A Construction of Resilient Functions with High Nonlinearity *

Thomas Johansson and Enes Pasalic

Dept. of Information Technology
Lund University, P.O. Box 118, 221 00 Lund, Sweden
{thomas, enes}@it.lth.se

October 23, 2000

Abstract

The relationship between nonlinearity and resiliency for a function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is considered. We give a construction of resilient functions with high nonlinearity. The construction leads to the problem of finding a set of linear codes with a fixed minimum distance, having the property that the intersection between any two codes is the all zero codeword only. This problem is considered, and existence results are provided. The constructed functions obtain a nonlinearity superior to previous construction methods.

I Introduction

A classical method for constructing keystream generators is to combine a set of linear feedback shift registers with a nonlinear Boolean function. Then the Boolean function $f(x)$, $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ must fulfill certain properties in order to increase the time/space complexity of different attacks. Common attacks are Siegenthaler correlation attack [23], Berlekamp-Massey linearity synthesis attack [13] and different linear approximation attacks [8]. There are at least four main criteria that $f(x)$ should fulfill. These are: balancedness, high nonlinearity, high algebraic degree, and some correlation immunity (for balanced functions, correlation immunity is usually referred to as reciliency).

In a modern design of a stream cipher, one might in many situations want to consider functions mapping to a block of output bits, i.e., functions of the form $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ (n-input m-output functions). In block cipher design such functions are referred to as S-boxes. S-boxes is a well studied subject, and different important criteria have been considered. These include the propagation criterion (PC), the strict avalanche criterion (SAC), etc. [17].

*This work has been presented at ISIT 2000.

For applications in stream ciphers, we turn our attention to the criteria mentioned above for Boolean functions. In particular, we consider the interesting relationship between resiliency and nonlinearity for balanced functions $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$.

For the case of Boolean functions ($m = 1$), the results in [4] provide a simple method of generating functions, $\{f\} : \mathbb{F}_2^n \mapsto \mathbb{F}_2$, with some fixed resiliency and high nonlinearity. This construction has been used as a basis for further improvements in e.g. [11, 19]. We now have quite a lot of results for the case $m = 1$. A nice summary of the current situation can be found in [11].

When $m > 1$ the situation is different. A few papers [10, 27] have appeared before, providing nonlinear functions with some resiliency. But, as will be demonstrated, it is possible to significantly improve upon these results. We will in this paper present a construction of highly nonlinear and resilient n-input m-output functions, where $m \geq 1$. The construction, which for $m = 1$ is the same as [4], is based on a coding theoretic problem, which to our knowledge is new. We are interested in finding a set of linear codes with a fixed minimum distance d, such that the intersection between any two codes is the all zero codeword only. This is referred to as a set of nonintersecting linear codes. The problem is to find the maximal cardinality of such a set. This is considered, and existence results are provided. The constructed functions obtain a nonlinearity superior to previous construction methods.

The paper is organized as follows. Section II provides basic definitions and notations both for 1-output and m-output functions, $m > 1$. In Section III we describe a new method for constructing highly nonlinear n-input m-output t-resilient functions and briefly discuss constraints on the parameters n, m and t. In Section IV, we show how error correcting codes can be used in the construction, and in Section V we provide some existence bounds regarding the cardinality of a set of nonintersecting linear codes. Some numerical values for constructed functions and a comparison with previous constructions [10, 27] are also presented.

II Preliminaries

We review some relevant notation, definitions and known results in the considered area. Since the function $f(x)$, $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, can be regarded as composed of m Boolean functions $f = (f_1, \ldots, f_m)$, we first introduce some concepts for a Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ [3, 4, 9]. A Boolean function $f(x)$ can be expressed in algebraic normal form (ANF), i.e., there are unique constants $a_0, a_1, \ldots, a_{12}, \ldots, a_{12\cdots n} \in \mathbb{F}_2$ such that

$$\begin{aligned} f(x_1, \ldots, x_n) = & a_0 + a_1x_1 + \cdots + a_nx_n + \\ & + a_{12}x_1x_2 + a_{13}x_1x_3 + \cdots + a_{12\cdots n}x_1x_2\cdots x_n, \end{aligned} \quad (1)$$

where addition and multiplication are in $\mathbb{F}_2$.

Definition 1 *The* algebraic degree *of $f(x)$, denoted deg(f), is defined to be the maximum degree appearing in the ANF.*

Many properties for Boolean functions are studied through the Walsh transform (or almost equivalently through the Walsh-Hadamard transform).

Definition 2 *The Walsh transform of a Boolean function $f(x)$ is defined to be the real-valued function $\mathcal{F}(\omega)$ over the vector space $\mathbb{F}_2^n$ given by*

$$\mathcal{F}(\omega) = \sum_x (-1)^{f(x)}(-1)^{\omega\cdot x} \;, \tag{2}$$

where the dot product *of vectors x and ω is defined as $x \cdot \omega = x_1\omega_1 + \cdots + x_n\omega_n$.*

We say that the Boolean function $f(x)$ is *balanced* if $P(f(x) = 1) = P(f(x) = 0) = 0.5$. Alternatively, using the Walsh transform, $f(x)$ is balanced if and only if $\mathcal{F}(0) = 0$.

Let $\mathcal{F}_n$ be the set of all Boolean functions in n variables. For two functions $f(x), g(x) \in \mathcal{F}_n$ the Hamming distance between them is defined as,

$$d_H(f, g) = |\{x|f(x) \neq g(x), x \in \mathbb{F}_2^n\}|. \tag{3}$$

Definition 3 *The* nonlinearity *of a Boolean function $f(x)$, denoted by N_f, is defined as*

$$N_f = \min_{g\in\mathcal{A}_n} d_H(f, g), \tag{4}$$

where $\mathcal{A}_n = \{a_0 + a_1x_1 + \cdots + a_nx_n|a_i \in \mathbb{F}_2, 0 \leq i \leq n\}$ is the set of all affine functions on n variables.

The nonlinearity of $f(x)$ can be obtained through the Walsh transform as follows,

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_2^n} |\mathcal{F}(\omega)|, \; \omega \neq 0. \tag{5}$$

Finding Boolean functions with maximal nonlinearity is an important and well studied problem. For n even, maximal nonlinearity is obtained by the *bent functions* [12, 18]. For n odd, maximal nonlinearity is only known for $n < 9$, and determining it for $n \geq 9$ is (probably) a very hard challenge [16]. Since bent functions are not balanced, another hard open problem is to find the maximum nonlinearity for balanced functions when n is even [7, 12, 20]

Continuing, the next definition concerns the function's ability not to leak information to the output when a subset of the input variables is kept fixed.

Definition 4 *A Boolean function $f(x)$ on n variables is said to be m-th order* correlation immune *(m-CI), if for any m-tuple of independent identically distributed binary random variables $X_{i_1}, X_{i_2}, \ldots, X_{i_m}$, we have*

$$I(X_{i_1}, X_{i_2}, \ldots, X_{i_m}; Z) = 0, \quad 1 \leq i_1 < i_2 < \cdots < i_m \leq n, \tag{6}$$

where $Z = f(X_1, X_2, \ldots, X_n)$, and $I(X; Z)$ denotes the mutual information [6].

The following lemma was first proved by Siegenthaler [22], and characterizes the correlation immunity in the Walsh transform domain.

Lemma 1 *A Boolean function $f(x_1, \ldots, x_n)$ is m-th order correlation immune (m-CI) if and only if*

$$\mathcal{F}(\omega) = 0, \quad \omega|1 \leq w_H(\omega) \leq m, \tag{7}$$

where $w_H(\omega)$ denotes the Hamming weight of ω, i.e., the number of ones in ω.

Finally, an m-th order correlation immune Boolean function which is balanced is called an m-th order *resilient* (m-resilient) function.

This paper will be directed towards the study of trade-offs between resiliency and nonlinearity. In the special case of Boolean functions (as assumed above), a lot of work has been done, see for example [4, 9, 11, 15, 19, 20, 26].

Now we generalize the notion above to functions $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. Let $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ be a function defined by $F(x) = (f_1(x), \ldots, f_m(x))$, where $f_1, \ldots, f_m$ are Boolean functions mapping $\mathbb{F}_2^n \mapsto \mathbb{F}_2$. We start with a formal definition of a resilient function.

Definition 5 *Let $F = (f_1, f_2, \ldots, f_m)$ be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ where $1 \leq m \leq n$, and let $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$.*

1. *F is said to be unbiased w.r.t. a fixed subset $T = \{j_1, \ldots, j_t\}$ of $\{1, \ldots, n\}$, if for every $(a_1, \ldots, a_t) \in \mathbb{F}_2^t$*

$$(f_1(x), \ldots, f_m(x))|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$$

runs through all the vectors in $\mathbb{F}_2^m$, each 2^{n-m-t} times, when $(x_{i_1}, \ldots, x_{i_{n-t}})$ runs through $\mathbb{F}_2^{n-t}$, where $t \geq 0$, $\{i_1, \ldots, i_{n-t}\} = \{1, \ldots, n\} - \{j_1, \ldots, j_t\}$ and $i_1 < \cdots < i_{n-t}$.

2. *F is said to be an (n, m, t)-resilient function if F is unbiased w.r.t. every $T \subseteq \mathbb{F}_2^n$ with $|T| = t$. The parameter t is called the resiliency of the function.*

The following lemma (*XOR Lemma*) is well known and gives the relationship between a resilient function and its component functions [21].

Lemma 2 *A function $F = (f_1, f_2, \ldots, f_m)$, where each f_i, $1 \leq i \leq m$, is a function $\mathbb{F}_2^n \mapsto \mathbb{F}_2$, is uniformly distributed (unbiased) if and only if all nonzero linear combinations of $f_1, \ldots, f_m$ are balanced.*

Hence, an immediate consequence of the previous lemma is the following.

Lemma 3 *A function $F = (f_1, f_2, \ldots, f_m)$ is an (n, m, t)-resilient function if and only if all nonzero linear combinations of $f_1, f_2, \ldots, f_m$ are $(n, 1, t)$-resilient functions.*

The definition of nonlinearity follows in a similar manner, taken from [14].

Definition 6 *The nonlinearity of $F = (f_1, f_2, \ldots, f_m)$, denoted by N_F, is defined as the minimum among the nonlinearities of all nonzero linear combinations of the component functions of F, i.e.,*

$$N_F = \min_{\hat{f} \in \hat{\mathcal{F}}} N_{\hat{f}} \tag{8}$$

where

$$\hat{\mathcal{F}} = \{\hat{f} | \hat{f} = \sum_{j=1}^{m} c_j f_j, c_j \in \{0, 1\}, (c_1, \ldots, c_m) \neq (0, \ldots, 0)\}. \tag{9}$$

Similarly, the *algebraic degree* of F is defined as the minimum of degrees of all nonzero linear combinations of the component functions of F, namely,

$$deg(F) = \min_{\hat{f}\in\hat{\mathcal{F}}} deg(\hat{f}), \tag{10}$$

where $\hat{\mathcal{F}}$ is defined in (9).

Some work on resilient functions have appeared. Important theoretical results were obtained by Stinson and Massey [25] when disproving a conjecture in [1]. They showed that there exists an infinite class of nonlinear functions with strictly higher resiliency than what is possible to obtain using linear functions with the same parameters. In [27] the converse of the conjecture in [1] was demonstrated, that is, if there exists a linear resilient function with certain parameters, then there exists a nonlinear resilient function with the same parameters. Thus, starting with a linear resilient function and applying a highly nonlinear permutation to it, a large number of distinct nonlinear resilient functions can be obtained.

The connection between linear resilient functions and linear codes was established in [1, 5], and the equivalence between resilient functions and large set of orthogonal arrays was considered in [24]. The main result can shortly be expressed as follows. There exists a linear (n, m, t)-resilient function if and only if there exists a linear $[n, m, t+1]$ code (equivalently, if there exists a large set of orthogonal arrays $LOA_{2^{n-m-t}}(t, n, 2)$ [2]).

Previous work on high nonlinearity for resilient functions is much more limited. Essentially, two constructions have appeared, see [10, 27]. In [10], concatenation of resilient functions with bent functions was used in order to obtain nonlinear resilient functions. In [27], a highly nonlinear permutation is applied to a linear resilient function. We will compare our results with these two constructions later on.

Finally, we want to pay attention to the fact that functions mapping $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ have been extensively studied in the area of *S-box design* for block ciphers [13]. Here, e.g., the concept of nonlinearity appears. However, the tradeoff between nonlinearity and resiliency has not been considered here.

III A construction of highly nonlinear (n, m, t)-resilient functions

In this section, we present our construction of t-resilient functions, $\{F\} : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ with high nonlinearity. We use the Walsh transform as a tool for proving the properties of F. For $m = 1$ the construction will coincide with the one given in [4]. It is summarized by the following theorem.

Theorem 4 *Let n, m, t and d be four positive integers with $n \geq 4, 1 \leq t \leq n-3, 1 \leq d \leq n-t, m \leq n-d$.*

For each pair (y, i), where $y \in \mathbb{F}_2^d$, $i = 1, \ldots, m$, let $A_y^i \in \mathbb{F}_2^{n-d}$ such that $w_H(A_y^i) \geq t+1$, where $w_H()$ denotes the Hamming weight.

For $a \in \mathbb{F}_2^{n-d}$, $c = (c_1, \ldots, c_m) \in \mathbb{F}_2^m$, *let*

$$s^*_{a,c} = |\{y \in \mathbb{F}_2^d | \sum_{i=1}^{m} c_i A_y^i = a\}|.$$

Finally let $s^* = \max_{c \in \mathbb{F}_2^m} \max_{a \in \mathbb{F}_2^{n-d}} s^*_{a,c}$.

We now define a function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ *by*

$$F(y, x) = (A_y^1 x, A_y^2 x, \ldots, A_y^m x),$$

where $y = (y_1, \ldots, y_d) \in \mathbb{F}_2^d, x = (x_1, \ldots, x_{n-d}) \in \mathbb{F}_2^{n-d}$. *Then the following holds:*

1. *F is uniformly distributed if* $\sum_{i=1}^m c_i A_y^i \neq 0$, *for any* $c \in \mathbb{F}_2^m, c \neq \mathbf{0}$.

2. *F is t-resilient if for any* $a \in \mathbb{F}_2^{n-d} \mid 0 \leq wt(a) \leq t$ *and* $c \in \mathbb{F}_2^m$, $c \neq \mathbf{0}$, *it holds that* $\sum_{i=1}^m c_i A_y^i \neq a$.

3. $N_F = 2^{n-1} - s^* 2^{n-d-1}$.

Proof.

1. Let $g_c : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ be a function defined by $g_c(y, x) = \sum_{i=1}^m c_i A_y^i x$ for $c \in \mathbb{F}_2^m$, $c \neq \mathbf{0}$. Then

$$\mathcal{F}_{g_c}(0) = \sum_{y,x} (-1)^{g_c(y,x)} = \sum_y \sum_x (-1)^{(c_1 A_y^1 + \cdots + c_m A_y^m)x} = 0,$$

since by assumption $\sum_{i=1}^m c_i A_y^i \neq 0$, for any $c \in \mathbb{F}_2^m, c \neq \mathbf{0}$. Now $\mathcal{F}_{g_c}(0) = 0$ implies that g_c is balanced and Lemma 2 then proves that $F(y, x)$ is also balanced.

2. We use Lemma 3 and show that all nonzero linear combinations of the component functions of F are $(n, 1, t)$-resilient functions. Let $g_c(y, x) = \sum_{i=1}^m c_i A_y^i x$ for some $c \in \mathbb{F}_2^m, c \neq \mathbf{0}$. Then, for any $(b, a) \in \mathbb{F}_2^n$ with $1 \leq w_H(b, a) \leq t$, we have

$$\begin{aligned}
\mathcal{F}_{g_c}(b, a) &= \sum_{y,x} (-1)^{g_c(y,x)} (-1)^{(b,a)\cdot(y,x)} \\
&= \sum_{y,x} (-1)^{\sum_{i=1}^m c_i A_y^i x} (-1)^{b\cdot y + a\cdot x} \\
&= \sum_y (-1)^{b\cdot y} \sum_x (-1)^{(c_1 A_y^1 + \cdots + c_m A_y^m + a)x}. \qquad (11)
\end{aligned}$$

Now $\sum_x (-1)^{(c_1 A_y^1 + \cdots + c_m A_y^m + a)x} = 0$ if $\sum_{i=1}^m c_i A_y^i \neq a$. Since $0 \leq w_H(a) \leq t$, this always holds and then $g_c(y, x)$ is t-resilient for any $c \in \mathbb{F}_2^m, c \neq \mathbf{0}$. Through Lemma 3 we get that $F(y, x)$ is t-resilient.

3. Let $g_c(y,x) = \sum_{i=1}^{m} c_i A_y^i x$ for some $c \in \mathbb{F}_2^m, c \neq \mathbf{0}$. Then, by (11),

$$\begin{aligned} \mathcal{F}_{g_c}(b,a) &= \sum_y (-1)^{b \cdot y} \sum_x (-1)^{(c_1 A_y^1 + \cdots + c_m A_y^m + a)x} \\ &= 2^{n-d} \sum_{\{y \mid \sum_{i=1}^{m} c_i A_y^i = a\}} (-1)^{b \cdot y}. \end{aligned} \tag{12}$$

Hence,

$$\begin{aligned} \max_{b,a} |\mathcal{F}_{g_c}(b,a)| &\leq 2^{n-d} \max_{c \in \mathbb{F}_2^m} \max_a s^*_{a,c} && (13) \\ &= s^* 2^{n-d}. && (14) \end{aligned}$$

If we let $b = 0$ in (12), we have

$$|\mathcal{F}_{g_c}(0,a)| = 2^{n-d} |\{y | \sum_{i=1}^{m} c_i A_{y_i} = a\}| = 2^{n-d} s^*_{a,c}.$$

It follows that

$$\begin{aligned} \max_{b,a} |\mathcal{F}_{g_c}(b,a)| &\geq \max_a |\mathcal{F}_g(0,a)| && (15) \\ &= 2^{n-d} \max_{c \in \mathbb{F}_2^m} \max_a s^*_{a,c} && (16) \\ &= s^* 2^{n-d}. && (17) \end{aligned}$$

Therefore, $\max_{b,a} |\mathcal{F}_{g_c}(b,a)| = s^* 2^{n-d}$. By eq. (5),

$$N_F = 2^{n-1} - s^* 2^{n-d-1}. \tag{18}$$

□

Note that in this construction the component functions are actually a concatenation of 2^d linear t-resilient functions in $n-d$ variables. Thus, $y \in \mathbb{F}_2^d$ can be viewed as a specific address to some linear function. Clearly, a large number of distinct functions with same parameters can be obtained by permuting the values of $(A_y^1, \ldots, A_y^m)$. Let us for convenience introduce the following notation,

$$A = \begin{pmatrix} A^1_{00\cdots 00} & A^2_{00\cdots 00} & \cdots & A^m_{00\cdots 00} \\ A^1_{00\cdots 01} & A^2_{00\cdots 01} & \cdots & A^m_{00\cdots 01} \\ \vdots & & & \\ A^1_{11\cdots 11} & A^2_{11\cdots 11} & \cdots & A^m_{11\cdots 11} \end{pmatrix}.$$

By equation (18), the nonlinearity of F depends only on two parameters, namely, s^* which is the maximum number of identical vectors appearing in any linear combination of A's columns, and d which is to be maximized in order to obtain highest nonlinearity. In our construction we focus on $s^* = 1$. This leaves us with a maximization problem on d. We would like to find the smallest value of $n-d$ under the condition that we can construct the matrix A with $s^* = 1$.

This leads to certain conditions on A. Our first observation is that if F is to be t-resilient, the vectors contained in each row of the matrix A spans an $[n-d, m, t+1]$ linear code. This follows directly from the condition

$$w_H(\sum_{i=1}^{m} c_i A_y^i) \geq t+1, \quad \forall c = (c_1, \ldots, c_m) \neq 0,$$

in 2. of Theorem 4. The second observation is that if the nonlinearity of F is to be maximized for a fixed parameter d, i.e., we want to achieve $s^* = 1$, then

$$\sum_{i=1}^{m} c_i A_y^i \neq \sum_{i=1}^{m} c_i A_{y'}^i, \quad \forall c = (c_1, \ldots, c_m) \neq 0,$$

if $y \neq y'$. We will consider these properties much more in the next section. But before that, we provide the main results of two previously known constructions, and show an example of our construction for comparison.

Zhang and Zheng [27] showed how to transform linear resilient functions into nonlinear resilient functions based on the following result.

Lemma 5 *[27] If there exists a linear (n, m, t)-resilient function, then there exists a nonlinear (n, m, t)-resilient function $F(x)$ whose nonlinearity satisfies $N_F \geq 2^{n-1} - 2^{n-\frac{1}{2}m}$ and whose algebraic degree is $m-1$.*

Another construction of nonlinear (n, m, t)-resilient functions was examined in [10]. The performance is given as follows.

Lemma 6 *[10] For any even l such that $l \geq 2m$, if there exists an $(n-l, m, t)$-resilient function $\psi(x)$, then there exists an (n, m, t)-resilient function $F(x)$ whose nonlinearity satisfies $N_F > 2^{n-1} - 2^{n-\frac{l}{2}-1}$.*

The resilient functions required in the above lemmas can be obtained through good error correcting codes. As proved in [10], there is a tradeoff between the nonlinearity and resiliency when the two constructions given above are compared. Lemma 5 gives higher nonlinearity than Lemma 6, while the latter gives larger resiliency for the same n and m.

In the following example we demonstrate our construction and show that it gives better nonlinearity for a particular choice of parameters. Other choices of the parameters n, m, t will be examined later.

Example 1 *Consider a function $F(y, x) : \mathbb{F}_2^{10} \mapsto \mathbb{F}_2^2$. Choose $d = 4$ in Theorem 1. Then the function defined by $F(y, x) = (A_y^1 x, A_y^2 x)$ will be a $(10, 2, 2)$-resilient function with nonlinearity $N_F = 480$, provided $s^* = 1$. The set of vectors A_y^1 and A_y^2 is given below in matrix form, where every entry in A specifies a linear t-resilient Boolean function on $n-d$ variables.*

$$A = \begin{pmatrix} (100110) & (111000) \\ (111000) & (011110) \\ (011110) & (100110) \\ (010011) & (011100) \\ (011100) & (001111) \\ (001111) & (010011) \\ (101001) & (001110) \\ (001110) & (100111) \\ (100111) & (101001) \\ (110100) & (000111) \\ (000111) & (110011) \\ (110011) & (110100) \\ (011010) & (100011) \\ (100011) & (111001) \\ (111001) & (011010) \\ (001101) & (110001) \end{pmatrix}$$

It is easily verified that the linear combinations of the vectors in each row of A yield new vectors all having the weight greater than or equal to 3 ($t+1$), as required. Furthermore, none of the vectors appear more than once in each column of A or in any linear combination of A's columns, i.e., $s^* = 1$. Thus, the function $F(y, x)$ is indeed 2-resilient and the nonlinearity is given by,

$$N_F = 2^{n-1} - 2^{n-d-1} = 480.$$

Since, $m = 2$ in the example above, it is not possible to obtain a nonlinear $(10, 2, 2)$-resilient function or any nonlinear $(n, 2, t)$-resilient function using the Zhang and Zheng construction.

Suppose, that we want to construct a $(10, 2, 2)$-resilient function using the construction in Lemma 6. Since $m = 2$, the requirement is that there must exist a $(10 - l, 2, 2)$-resilient function in order to construct a $(10, 2, 2)$-resilient function. According to Lemma 6, l is even and $l \geq 2m$. For $l \geq 6$ it is easily proved that a $(10 - l, 2, 2)$-resilient function does not exist. Thus, the only possibility is to take $l = 4$, which gives a nonlinearity of,

$$N_F > 2^{n-1} - 2^{n-\frac{l}{2}-1} = 384.$$

IV How to construct the matrix A

As mentioned before, the nonlinearity depends on the value of d. Hence, we first note that for any given (n, m, t), n being the number of input variables, m the number of output variables and t the order of resiliency, d must satisfy the following inequality,

$$\binom{n-d}{t+1} + \binom{n-d}{t+2} + \cdots + \binom{n-d}{n-d} \geq 2^d. \tag{19}$$

The inequality is a simple consequence of the fact that for any component function of F we have to choose the vectors in $\mathbb{F}_2^{n-d}$ with weight greater than the order of resiliency. Thus, for any n, t, let d_{max} be the largest value of d such that (19) holds. An upper bound on the nonlinearity for this construction, denoted N_F^{ub}, is obtained as,

$$N_F^{ub} \leq 2^{n-1} - 2^{n-d_{max}-1}.$$

Computing the values of d_{max} by using (19), Table 1 is obtained.

$N_F(d_{max})$	n					
t	7	8	9	10	11	12
1	56 (3)	112 (3)	240 (4)	480 (4)	992(5)	1984(5)
2	48 (2)	112 (3)	240 (4)	480 (4)	992(5)	1984(5)
3	48 (2)	96 (2)	224 (3)	480 (4)	960(4)	1984(5)
4	32 (1)	96 (2)	192 (2)	448 (3)	960(4)	1920(4)

Table 1: Upper bound on N_F for the construction.

We interpret the entries in the table as follows. Consider the particular values of $n = 10$ and $t = 2$. The maximum nonlinearity equals $N_F = 480$ and $d_{max} = 4$. Since the upper bound is met with equality for $m = 1$, it also reflects the results obtained in [4]. Note that this construction is not optimal for $m = 1$. In a few cases improvements have been found, e.g., for $n = 10, t = 1$, $N_F = 484$ was obtained in [11]

An interesting question is how many additional output variables we can have, while keeping the same maximal value for the nonlinearity N_F. In the example in the previous section we verified that for $m = 2$, $n = 10$, and $t = 2$ we were able to fill up 16 rows of the matrix A without violating the constraints given in Theorem 1, getting the same nonlinearity $N_F = 480$ as in the case $m = 1$.

In order to construct the matrix A, we rely first on the following lemma.

Lemma 7 *Let $c_0, \ldots, c_{m-1}$ be a basis of a binary $[n-d, m, t+1]$ linear code C. Let β be a primitive element in $\mathbb{F}_{2^m}$ and $(1, \beta, \ldots, \beta^{m-1})$ be a polynomial basis of $\mathbb{F}_{2^m}$. Define a bijection $\phi : \mathbb{F}_{2^m} \mapsto C$ by*

$$\phi(a_0 + a_1\beta + \cdots a_{m-1}\beta^{m-1}) = a_0c_0 + a_1c_1 + \cdots a_{m-1}c_{m-1}.$$

Consider the matrix

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

For any linear combination of columns (not all zero) of the matrix A^*, each nonzero codeword of C will appear exactly once.

Proof. Since ϕ is a bijection, it is enough to show that the matrix

$$\begin{pmatrix} 1 & \beta & \dots & \beta^{m-1} \\ \beta & \beta^2 & \dots & \beta^m \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{2^m-2} & 1 & \dots & \beta^{m-2} \end{pmatrix}$$

has the property that each element in $\mathbb{F}_{2^m}^*$ will appear once in any nonzero linear combination of columns of the above matrix.

Any nonzero linear combination of columns can be written as

$$(c_0 + c_1\beta + \cdots + c_{m-1}\beta^{m-1}) \begin{pmatrix} 1 \\ \beta \\ \vdots \\ \beta^{2^m-2} \end{pmatrix},$$

for some $c_0, c_1 \dots, c_{m-1} \in \mathbb{F}_2$, and the statement is obvious.

The conclusion from the lemma is that by using a linear $[n-d, m, t+1]$ code we can fill $2^m - 1$ out of the 2^d rows of matrix A. Each nonzero codeword will then appear exactly once in each column and row. Then we can select another linear $[n-d, m, t+1]$ code and fill another $2^m - 1$ rows of matrix A. In order to maximize the nonlinearity, no vector in A should appear more than once in each column (or row). Hence, the intersection between the two codes should be the all zero word. Continuing to select more codes to fill the matrix A, the intersection with any other previously selected code must again be only the all zero word. This leads us to the following definition.

Definition 7 *A set of linear $[n', m, t+1]$ codes $\{C_1, C_2, \dots, C_s\}$ such that*

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

is called a set of linear $[n', m, t+1]$ nonintersecting codes.

For fixed values $n', m, t+1$, we are interested in the maximal cardinality of a set of linear $[n', m, t+1]$ nonintersecting codes. Combining the idea of nonintersecting codes with the previous construction we can summarize in the following result.

Theorem 8 *If there exists a set of linear $[n-d, m, t+1]$ nonintersecting codes with cardinality $\lceil 2^d/(2^m-1) \rceil$ then there exists a t-resilient function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ with nonlinearity*

$$N_F = 2^{n-1} - 2^{n-d-1}.$$

Example 2 *Continuing with the same numerical values as in the previous example, i.e., $n = 10$, $t = 2$, $m = 2$, we choose $d = 4$. The requirement is now to find $\lceil 2^d/(2^m-1) \rceil = 6$ nonintersecting linear $[n-d, m, t+1] = [6, 2, 3]$ codes in order to maximize the nonlinearity to $N_F = 2^{n-1} - 2^{n-d-1} = 480$. By computer search, we verified that cardinality 6 was indeed possible, and the matrix A given in the previous example was actually constructed through these 6 codes.*

Now consider the same problem but for $m = 3$. Again, selecting $d = 4$ we must now have $\lceil 2^d/(2^m-1) \rceil = 3$ nonintersecting linear $[6, 3, 3]$ codes. This could not be found by computer search. Hence, we must decrease d by one, $d = 3$. This will result in a nonlinearity of $N_F = 448$.

V Lower bounds on the cardinality of a set of linear nonintersecting codes

In this section we prove two lower (existence) bounds on the cardinality of a set of nonintersecting linear codes. Using these bounds we are able to prove that there exist resilient functions having higher nonlinearity than obtained using previous constructions, i.e. [10, 27]. We do not discuss a practical construction of such functions, but it should be pointed out that the technique used in obtaining the bounds to be presented may be modified into a search algorithm. Firstly, we give a general lower bound on the cardinality of a set of nonintersecting linear codes using Gilbert-Varshamov type of arguments. We need an well-known lemma stated here without proof (for a proof see e.g. [28]).

Lemma 9 *Let $\mathbb{F}_2^n$ be an n-dimensional vector space over $\mathbb{F}_2$ and $0 \leq k \leq m \leq n$. Let $N(m,n)$ denote the number of m-dimensional vector subspaces of $\mathbb{F}_2^n$. Furthermore, let $N'(k,m,n)$ denote the number of m-dimensional vector subspaces containing a given k-dimensional vector subspace of $\mathbb{F}_2^n$. Then the following is valid,*

$$N(m,n) = \frac{\prod_{i=n-m+1}^{n}(2^i - 1)}{\prod_{i=1}^{m}(2^i - 1)}, \tag{20}$$

$$N'(k,m,n) = N(m-k, n-k). \tag{21}$$

Let $M(n,m,d_{min})$ denote the maximal cardinality of a set of nonintersecting linear codes for any given code parameters n, m, d_{min}. Using the Lemma 9 above we are able to obtain the following existence bound on $M(n,m,d_{min})$.

Theorem 10 *Let the codes in the set have parameters $[n,m,d_{min}]$ and let $S = \{x \in F_2^n | 1 \leq w_H(x) \leq d_{min} - 1\}$. Then $M(n,m,d_{min})$ is lower-bounded by*

$$M(n,m,d_{min}) \geq \left\lceil \frac{N(m,n) - |S|N(m-1,n-1)}{(2^m - 1)(N(m-1,n-1) - 1)} \right\rceil. \tag{22}$$

Proof. Since the minimum distance of all the codes is d_{min}, none of them is allowed to intersect the sphere S. Let $\mathcal{C}$ denote the set of all linear codes of length n and dimension m. According to Lemma 9, the total number of codes is $N(m,n)$.

Any element (vector) in S is a 1-dimensional vector space. The number of codes containing an arbitrary word $x \in S$ is $N(m-1,n-1)$. Removing all codes in $\mathcal{C}$ intersecting an element in S, i.e. all codes having too low minimum distance, leaves us with at least

$$N(m,n) - N(m-1,n-1)|S| \tag{23}$$

codes in $\mathcal{C}$. In general, some codes will contain more than one codeword from S, and hence (23) is an upper bound on the number of codes intersecting the sphere S.

Now we can chose any code, say C^1, of the remaining codes in $\mathcal{C}$. An upper bound on the number of codes intersecting C^1 in more than the zero word is now derived.

$$|\{C \in \mathcal{C} | C \cap C^1 \neq \{0\}\}| \leq (2^m - 1)(N(m-1,n-1) - 1).$$

This inequality is a consequence of the simple fact that any of $2^m - 1$ nonzero codewords of C^1 can be in at most $N(m-1, n-1) - 1$ codes.

We now continue to select a new code C^2 and remove all codes that intersect C^2, etc. It then follows that an Mth code can be added to the set of nonintersecting codes if the following inequality holds,

$$N(m,n) - |S|N(m-1,n-1) - (M-1)(2^m-1)(N(m-1,n-1)-1) \geq 0. \quad (24)$$

From (24) one obtain (22) as stated.

A second lower bound on the cardinality of a set of nonintersecting linear codes is obtained by considering the set of all possible permutations on the codewords (i.e. column permutations) for a given linear code C. Thus, the condition for this lower bound is the existence of a linear $[n, m, d_{min}]$ code C together with its weight distribution. Once we know one such code, we are able to compute a lower bound on $M(n, m, d_{min})$ which will depend on the weight distribution.

Theorem 11 (Permutation bound) *Let C be a given $[n, m, d_{min}]$ linear code specified by its weight distribution $T(D) = \sum_{i=d_{min}}^{n} w_i D^i$. Then*

$$M(n, m, d_{min}) \geq \left\lceil \frac{n!}{\sum_{i=d_{min}}^{n} w_i^2 i!(n-i)!} \right\rceil \quad (25)$$

Proof. Let $A = \{1, 2, \ldots, n\}$ and let $S_n = \{\pi : A \mapsto A\}$ be a set of all permutations on n letters acting on C with cardinality $n!$. Furthermore, let $C^{w_i} = \{c \in C : w_H(c) = i\}$ be a set of cardinality $|C^{w_i}| = w_i$. If Π^{w_i} is the set of all permutations that map any codeword in C^{w_i} to some codeword contained in C^{w_i}, i.e.,

$$\Pi^{w_i} = \{\pi \in S_n : \pi(c) \in C^{w_i}, \text{ for some } c \in C^{w_i}\},$$

then we have $|\Pi^{w_i}| = w_i^2 i!(n-i)!$.

The idea is to remove all permutations π which maps any nonzero codeword of C into C. Thus, the number of permutations to be discarded in order to obtain a code $\pi(C)$ which does not intersect C in more than the zero word is given by

$$\sum_{i=d_{min}}^{n} w_i^2 i!(n-i)!, \quad (26)$$

and the condition for a second code will be $n! > \sum_{i=d_{min}}^{n} w_i^2 i!(n-i)!$. Clearly we can proceed in the same manner, discarding all permutations which maps any nonzero codeword of C into $\pi(C)$, as long as we have remaining permutations.

Thus, the M-th code can be added provided

$$n! - (M-1) \sum_{i=dmin}^{n} w_i^2 i!(n-i)! \geq 0. \quad (27)$$

Rearranging (27) we obtain (25) as claimed.

In the next section these two bounds will be applied to prove the existence of resilient functions with higher nonlinearity than those obtained in [10, 27].

VI Numerical results on the nonlinearity for resilient functions

The purpose of this section is to combine all the results given sofar in order to give numerical values on the parameters that we can achieve.

In [10] the author considered the construction of $[36, 8, t]$ nonlinear resilient functions for different orders of resiliency t. In the table below we show through our construction that there exist functions with higher nonlinearity, or in other words, the lower bound on the nonlinearity is shifted upwards. The existence of functions with parameters as in Table 2 is obtained using the sphere bound in Theorem 10 together with Theorem 8, except for the boldface entry which is computed using the permutation bound in Theorem 11. For this specific entry, we started with a $[24, 12, 8]$ Golay code and modified it into a $[23, 8, 8]$ code. Thus, with parameter $d = 13$ we had to find at least 33 nonintersecting linear codes in order to fill 8192 rows of matrix A. Using the weight distribution of $[23, 8, 8]$ and the equation (25) we could prove that there exist at least 34 nonintersecting linear codes, which yields the lower bound on nonlinearity as given in Table 2.

t	7	5	4	3	2	1
Bound [10]	$2^{35} - 2^{27}$	$2^{35} - 2^{26}$	$2^{35} - 2^{25}$	$2^{35} - 2^{24}$	$2^{35} - 2^{23}$	$2^{35} - 2^{22}$
New bound	$\mathbf{2^{35} - 2^{22}}$	$2^{35} - 2^{23}$	$2^{35} - 2^{22}$	$2^{35} - 2^{22}$	$2^{35} - 2^{21}$	$2^{35} - 2^{21}$

Table 2: Lower bounds on N_F for $[36, 8, t]$-resilient functions

Since the cardinality of the set of nonintersecting linear codes to be found depends on the size of input parameters, i.e. n, m, t, we can calculate the lower bound on the number of these codes for arbitrary values of n. But for moderate n, one can also consider search algorithms based on the ideas behind the lower bounds. Such a computer search has also been implemented, and the obtained results are presented in the tables below.

N_F	$n = 9$		$n = 10$		$n = 11$		$n = 12$	
m	Th. 8	[10]	Th. 8	[10]	Th. 8	[10]	Th. 8	[10]
2	240	224	480	448	992	960	1984	1920
3	224	–	480	448	992	896	1984	1920
4	224	–	448	–	960	–	1920	–
5	224	–	448	–	960	–	1920	–
6	192	–	448	–	960	–	1920	–

Table 3: Highest achieved N_F for 1-resilient functions.

N_F	$n=9$		$n=10$		$n=11$		$n=12$	
m	Th. 8	[10]Th. 8		[10]	Th. 8	[10]	Th. 8	[10]
2	240	192	480	384	992	896	1984	1792
3	192	–	448	–	960	–	1984	1792
4	128	–	384	–	896	–	1920	–
5	0	–	256	–	768	–	1792	–
6	0	–	0	–	512	–	1536	–

Table 4: Highest achieved N_F for 2-resilient functions.

N_F	$n=9$		$n=10$		$n=11$		$n=12$	
m	Th. 8	[10]	Th. 8	[10]	Th. 8	[10]	Th. 8	[10]
2	192	–	448	384	960	768	1984	1792
3	192	–	384	–	896	–	1920	–
4	128	–	256	–	768	–	1792	–
5	0	–	0	–	512	–	1536	–
6	0	–	0	–	512	–	1024	–

Table 5: Highest achieved N_F for 3-resilient functions.

VII Conclusion

A new construction of highly nonlinear (n, m, t)-resilient functions has been presented. The construction leads to interesting coding theoretic questions regarding the maximal cardinality of a set of $[n, m, d_{min}]$ codes with the property that the intersection of any two codes is the all zero codeword. We have found no previous work that has considered this subject, although we have noted some similarities in conjunction with the Griesmer bound as well as to codes for unequal error protection.

Comparing with the two different designs presented in [10, 27], the proposed construction gives a much better nonlinearity for the same value of resiliency. Still, further improvements could be possible in some cases, possibly through construction methods presented in [19].

References

[1] B. I. Bennett, G. Brassard, and J. M. Robert, "Privacy amplification by public discussion", *SIAM Journal on Computing*, vol. 17, pp. 210–229, 1988.

[2] J. Bierbrauer, K. Gopalakrishnan, D. R. Stinson, "Bounds on resilient functions and orthogonal arrays", *Advances in Cryptology - CRYPTO'94, Lecture Notes in Computer Science*, vol. 839, pp. 247–256, Springer-Verlag, 1994.

[3] P. Camion, C. Carlet, P. Charpin and N. Sendrier, "On correlation-immune functions", *Advances in Cryptology - CRYPTO'91, Lecture Notes in Computer Science*, vol. 1233, pp. 422–433, Springer-Verlag, 1997.

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

[5] B. Chor, O. Goldreich, J. Håstad, and J. Friedman, S. Rudich, and R. Smolensky, "The bit extraction problem or t-resilient functions ". *IEEE Simposium on Foundations of Computer Science*, pp. 396–407, 1986.

[6] T. M. Cover, J. A. Thomas, "Elements of information theory ". *John Wiley & Sons Inc.*, 1991.

[7] H. Dobbertin. "Construction of bent functions and balanced Boolean functions with high nonlinearity", In *Fast Software Encryption*, 1994 Leuven Workshop, LNCS, vol. 1008, pp. 61–74. Springer Verlag, May 1983.

[8] C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers, *Number 561, Lecture Notes in Computer Science*, Springer-Verlag, 1991.

[9] E. Filiol, and C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity" *Advances in Cryptology - EUROCRYPT'98, Lecture Notes in Computer Science*, vol. 1403, pp. 475–488, Springer-Verlag, 1998.

[10] K. Kurosawa, T. Satoh, and K. Yamamoto "Highly nonlinear t-Resilient functions". *Journal of UniverComputer Science*, vol. 3, no. 6, pp. 721–729, Springer Pub. Co., 1997.

[11] S. Maitra, and P. Sarkar, "Construction of nonlinear Boolean functions with important cryptographic properties", *Advances in Cryptology - EUROCRYPT'00, Lecture Notes in Computer Science*, vol. 1807, pp. 491–512, Springer-Verlag, 2000.

[12] W. Meier, and O. Staffelbach, " Nonlinearity criteria for cryptographic functions", *Advances in Cryptology - EUROCRYPT'89, Lecture Notes in Computer Science*, pp. 549–562, Springer-Verlag, 1990.

[13] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of applied cryptography,* CRC Press, 1997.

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

[15] E. Pasalic, and T. Johansson, "Further results on on the relation between nonlinearity and resiliency of Boolean functions", *IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science*, vol. 1746, pp. 35–45, Springer-Verlag, 1998.

[16] N. J. Patterson, D. H. Wiedemann. "The covering radius of the $[2^{15}, 16]$ Reed–Muller code is at least 16276", In *IEEE Trans. on Inf. Theory*, No. 3, pages 354–356. Springer Verlag, May 1983.

[17] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions", *Advances in Cryptology - EUROCRYPT'1990, Lecture Notes in Computer Science*, vol. 473, pp. 161–173, Springer-Verlag, 1991.

[18] O. S. Rothaus, "On bent functions", In *Journal of Combinatorial Theory*, Series A20, pages 300–305, 1975.

[19] P. Sarkar, and S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions", *Advances in Cryptology - CRYPTO'00, Lecture Notes in Computer Science*, vol. 1880, pp. 515–532, Springer-Verlag, 2000.

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

[21] J. Seberry, X. M. Zhang, and Y. Zheng, "Relationships among nonlinearity criteria", *Advances in Cryptology - EUROCRYPT'94, Lecture Notes in Computer Science*, vol. 950, pp. 376–388, Springer-Verlag, 1994.

[22] T. Siegenthaler, " Correlation-immunity of nonlinear combining functions for cryptographic applications". *IEEE Transactions on Inform. Th.*, vol. IT-30(5), pp. 776–780, 1984.

[23] T. Siegenthaler, " Decrypting a class of stream ciphers using ciphertext only". *IEEE Transactions on Computers*, vol. C-34, pp. 81–85, 1985.

[24] D. R. Stinson, "Resilient functions and large sets of orthogonal arrays", *Congressus Numerantium*, 92, pp. 105–110, 1993.

[25] D. R. Stinson, and J. L. Massey, "An infinite class of counterexamples to a conjecture concerning non-linear resilient functions", *Journal of Cryptology, Lecture Notes in Computer Science*, vol. 765, pp. 181–199, Springer-Verlag, 1994.

[26] Y. V. Tarannikov, "On resilient Boolean functions with maximum possible nonlinearity", *Cryptology ePrint Archive, eprint.iacr.org, No.2000/005*, 2000.

[27] X. M. Zhang, and Y. Zheng, "On nonlinear resilient functions", *Advances in Cryptology - EUROCRYPT'95, Lecture Notes in Computer Science*,vol. 921, pp. 274–288, Springer-Verlag, 1995.

[28] Z. Wan, "Geometry of classical groups over finite fields" *Studentlitteratur*, Lund, 1993.