the other we mention the constructions of Siegenthaler, Camion et al., Maiorana-MacFarland, the Direct sum and the Partial-Spread constructions. Next we establish a connection between Δ-resilient functions and Δ-orthogonal arrays. We also give two concrete examples of Δ-resilient functions that have better trade-off between degree/nonlinearity and resiliency compared with the classical theory. In Sect. 4 we generalize functions which satisfy SAC and PC of some monotone decreasing sets. Then a relation between them and Δ-resilient functions is proven. In this setting we also investigate the question when a function may possess linear structures. Finally we investigate the algebraic degree and show a generalization of Kurosawa and Satoh's construction of PC functions using a relation between monotone span programs and linear codes.

2 Background

Define the set $\mathcal{P} = \{1, \ldots, n\}$ and denote the power set of $\mathcal{P}$ by $P(\mathcal{P})$. The set Γ ($\Gamma \subseteq P(\mathcal{P})$) is called monotone increasing if for each set A in Γ, each set containing A is also in Γ. Similarly, the set Δ ($\Delta \subseteq P(\mathcal{P})$) is called monotone decreasing, if for each set B in Δ each subset of B is also in Δ. A monotone increasing set Γ can be described efficiently by the set Γ^- consisting of the minimal elements (sets) in Γ, i.e., the elements in Γ for which no proper subset is also in Γ. Similarly, the set Δ^+ consists of the maximal elements (sets) in Δ, i.e., the elements in Δ for which no proper superset is also in Δ. We set

$\Gamma = \Delta^c$ ($\Delta^c = P(\mathcal{P}) \setminus \Delta$). Note that Γ is monotone increasing if and only if Δ is monotone decreasing.

The dual sets $\Delta^\perp$ and $\Gamma^\perp$ to Γ and Δ, respectively, are defined by $\Gamma^\perp = \{A : A^c \in \Delta\}$ and $\Delta^\perp = \{A : A^c \in \Gamma\}$. It is easy to see that $\Delta^\perp$ is monotone decreasing and $\Gamma^\perp$ is monotone increasing. For two monotone decreasing sets Δ_1 and Δ_2 define $\Delta_1 \uplus \Delta_2 = \{A = A_1 \cup A_2; A_1 \in \Delta_1, A_2 \in \Delta_2\}$. Note that $\Delta_1 \uplus \Delta_2$ is again a monotone decreasing set.

As it has been pointed out in [FM02,NN03], $\delta(x, y)$ has similar properties as a metric and $\sup(x)$ has similar properties as a norm. Notice that $\sup(x)$ and $\delta(x, y) = \sup(x - y)$ are subsets of $\mathcal{P}$ and that $\mathcal{P}$ is partially ordered (i.e., $x \preceq y$ if and only if $\sup(x) \subseteq \sup(y)$). For a vector $u \in \mathbb{F}_2^n$, let $\overline{u} = u \oplus 1$ (where 1 denotes the all-1 vector), i.e., $\sup(\overline{u}) = \sup(u)^c$. The dot product $w \cdot x$ is equal to the component-wise inner product.

For an element $A \in \Delta \setminus \{0\}$, the subspace defined by A is given by $U_A = \{u : \sup(u) \subseteq A\}$. The dual $U_A^\perp$ of the subspace U_A is the subspace consisting of the elements x such that $x \cdot y = 0$ for all $y \in U_A$. Consequently, $U_A^\perp$ is defined by A^c, i.e., $U_A^\perp = U_{A^c} = \{u : \sup(u) \subseteq A^c\}$.

Let $f(x) = f(x_1, \ldots, x_n)$ be a Boolean function on $\mathbb{F}_2^n$. The *Walsh transform* W_f of a Boolean function $f(x)$ plays an important role in our work. It is a real-valued function, which is defined as follows

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

A function with equally distributed outputs is called a balanced function. It is clear that for balanced functions $W_f(0) = 0$. A Boolean function $f(x)$ on $\mathbb{F}_2^n$ is said to be a *plateaued* function [CaPr03,ZZ99b] if its Walsh transform W_f takes only three values 0 and $\pm\lambda$, where λ is a positive integer, called the *amplitude* of the plateaued function.

The *nonlinearity* N_f of a Boolean function f, which is defined by the minimum distance of the function to the set of affine functions $\mathcal{A}$, i.e., $N_f = \min_{g \in \mathcal{A}} d(f, g)$, can be expressed using its Walsh transform as follows: $N_f = 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |W_f(w)|$.

Other representations of a Boolean function $f(x)$ are the *algebraic normal form* (ANF)

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u, \quad a_u \in \mathbb{F}_2,$$

and the *numerical normal form* (NNF)

$$f(x) = \sum_{u \in \mathbb{F}_2^n} \lambda_u x^u, \quad \lambda_u \in \mathbb{C}.$$

The degree of the ANF is called the *algebraic degree* or shortly *degree* (denoted by $\deg(f)$), the degree of the NNF is called the *numerical degree* of the Boolean

function. The *autocorrelation* r_f of a Boolean function f on $\mathbb{F}_2^n$ is a real-valued transformation, defined by

$$r_f(u) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+u)} .$$

We will also need an important property of the sum of characters (see e.g., [J92, p. 263]).

Lemma 1. *For any subspace $V \subseteq \mathbb{F}_2^n$, we have*

$$\sum_{x \in V} (-1)^{w \cdot x} = \begin{cases} |V| & \text{if } w \in V^{\perp}; \\ 0 & \text{otherwise.} \end{cases}$$

3 Δ-Resilient Functions

3.1 Definition and Relation with the Classical Definition of Resiliency

In this section we generalize the definitions of resilient and correlation-immune (CI) functions with respect to a monotone decreasing set Δ. We assume that the set Δ is the maximal possible monotone decreasing set for which the function satisfies the corresponding property. The monotone increasing set Γ corresponding with Δ is defined by $\Gamma = \Delta^c$.

Definition 1. *Let $f(x) = f(x_1, \ldots, x_n)$ be a Boolean function on $\mathbb{F}_2^n$ and Δ be a monotone decreasing set. Then $f(x)$ is called* **Δ-resilient** *iff $f(x) \oplus w \cdot x$ is a balanced function for all w such that $\sup(w) \in \Delta$. Furthermore, $f(x)$ is called* **Δ-CI** *iff $f(x) \oplus w \cdot x$ is a balanced function for all w such that $\sup(w) \in \Delta \setminus \{\emptyset\}$.*

When $\Delta = \{A : |A| \leq t\}$ the definitions of Δ-resilient function and t-resilient function, (resp. Δ-CI function and t-CI function) coincide. The property balancedness of $f(x) \oplus w \cdot x$ can be translated in terms of Walsh spectrum into $W_f(w) = 0$. Denote the set of vectors which have zero Walsh value by ZW_f, then $\Delta \subseteq \{sup(u) : u \in \mathrm{ZW}_f\}$. Note that $\mathrm{ZW}_f \cap \Gamma$ is not necessarily empty.

Example 1. Consider the sets Δ^+ and Γ^- in the set $\mathbb{F}_2^4$: $\Delta^+ = \{\{1,2\},\{3,4\}\}$ and $\Gamma^- = \{\{1,4\},\{2,4\},\{1,3\},\{2,3\}\}$. It is easy to verify that $\Gamma = \Delta^c$ and $\Gamma \cap \Delta = \emptyset$. A function which is Δ-resilient has zero Walsh coefficients for the inputs w, where $\sup(w) \in \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{3,4\}\}$, i.e., for the vectors $w \in \{(0,0,0,0),(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1),(1,1,0,0),(0,0,1,1)\}$.

Next we establish the relationship with the classical definition of resiliency. For the monotone sets Γ and Δ define the parameters

$$t_1 = \min\{|A| : A \in \Gamma^-\} \qquad \text{and} \qquad t_2 = \max\{|A| : A \in \Delta^+\} .$$

From the definition of t_1 and the fact that Γ is a monotone increasing set, each subset of size $t_1 - 1$ belongs to Δ, which implies that a Δ-resilient function is also

(t_1-1)-resilient. Analogously, a Δ-CI function is (t_1-1)-CI. The parameter t_2 defines the maximum dimension of a subspace in which the Δ-resilient function is resilient.

The following theorem shows a necessary and sufficient condition for Δ-resilient functions concerning its balancedness properties on affine subspaces.

Theorem 1. *A Boolean function f on $\mathbb{F}_2^n$ is Δ-resilient if and only if f is balanced when restricted to any of the affine subspaces $a+U_A$, where $A \in \Delta^\perp$.*

Proof. It suffices to show that a Boolean function f on $\mathbb{F}_2^n$ is resilient on the subspace V if and only if f is balanced on the affine subspaces $a+V^\perp$, for all $a \in \mathbb{F}_2^n$. Assume f is resilient on the subspace V, or equivalently $W_f(v)=0$ for all $v \in V$. Now $\forall a \in \mathbb{F}_2^n$ using the equation (1) the following equations are equivalent

$$\begin{aligned}
\sum_{v\in V}(-1)^{a\cdot v}W_f(v) &= 0\\
\sum_{v\in V}(-1)^{a\cdot v}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+v\cdot x} &= 0\\
\sum_{x\in a+V^\perp}(-1)^{f(x)}\sum_{v\in V}(-1)^{(a+x)\cdot v}+\sum_{x\notin a+V^\perp}(-1)^{f(x)}\sum_{v\in V}(-1)^{(a+x)\cdot v} &= 0\\
|V|\sum_{x\in a+V^\perp}(-1)^{f(x)} &= 0.
\end{aligned}$$

The proof of the converse part of the theorem follows from the equivalence of the above equations. □

Remark 1. From the definition of resiliency, we deduce that if at most t components of a t-resilient function are fixed (this defines a subspace V of dimension $n-t$), the output is balanced. The previous theorem generalizes this property by proving that the function is also balanced on all affine subspaces of $V^\perp$.

Example 2. A possible truth table of the Δ-resilient function defined by Example 1 is given by the vector $(0,1,0,1,1,1,0,0,0,0,1,1,1,0,1,0)$. This function is exactly 1-resilient. Moreover the function is resilient with respect to two subspaces of dimension 2 whose basis is given by $< e_1, e_2 >$ and $< e_3, e_4 >$, where e_i is the all zero vector except for position i. One can check that the conditions of Theorem 1 are satisfied.

3.2 Algebraic and Numerical Degree

Theorem 2. *For a Δ-resilient function f on $\mathbb{F}_2^n$ all ANF coefficients a_u of f with $\sup(u) \in \Gamma^\perp$ and $wt(u)>1$ are equal to zero. If $\sup(u) \in \Gamma^\perp$ and $wt(u)=1$ then $a_u=1$.*

Proof. The Siegenthaler's inequality $\deg(f) \leq n - t - 1$ for t-resilient functions on $\mathbb{F}_2^n$ relies on the observation that the coefficient a_u of the term x^u in the ANF of f satisfies the following relation [XM88]

$$a_u = 2^{wt(u)-1} - 2^{-wt(\overline{u})-1} \sum_{w \preceq \overline{u}} W_f(w) \mod 2\,. \tag{1}$$

Consider now u with $\sup(u) \in \Gamma^\perp$: then $\sup(\overline{u}) \in \Delta$ and hence $\sup(w) \subseteq \sup(\overline{u}) \in \Delta$ for all $w \preceq \overline{u}$. By definition of Δ-resilient functions $W_f(w) = 0$ for $\sup(w) \in \Delta$. Therefore $a_u = 0$ for all u such that $\sup(u) \in \Gamma^\perp$ and $wt(u) > 1$, but when $\sup(u) \in \Gamma^\perp$ and $wt(u) = 1$ we obtain $a_u = 1$. Note that this is a generalization of the Siegenthaler's inequality for t-resilient functions since if $\Delta = \{A : |A| \leq t\}$ we have $\Gamma^\perp = \{B : |B| \geq n - t\}$. □

Remark 2. For a Δ-CI function f on $\mathbb{F}_2^n$ all coefficients a_u from the ANF of f with $\sup(u) \in \Gamma^\perp$, $wt(u) > 1$ and $W_f(0) \neq 2^n \pm 2^{n-wt(u)-1}$ are equal to zero. If $\sup(u) \in \Gamma^\perp$, $wt(u) = 1$ and $W_f(0) \neq 2^n - 2^{n-2}$ then $a_u = 1$. The proof for Δ-CI functions is analogous to the previous proof. This result generalizes the Siegenthaler's inequality for t-CI functions of degree d, i.e., $t \leq n - d$.

Remark 3. Notice that because of the factor mod 2 in (1) the coefficient a_u is 1 for u such that $\sup(u) \subseteq [\Delta^\perp]^+$ and $W_f(\overline{u}) = \pm 2^{n-wt(u)+1}$. The maximum weight of such u defines the normal algebraic degree of the Boolean function. Knowledge of the coefficients of the ANF of f enables us to derive bounds (upper and lower) on the nonlinearity as shown in [ZZI99, Theorem 18 and Theorem 30].

We now generalize the definition of degree to this new setting.

Definition 2. *Define a monotone decreasing set* $Deg = \{A : A \subseteq \sup(u),\ a_u \neq 0\}$. *We call the set* Deg^+ *the "degree-set" of* f.

Remark 4. The "degree-set" of f satisfies the following relation $Deg \subseteq \Delta^\perp \cup \{A : A \in \Gamma^\perp, |A| = 1\}$. Moreover, the equality does not always hold; it is even possible that $Deg^+ \cap [\Delta^\perp]^+ = \emptyset$.

Example 3. Applying Theorem 2 to the function of Example 1, we obtain that all coefficients a_u for u such that $\sup(u) \in \Gamma^\perp$ are zero, which gives additional information compared to the Siegenthaler's inequality. Note that $[\Gamma^\perp]^- = \{\{3,4\},\{1,2\}\}$ and $[\Delta^\perp]^+ = \{\{2,4\},\{2,3\},\{1,4\},\{1,3\}\}$. Because the ANF of f is given by $x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_1 \oplus x_3$, the equality $Deg^+ = [\Delta^\perp]^+$ holds in this example.

Theorem 3. *For a* Δ*-resilient function* $f(x)$ *on* $\mathbb{F}_2^n$ *all coefficients* λ_u *from NNF of* $g(x) = f(x) \oplus x_1 \oplus \cdots \oplus x_n$ *with* $\sup(u) \in \Gamma^\perp$ *are equal to zero. Moreover, all coefficients* λ_u *from NNF of* g *with* $\sup(u) \in [\Delta^\perp]^+$ *are non-zero.*

Proof. In [CG01] the authors characterize a t-resilient function f by the numerical degree of the function $g(x) = f(x) \oplus x_1 \oplus \cdots \oplus x_n$. Analogous to the Siegenthaler's inequality the numerical degree of function $g(x)$ is less than or equal to $n - t - 1$. The proof uses the connection between Walsh coefficients, i.e., $W_f(w) = W_g(\overline{w})$ and the observation that the coefficient λ_u of the term x^u in the NNF of g satisfies the following relation

$$\lambda_u = 2^{-n}(-2)^{wt(u)-1} \sum_{u \preceq w} W_g(w)\,. \tag{2}$$

Consider now u with $\sup(u) \in \Gamma^\perp$: then $\sup(\overline{u}) \in \Delta$ and hence $\sup(v) \subseteq \sup(\overline{u}) \in \Delta$ for all $v \preceq \overline{u}$. By rewriting (2) into

$$\lambda_u = 2^{-n}(-2)^{n-wt(\overline{u})-1} \sum_{v \preceq \overline{u}} W_f(v) \tag{3}$$

and by using the definition of Δ-resilient functions, we obtain that $\lambda_u = 0$ for all u such that $\sup(u) \in \Gamma^\perp$.

Note that there is one-to-one mapping between the coefficients λ_u equal to zero and the resiliency (see (3)). Namely let f be Δ-resilient and assume that there exists a zero coefficient λ_u from the NNF of g with $\sup(u) \in [\Delta^\perp]^+$ then f is $(\Delta \cup \sup(\overline{u}))$-resilient. As a consequence, the numerical degree of the function is equal to $\max\{|A| : A \in [\Delta^\perp]^+\}$. □

Remark 5. From the previous proof, it is easy to derive that for Δ-CI functions f the coefficients λ_u of the NNF of g are nonzero if $\sup(u) \in \Gamma^\perp$ and also if $\sup(u) \in [\Delta^\perp]^+$ when $W_f(0) \neq -W_f(\overline{u})$.

3.3 Nonlinearity

In this section we improve the divisibility results on the Walsh coefficients of resilient functions which leads to an upper bound on the nonlinearity. Let f_v be the $(n - wt(v))$-variable function formed from f for which $x_j = 0$ if $v_j = 1$. The divisibility result by Sarkar and Maitra [SM00] can be generalized in the following way:

Theorem 4. *Let f be a Δ-resilient function on $\mathbb{F}_2^n$. Then the Walsh coefficients of f satisfy the following divisibility conditions:*

$$W_f(v) = 0 \mod 2^{t_3(v)+1}, \text{ where } sup(v) \in \Gamma \text{ and}$$
$$t_3(v) = \min\{wt(w) : w \preceq v, sup(w) \in \Gamma^-\}\,.$$

Proof. In [CS02] the following relation has been proven:

$$\sum_{u \preceq v} W_f(u) = 2^{wt(v)} W_{f_{\overline{v}}}(0) = 2^n - 2^{wt(v)+1} wt(f_v). \tag{4}$$

Choose $v \in \Gamma^-$, hence for any $u \preceq v$ we have $u \in \Delta$ thus $W_f(u) = 0$. Then the relation (4) reduces to $W_f(v) = 2^n - 2^{wt(v)+1}wt(f_v)$, which proves the result for $v \in \Gamma^-$ because $wt(v) = t_3(v)$.

We will not consider the trivial case when $\Gamma^- = \{\mathcal{P}\}$. We proceed further by induction on the weight of v. Let $v \in \Gamma \setminus \Gamma^-$. Then from relation (4) we have $W_f(v) = 2^n - 2^{wt(v)+1}wt(f_v) - \sum_{u \preceq v} W_f(u)$. By the hypothesis $W_f(u) = 0 \mod 2^{t_3(u)+1}$ for any $u \preceq v$ and $u \in \Gamma$. Because $t_3(v)$ is increasing for decreasing weight of v, it follows that $t_3(u) > t_3(v)$ for all $u \preceq v, u \in \Gamma$, which completes the induction step and the proof. □

Remark 6. Note that $t_3(v) \geq t_1 = t + 1$ for v with $sup(v) \in \Gamma$, therefore we have a stronger result comparing to the divisibility of 2^{t+2} proven in [SM00] for t-resilient functions, since some of the coefficients are divisible by a higher power of 2.

Now we extend the result of Carlet and Sarkar in [CS02], namely $W_f(v) = 0 \mod 2^{t+2+\left\lfloor \frac{n-t-2}{\deg(f)} \right\rfloor}$.

Theorem 5. *Let f be a Δ-resilient function on $\mathbb{F}_2^n$. Then the Walsh coefficients of f satisfy the following divisibility conditions:*

$$W_f(v) = 0 \mod 2^{t_3(v)+1+\left\lfloor \frac{n-t_3(v)-1}{t_4(v)} \right\rfloor},$$

where $sup(v) \in \Gamma$ and with parameters $t_3(v)$ (as defined in Theorem 4) and $t_4(v) = \max\{|A| : A \in Deg^+,\ A \subseteq \sup(\overline{u})$ with $u \preceq v, sup(u) \in \Gamma^-\}$.

Proof. In [CS02], the following relation has been proven

$$\sum_{u \preceq v} W_f(u) = 2^{wt(v)} W_{f_{\overline{v}}}(0) = 2^n - 2^{wt(v)+1}wt(f_v)\,. \tag{5}$$

Let f be a Δ-resilient function. If $sup(v) \in \Gamma^-$, then for any $u \preceq v$ we have $u \in \Delta$ thus $W_f(u) = 0$. Hence (5) reduces to $W_f(v) = 2^n - 2^{wt(v)+1}wt(f_v)$. Applying McEliece's [MS] theorem for cyclic codes on f_v we obtain that $wt(f_v) = 0 \mod 2^{\left\lfloor \frac{n-t_3(v)-1}{t_4(v)} \right\rfloor}$, since $t_3(v) = wt(v)$ and $t_4(v) = \deg(f_v)$. This proves the result for v with $sup(v) \in \Gamma^-$.

Let $sup(v) \in \Gamma \setminus \Gamma^-$. By the hypothesis $W_f(u) = 0 \mod 2^{t_3(u)+1+\left\lfloor \frac{n-t_3(u)-1}{t_4(u)} \right\rfloor}$ for any $u \preceq v$ and $sup(u) \in \Gamma$. Since $t_4(u)$ is increasing with respect to $wt(u)$ we obtain that $W_f(u) = 0 \mod 2^{t_3(u)+1+\left\lfloor \frac{n-t_3(u)-1}{t_4(v)} \right\rfloor}$ for any $u \preceq v$ and $sup(u) \in \Gamma$. Note that by Remark 4 the degree of f_v is less or equal to $t_4(v)$. Rewrite (5) in the form $W_f(v) = 2^n - 2^{wt(v)+1}wt(f_v) - \sum_{u \preceq v} W_f(u)$. To conclude the proof note that $t_3(u)$ is decreasing with respect to $wt(u)$ and that $t_4(v) \geq \deg(f_v)$. □

Remark 7. The parameters $t_3(v)$ and $t_4(v)$ satisfy an inequality similar to the Siegenthaler's inequality.

$$t_3(v) + t_4(v) \leq n.$$

Thus Theorem 5 improves the result from Theorem 4 when $t_3(v)$ and/or $t_4(v)$ are smaller.

Example 4. Consider again the function of Example 1. By definition of Γ^- and Deg^+ (see Example 3), the parameters $t_3(v) = 2$ and $t_4(v) = 1$ for all $v \in \Gamma$. Consequently, the Walsh values of the function are divisible by 8.

The divisibility results of the Walsh coefficients for Δ-resilient functions result in bounds on the nonlinearity of these functions. Since the proof is similar to the one of [CS02], we only state the theorem.

Theorem 6. *Let f be a Δ-resilient function on $\mathbb{F}_2^n$. Denote* $L_1 = \max_{sup(v)\in\Gamma} \left\{ t_3(v) + 1 + \left\lfloor \frac{n-t_3(v)-1}{t_4(v)} \right\rfloor \right\}$, $L_2 = \min_{sup(v)\in\Gamma} \left\{ t_3(v) + 1 + \left\lfloor \frac{n-t_3(v)-1}{t_4(v)} \right\rfloor \right\}$ *and let* $\mathrm{nlmax}(n)$ *be the maximum possible nonlinearity for n-variable functions. Then*

1. *If n is even and $L_1 > \frac{n}{2} - 1$, then $N_f \leq 2^{n-1} - 2^{L_1}$.*
2. *If n is even and $L_1 \leq \frac{n}{2} - 1$, then $N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{L_2}$.*
3. *If n is odd and $2^{n-1} - 2^{L_1} \leq \mathrm{nlmax}(n)$, then $N_f \leq 2^{n-1} - 2^{L_1}$.*
4. *If n is odd and $2^{n-1} - 2^{L_1} > \mathrm{nlmax}(n)$, then N_f is less than or equal to the highest multiple of 2^{L_2} which is not greater than* $\mathrm{nlmax}(n)$.

3.4 Constructions of Δ-Resilient Functions

Lemma 2. *If f is a Δ-resilient function on $\mathbb{F}_2^n$, then $g(x) = f(x) \oplus 1$ and $h(x) = f(x_1 \oplus c_1, \ldots, x_n \oplus c_n)$ where $c \in \mathbb{F}_2^n$ are Δ-resilient.*

Proof. The theorem follows immediately from the definition of Δ-resiliency and the fact that $W_f(w) = W_h(w) = -W_g(w)$ for all $w \in \mathbb{F}_2^n$. □

The Constructions of Siegenthaler and Camion et al.

Theorem 7. *Let f_1 and f_2 be two Δ-resilient functions on $\mathbb{F}_2^n$. The function f on $\mathbb{F}_2^{n+1}$ defined by*

$$f(x_1, \ldots, x_{n+1}) = x_{n+1} f_1(x_1, \ldots, x_n) \oplus (1 \oplus x_{n+1}) f_2(x_1, \ldots, x_n)$$

is $\widetilde{\Delta}$-resilient, where $\widetilde{\Delta} = \Delta \uplus P(\{n+1\})$. Furthermore, if $w \in \Gamma$ and for any $u \preceq w$ it holds that $W_{f_1}(u) + W_{f_2}(u) = 0$ then f is $\hat{\Delta}$-resilient, where $\hat{\Delta} = \widetilde{\Delta} \cup P(\mathrm{sup}(w))$.

Proof. Let $\widetilde{\lambda} = (\lambda_1, \ldots, \lambda_n)$ and $\lambda = (\widetilde{\lambda}, \lambda_{n+1})$. The Walsh coefficients of f satisfy the following relation:

$$W_f(\lambda) = W_{f_2}(\widetilde{\lambda}) + (-1)^{\lambda_{n+1}} W_{f_1}(\widetilde{\lambda}) \,. \tag{6}$$

If λ satisfies $\mathrm{sup}(\lambda) \in \widetilde{\Delta}$, then $\mathrm{sup}(\widetilde{\lambda}) \in \Delta$. Since f_1 and f_2 are Δ-resilient functions it follows (from (6)) that $W_f(\lambda) = 0$.

If λ satisfies $\mathrm{sup}(\lambda) \in \hat{\Delta}$ we have the following two cases:

– $\sup(\lambda) \in \Delta \uplus P(\{n+1\})$, for which it is already proven that $W_f(\lambda) = 0$.
– $\sup(\lambda) \in P(\sup(w))$ for some $w \in \Gamma$. We have now that $\lambda_{n+1} = 0$ and thus $W_f(\lambda) = W_{f_1}(\overline{\lambda}) + W_{f_2}(\overline{\lambda}) = 0$ since $\lambda \preceq w$.

□

Remark 8. We extend Siegenthaler's result [S84] that states "if f_1 and f_2 are t-resilient then f is t-resilient" by showing that if f_1 and f_2 are Δ-resilient, then f is $\widetilde{\Delta}$-resilient. Similarly, we generalize the result of Camion et al. [CCCS92] which states "if also for all v such that $wt(v) = t+1$ holds that $W_{f_1}(v) + W_{f_2}(v) = 0$, f is $(t+1)$-resilient", because we show that if f_1 and f_2 are Δ-resilient then f is $\hat{\Delta}$-resilient.

The following construction can be seen as a special case of the previous one.

Lemma 3. *Let f_1 be a Δ-resilient function on $\mathbb{F}_2^n$. Then the functions*

$$f(x_1, \ldots, x_{n+1}) = f_1(x_1, \ldots, x_n) \oplus 0.x_{n+1}$$
$$g(x_1, \ldots, x_{n+1}) = f_1(x_1, \ldots, x_n) \oplus x_{n+1}(f_1(x_1, \ldots, x_n) \oplus f_1(x_1 \oplus 1, \ldots, x_n \oplus 1))$$

are $\Delta \uplus P(\{n+1\})$-resilient functions on $\mathbb{F}_2^{n+1}$, and the function

$$h(x_1, \ldots, x_{n+1}) = f_1(x_1, \ldots, x_n) \oplus x_{n+1}$$

is a $(\Delta \uplus P(\{n+1\})) \cup P(\{1, \ldots, n\})$-resilient function on $\mathbb{F}_2^{n+1}$.

Proof. First rewrite the functions in the form

$$f(x_1, \ldots, x_{n+1}) = f_1(x_1, \ldots, x_n)(x_{n+1} \oplus 1) \oplus f_1(x_1, \ldots, x_n)x_{n+1}$$
$$g(x_1, \ldots, x_{n+1}) = f_1(x_1, \ldots, x_n)(x_{n+1} \oplus 1) \oplus f_1(x_1 \oplus 1, \ldots, x_n \oplus 1)x_{n+1}$$
$$h(x_1, \ldots, x_{n+1}) = f_1(x_1, \ldots, x_n)(x_{n+1} \oplus 1) \oplus (f_1(x_1, \ldots, x_n) \oplus 1)x_{n+1}.$$

Now applying Theorems 2 and 7 the results follow. □

The following corollary can be derived from Theorem 3.

Corollary 1. *Let $f(x) = w \cdot x$ be a linear function on $\mathbb{F}_2^n$ and $wt(w) = d$, i.e., without lost of generality we can suppose that $f(x) = x_1 \oplus \ldots \oplus x_d$. Then $f(x)$ is $(\cup_{i=1}^{d} P(\{1, \ldots, n\} \setminus \{i\}))$-resilient function.*

Proof. Note that $\Delta = (\cup_{i=1}^{d} P(\{1, \ldots, n\} \setminus \{i\}))$ could be rewritten as $\Delta = P(\{d+1, \ldots, n\}) \uplus \{A : A \subset \{1, \ldots, d\}\}$. It is easy to see now that $\{1, \ldots, d\} \notin \Delta$ and hence f is $(d-1)$-resilient. Also in accordance with Theorem 2 we have $\{i\} \in \Gamma^{\perp}$ for $i = 1, \ldots, d$. □

Direct Sum and Secondary Constructions.

Theorem 8. *Let f_1 be a Δ_1-resilient function on $\mathbb{F}_2^{n_1}$ and f_2 be a Δ_2-resilient function on $\mathbb{F}_2^{n_2}$ then the direct sum*

$$f : \mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} : (x, y) \mapsto f(x, y) = f_1(x) \oplus f_2(y)$$

is a $(\widetilde{\Delta} = \Delta_1 \uplus \Delta_2 \uplus S)$-resilient function on $\mathbb{F}_2^{n_1+n_2}$ where $S = \{\emptyset, \{1\}, \cdots, \{n_1\}, \{n_1 + 1\}, \cdots, \{n_2 + n_1\}\}$.

Proof. For $\lambda = (\lambda_1, \lambda_2)$, where $\lambda_1 \in \mathbb{F}_2^{n_1}$ and $\lambda_2 \in \mathbb{F}_2^{n_2}$, the Walsh coefficient equals to $W_f(\lambda_1, \lambda_2) = W_{f_1}(\lambda_1)W_{f_2}(\lambda_2)$. For each $\lambda = (\lambda_1, \lambda_2)$ with $sup(\lambda) \in \widetilde{\Delta}$, at least one of λ_i satisfies $sup(\lambda_i) \in \Delta_i$, since all elements of S have weight maximum one. □

Remark 9. The classical theorem says that for the direct sum of a t_1-resilient function and t_2-resilient function yields a $(t_1 + t_2 + 1)$-resilient function [ZZ97], which is reflected here by the set $\widetilde{\Delta}$.

The following lemma shows how to construct new Δ'-resilient functions from a given Δ-resilient function where $\Delta' \subseteq \Delta$. This theorem is an extension of Theorem 3 from [C97a].

Lemma 4. *Consider a Boolean function f on $\mathbb{F}_2^n$ which is Δ-resilient. If there exists a subspace W and a subset $\Delta' \subseteq \Delta$ such that $U_A \cap W = \emptyset$ for all $A \in \Delta'$ and the restriction of f to $W^\perp$ is equal to the constant c, then the function f' obtained from f by replacing the constant c by the constant $c \oplus 1$ for all elements of $W^\perp$ is Δ'-resilient.*

Proof. Recall that by equation (1) for $v \in U_A$ we have $\sum_{x \in W^\perp} (-1)^{1+v \cdot x} = 0$. Thus the Walsh value of $v \in U_A$ can be computed as follows:

$$\begin{aligned}
W_f(v) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+v \cdot x} \\
&= \sum_{x \in W^\perp} (-1)^{f(x)+v \cdot x} + \sum_{x \notin W^\perp} (-1)^{f(x)+v \cdot x} \\
&= \sum_{x \notin W^\perp} (-1)^{f(x)+v \cdot x} \\
&= \sum_{x \notin W^\perp} (-1)^{f'(x)+v \cdot x} \\
&= \sum_{x \in W^\perp} (-1)^{f'(x)+v \cdot x} + \sum_{x \notin W^\perp} (-1)^{f'(x)+v \cdot x} \\
&= W_{f'}(v).
\end{aligned}$$

□

The following construction is a generalization of the change of basis construction.

Lemma 5. *Let Δ be a set containing less than n elements. Then any Boolean function f on $\mathbb{F}_2^n$ which has at least n linearly independent vectors $w \in \mathbb{F}_2^n$ such that $W_f(w) = 0$ can be transformed into a Δ-resilient function.*

Proof. For a nonsingular matrix D, it holds that $g(x) = f(D^{-1}x)$ if and only if $W_g(w) = W_f(Dw)$. Taking n linearly independent vectors which have zero Walsh value as rows of D, leads to the construction of a Δ-resilient function. □

The Maiorana-MacFarland and Partial-Spread Constructions.

Theorem 9. *Let ϕ be a function from $\mathbb{F}_2^{n-r}$ into $\mathbb{F}_2^r$ and let g be an arbitrary Boolean function on $\mathbb{F}_2^{n-r}$, then the function f defined by*

$$\mathbb{F}_2^r \times \mathbb{F}_2^{n-r} \to \mathbb{F}_2 : (x, y) \mapsto f(x, y) = x \cdot \phi(y) \oplus g(y)$$

is Δ-resilient with $\Delta = \{A : \exists y \in \mathbb{F}_2^{n-r},\ \text{such that}\ \ \sup(\phi(y)) \subseteq A\}^c$. Moreover, if ϕ is injective (resp. takes each value exactly 2 times), the function is plateaued with amplitude 2^r (resp. 2^{r+1}).

Proof. Calculate the Walsh spectrum of the function (see [C97a])

$$W_f(u, v) = \sum_{x \in \mathbb{F}_2^r,\ y \in \mathbb{F}_2^{n-r}} (-1)^{x \cdot \phi(y) + g(y) + x \cdot u + y \cdot v} = 2^r \sum_{y \in \phi^{-1}(u)} (-1)^{g(y) + y \cdot v},$$

where $u \in \mathbb{F}_2^r$ and $v \in \mathbb{F}_2^{n-r}$. As a consequence, $W_f(u, v) = 0$ if there exists no y such that $\phi(y) = u$. □

Remark 10. This construction always leads to $P(\{r+1, \ldots, n\}) \subseteq \Delta$ because ϕ is a mapping from $\mathbb{F}_2^{n-r}$ into $\mathbb{F}_2^r$. It is clear that the higher the weight of the elements in the image of ϕ are, the higher the values t_2 and $|\Delta|$ are.

In [C97a], Carlet showed how to construct resilient functions using the construction of bent functions in the class $\mathcal{PS}_{ap}$ (a subclass of the Partial-Spreads class introduced in [D74]). We generalize this construction for Δ-resilient functions.

In this construction, the field $\mathbb{F}_2^n$ is identified with the field $\mathbb{F}_{2^n}$. The dot product via this identification is equal to $Tr_{\mathbb{F}_{2^n}}(xy)$, where $Tr_{\mathbb{F}_{2^n}}$ is the trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The notion of resiliency depends on the choice of the dot product on $\mathbb{F}_{2^n}$. For an even characteristic, there exists a dual basis $\{\alpha_1, \ldots, \alpha_n\}$ such that $Tr_{\mathbb{F}_{2^n}}(xy) = \sum_{i=1}^n x_i y_i = x \cdot y$. Recall that for each linear mapping $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ there exists a mapping $\phi^* : \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$ (called the adjoint) such that for every $x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^n}$ one has that $Tr_{\mathbb{F}_{2^m}}(x\phi(y)) = Tr_{\mathbb{F}_{2^n}}(y\phi^*(x))$ or in other words $x \cdot \phi(y) = y \cdot \phi^*(x)$.

Theorem 10. *Let g be a Boolean function on $\mathbb{F}_{2^m}$, ϕ a linear mapping from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$ and $a \in \mathbb{F}_{2^m}$ such that $a + \phi(y) \neq 0, \forall y \in \mathbb{F}_{2^n}$. Then the Boolean function f which is defined by*

$$\mathbb{F}_{2^m} \times \mathbb{F}_{2^n} \to \mathbb{F}_2 : (x, y) \mapsto f(x, y) = g\left(\frac{x}{a + \phi(y)}\right) + b \cdot y\,,$$

with $b \in \mathbb{F}_{2^n}$ is Δ-resilient with

$$\Delta = \{A : \exists z \in \mathbb{F}_{2^m}, \text{ such that } \sup(\phi^*(z) + b) \subseteq A\}^c.$$

Proof. We refer to [C97a] for the computation of the Walsh transform for f in $(u, v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$:

$$\begin{aligned} W_f(u,v) &= \sum_{z \in \mathbb{F}_{2^m},\ y \in \mathbb{F}_{2^n}} (-1)^{g(z)+(b+v)\cdot y + z(a+\phi(y))\cdot u} \\ &= \sum_{z \in \mathbb{F}_{2^m},\ y \in \mathbb{F}_{2^n}} (-1)^{g(z)+(b+v)\cdot y + (za)\cdot u + \phi^*(uz)\cdot y} \\ &= \sum_{z \in \mathbb{F}_{2^m}} (-1)^{g(z)+(za)\cdot u} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{(b+v+\phi^*(uz))\cdot y} \\ &= 2^n \sum_{\substack{z \in \mathbb{F}_{2^m} \\ \phi^*(uz)+v+b=0}} (-1)^{g(z)+u\cdot(az)}. \end{aligned}$$

If $(u, v) \in \Delta$, then the set $\{z \in \mathbb{F}_{2^m} : \phi^*(uz) + v + b = 0\}$ is empty. Consequently $W_f(u, v)$ is equal to 0 for all $(u, v) \in \Delta$. □

Remark 11. Note that $P(\{1, \cdots, m\}) \subseteq \Delta$. The higher the weight of the elements of D is, the higher t_2 (corresponding to the order of resiliency) and $|\Delta|$ are.

3.5 Relations with Codes and Orthogonal Arrays

The following construction shows a relation between Δ-resilient functions and linear $[n, k, d]$-codes, which is a generalization of a result from [WD97].

Lemma 6. *Let G be a generator matrix of an $[n, k, d]$-code $\mathcal{C}$ and let f be a balanced function on $\mathbb{F}_2^n$. Define $\Delta_u = P(\{1, \ldots, n\} \setminus \sup(u)) \uplus \{A : A \subset \sup(u)\}$ for $u \in \mathcal{C}$. Then $f(xG^T)$ is a $(\cap_{u \in \mathcal{C}}\ \Delta_u)$-resilient function.*

Proof. Denote $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ as the function $x \mapsto xG^T$. We use the relation, derived in [DGV94,GS02], between the Walsh coefficients of $f \circ F$ and the Walsh coefficients of f and $l_w \circ F$, where $l_w \circ F$ denotes the linear combination of the components of F defined by w:

$$W_{f \circ F}(v) = 2^{-k} \sum_{w \in \mathbb{F}_2^k} W_f(w) W_{l_w \circ F}(v), \quad \forall v \in \mathbb{F}_2^n\,. \tag{7}$$

Note that the function $l_w \circ F = w \cdot xG^T = wG \cdot x$ is linear and thus by Corollary 1 $l_w \circ F$ is a Δ_u-resilient function, where $u = wG$ is a codeword of $\mathcal{C}$. Now (7) concludes the proof. □

Remark 12. Because $\{A : |A| \leq d - 1\} \subseteq \cap_{u \in \mathcal{C}}\ \Delta_u$, Lemma 6, generalizes the property that the function $f(xG^T)$ is at least $(d - 1)$-resilient as proven in [WD97].

Based on a connection between k-CI functions and $(M, n, 2, k)$ orthogonal arrays we show an analogous relation between Δ-CI functions, $(M, n, 2, \Delta)$-orthogonal arrays. We first introduce a generalization of the definition of orthogonal array in the new metric:

Definition 3. *An orthogonal (M, n, q, Δ) array is an $M \times n$ matrix V with entries from a set of q elements, strength Δ which is a decreasing monotone set and index μ. Any set $A \in \Delta^+$ of columns of V contains all $q^{|A|}$ possible row vectors exactly $\mu = Mq^{-|A|}$ times.*

For $\Delta = \{A : |A| \leq k\}$, this definition coincides with the definition of (M, n, q, k) orthogonal array. As shown in [CCCS92], the extended truth table of a k-CI function f on $\mathbb{F}_2^n$ forms an $(M, n, 2, k)$ orthogonal array, where the extended truth table is defined as the $wt(f) \times n$ table with rows determined by the elements x for which $f(x) = 1$. A natural generalization in the new metric is given in the next theorem.

Theorem 11. *A Boolean function f on $\mathbb{F}_2^n$ is Δ-CI if and only if its extended truth table is an orthogonal $(M, n, 2, \Delta)$ array.*

3.6 Example of Modified Combination Generator

We give some concrete examples of the modified combination generator as explained in the introduction.

1. Suppose the generator consists of 5 LFSRs of lengths 61, 63, 21, 31, and 33 respectively. Let the security parameter for the (fast) correlation attack be equal to 60. Consequently in order to be secure against the (fast) correlation attack, we need a combination function which is resilient with respect to the 3^{rd}, 4^{th}, 5^{th} and also the 3^{rd}+4^{th}, 3^{rd}+5^{th} LFSR, i.e. a Δ resilient function with $\Delta = \{\{3, 4\}, \{3, 5\}\}$. The function $f(x_1, \ldots, x_5) = x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4 \oplus x_3x_5 \oplus x_1 \oplus x_2$ satisfies this property. Remark that this function has degree 4 and nonlinearity 10. High degree and high nonlinearity are important properties for resisting other attacks like for instance Berlekamp-Massey attack [M69], algebraic attack [CM03] and best affine approximation attack [DXS91].
2. The function $f(x_1, \ldots, x_5) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3$ is a Δ-resilient function with $\Delta = \{\{1, 2\}, \{1, 4\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}$. Moreover, the function has degree 3 and maximum nonlinearity 12. The LFSRs of the corresponding modified combination generator with security parameter 60 should have for instance lengths 21, 23, 61, 25, and 27 respectively.

When we consider the same models of combination generators in the classical theory, the combination function should be in both cases 2-resilient in order to resist (fast) correlation attacks. Following Siegenthaler's inequality, the corresponding function has degree less than or equal to 2. Note that now using Δ-resilient functions the choice of the lengths of the LFSRs may not be uniform, which is the case when we use t-resilient functions. This also allows to relax the

requirements to the rest of the parameters like nonlinearity, algebraic degree, etc. Moreover, by Carlet-Sarkar's result on the divisibility of the Walsh coefficients, the maximum Walsh value is greater or equal than 16, resulting in a nonlinearity less than or equal to 8.

These examples are just illustrative and need to be scaled up in order to be used in reality. However, it already shows the advantages of considering resiliency with respect to specified monotone sets since the strong trade-offs between resiliency and degree, resiliency and nonlinearity can be avoided.

4 Functions Satisfying Propagation Characteristics with Respect to Δ-sets

Analogously to the definitions of Δ-resilient and Δ-correlation immune (CI) function, we define functions which satisfy the propagation characteristic of degree Δ_1 and of order Δ_2 (PC(Δ_1) of order Δ_2), the propagation characteristic of degree Δ_1 (PC(Δ_1)), and the strict avalanche criteria of order Δ_2 (SAC(Δ_2)), where $\Delta, \Delta_1, \Delta_2$ are monotone decreasing sets.

Definition 4. *For two monotone decreasing sets Δ_1 and Δ_2 the function f satisfies* **PC(Δ_1) of order** Δ_2 *iff for every w, such that* $\sup(w) \in \Delta_1 \setminus \{\emptyset\}$ *the function $f(x) \oplus f(x \oplus w)$ is Δ_2-CI. If $\Delta_2 = \emptyset$, the function f is said to be* **PC(Δ_1)**. *If $\Delta_1 = \{A : |A| = 1\}$, the function f satisfies* **SAC(Δ_2)**.

Again if $\Delta_1 = \{A : |A| \leq \ell\}$ and $\Delta_2 = \{B : |B| \leq k\}$ the definitions of PC(Δ_1) function of order Δ_2 and PC(ℓ) function of order k, PC(Δ_1) function and PC(ℓ) function; SAC(Δ_2) function and SAC(k) function coincide. The property balancedness of $f(x) \oplus f(x \oplus w)$ implies for the autocorrelation $r_f(w) = 0$.

4.1 A Relation with Δ-Resilient Functions

We generalize the well-known relation $p+t \leq n-1$ between the order of resiliency t and the degree of propagation p of a Boolean function on $\mathbb{F}_2^n$ as proven in [ZZ00,ChPa02].

Theorem 12. *For a Δ_1-resilient function on $\mathbb{F}_2^n$ which satisfies PC of degree Δ_2 holds that $\Delta_2 \cap \Gamma_1^\perp = \emptyset$ and $\Delta_1 \cap \Gamma_2^\perp = \emptyset$.*

Proof. The Wiener-Khintchine theorem establishes a relation between the squared Walsh and autocorrelation coefficients of a function in $\mathbb{F}_2^n$ [PVV+91]:

$$r_f(u) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} W_f(x)^2 (-1)^{x \cdot u} .$$

Based on it, the following relation, with respect to any linear subspace V, was derived in [CCCF01]:

$$\sum_{u \in V} r_f(u) = \frac{1}{|V^\perp|} \sum_{x \in V^\perp} W_f(x)^2 . \tag{8}$$

Let A be an arbitrary element of $\Delta_2 \setminus \{0\}$. Note that the coefficient $r_f(0)$ is equal to 2^n. Now applying the definition of PC of degree Δ_2 we obtain

$$\sum_{u \in U_A} r_f(u) = r_f(0) = 2^n = \frac{1}{|U_A^\perp|} \sum_{x \in U_A^\perp} W_f(x)^2 .$$

Thus

$$|U_A^\perp| \; 2^n = \sum_{x \in U_A^\perp} W_f(x)^2 = \sum_{x \in U_{A^c}} W_f(x)^2.$$

As a consequence $A^c \notin \Delta_1$ or also $A \notin \Gamma_1^\perp$ because otherwise the right side of the equation above would be zero. This holds for all $A \in \Delta_2$ and thus $\Delta_2 \cap \Gamma_1^\perp = \emptyset$, which is equivalent to $\Delta_2 \subseteq \Delta_1^\perp$. This in turn is equivalent to $\Gamma_2^\perp \subseteq \Gamma_1$, equivalent to $\Delta_1 \subseteq \Delta_2^\perp$ and finally equivalent to $\Delta_1 \cap \Gamma_2^\perp = \emptyset$. □

4.2 Linear Structures

Next we derive a condition for the existence of linear structures for a Δ_1-resilient function which satisfies $PC(\Delta_2)$. A *linear structure* of a function is an element $a \in \mathbb{F}_2^n$ for which $f(x) \oplus f(x \oplus a)$ is a constant. Linear structures should be avoided, for example, in order to resist differential attacks [B93].

Theorem 13. *Let f be a Δ_1-resilient function on $\mathbb{F}_2^n$ that satisfies $PC(\Delta_2)$. If there exists a non-empty element $A \in \Delta_2^+ \cap [\Delta_1^\perp]^+$, then all b with $\sup(b) = B$, $B \in \Gamma_2^-$ and $A \subset B$ are linear structures of f.*

Proof. Let $A \in \Delta_2^+ \cap [\Delta_1^\perp]^+$. From (8) for $V = U_A$ and the assumption, we deduce that there exists x, such that $\sup(x) = A^c \in \Gamma_1^-$ and $W_f(x)^2 = 2^n |U_A^\perp|$ since $W_f(y) = 0 \; \forall y \in U_A^\perp, \; y \neq x$ ($\sup(y) \in \Delta_1$). Next we apply (8) for $V = U_B$, where $B \in \Gamma_2^-$ and $A \subset B$:

$$r_f(0) + r_f(b) = \frac{2}{|U_A^\perp|} \sum_{x \in U_B^\perp} W_f(x)^2 .$$

Because $U_B^\perp \subseteq U_A^\perp$, there are two possibilities:

1. $\sup(x) \subseteq U_B^\perp$, which leads to $r_f(b) = 2^n$;
2. $\sup(x) \nsubseteq U_B^\perp$, which leads to $r_f(b) = -2^n$.

The fact that $|r_f(b)| = 2^n$ implies that b is linear structure of f. □

The following theorem gives a condition on the existence of linear structures for functions which satisfy $PC(\Delta)$. The proof is similar to the one of Theorem 13.

Theorem 14. *Let f be a Boolean function on $\mathbb{F}_2^n$ that satisfies $PC(\Delta)$. If there exists an element $x \in \mathbb{F}_2^n \setminus \{0\}$ such that $\sup(x) \in A^\perp$ for $A \in \Delta^+$ which satisfies $W_f(x) = 2^{n - \frac{|U_A|}{2}}$, then all b with $\sup(b) = B$ and $B \in \Gamma^-, A \subseteq B$ are linear structures of f.*

4.3 Algebraic Degree

First note that the functions satisfying $PC(\mathcal{P}(P))$ are the perfect nonlinear functions (bent functions of characteristic two). From the definition of resiliency, we deduce that for a Boolean function on $\mathbb{F}_2^n$ which satisfies $PC(\Delta_1)$ of order Δ_2, the functions $f(x) \oplus f(x \oplus w)$ are Δ_2-resilient for all $w \in \Delta_1 \setminus \{0\}$. By Theorem 1, the functions $f(x) \oplus f(x \oplus w)$ are balanced for all $w \in \Delta_1 \setminus \{0\}$ on any of the subspaces $a + U_A$, where $A \in \Delta_2^{\perp}$.

The following theorem generalizes the bound on the degree d of a function on $\mathbb{F}_2^n$ satisfying the SAC(k) property [PVV+91], namely $d \leq n - k - 1$.

Theorem 15. *If f satisfies SAC of order Δ then all coefficients a_u from the ANF of f with* $\sup(u) \in \Gamma^{\perp}$ *are equal to zero. Moreover, for all sets $A \in \Gamma^{\perp}$: $|A| > 1$.*

Proof. Assume that $a_u = 1$ for u such that $sup(u) \in \Gamma^{\perp}$ or equivalently $sup(\overline{u}) \in \Delta$. The function $f_{\overline{u}}$ will have maximum degree $wt(u)$ which contradicts the $PC(1)$ property. Note that a function of maximum degree has a non-zero auto-correlation spectrum [PVV+91].

The condition $|A| > 1$ for all $A \in \Gamma^{\perp}$ comes from the fact that a linear function does not satisfy $PC(1)$. □

Corollary 2. *For functions satisfying $PC(\Delta_1)$ of order Δ_2, where $\forall\ A \in \Gamma_2^{\perp}$: $|A| > 1$, the ANF coefficients a_u of f with* $\sup(u) \in \Gamma_2^{\perp}$ *are equal to zero.*

4.4 Constructions

The set of functions which satisfy $PC(\Delta_1)$ of order Δ_2 are globally invariant under the complementation of any of its coordinates, composition with any permutation on $\{1, \ldots, n\}$ which keeps Δ_1, Δ_2 invariant, and the addition of any affine function. We first generalize the change of basis construction.

Theorem 16. *Let Δ be a set containing less than n elements. Then any Boolean function f on $\mathbb{F}_2^n$ which has at least n linearly independent vectors w such that $r_f(w) = 0$ can be transformed into a function that satisfies the PC criterion of degree Δ.*

In [NN03], many coding theoretic notions are generalized in this new setting. A generalization of the linear $[n, k, d]$-code is called an *error-set correcting* code. We slightly change the original notation here and call an Δ-code $\widetilde{C}$ a code of length n and for which codewords x satisfy $\sup(x) \in \Gamma$, where $\Gamma = \Delta^c$. The generator matrix of the code $\widetilde{C}$ can be defined by using the matrix M of a Monotone Span Program.

Definition 5. *[KW93] A Monotone Span Program (MSP) $\mathcal{M}$ is defined by the quadruple $(\mathbb{F}, M, \epsilon, \psi)$, where $\mathbb{F}$ is a finite field, M is a matrix (with m rows and $d \leq m$ columns) over $\mathbb{F}$, $\psi : \{1, \ldots, m\} \to \{1, \ldots, n\}$ is a surjective functions and $\epsilon = (1, 0, \ldots, 0)$ is a fixed non-zero vector, called target vector. The size of $\mathcal{M}$ is the number of rows and is denoted as size($\mathcal{M}$).*

The properties that matrix M (from the MSP $\mathcal{M}$) posses are in one-to-one correspondence with a monotone increasing set Γ. In this case it is said that M computes Γ.

Definition 6. *[NN03] An MSP is called Δ-non-redundant (denoted by Δ-rMSP) when $v \in \ker(M^T) \iff v \neq 0$ and $\sup(v) \in \Gamma$ ($\Gamma = \Delta^c$).*

It is shown in [NN03] how the generator matrix of an Δ-code can be deduced from the results in [V97].

Theorem 17. *Let $\mathcal{M}$ be a Δ-rMSP computing Γ and let $M^\perp$ be the matrix of the dual $\mathcal{M}^\perp$ MSP computing $\Gamma^\perp$. Then a generator matrix G of an Δ-code is given by $G = (M^\perp)^T$.*

The best known and general construction for PC(ℓ) functions of order k is due to Kurosawa and Satoh [KS97]. This construction uses linear codes. It was later generalized by Carlet [C97b] who also takes nonlinear codes into account. We present a further generalization.

Theorem 18. *Let g be an arbitrary function on $\mathbb{F}_2^s$ and Q be an $s \times t$-matrix. Define Δ_1 on $\{1, \ldots, t\}$ and Δ_2 on $\{t+1, \ldots, t+s\}$. Let M_1 be a matrix in Δ_1-rMSP computing Γ_1 and $M_1^\perp$ be the matrix in $\Delta_1^\perp$-rMSP computing $\Gamma_1^\perp$. Let M_2 be a matrix in Δ_2-rMSP computing Γ_2 and $M_2^\perp$ be the matrix in $\Delta_2^\perp$-rMSP computing $\Gamma_2^\perp$. Let $G_1 = (M_1^\perp)^T$ be the generator matrix of a Δ_1-code and let $G_2 = (M_2^\perp)^T$ be the generator matrix of a Δ_2-code. Define the function f on $\mathbb{F}_2^{s+t}$ as follows:*

$$f(x_1, \ldots, x_s, y_1, \ldots, y_t) = [x_1, \ldots, x_s] Q [y_1, \ldots, y_t]^T \oplus g(x_1, \ldots, x_s)\,.$$

Set $Q = G_2^T G_1$ then the function f satisfies PC(Δ_ℓ) of order Δ_k, where $\Delta_\ell = \Delta_1^\perp \uplus \Delta_2^\perp$ and $\Delta_k = \Delta_1 \uplus \Delta_2$.

Proof. Analogous to the proof in [KS97] it is easy to see that if the matrix Q satisfies the following two conditions then f satisfies PC(Δ_ℓ) of order Δ_k:

- $\sup(Qa) \notin \Delta_k$ for any $a \in \mathbb{F}_2^t$, $a \neq 0$ and $\sup(a) \in \Delta_\ell$,
- $\sup(bQ) \notin \Delta_k$ for any $b \in \mathbb{F}_2^s$, $b \neq 0$ and $\sup(b) \in \Delta_\ell$.

Next we verify that $Q = G_2^T G_1$ satisfies both conditions. Indeed by Definition 6 $G_1 a = (M_1^\perp)^T a \neq 0$ if $\sup(a) \in \Delta_1^\perp$ and thus by Theorem 17 $\sup(Qa) = \sup(G_2^T(G_1 a)) \notin \Delta_1$. Analogous $bG_2^T = bM_2^\perp \neq 0$ if $\sup(b) \in \Delta_2^\perp$ and thus $\sup(bQ) = \sup((bG_2^T)G_1) \notin \Delta_2$. These checks conclude the proof. □

Remark 13. Let $\Delta_k = \{A : |A| \leq k\}$ and $\Delta_\ell = \{B : |B| \leq \ell\}$, then $\Delta_\ell^\perp = \{B : |B| \leq n-1-\ell\}$. So, it is easy to verify that $\Delta_k \subseteq \Delta_\ell^\perp$ (in this case) corresponds to $k + \ell \leq n - 1$.

Constructions of functions satisfying propagation characteristics that are not based on codes have been proposed by Gouget [G04]. We now give two examples of them.

Theorem 19. *Let f be a Boolean function on $\mathbb{F}_2^{2n+1}$ defined by*

$$\begin{aligned} f : \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2 &\to \mathbb{F}_2 : \\ (x, y, z) &\mapsto z(g(x) \oplus y_1 \oplus \cdots \oplus y_n) \oplus x \cdot y, \end{aligned}$$

where g is an arbitrary function on $\mathbb{F}_2^n$. If $g(1) = 1$, then f is balanced. The function f satisfies the properties:

1. *$PC(\Delta)$ with $\Delta = \big\{\{1, \cdots, 2n\}, A_1, \ldots, A_n\big\}$, where $A_i = \{1, \ldots, 2n{+}1\}\backslash\{i\}$.*
2. *$PC(\Delta_1)$ of order Δ_2 with the property that $\Delta_1 \uplus \Delta_2 = \Delta$.*

Proof. We refer to [G04] for the proof of the balancedness of f. In order to proof the first part of the theorem, we compute the derivative of f with respect to $(a, b, c) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2$:

$$\begin{aligned} D_{a,b,c}f(x, y, z) = z(g(x) \oplus g(x \oplus a)) \oplus c(g(x \oplus a) \oplus y_1 \oplus \cdots \oplus y_n \oplus b_1 \oplus \cdots \oplus b_n) \\ \oplus z(b_1 \oplus \cdots \oplus b_n) \oplus a \cdot y \oplus b \cdot x \oplus a \cdot b. \end{aligned}$$

It is easy to check that if $sup(a, b, c) \subseteq \Delta$, the derivative $D_{a,b,c}f(x, y, z)$ becomes a linear function in the y-variables. This also means that $D_{a,b,c}f(x, y, z)$ is a balanced function.

For the second part of the proof, let $A \in \Delta_1$ and $B \in \Delta_2$ such that $A \cup B \in \Delta$. Then the derivative with respect to B of the function obtained by fixing the variables corresponding to A is again a function which will linearly depend on y. □

The next construction from [G04] is a generalization of the construction of Honda et al. and can reach a high degree [HSIK97].

Theorem 20. *Let f be a Boolean function on $\mathbb{F}_2^n$ defined by*

$$\begin{aligned} f : \mathbb{F}_2^s \times \mathbb{F}_2^{n-s-1} \times \mathbb{F}_2 &\to \mathbb{F}_2 : \\ (x, y, z) &\mapsto f_1(x) \oplus f_2(y) \oplus f_3(z) \oplus x \cdot \phi(y) \oplus z(x_1 \oplus \cdots \oplus x_n), \end{aligned}$$

where f_1, f_2, f_3 are functions on $\mathbb{F}_2^s, \mathbb{F}_2^{n-s-1}$ and $\mathbb{F}_2$ respectively. The function ϕ is a mapping from $\mathbb{F}_2^{n-s-1}$ into $\mathbb{F}_2^s$. Then f satisfies the propagation criterion of order

$$\Delta = \Big\{\big\{\emptyset, \{1\}, \{2\}, \ldots, \{s\}\big\} \uplus \Delta_2 \uplus \big\{\emptyset, \{n\}\big\}\Big\} \cup \Big\{\Delta_1 \uplus \big\{\emptyset, \{n\}\big\}\Big\},$$

where Δ_1 and Δ_2 are defined on $\{1, \ldots, s\}$ and $\{s + 1, \ldots, n - 1\}$ respectively, if and only if ϕ satisfies the properties:

1. *the function $x \cdot \phi(y)$ is balanced if and only if $sup(x) \in \Delta_1$;*
2. *the function $\phi(y) \oplus \phi(y \oplus x)$ is different from the all-zero and the all-one function for all x such that $sup(x) \in \Delta_2$.*

Proof. Let compute the derivative of f with respect to the triple $(a, b, c) \in \mathbb{F}_2^s \times \mathbb{F}_2^{n-s-1} \times \mathbb{F}_2$:

$$\begin{aligned} D_{(a,b,c)}f(x,y,z) &= D_a f_1(x) \oplus D_b f_2(y) \oplus D_c f_3(z) \oplus x \cdot (\phi(y) \oplus \phi(y \oplus b)) \oplus \\ &\quad a \cdot \phi(y \oplus b) \oplus z(a_1 \oplus \cdots \oplus a_s) \oplus c(x_1 \oplus \cdots \oplus x_s \oplus a_1 \oplus \cdots \oplus a_s). \end{aligned}$$

Note first that when $\mathrm{wt}(a) = 1$ the derivative is a linear function in z, hence $\big\{\{1\}, \{2\}, \ldots, \{s\}\big\} \uplus P(\{s+1, \ldots, n-1\}) \uplus \big\{\emptyset, \{n\}\big\} \in \Delta$.

On the other hand, when $\mathrm{wt}(a) = 0$ and $\sup(b) \in \Delta_2$ the second condition ensures that the derivative is balanced independently of $\mathrm{wt}(c)$. Thus $\Delta_2 \uplus \big\{\emptyset, \{n\}\big\} \in \Delta_2$. Therefore combining both observations (and taking into account the monotone decreasing property) we derive that $\Big\{\big\{\emptyset, \{1\}, \{2\}, \ldots, \{s\}\big\} \uplus \Delta_2 \uplus \big\{\emptyset, \{n\}\big\}\Big\} \in \Delta$. Last notice that when $\mathrm{wt}(b) = 0$ and $\sup(a) \in \Delta_1$ the first condition ensures that the derivative is balanced. So, we have also that $\Delta_1 \uplus \big\{\emptyset, \{n\}\big\} \in \Delta$ which completes the proof. □

5 Conclusions and Open Problems

In this paper we have shown that many classical notions, constructions and results from the theory of cryptographic properties of Boolean functions can be extended to a more general setting: t-resiliency and PC properties can be represented as Δ-resiliency or PC properties with respect to Δ, where $\Delta = \{A : |A| \leq t\}$. Instead of working with numbers, we work with sets, which give us more flexibility in satisfying incompatible requirements as shown in Sect. 3.6. We have also defined analogous notions for the algebraic and the numerical degree of a Boolean function. Then we have proven equivalent results to most of the known inequalities in this new setting. It is much easier to adjust the parameters of a function, when one works with sets compared to numbers. When a trade-off needs to be achieved between parameters of a function, we can easily reduce a set (e.g., Δ) with some of its elements in order to satisfy the condition, comparing to the previous case where we need to reduce the number (e.g., t to $t-1$ for example) discarding all sets of a fixed cardinality (e.g., with cardinality t).

This approach gives more insight and better understanding in the behaviour of a Boolean function. More precisely, it allows us to determine which structural properties contributes to different known results like for instance the Siegenthaler's inequality. Future work will investigate if these insights lead to new constructions of t-resilient functions (functions satisfying PC properties) by going over special monotone set resilient function (PC functions).

We leave as an open question whether such functions exist for any Δ. In the theory of Secret Sharing Schemes (SSS), a scheme (or equivalently a monotone increasing set) is called *ideal* if each player has a share of minimal size. But it is known that for "many" monotone sets there is no ideal scheme, i.e., there is no finite field in which the SSS is ideal. For Boolean functions we consider only this ideal case, since every coordinate (input) in the function is considered as

a player's share. Thus in the binary field there are monotone sets Γ for which there does not exist a corresponding MSP (equivalently SSS). We do not know a relation between MSPs and Δ-resilient functions, but it seems likely that there exist sets Δ for which there does not exist a corresponding Δ-resilient function.

References

[B93] E. Biham, Differential Cryptanalysis of the Full 16-Round DES, *Crypto 1992, LNCS 740,* Springer-Verlag, pp. 487-496, 1993.

[CCCS92] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On Correlation Immune Functions, *Crypto 1991, LNCS 576,* Springer-Verlag, pp. 86-100, 1992.

[CCCF00] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions, *Eurocrypt 2000, LNCS 1807,* Springer-Verlag, pp. 507-522, 2000.

[CCCF01] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On Cryptographic Properties of the Cosets of $RM(1,m)$, *IEEE Trans. Information Theory,* Vol. 47(4), pp. 1494-1513, 2001.

[C93] C. Carlet, Partially-Bent Functions, *Designs, Codes and Cryptography,* Vol. 3(2), pp. 135-145, 1993.

[C97a] C. Carlet, More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings, *Eurocrypt 1997, LNCS 1233,* Springer-Verlag, pp. 422-433, 1997.

[C97b] C. Carlet, On Cryptographic Propagation Criteria for Boolean Functions, *Information and Computation,* Vol. 151(1-2), pp. 32-56, 1999.

[C00] C. Carlet, On the Coset Weight Divisibility and Nonlinearity of Resilient Functions, Sequences and their Applications 2001, *Discrete Mathematics and Theoretical Computer Science,* pp. 131-144, 2001.

[CG01] C. Carlet, P. Guillot, Bent, Resilient Functions and the Numerical Normal Form, *Discrete Mathematics and Theoretical Computer Science,* pp. 87-96, 2001.

[CS02] C. Carlet, P. Sarkar, Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions, *Finite fields and Applications,* Vol. 8, pp. 120-130, 2002.

[CaPr03] C. Carlet, E. Prouff, On Plateaued Functions and Their Constructions, *Fast Software Encryption 2003, LNCS 2887,* Springer-Verlag, pp. 57-78, 2003.

[ChPa02] P. Charpin, E. Pasalic, On Propagation Characteristics of Resilient Functions, *Selected Areas in Cryptography 2002, LNCS 2595,* Springer-Verlag, pp. 356-365, 2002.

[CLLS96] S. Chee, S. Lee, D. Lee, S.H. Sung, On the Correlation Immune Functions and Their Nonlinearity, *Asiacrypt 1996, LNCS 1163,* Springer-Verlag, pp. 232-243, 1996.

[CM03] N. Courtois, W. Meier, Algebraic Attacks on Stream Ciphers with Linear Feedback, *Eurocrypt 2003, LNCS 2656,* Springer-Verlag, pp. 345-359, 2003.

[DGV94] J. Daemen, R. Govaerts, J. Vandewalle, Correlation Matrices, *Fast Software Encryption 1994, LNCS 1008,* Springer-Verlag, pp. 275-285, 1995.

[D95] J. Daemen, *Cipher and Hash Function Design,* PhD thesis, Katholieke Universiteit Leuven, 1995.

[D74] J. Dillon, *Elementary Hadamard Difference Sets,* PhD thesis, University of Maryland, 1974.

[DXS91] C. Ding, G. Xiao, W. Shan, Stability Theory of Stream Ciphers, Springer, 1991.

[DSS01] Y. Dodis, A. Sahai, A. Smith, On Perfect and Adaptive Security in Exposure Resilient Functions, *Eurocrypt 2001, LNCS 2045,* Springer-Verlag, pp. 301-324, 2001.

[FM02] S. Fehr, U. Maurer, Linear VSS and Distributed Commitments Based on Secret Sharing and Pairwise Checks, *Crypto 2002, LNCS 2442,* Springer-Verlag, pp. 565-580, 2002.

[G04] A. Gouget, Etude des propriétés cryptographiques des fonctions booléennes et algorithme de confusion pour le chiffrement symétrique, Phd. thesis, Université de Caen, 2004.

[GS02] K. Gupta, P. Sarkar, Improved Construction of Nonlinear Resilient S-Boxes, *Asiacrypt 2002, LNCS 2501,* Springer-Verlag, pp. 466-483, 2002.

[HSIK97] T. Honda, T. Satoh, T. Iwata, K. Kurosawa, Probabilistic higher order differential attack and higher order bent functions, *SAC 1997*, LNCS 1556, Springer-Verlag, pp. 64–72, 1997.

[JJ99] T. Johansson, F. Jönsson, Fast Correlation Attacks Based on Turbo Code Techniques, *Crypto 1999, LNCS 1666,* Springer-Verlag, pp. 181-197, 1999.

[J92] D. Jungnickel, *Finite Fields. Structure and Arithmetics,* BI, Wissenschaftverslag, 1992.

[K99] K. Kurosawa, Almost Security of Cryptographic Boolean Functions, Cryptology e-print archive, http://eprint.iacr.org/2003/075.

[KJS01] K. Kurosawa, T. Johansson, D.R. Stinson, Almost k-wise Independent Sample Spaces and Their Cryptologic Applications, *Journal of Cryptology,* Vol. 14(4), pp. 231-253, 2001.

[KS97] K. Kurosawa, T. Satoh, Design of SAC/PC(ℓ) of order k Boolean Functions and Three Other Cryptographic Criteria, *Eurocrypt 1997, LNCS 1233,* Springer-Verlag, pp. 434-449, 1997.

[KW93] M. Karchmer, A. Wigderson, On Span Programs, *Proc. of 8-th Annual Structure in Complexity Theory Conference,* pp. 102-111, 1993.

[L91] P. Langevin, On the Covering Radius of $RM(1,9)$ in $RM(3,9)$, *Eurocode 1990, Coding Theory and Applications, LNCS 514,* Springer-Verlag, pp. 51-59, 1991.

[MS] F.J. MacWilliams, N.J. Sloane, *The Theory of Error Correcting Codes,* North Holland, Amsterdam, 1977.

[M93] K. Martin, *Discrete Structures in the Theory of Secret Sharing,* PhD thesis, Royal Holloway and Bedford New College, 1993.

[M69] J.L. Massey, Shift-Register Synthesis and BCH Decoding, *IEEE Trans. Information Theory,* pp. 122-127, 1969.

[MS92] W. Meier, O. Staffelbach, Fast Correlation Attacks on Certain Stream Ciphers, *Journal of Cryptology,* pp. 67–86, 1992.

[NN03] V. Nikov, S. Nikova, On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Schemes, Cryptology e-print archive, http://eprint.iacr.org/2003/210.

[PVV+91] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle, Propagation Characteristics of Boolean Functions, *Eurocrypt 1990, LNCS 473,* Springer-Verlag, pp. 161-173, 1991.

[RS87] R.A. Rueppel, O.J. Staffelbach, Products of Linear Recurring Sequences with Maximum Complexity, *IEEE Trans. Information Theory,* Vol. 33(1), pp. 124–131, 1987.

[S] D. Stinson, *Combinatorial Designs and Cryptography, Surveys in combinatorics,* 1993, Cambridge University Press, New York, NY, 1993.

[S84] T. Siegenthaler, Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications, *IEEE Trans. Information Theory,* pp. 776–780, 1984.

[S85] T. Siegenthaler, Decrypting a Class of Stream Ciphers Using Ciphertext Only, *IEEE Trans. Computers,* pp. 81–85, 1985.

[SM00] P. Sarkar, S. Maitra, New directions in Design of Resilient Boolean Functions, Cryptology e-print archive, http://eprint.iacr.org/2000/009.

[SZZ95] J. Seberry, X.-M. Zhang, Y. Zheng, Relationship Between Propagation Characteristics and Nonlinearity of Cryptographic Functions, *Journal of Universal Computer Science,* Vol. 1(2), pp. 136-150, 1995.

[V97] M. Van Dijk, *Secret Key Sharing and Secret Key Generation,* PhD Thesis, 1997, TU Eindhoven.

[WD97] C.-K. Wu, E. Dawson, Construction of Cryptographic Correlation-Immune Boolean Functions, *Information and Communications Security 1997, LNCS 1334,* Springer-Verlag, pp. 170-180, 1997.

[XM88] G.Z. Xiao, J.L. Massey, A spectral Characterization of Correlation-Immune Combining Functions, *IEEE Trans. Information Theory,* Vol. 34, pp. 569-571, May 1988

[ZZ97] Y. Zheng, X.M. Zhang, Cryptographically Resilient Functions, *IEEE Trans. Information Theory*, Vol. 43(5), pp. 1740-1747, 1997.

[ZZ99a] Y. Zheng, X.M. Zhang, Strong Linear Dependence of Unbiased Distribution on Non-propagative Vectors, *Selected Areas in Cryptography 1999, LNCS 1758,* Springer-Verlag, pp. 92-105, 1999.

[ZZ99b] Y. Zheng, X.M. Zhang, Plateaued Functions, *International Conference on Information and Communications Security, LNCS 1726,* Springer-Verlag, pp. 284-300, 1999.

[ZZI99] Y. Zheng, X.M. Zhang, H. Imai, Connections Between Nonlinearity and Restrictions, Terms and Hypergraphs of Boolean Functions, *IEEE International Symposium on Information Theory 1998,* IEEE Press, pp. 439, 1998.

[ZZ00] Y. Zheng, X.M. Zhang, On Relationship Among Avalanche, Nonlinearity, and Propagation Criteria, *Asiacrypt 2000, LNCS 1976,* Springer-Verlag, pp. 470-483, 2000.