Constructions of Resilient S-Boxes with Strictly Almost Optimal Nonlinearity Through Disjoint Linear Codes

WeiGuo Zhang (张卫国) and Enes Pasalic

***Abstract*—In this paper a novel approach of finding disjoint linear codes is presented. The cardinality of a set of $[u, m, t+1]$ disjoint linear codes largely exceeds all the previous best known methods used for the same purpose. Using such sets of disjoint linear codes, not necessarily of the same length, we have been able to provide a construction technique of t-resilient S-boxes $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ (n even, $1 < m \leq \lfloor n/4 \rfloor$) with *strictly almost optimal nonlinearity* $> 2^{n-1} - 2^{n/2}$. This is the first time that the bound $2^{n-1} - 2^{n/2}$ has been exceeded by multiple output resilient functions. Actually, the nonlinearity of our functions is in many cases equal to the best known nonlinearity of balanced Boolean functions. A large class of previously unknown cryptographic resilient S-boxes is obtained, and several improvements of the original approach are proposed. Some other relevant cryptographic properties are also briefly discussed. It is shown that these functions may reach Siegenthaler's bound $n-t-1$, and can be either of optimal algebraic immunity or of slightly suboptimal algebraic immunity, which was confirmed by simulations.**

***Index Terms*—Boolean functions, nonlinearity, resiliency, S-boxes, stream ciphers, disjoint linear codes.**

I. Introduction

A classical method for constructing keystream generators is to combine a set of linear feedback shift registers (the scheme being known as the nonlinear combiner [20]) with a nonlinear Boolean function. The Boolean function $f(X_n)$, $f : GF(2)^n \mapsto GF(2)$, where $X_n = (x_1, \ldots, x_n) \in GF(2)^n$, must fulfil certain properties in order to increase the time/space complexity of different attacks. Common attacks are the correlation attack introduced by [25], Berlekamp-Massey linearity synthesis attack [16] and different linear approximation attacks [9]. The most important criteria these functions should satisfy are: balancedness, high nonlinearity, high algebraic degree, some correlation immunity (for balanced functions, correlation immunity is usually referred to as resiliency), and good resistance to algebraic attacks. Especially, the nonlinearity measures the distance of f to the set of affine functions, whereas the resiliency provides the balancedness of the output (equal number of zeros and ones when $X_n \in GF(2)^n$) even though a certain number of input variables is kept fixed. A high nonlinearity and resiliency order result then in a greater ability of the cipher (for instance in the case of nonlinear combiners) to resist various kind of affine approximations of the cipher.

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

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

DOI: https://doi.org/10.1109/TIT.2014.2300067

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 $F : GF(2)^n \mapsto GF(2)^m$ (n-input m-output functions), where $m > 1$. In the block cipher design such functions are referred to as (n, m) S-boxes (substitution boxes). S-boxes are well studied objects, and different important criteria have been considered. Apart from the standard criteria of having high nonlinearity and high algebraic degree, other criteria include balancedness, differential properties etc..

The design of resilient S-boxes with high nonlinearity plays an important role in designing certain stream cipher schemes and have received a lot of attention since mid-1990s. Unlike the design of Boolean functions, the construction of highly nonlinear resilient S-boxes appears to be more difficult and is more structure based. This is especially true when the resiliency criterion is concerned, the criterion introduced by Chor *et al.* [7], and independently by Bennett *et al.* [1]. Informally, a function $F : GF(2)^n \mapsto GF(2)^m$, represented as a collection of m Boolean functions, i.e., $F = (f_1, \ldots, f_m)$, is resilient of order t if any nonzero linear combination (of weight at most t) of its component functions f_i still generate a balanced output. For convenience, the notation (n, m, t) will refer to a t-resilient (n, m) S-box, whereas for $t = 0$ an $(n, m, 0)$ S-box simply refers to a balanced (n, m) S-box. In the case of Boolean functions ($m = 1$), it turns out that balanced correlation immune functions introduced by Siegenthaler [25] are a special case of resilient functions. The best affine approximation attack [9] and linear approximation attack [17] show that the nonlinearity is a vital criterion for designing cryptographically strong S-boxes. For even $n \geq 2m$, the (n, m) S-boxes achieving the maximum possible nonlinearity $2^{n-1} - 2^{n/2-1}$ are called perfect nonlinear S-boxes [23]. However, perfect nonlinear S-boxes can not be resilient. To the best of our knowledge, for $m > 1$, the nonlinearity of the resilient (n, m) S-boxes obtained by the existing constructions is at most $2^{n-1} - 2^{\lfloor n/2 \rfloor}$, and it is an open problem whether this value is the maximum possible.

An (n, m) S-box is called *strictly almost optimal* if its nonlinearity exceeds the value $2^{n-1} - 2^{\lfloor n/2 \rfloor}$. In this paper, we will show that resilient (n, m) S-boxes with strictly almost optimal nonlinearity can be constructed.

We first give a brief summary of previous results related to the construction of highly nonlinear resilient (n, m) S-boxes.

1) Zhang and Zheng [29] proposed a method for transforming a linear (n, m, t) S-box F to a nonlinear (n, m, t)

resilient S-box $F' = G(F)$ whose nonlinearity is $N_{F'} = 2^{n-m}N_G$, where G is a permutation on $\mathbb{F}_2^m$ and N_G is the nonlinearity of G. Note that, as $N_G \leq 2^{m-1} - 2^{(m-1)/2}$ [3], we always have $N_{F'} \leq 2^{n-1} - 2^{n-(m+1)/2}$.

2) Kurosawa *et al*. [14] gave a simple method to construct new resilient S-boxes from old ones. Let $\Phi(X_{n-l})$ be an $(n-l, m, t)$ S-box with nonlinearity N_Φ, and $\Psi(Y_l)$ be a (l, m) perfect nonlinear S-box. Then $F(X_{n-l}, Y_l) = \Phi(X_{n-l}) \oplus \Psi(Y_l)$ is an (n, m, t) S-box with nonlinearity $N_F = 2^{n-1} - 2^{n-l/2-1} + 2^{l/2}N_\Phi$. Obviously, F is strictly almost optimal if and only if Φ is strictly almost optimal.
3) Chen and Fu [5] also presented a generalized linear method for constructing new resilient S-boxes from old ones, with the basic idea that $F \oplus G$ is an (n_1+n_2, m, t_1+t_2+1) S-box if F and G are (n_1, m, t_1) and (n_2, m, t_2) S-boxes, respectively.
4) Cheon [6] proposed a method to construct (n, m, t) resilient S-boxes for any non-negative integer D, whenever an $[n-D-1, m, t+1]$ linear code exists. This function has algebraic degree D and nonlinearity $2^{n-1} - 2^{n-D-1} \cdot \lfloor 2^{n/2} \rfloor + 2^{n-D-2}$. This method may provide high algebraic degree but it does not provide good nonlinearity.
5) Johansson and Pasalic [12] showed that a sufficiently large set of $[n-d, m, t+1]$ disjoint linear codes can produce a (n, m, t) S-box with nonlinearity $2^{n-1} - 2^{n-d-1}$. This method leads to the problem of constructing a set of disjoint linear codes [4], [21].
6) Instead of using disjoint linear codes, Pasalic and Maitra [24] only considered one single linear code along with highly nonlinear S-boxes for their construction. Given a $[u, m, t+1]$ linear code they showed that it is possible to construct an (n, m, t) S-box with high nonlinearity for $n > u$.
7) In [11], Gupta and Sarkar gave a simple modification of the construction due to Zhang and Zheng [29], and obtained (n, m, t) S-boxes with algebraic degree $d > m$. The other construction used a sharpened version of the Maiorana-McFarland technique to construct nonlinear resilient functions. They improved the results in [24] by utilizing all the $2^k - 1$ nonzero codewords of a $[u, m, t+1]$ linear code rather than only 2^{k-1} codewords.

However, none of the methods mentioned above generate (n, m, t) S-boxes with strictly almost optimal nonlinearity.

Our approach taken here follows the basic ideas introduced in [12], which resolves the problem of using the (nonzero) codewords of $[u, m, t+1]$ disjoint linear codes in order to construct a strictly almost optimal m-resilient function $F : GF(2)^n \mapsto GF(2)^m$ for $n > u$. If $[u, m, t+1]$ disjoint linear codes of a single length u are used, the construction may be viewed as a concatenation of linear functions in u variables whose weight is at least $t+1$. These linear t-resilient functions are concatenated in a suitable manner, using a suitable different placement, to provide m component functions of F. This particular placement of linear subfunctions ensures that these linear subfunctions are never repeated in the concatenation even in the case the linear combinations of the component functions are considered. Such a function F is an (n, m, t) function, and its nonlinearity equals to $2^{n-1} - 2^{u-1}$; see Section IV and Lemma 2 for further details.

The best known technique for finding a large set of disjoint linear codes has been proposed in [4] and later it has been generalized to nonbinary codes using algebraic geometry methods [21]. The latter technique only improves some lower bounds on the number of disjoint linear codes in a few cases of practical interest, whereas the former approach uses flats of appropriate dimension in suitable projective spaces corresponding to disjoint linear codes. However, the approaches above are both limited by certain divisibility restrictions. In the case of $[u, m, t+1]$ disjoint linear codes from projective geometry the condition is that $m|u$, whereas the approach based on algebraic geometry uses a concatenation such that from a small $[u, m, d]$ linear code one can obtain a number of $[ru, sm, vd]$ disjoint linear codes, where the parameters r, s, v can be determined using some results from algebraic geometry.

To illustrate the quality of the lower bound given in [21] we consider a construction of $[18, 4, 6]$ disjoint linear codes for which it has been deduced that the number of these codes is ≥ 24. Note that since $4 \nmid 18$ the method in [4] is not applicable. On the other hand, using our approach given in the next section the number of these codes is 12882 which is a tremendous improvement compared to the above methods.

Another contribution of this work is imposed by our basic goal, which is crossing the nonlinearity bound $2^{n-1} - 2^{n/2}$ attained by so called almost optimal functions. It can be easily checked that the use of codewords of length greater than $n/2$ would imply that the nonlinearity of such functions is $\leq 2^{n-1} - 2^{n/2}$, thus the maximum length of our codes is then $n/2$. On the other hand, we cannot possibly have sufficiently many $[n/2, m, t]$ disjoint linear codes for the construction of an (n, m, t) function since the nonlinearity of such a function would be $2^{n-1} - 2^{\frac{n}{2}-1}$ which corresponds to bent functions. Therefore, to achieve higher nonlinearity of almost optimal functions, we are obliged to use some disjoint linear codes of smaller length than $n/2$ as well. Consequently, our function can also be represented as a concatenation of linear functions in $n/2$ variables together with linear functions in smaller number of variables (the number of variables k will later correspond to the length of the smallest code used). The efficiency of our method for finding a large set of disjoint linear codes together with the novel approach and combining these smaller codes in the construction leads to currently superior nonlinearities of our functions. Furthermore, the approach taken here can be combined with some known methods of obtaining highly nonlinear balanced Boolean functions [10], [26]. The nonlinearities of balanced S-boxes designed in this way is comparable to the best known nonlinearities of balanced Boolean functions.

The rest of this paper is organized as follows: Section II introduces some basic definitions and discusses cryptographic criteria for S-boxes. In Section III, a large set of $[n, m, t+1]$ disjoint linear codes are constructed. Based on the use of disjoint linear codes, Section IV provides a construction technique for resilient S-boxes with nonlinearity $> 2^{n-1} - 2^{n/2}$, where n is even and $1 < m \leq \lfloor n/4 \rfloor$. This construction technique is improved in Section V, and furthermore the

construction of balanced S-boxes with extremely good nonlinearity is proposed. In Section VI we consider the algebraic properties of our S-boxes. Finally, Section VII concludes this paper.

II. Preliminaries

A. Boolean functions

Let $\mathcal{B}_n$ denote the set of Boolean functions in n variables, and denote by $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ the vector space $GF(2)^n$ and the corresponding finite field $GF(2^n)$, respectively. $\mathbb{F}_{2^n}$ is identified with $\mathbb{F}_2^n$ in this paper. A Boolean function $f(X_n) \in \mathcal{B}_n$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $X_n \in \mathbb{F}_2^n$ and $\mathbb{F}_2^n$ is the vector space of tuples of elements from $\mathbb{F}_2$. To avoid confusion with the additions of integers in $\mathbb{R}$, denoted by $+$ and Σ_i, we denote the additions over $\mathbb{F}_2$ by $\oplus$ and $\bigoplus_i$. For simplicity, we denote the addition of vectors of $\mathbb{F}_2^n$ by $+$ throughout this article. For $X_n = (x_1, \ldots, x_n)$, a Boolean function $f(X_n) \in \mathcal{B}_n$ is generally represented by its algebraic normal form (ANF):

$$f(X_n) = \bigoplus_{b \in \mathbb{F}_2^n} \lambda_b (\prod_{i=1}^{n} x_i^{b_i}), \tag{1}$$

where $\lambda_b \in \mathbb{F}_2,\ b = (b_1, \ldots, b_n) \in \mathbb{F}_2^n$. The algebraic degree of $f(X_n)$, denoted by $deg(f)$, is the maximal value of $wt(b)$ such that $\lambda_b \neq 0$, where $wt(b)$ denotes the Hamming weight of b. f is called an affine function when $deg(f) = 1$. An affine function with constant term equal to zero is called a linear function. Any linear function on $\mathbb{F}_2^n$ is denoted by:

$$\omega \cdot X_n = \omega_1 x_1 \oplus \cdots \oplus \omega_n x_n,$$

where $\omega = (\omega_1, \ldots, \omega_n),\ X_n = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$.

The Walsh transform of $f \in \mathcal{B}_n$ in point ω is denoted by $W_f(\omega)$ and calculated as

$$W_f(\omega) = \sum_{X_n \in \mathbb{F}_2^n} (-1)^{f(X_n) \oplus \omega \cdot X_n}. \tag{2}$$

Let $supp(f) = \{X_n \in \mathbb{F}_2^n \mid f(X_n) = 1\}$ denote the support of f. $f \in \mathcal{B}_n$ is said to be balanced if its output column in the truth table contains equal number of 0's and 1's, i.e., $\#supp(f) = 2^{n-1}$, or equivalently, $W_f(0) = 0$.

Definition 1: The nonlinearity of a Boolean function $f \in \mathcal{B}_n$, denoted by N_f, is defined as the distance to the set of all affine functions,

$$N_f = \min_{\rho \in A(n)} \#\{X_n \in \mathbb{F}_2^n : f(X_n) \neq \rho(X_n)\}, \tag{3}$$

where $A(n)$ is the set of all affine functions on $\mathbb{F}_2^n$.

The nonlinearity of f can be obtained through the Walsh transform as follows [19]:

$$N_f = 2^{n-1} - \frac{1}{2}\mathcal{L}(f), \text{ where } \mathcal{L}(f) = \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|. \tag{4}$$

Parseval's equation [15] states that

$$\sum_{\omega \in \mathbb{F}_2^n} (W_f(\omega))^2 = 2^{2n}, \tag{5}$$

which implies that $N_f \leq 2^{n-1} - 2^{n/2-1}$. The equality occurs if and only if $f \in \mathcal{B}_n$ are bent functions, where n is even. $f \in \mathcal{B}_n$ is said to be strictly almost optimal if $N_f > 2^{n-1} - 2^{\lfloor n/2 \rfloor}$.

In [28], a spectral characterization of resilient Boolean functions has been derived, which is stated here as a definition.

Definition 2: A Boolean function $f \in \mathcal{B}_n$ is t-resilient if and only if its Walsh transform satisfies

$$W_f(\omega) = 0, \quad \text{for } 0 \leq wt(\omega) \leq t,\ \omega \in \mathbb{F}_2^n. \tag{6}$$

Definition 3 ([18]): Given $f \in \mathcal{B}_n$, define

$$AN(f) = \{g \in \mathcal{B}_n \mid f \cdot g = 0\}.$$

Any function $g \in AN(f)$ is called an *annihilator* of f. The *algebraic immunity*, denoted by $AI(f)$, of function f is the minimum degree of all non-zero annihilators of f and $f \oplus 1$.

B. Cryptographic criteria for S-boxes

In this section we give an overview of some of the most important cryptographic criteria related to S-boxes. Note that there are other criteria such as propagation properties, avalanche criterion etc. but these are not considered in the sequel and therefore their definitions are omitted.

An (n, m) S-box can be represented as a mapping $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, which in turn can be viewed as a collection of m Boolean functions so that $F(X_n) = (f_1(X_n), \ldots, f_m(X_n))$, where $f_1, \ldots, f_m \in \mathcal{B}_n$. The algebraic degree of F, denoted by $\deg(F)$, is defined as the minimum among the algebraic degrees of all nonzero linear combinations of the component functions of F, namely,

$$\deg(F) = \min_{c \in \mathbb{F}_2^{m*}} \deg\left(\bigoplus_{i=1}^{m} c_i f_i(X_n)\right), \tag{7}$$

where $c = (c_1, \ldots, c_m) \in \mathbb{F}_2^{m*}$, $\mathbb{F}_2^{m*} = \mathbb{F}_2^m \backslash \{\mathbf{0}\}$.

In a similar way the algebraic immunity of an (n, m) S-box is defined as,

$$AI(F) = \min_{c \in \mathbb{F}_2^{m*}} AI\left(\bigoplus_{i=1}^{m} c_i f_i(X_n)\right). \tag{8}$$

It is known that $AI(F) \leq \lceil n/2 \rceil$. We call the algebraic immunity of F is optimal if $AI(F) = \lceil n/2 \rceil$, and is suboptimal if $AI(F) = \lceil n/2 \rceil - 1$.

Definition 4 ([29]): An (n, m) S-box

$$F(X_n) = (f_1(X_n), \ldots, f_m(X_n))$$

is called t-resilient if and only if for any $c = (c_1, \ldots, c_m) \in \mathbb{F}_2^{m*}$, $f_c(X_n) = \bigoplus_{i=1}^{r} c_i f_i(X_n)$ is a t-resilient function.

Siegenthaler [25] showed that $deg(f_c) \leq n - t - 1$ for $c \in \mathbb{F}_2^{m*}$. Then, we also have $deg(F) \leq n - t - 1$. When $deg(F) = n - t - 1$, we call F reach Siegenthaler's bound.

Definition 5: The nonlinearity of an (n, m) S-box $F = (f_1, \ldots, f_m)$, denoted by N_F, is defined as

$$N_F = \min_{c \in \mathbb{F}_2^{m*}} N_{f_c} \tag{9}$$

where $f_c = \bigoplus_{i=1}^{m} c_i f_i$.

Obviously, we can use the linearity measure as previously so that $N_F = 2^{n-1} - \frac{1}{2}\Lambda(F)$ where

$$\Lambda(F) = \max_{c \in \mathbb{F}_2^{m*}} \mathcal{L}(f_c). \tag{10}$$

A function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called a perfect nonlinear (n, m) S-box if for every nonzero $c \in \mathbb{F}_2^m$ the function f_c is a bent function, and therefore unbalanced. It is known that S-boxes with this property only exist when $m \leq n/2$ [23]. When $m = n$, those F, that achieve the minimum possible value for $\Lambda(F)$ are called *maximally nonlinear*, and these functions have the maximum resistance against linear cryptanalysis. For odd n, this value is known to be $2^{(n+1)/2}$ [3]. For even n, it is possible to obtain an (n, n) S-box with $\Lambda(F) = 2^{n/2+1}$ though it is still an open problem whether this value is the minimum possible. The minimum known value of $\Lambda(F)$ of balanced (n, n) S-boxes (permutations on $\mathbb{F}_2^n$) is $2^{\lfloor n/2 \rfloor+1}$. A list of known power permutations on $\mathbb{F}_{2^n}$ with best known nonlinearity can be found in [2]. The algebraic degree of a power permutation $F : x \mapsto x^d$ on $\mathbb{F}_{2^n}$ can be calculated by $deg(F) = wt([d])$ [22], where $[d]$ denotes the binary representation of d. For instance, $deg(F) = n - 1$ if F is an inverse permutation on $\mathbb{F}_{2^n}$ with $d = 2^n - 2$.

Remark 1: Note that any (n, m) S-box F_r can be obtained by removing $n-m$ coordinate functions of an (n, n) S-box F. There exists a balanced (n, m) S-box with $\Lambda(F_r) = 2^{\lfloor n/2 \rfloor+1}$ and $deg(F_r) \geq deg(F)$, where $m \leq n < 2m$.

III. How to construct a large set of $[u, m, t + 1]$ disjoint linear codes

In this section we give a theoretical framework for finding large sets of disjoint linear codes. These results, apart from their potential significance in coding theory, are frequently used in subsequent sections as a basis for the construction methods described there.

Definition 6 ([12]): A set of $[u, m]$ linear codes $\mathcal{C} = \{C_1, C_2, \ldots, C_N\}$ such that

$$C_i \cap C_j = \{\mathbf{0}\}, \quad 1 \leq i < j \leq N \tag{11}$$

is called a set of $[u, m]$ disjoint linear codes. Let d_i be the minimum weight of the nonzero code vectors in C_i, $0 \leq i \leq N$. $\mathcal{C} = \{C_1, C_2, \ldots, C_N\}$ is also called a set of $[u, m, d]$ disjoint linear codes, where $d = \min\{d_1, d_2, \ldots, d_N\}$. We use $M(u, m, d)$ to denote the currently known maximal cardinality of a set of $[u, m, d]$ disjoint linear codes.

In what follows, a method of constructing $[u, m]$ disjoint linear codes with large cardinality is described.

Lemma 1: Let $u \geq 4$, $m \geq 2$ be two integers with $u \geq 2m$. Let γ be a primitive element in $\mathbb{F}_{2^{u-m}}$, and $(1, \gamma, \ldots, \gamma^{u-m-1})$ be a polynomial basis of $\mathbb{F}_{2^{u-m}}$. Define a bijection $\pi : \mathbb{F}_{2^{u-m}} \mapsto \mathbb{F}_2^{u-m}$ by

$$\pi(b_0 + b_1\gamma + \cdots + b_{u-m-1}\gamma^{u-m-1}) = (b_0, b_1, \cdots, b_{u-m-1}).$$

Let

$$G_i = \begin{pmatrix} 100\cdots00 & \pi(\gamma^i) \\ 010\cdots00 & \pi(\gamma^{i+1}) \\ \vdots & \vdots \\ 000\cdots01 & \pi(\gamma^{i+m-1}) \end{pmatrix}_{m\times u} \tag{12}$$

be the generator matrix of a $[u, m]$ linear code C_i, for $i = 0, \ldots, 2^{u-m} - 2$. Then, $\{C_0, C_1, \ldots, C_{2^{u-m}-2}\}$ is a set of $[u, m]$ disjoint linear codes.

Proof: For any $0 \leq i < j \leq 2^{u-m} - 2$, suppose that there exist two vectors $\mu, \nu \in \mathbb{F}_2^m$ such that $\mu \cdot G_i = \nu \cdot G_j$, then we always have $\mu = \nu = \mathbf{0}$, i.e., $C_i \cap C_j = \{\mathbf{0}\}$. This concludes the proof. ∎

Theorem 1: A set of $[u, m, 1]$ disjoint linear codes with cardinality

$$M(u, m, 1) = \sum_{j=1}^{s} 2^{u-jm} + 1 \tag{13}$$

can be constructed, where $s = \lfloor \frac{u}{m} \rfloor - 1$.

Proof: Let I_m be an $m \times m$ identity matrix and $\mathbf{0}_{m\times l}$ be an $m \times l$ zero matrix. For $j = 1, \ldots, s$, let γ_j be a primitive element in $\mathbb{F}_{2^{u-jm}}$ and $(1, \gamma_j, \ldots, \gamma_j^{u-jm-1})$ be a polynomial basis of $\mathbb{F}_{2^{u-jm}}$. Define a bijection $\pi_j : \mathbb{F}_{2^{u-jm}} \mapsto \mathbb{F}_2^{u-jm}$ by

$$\pi_j(b_0+b_1\gamma+\cdots+b_{u-jm-1}\gamma^{u-jm-1}) = (b_0, b_1, \ldots, b_{u-jm-1}).$$

Let $h_j = 2^{u-jm}$. For $i = 0, \ldots, h_j - 2$, let $G_i^{(j)} = (\mathbf{0}_{m\times(j-1)m}\ I_m\ R^i_{m\times(u-jm)})$ be the generator matrix of the code $C_i^{(j)}$, where

$$R^i_{m\times(u-jm)} = \begin{pmatrix} \pi_j(\gamma_j^i) \\ \pi_j(\gamma_j^{i+1}) \\ \vdots \\ \pi_j(\gamma_j^{i+m-1}) \end{pmatrix}_{m\times(u-jm).} \tag{14}$$

From Lemma 1, $S_j = \{C_i^{(j)} \mid i = 0, 1, \ldots, h_j - 2\}$ is a set of $[u, m]$ disjoint linear codes. For $j = 1, \ldots, s$, let $G^{(j)} = (\mathbf{0}_{m\times(j-1)m}\ I_m\ \mathbf{0}_{m\times(u-jm)})$ be the generator matrix of the code $C^{(j)}$. Let $G' = (\mathbf{0}_{m\times sm}\ R^i_{m\times(u-sm)})$ be the generator matrix of the code C'. It is obvious that $S_1 \cup S_2 \cup \cdots \cup S_s \cup \{C^{(1)}\} \cup \{C^{(2)}\} \cup \cdots \cup \{C^{(s)}\} \cup \{C'\}$ is a set of $[u, m]$ disjoint linear codes. By simple counting,

$$M(u, m, 1) = \sum_{j=1}^{s}(2^{u-jm} - 1) + s + 1 = \sum_{j=1}^{s} 2^{u-jm} + 1,$$

which gives the result. ∎

It can be easily verified that if $m \mid u$, C' is a $[u, m, 1]$ linear code. On the other hand, if $m \nmid u$, it might be the case that C' is a $[u, m, 2]$ linear code. Note that for any $1 \leq k \leq s$, S_j is a set of $[u, m, 1]$ disjoint linear codes. The following two corollaries are a simple consequence of the above result.

Corollary 1: There exists a set of $[u, m, 2]$ disjoint linear codes of cardinality

$$M(u, m, 2) = \begin{cases} \sum_{j=1}^{s}(2^{u-jm} - 1), & \text{if } m \mid u \\ \sum_{j=1}^{s}(2^{u-jm} - 1) + 1, & \text{if } m \nmid u \end{cases}, \tag{15}$$

where $s = \lfloor \frac{u}{m} \rfloor - 1$.

Proof: Note that none of the codes $C^{(j)}$, with the generator matrix $G^{(j)} = (\mathbf{0}_{m\times(j-1)m}\ I_m\ \mathbf{0}_{m\times(u-jm)})$, is of minimum distance 2. Thus, for each $j = 1, \ldots, s$, one such code is subtracted from $M(u, m)$ and the result follows. ∎

Corollary 2: There exists a set of $[u, m, 3]$ disjoint linear codes of cardinality

$$M(u, m, 3) = \sum_{j=1}^{s}(2^{u-jm} + jm) - s(u + m) + \epsilon \tag{16}$$

where $s = \lfloor \frac{u}{m} \rfloor - 1$ and

$$\epsilon = \begin{cases} 1, & \text{if there exists an } [u - sm, m, \geq 3] \text{ code} \\ 0, & \text{otherwise} \end{cases} \quad (17)$$

Proof: In this case, we have to exclude the codes of minimum distance $d < 3$. Clearly, we have to exclude all the codes with the generator matrix $G^{(j)} = (\mathbf{0}_{m\times(j-1)m}\ I_m\ \mathbf{0}_{m\times(u-jm)})$, for $j = 1, \ldots, s$, and the code C' defined in the proof of Theorem 1. In addition, not all the codes given by $G_i^{(j)} = (\mathbf{0}_{m\times(j-1)m}\ I_m\ R^i_{m\times(u-jm)})$ have the minimum distance > 2. Indeed, some of the rows $\pi(\gamma^i)$ of the matrix $R^i_{m\times(u-jm)}$ will have Hamming weight equal to one, for all $i = 0, \ldots, u - jm - 1$. Furthermore, even the matrices $R^{2^{u-jm}-m}_{m\times(u-jm)}, \ldots, R^{2^{u-jm}-2}_{m\times(u-jm)}$, that is, $(m-1)$ matrices $R^i_{m\times(u-jm)}$, for $i = 2^{u-jm} - m, \ldots, 2^{u-jm} - 2$, will have at least one codeword of weight one. Therefore,

$$\begin{aligned} & M(u,m,3) \\ = \ & M(u,m,1) - \big[\sum_{j=1}^{s}(u-jm) + (s+1) + \sum_{j=1}^{s}(m-1)\big] \\ = \ & \sum_{j=1}^{s} 2^{u-jm} + 1 - su - 1 + m\sum_{j=1}^{s}(j-1) \\ = \ & \sum_{j=1}^{s}(2^{u-jm} - u) + m\sum_{j=1}^{s}(j-1) \end{aligned}$$

which gives the result after a simple rearranging. ∎

Example 1: In [4], the number of $[u, m, t+1]$ disjoint linear codes, in the case $u = mh$, was given by $M(u, m, t+1) = \sum_{i=t+1}^{h} \binom{h}{i}(2^m - 1)^{i-1}$. For $u = 6, m = 2, t = 2$, this number equals to $M(6, 2, 3) = 9$. On the other hand, by Corollary 2, this number is calculated as $\sum_{j=1}^{s}(2^{u-jm} - u) + m\sum_{j=1}^{s}(j-1)$, which yields $M(6, 2, 3) = 10$, for $s = \lfloor \frac{u}{m} \rfloor - 1 = 2$.

There are many more examples for which our method compares favourably (actually in much larger extent than indicated in Example 1) to the methods in [4] and [21]. Furthermore, there is no restriction on the divisibility of the code parameters, which appears to be the case for the methods employing projective and/or algebraic geometry. A detailed list of the number of disjoint linear codes achieved by our method is given in the Appendix in Table IV. The codes of larger minimum distance than 3 were found by computer search using the ideas presented in Theorem 1.

Note that the nonlinearity of an (n, m, t) S-box proposed in [12] is closely related to the cardinality of the set of $[u, m, t+1]$ disjoint linear codes. Therefore, as the number of disjoint linear codes using our approach is in most of the cases larger than previously known (at least of the same cardinality), the nonlinearity of resilient S-boxes can be significantly improved compared to known construction methods. In the next section, we propose a method for constructing strictly almost optimal resilient S-boxes by using two sets of disjoint codes of different length.

IV. Construction of strictly almost optimal (n, m, t) functions using two sets of disjoint linear codes of different length

The construction of (n, m, t) functions by using all the nonzero codewords of a $[u, m, t+1]$ linear code is due to the following technical result. Thereinafter, for conciseness, we use a shorthand notation $N(u)$ instead of $M(u, m, t+1)$.

Lemma 2 ([12]): Let $\theta_0, \ldots, \theta_{m-1}$ be a basis of a $[u, m, t+1]$ linear code C. Let β be a primitive element in $\mathbb{F}_{2^m}$, and let $(1, \beta, \ldots, \beta^{m-1})$ be a polynomial basis of $\mathbb{F}_{2^m}$. Define a bijection $\phi : \mathbb{F}_{2^m} \mapsto C$ by

$$\phi(b_0 + b_1\beta + \cdots + b_{m-1}\beta^{m-1}) = b_0\theta_0 + \cdots + b_{m-1}\theta_{m-1}. \quad (18)$$

Consider the matrix A, whose entries are codewords (each column containing all the codewords of C), defined by,

$$A = \begin{pmatrix} \phi(1) & \phi(\beta) & \ldots & \phi(\beta^{m-1}) \\ \phi(\beta) & \phi(\beta^2) & \ldots & \phi(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(\beta^{2^m-2}) & \phi(1) & \ldots & \phi(\beta^{m-2}) \end{pmatrix}. \quad (19)$$

Then, for any nonzero linear combination of columns of the matrix A, each nonzero codeword of C appears exactly once as an element of the resultant column.

Thus, provided the existence of sufficiently many $[u, m, t+1]$ disjoint linear codes, say N disjoint linear codes, such that $N \cdot (2^m - 1) \geq 2^{n-u}$, an (n, m, t) function F with nonlinearity $N_F = 2^{n-1} - 2^{u-1}$ could be constructed. For convenience of the reader, we illustrate this technique by a small example.

Example 2: We use two disjoint $[4, 2, 2]$ linear codes, say C_1 and C_2, to construct $F : \mathbb{F}_2^6 \mapsto \mathbb{F}_2^2$. Let the generator matrices of C_1, C_2 be given by,

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad G_2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

In this case, we have $u = 4$, $m = 2$, and $t = 1$. The main idea of using the codewords of disjoint linear codes is to associate the codewords to linear functions through the inner product so that for $c, X_u \in \mathbb{F}_2^u$ we have $c \cdot X_u = c_1x_1 \oplus \ldots \oplus c_ux_u$. To construct $F = (f_1, f_2)$, where $F : \mathbb{F}_2^6 \mapsto \mathbb{F}_2^2$, the functions f_1 and f_2 are viewed as the concatenation of four linear functions on $\mathbb{F}_2^4$. Let us define the matrix $\tilde{A}$, where $a_{i,j} \in \mathbb{F}_2^4$ for $i = 0, \ldots, 3$, $j = 0, 1$, as follows,

$$\tilde{A} = \left(\begin{array}{cc} (1,0,0,1) & (1,1,0,0) \\ (1,1,0,0) & (0,1,0,1) \\ (0,1,0,1) & (1,0,0,1) \\ \hline (0,1,1,1) & (1,0,1,0) \end{array}\right).$$

Then, denoting $\tilde{A}_{i,j}(X_4) = \tilde{A}_{i,j} \cdot X_4$, where $X_4 = (x_1, \ldots, x_4)$, the functions f_j can be specified as,

$$f_j(X_4, Y_2) = (y_1 \oplus 1)(y_2 \oplus 1)\tilde{A}_{0,j}(X_4) \oplus y_1(y_2 \oplus 1)\tilde{A}_{1,j}(X_4) \oplus (y_1 \oplus 1)y_2\tilde{A}_{2,j}(X_4) \oplus y_1y_2\tilde{A}_{3,j}(X_4).$$

In terms of concatenation, the functions f_j can be represented as,

$$f_j(X_4, Y_2) = \tilde{A}_{0,j}(X_4)||\tilde{A}_{1,j}(X_4)||\tilde{A}_{2,j}(X_4)||\tilde{A}_{3,j}(X_4),$$

which means that for any fixed $Y_2 \in \mathbb{F}_2^2$ the function $f_j(X_4, Y_2)$ is a linear function in $x_1, \ldots, x_4$ given as $\tilde{A}_{\widehat{Y_2},j}(x)$, where $\widehat{Y_2}$ denotes the decimal representation of $Y_2 \in \mathbb{F}_2^2$. For instance, if $Y_2 = (0,0)$ then

$$f_0(X_4, 0, 0) = \tilde{A}_{0,0} \cdot (x_1, \ldots, x_4) = x_1 \oplus x_4.$$

Notice that the first three rows of $\tilde{A}$ correspond to A in Lemma 2 constructed using C_1, whereas the fourth row uses the codewords of C_2 and is obtained from A (corresponding to C_2) by deleting the last two rows. The resulting column of $\tilde{A}$, obtained by summing the columns of $\tilde{A}$, also contains distinct vectors of $\mathbb{F}_2^4$ due to Lemma 2. Thus, $F : \mathbb{F}_2^6 \mapsto \mathbb{F}_2^2$ represents a (6,2) 1-resilient S-box, and $N_F = 2^5 - \frac{1}{2}2^4 = 24$.

Since we only consider n even and our primary goal is the construction of strictly almost optimal functions with nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}}$, we are forced to use disjoint linear codes of different length. Indeed, if all the disjoint linear codes would be of the same length then $[u, m, t+1]$ disjoint linear codes for $u > n/2$ would only give the nonlinearity $\leq 2^{n-1} - 2^{\frac{n}{2}}$ (in the best case for $u = n/2+1$ we would get $N_F = 2^{n-1} - 2^{\frac{n}{2}}$). This is easily verified by noting that for $u = n/2+1$, there will be at least one linear function in $\mathcal{B}_n$ that completely matches to some linear subfunction in u variables. This would imply that the Walsh coefficients, corresponding to these linear functions, are of magnitude 2^u, and consequently $N_F = 2^{n-1} - 2^{\frac{n}{2}}$, see e.g. [12] for further details. On the other hand, in the extreme case when $u = n/2$, there does not exist sufficiently many vectors of weight $\geq t+1$ in $\mathbb{F}_2^{n/2}$ so that $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ can be constructed. This is justified by noticing that we need to specify $2^{n/2}$ *distinct* linear functions of weight at least $t+1$ (t-resilient linear function), and there are only $\sum_{i=t+1}^{n/2} \binom{n/2}{i} < 2^{n/2}$ distinct t-resilient linear functions on $\mathbb{F}_2^{n/2}$ available.

Hence, to construct an (n, m, t) function F, with strictly almost optimal nonlinearity, the following inequality must be satisfied with $k < n/2$:

$$N(n/2) \cdot (2^m - 1) \cdot 2^{n/2} + N(k) \cdot (2^m - 1) \cdot 2^k \geq 2^n. \quad (20)$$

Indeed, since the truth table of F is of length 2^n and any codeword of length $n/2$, respectively k, specifies one linear function in $n/2$ and k variables, respectively, the above condition ensures there are sufficiently many codewords to be used in the concatenation. Notice that our construction may be viewed as a concatenation of linear functions in k variables with repetition, since any linear function in $n/2 > k$ variables can be represented as a concatenation of $2^{n/2-k}$ suitable linear functions in k variables. Furthermore, assuming that all the codewords of length $n/2$ are used, to satisfy the above condition with equality we may only use a portion of these $N(k)$ disjoint linear codes of length k. Let this number of disjoint linear codes of length k, needed in the construction to satisfy the above condition with equality, be denoted by $N(k)^*$, where obviously $N(k)^* \leq N(k)$. Then, it might be the case that we only need some λ rows (cf. Example 2), where $0 < \lambda \leq 2^m - 1$, of the function matrix A associated to the last code used $C_{N(k)^*}$ to satisfy,

$$N(n/2) \cdot (2^m - 1) \cdot 2^{n/2} + (N(k)^* - 1) \cdot (2^m - 1) \cdot 2^k + \lambda \cdot 2^k = 2^n. \quad (21)$$

Actually, the parameter λ will play an important role in the estimate of the algebraic degree through the following result.

Lemma 3: Let $0 < \lambda \leq 2^m - 1$ be defined by (21) for positive integers $N(n/2), N(k)^*, m, k > 1$. Then, $\lambda \neq 2^m - 1$.

Proof: Assume, on the contrary, that $\lambda = 2^m - 1$. Then, the equation (21) can be rewritten as,

$$(2^m - 1)[N(n/2) \cdot 2^{n/2} + (N(k)^* - 1) \cdot 2^k + 2^k] = (2^m - 1)s = 2^n.$$

This is obviously not possible, thus $\lambda \neq 2^m - 1$. ∎

In other words, if two sets of disjoint linear codes of different length are used in the construction the function matrix A associated to the last code $C_{N(k)^*}$ used will always be shortened through deletion of some rows.

The construction idea presented in Example 2, based on the use of two disjoint linear codes, can easily be extended to involve as many as possible disjoint $[n/2, m, \geq t+1]$ linear codes along with the usage of disjoint linear codes of shorter length k so that (20) is satisfied. Of course, in terms of nonlinearity, it would be desirable to use the least possible k provided the existence of sufficiently many disjoint $[k, m, \geq t+1]$ linear codes so that $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ can be constructed. The possibility of finding sufficiently many disjoint linear codes of length $n/2$, respectively k, is directly related to the parameters E_0 and E_1, respectively, introduced in the construction below.

Construction 1: Let $n \geq 12$ be even and m, $t < \lfloor n/4 \rfloor$ be positive integers. Let $\mathscr{C} = \{C_1, \ldots, C_{N(n/2)}\}$ be a set of $[n/2, m, t+1]$ disjoint linear codes of cardinality $N(n/2)$, and associate to each code a mapping $\rho_i : \mathbb{F}_{2^m} \mapsto C_i, 1 \leq i \leq N(n/2)$, such that

$$b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1} \xmapsto{\rho_i} b_0\theta_0^{(i)} + \cdots + b_{m-1}\theta_{m-1}^{(i)}, \quad (22)$$

where α is primitive in $\mathbb{F}_{2^m}$, and $\theta_0^{(i)}, \ldots, \theta_{m-1}^{(i)}$ is a basis of C_i. Define the matrix A_i by

$$A_i = \begin{pmatrix} \rho_i(1) & \rho_i(\alpha) & \ldots & \rho_i(\alpha^{m-1}) \\ \rho_i(\alpha) & \rho_i(\alpha^2) & \ldots & \rho_i(\alpha^m) \\ \vdots & \vdots & \ddots & \vdots \\ \rho_i(\alpha^{2^m-2}) & \rho_i(1) & \ldots & \rho_i(\alpha^{m-2}) \end{pmatrix}. \quad (23)$$

Let $E_0 = \{e_1, e_2, \ldots, e_\kappa\}$ be any subset of $\mathbb{F}_2^{n/2} \setminus \{\mathbf{0}\}$ with cardinality $\kappa = |E_0| = N(n/2) \cdot (2^m - 1)$. Define $T_0 = C_1 \cup C_2 \cup \cdots \cup C_{N(n/2)}$. For $1 \leq i \leq m$, let ψ_i be a bijective mapping from E_0 to $T_0 \setminus \{\mathbf{0}\}$ such that

$$\begin{pmatrix} \psi_1(e_1) & \psi_2(e_1) & \ldots & \psi_m(e_1) \\ \psi_1(e_2) & \psi_2(e_2) & \ldots & \psi_m(e_2) \\ \vdots & \vdots & \ddots & \vdots \\ \psi_1(e_\kappa) & \psi_2(e_\kappa) & \ldots & \psi_m(e_\kappa) \end{pmatrix} = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_{N(n/2)} \end{pmatrix}. \quad (24)$$

Let $\mathscr{C}' = \{C'_1, \ldots, C'_{N(k)}\}$ be a set of $[k, m, t+1]$ disjoint linear codes with cardinality $N(k)$, and k be the minimum integer in the range $[2m, n/2 - 1]$ such that the inequality (20) is satisfied, which is a necessary condition for our

construction. Denote also by $N(k)^* \leq N(k)$ the portion of these codes satisfying (20) with equality, i.e., satisfying (21). Let $\varrho_j : \mathbb{F}_{2^m} \mapsto C'_j, 1 \leq j \leq N(k)$, be defined by

$$b_0+b_1\beta+\cdots+b_{m-1}\beta^{m-1} \stackrel{\varrho_j}{\longmapsto} b_0\eta_0^{(j)}+\cdots+b_{m-1}\eta_{m-1}^{(j)} \quad (25)$$

where β is primitive in $\mathbb{F}_{2^m}$, and $\eta_0^{(j)}, \ldots, \eta_{m-1}^{(j)}$ is a basis of C'_j. Define the matrix B_j by

$$B_j = \begin{pmatrix} \varrho_j(1) & \varrho_j(\beta) & \ldots & \varrho_j(\beta^{m-1}) \\ \varrho_j(\beta) & \varrho_j(\beta^2) & \ldots & \varrho_j(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \varrho_j(\beta^{2^m-2}) & \varrho_j(1) & \ldots & \varrho_j(\beta^{m-2}) \end{pmatrix} \quad (26)$$

Let $\overline{E_0} = \mathbb{F}_2^{n/2} \setminus E_0$ and $E_1 = \overline{E_0} \times \mathbb{F}_2^{n/2-k} = \{\epsilon_1, \epsilon_2, \ldots, \epsilon_\delta\}$ with $\delta = 2^{n/2-k} \cdot \left(2^{n/2} - N(n/2) \cdot (2^m - 1)\right)$. Define

$$T_1 = C'_1 \cup C'_2 \cup \cdots \cup C'_{N(k)^*}.$$

For $1 \leq i \leq m$, let φ_i be an injective mapping from E_1 to T_1 such that

$$\begin{pmatrix} \varphi_1(\epsilon_1) & \varphi_2(\epsilon_1) & \ldots & \varphi_m(\epsilon_1) \\ \varphi_1(\epsilon_2) & \varphi_2(\epsilon_2) & \ldots & \varphi_m(\epsilon_2) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(\epsilon_\delta) & \varphi_2(\epsilon_\delta) & \ldots & \varphi_m(\epsilon_\delta) \end{pmatrix} = \begin{pmatrix} \widetilde{B_1} \\ B_2 \\ \vdots \\ B_{N(k)^*} \end{pmatrix}_{\delta \times m} \quad (27)$$

where

$$\begin{pmatrix} \widetilde{B_1} \\ B_2 \\ \vdots \\ B_{N(k)^*} \end{pmatrix}_{\delta \times m}$$

denotes that only $\lambda \neq 2^m - 1$ rows of $B_{N(k)^*}$ are used for the adjustment, so that the overall matrix is of size $\delta \times m$. Let $X_n = (X'_{n/2}, X''_{n/2}) = (X'_{n-k}, X''_k) \in \mathbb{F}_2^n$, where $X'_{n/2}, X''_{n/2} \in \mathbb{F}_2^{n/2}$, $X'_{n-k} \in \mathbb{F}_2^{n-k}$, and $X''_k \in \mathbb{F}_2^k$. The function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is then defined as,

$$F(X_n) = (f_1(X_n), f_2(X_n), \ldots, f_m(X_n)),$$

where for $i = 1, 2, \ldots m$,

$$f_i(X_n) = \begin{cases} \psi_i(X'_{n/2}) \cdot X''_{n/2} & \text{if } X'_{n/2} \in E_0 \\ \varphi_i(X'_{n-k}) \cdot X''_k & \text{if } X'_{n-k} \in E_1 \end{cases}. \quad (28)$$

Theorem 2: Let $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ be as in Construction 1. Then F is a t-resilient (n, m) S-box with strictly almost optimal nonlinearity

$$N_F = 2^{n-1} - 2^{n/2-1} - 2^{k-1}. \quad (29)$$

Proof: For any $\mathbf{0} \neq c = (c_1, \ldots, c_m) \in \mathbb{F}_2^m$, let $\psi_c = c_1\psi_1 + \cdots + c_m\psi_m$. Note that for $i = 1, \ldots, m$, ψ_i is an injective mapping, and $C_{i_1} \cap C_{i_2} = \emptyset$ for $1 \leq i_1 < i_2 \leq m$. By Lemma 1, it is not difficult to show that ψ_c is injective. Similarly, $\varphi_c = c_1\varphi_1 + \cdots + c_m\varphi_m$ is injective. Let $\alpha = (\beta', \beta'') = (\gamma', \gamma'') \in \mathbb{F}_2^n$, where β', $\beta'' \in \mathbb{F}_2^{n/2}$, $\gamma' \in \mathbb{F}_2^{n-k}$ and $\gamma'' \in \mathbb{F}_2^k$. Then,

$$W_{f_c}(\alpha) = \sum_{X_n \in \mathbb{F}_2^n} (-1)^{f_c(X_n) \oplus \alpha \cdot X_n} = U_0 + U_1, \quad (30)$$

where

$$\begin{aligned} U_0 &= \textstyle\sum_{X'_{n/2} \in E_0} \sum_{X''_{n/2} \in \mathbb{F}_2^{n/2}} (-1)^{\psi_c(X'_{n/2}) \cdot X''_{n/2} \oplus (\beta', \beta'') \cdot (X'_{n/2}, X''_{n/2})} \\ &= \textstyle\sum_{X'_{n/2} \in E_0} (-1)^{\beta' \cdot X'_{n/2}} \sum_{X''_{n/2} \in \mathbb{F}_2^{n/2}} (-1)^{(\psi_c(X'_{n/2}) + \beta'') \cdot X''_{n/2}} \end{aligned}$$

and

$$U_1 = \sum_{X'_{n-k} \in E_1} (-1)^{\gamma' \cdot X'_{n-k}} \sum_{X''_k \in \mathbb{F}_2^k} (-1)^{(\varphi_c(X'_{n-k}) + \gamma'') \cdot X''_k}.$$

When $\psi_c^{-1}(\beta'') = \emptyset$, we have $U_0 = 0$; or otherwise $U_0 = 2^{n/2} \cdot (-1)^{\beta' \cdot \psi_c^{-1}(\beta'')} = \pm 2^{n/2}$. Therefore, $U_0 \in \{0, \pm 2^{n/2}\}$. Similarly, $U_1 \in \{0, \pm 2^k\}$. Hence,

$$W_{f_c} \in \{0, \pm 2^k, \pm 2^{n/2}, \pm(2^{n/2} - 2^k), \pm(2^{n/2} + 2^k)\}.$$

By (4), $N_{f_c} = 2^{n-1} - 2^{n/2-1} - 2^{k-1}$. Thus, F is strictly almost optimal with

$$N_F = 2^{n-1} - 2^{n/2-1} - 2^{k-1}.$$

When $0 \leq wt(\alpha) \leq t$, we have $wt(\beta'') \leq t$ and $wt(\gamma'') \leq t$. Noticing that $\psi_c(X'_{n/2}) \in T_0$, $\varphi_c(X'_{n-k}) \in T_1$, we have $wt(\psi_c(X'_{n/2})) \geq t+1$ and $wt(\varphi_c(X'_{n-k})) \geq t+1$. Obviously, $\psi_c(X'_{n/2}) + \beta'' \neq 0$ and $\varphi_c(X'_{n-k}) + \gamma'' \neq 0$. Thus, $U_0 = U_1 = 0$, which implies that $W_{f_c}(\alpha) = 0$, for any α such that $0 \leq wt(\alpha) \leq t$. By Definition 2, f_c is a t-resilient function, and so is F. ∎

Example 3: By Corollary 1, there exist 18 disjoint $[6, 2, \geq 2]$ linear codes, and 8 disjoint $[5, 2, \geq 2]$ linear codes. Since $2^6 \cdot 18 \cdot (2^2-1) + 2^5 \cdot 8 \cdot (2^2-1) > 2^{12}$, it is possible to construct a $(12, 2, 1)$ resilient S-box with nonlinearity $2^{11} - 2^5 - 2^4$=2000, which is greater than 1984 [12]. Actually, the best known nonlinearity of a balanced Boolean function for $n = 12$ equals to 2010 [10], [26]. Note also that the nonlinearity of a bent function is $2^{11} - 2^5 = 2016$. However, if we drop the resiliency and consider a construction of a $(12, 2, 0)$ function the nonlinearity may further increase. In this case, for $t = 0$, we may use

$$M(6, 2, 1) = \sum_{j=1}^{2} 2^{6-2j} + 1 = 21$$

disjoint $[6, 2, \geq 1]$ linear codes (these can be found by our algorithm) such that only two disjoint $[4, 2, \geq 1]$ codes are needed in the construction. Indeed, $21 \cdot 3 \cdot 2^6 + 2 \cdot 3 \cdot 2^4 > 2^{12}$, and thus the nonlinearity is strictly almost optimal, and given by $2^{11} - 2^5 - 2^3 = 2008$, which is the best nonlinearity of a balanced (12,2) S-box currently known.

In Table V (in Appendix), we give an extended list of resilient S-boxes with currently best known nonlinearity. In many cases our nonlinearity is comparable to the best known nonlinearities of balanced Boolean functions. This indicates the possibility of designing resilient S-boxes without any degradation in nonlinearity when compared to balanced Boolean functions. In Table I, a nonlinearity comparison, related to the design of $(36, 8, t)$-resilient S-boxes using different methods, is given. It is clear that our approach, in terms of nonlinearity, is superior to other methods.

TABLE I
COMPARISON OF THE NONLINEARITY OF $(36, 8, t)$-RESILIENT S-BOXES USING DIFFERENT METHODS

t	ours	[11]	[24]	[14]
1	$2^{35}-2^{17}-2^{15}$	$2^{35}-2^{18}$	$2^{35}-2^{18}$	$2^{35}-2^{22}$
2	$2^{35}-2^{17}-2^{15}$	$2^{35}-\frac{9}{16}2^{20}$	$2^{35}-2^{20}$	$2^{35}-2^{23}$
3	$2^{35}-2^{17}-2^{16}$	$2^{35}-2^{20}$	$2^{35}-2^{20}$	$2^{35}-2^{24}$
4	$2^{35}-2^{18}$	$2^{35}-2^{22}$	$2^{35}-2^{23}$	$2^{35}-2^{25}$
5	$2^{35}-2^{19}$	$2^{35}-\frac{19}{32}2^{23}$	$2^{35}-2^{23}$	$2^{35}-2^{26}$

V. IMPROVED CONSTRUCTION

In the previous construction, two disjoint sets of respective length $n/2$ and k were used. However, in certain cases (especially for large $\frac{n}{m}$), there is a possibility that many disjoint sets of length strictly less than k may serve for the same purpose. Indeed, let again $N(n/2)$ denote the cardinality of a set of $[n/2, m, t+1]$ disjoint linear codes, and let $N(k_i)$ denote the cardinality of a set of $[k_i, m, t+1]$ disjoint linear codes. Then, it might be the case that $2^{n/2}N(n/2)(2^m-1)+\sum_i 2^{k_i}N(k_i)(2^m-1) \geq 2^n$, where each k_i is less than k used in Construction 1. This case arises when $n \gg m$, and consequently we may even get higher nonlinearities than those obtained by our original method. The possibility of finding sufficiently many disjoint linear codes of length less than k is related to the binary indicator $(a_{2m}, a_{2m+1}, \ldots, a_{n/2}) \in \mathbb{F}_2^{n/2-2m+1}$ defined in the construction below.

Construction 2: Let $n \geq 12$ be even and m, $t < \lfloor n/4 \rfloor$ be positive integers. For $2m \leq u \leq n/2$, let $\mathbb{C}_u = \{C_1^{(u)}, \ldots, C_{N(u)}^{(u)}\}$ be a set of $[u, m, t+1]$ disjoint linear codes with cardinality $N(u)$, and associate to each code a mapping $\phi_u^{(i)} : \mathbb{F}_{2^m} \mapsto C_i^{(u)}, 1 \leq i \leq N(u)$, such that

$$b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1} \overset{\phi_u^{(i)}}{\longmapsto} b_0\theta_0^{(i)} + \cdots + b_{m-1}\theta_{m-1}^{(i)}, \quad (31)$$

where α is primitive in $\mathbb{F}_{2^m}$, and $\theta_0^{(i)}, \cdots, \theta_{m-1}^{(i)}$ is a basis of $C_i^{(u)}$. Define the matrix A_i by,

$$A_i^{(u)} = \begin{pmatrix} \phi_u^{(i)}(1) & \phi_u^{(i)}(\alpha) & \ldots & \phi_u^{(i)}(\alpha^{m-1}) \\ \phi_u^{(i)}(\alpha) & \phi_u^{(i)}(\alpha^2) & \ldots & \phi_u^{(i)}(\alpha^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_u^{(i)}(\alpha^{2^m-2}) & \phi_u^{(i)}(1) & \ldots & \phi_u^{(i)}(\alpha^{m-2}) \end{pmatrix}. \quad (32)$$

For $2m \leq u \leq n/2$, let $E_u' = E_u \times \mathbb{F}_2^u$, where $E_u = \{e_1, e_2, \ldots, e_{\kappa(u)}\}$ is a subset of $\mathbb{F}_2^{n-u}$. Let $(a_{2m}, a_{2m+1}, \ldots, a_{n/2}) \in \mathbb{F}_2^{n/2-2m+1}$ be a binary vector of the minimum integer value $\sum_{j=0}^{n/2-2m} a_{2m+j}2^j$ where,

$$a_u = \begin{cases} 1 & \text{if } E_u \neq \emptyset \\ 0 & \text{if } E_u = \emptyset \end{cases}$$

such that the following conditions are satisfied:

- $|E_u'| = \kappa(u) \leq N(u) \cdot (2^m - 1)$;
- $\bigcup_{u=2m}^{n/2} E_u' = \mathbb{F}_2^n$;
- and $E_{u_1}' \cap E_{u_2}' = \emptyset$, where $2m \leq u_1 < u_2 \leq n/2$.

Define $T_u = C_1 \cup C_2 \cup \cdots \cup C_{N(u)}$. For $1 \leq j \leq m$, let ψ_j be an injective mapping from E_u to T_u such that

$$\begin{pmatrix} \psi_1(e_1) & \ldots & \psi_m(e_1) \\ \psi_1(e_2) & \ldots & \psi_m(e_2) \\ \vdots & \ddots & \vdots \\ \psi_1(e_{\kappa(u)}) & \ldots & \psi_m(e_{\kappa(u)}) \end{pmatrix} = \begin{pmatrix} \widetilde{A_1^{(u)}} \\ A_2^{(u)} \\ \vdots \\ A_{N(u)}^{(u)} \end{pmatrix}_{\kappa(u)\times m} \quad (33)$$

Let $X_n = (X_{n-u}', X_u'') \in \mathbb{F}_2^n$ where $X_{n-u}' \in \mathbb{F}_2^{n-u}$ and $X_u'' \in \mathbb{F}_2^u$. An (n, m) S-box, $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, is then defined as,

$$F(X_n) = (f_1(X_n), f_2(X_n), \ldots, f_m(X_n)),$$

where for $j = 1, \ldots, m$

$$f_j(X_n) = \psi_i(X_{n-u}') \cdot X_u'', \quad X_{n-u}' \in E_u,\ 2m \leq u \leq n/2.$$

Theorem 3: Let $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ be as in Construction 2. Then F is a t-resilient S-box with

$$N_F = 2^{n-1} - 2^{n/2-1} - \sum_{u=2m}^{n/2-1} a_u \cdot 2^{u-1}. \quad (34)$$

In Table II, we see that Theorem 3 can improve upon the results of Theorem 2, and this is especially true for the large ratios of n and m, as suggested previously.

A. A construction of strictly almost optimal $(n, m, 0)$ S-boxes

The purpose of this section is to demonstrate that balanced S-boxes with extremely good nonlinearity can be constructed by combining our approach with other methods. More precisely, disjoint linear codes can be interlinked with the ideas used in the construction of perfect nonlinear S-boxes by Nyberg in [23] along with the method, independently proposed by Dobbertin [10] and Seberry et al. [26], of constructing highly nonlinear balanced Boolean functions.

By Theorem 1, there exists a set of $[n, n/2, 1]$ disjoint linear codes $\mathcal{C} = \{C_0, C_1, \cdots, C_{2^{n/2}-1}, C_{2^{n/2}}\}$ with cardinality $2^{n/2}+1$, which essentially corresponds to the number of points in the projective plane $\mathbf{PG}(1, \mathbb{F}_{2^{n/2}})$ (cf. [13] or any other textbook on projective geometry). Any point, being a linear subspace of dimension $n/2$ of $\mathbb{F}_2^n$, can be identified with an $[n, n/2, 1]$ linear code but not necessarily to the particular codes from $\mathcal{C}$. We below describe the construction of partial spread ($\mathcal{PS}$) family bent functions, introduced by Dillon [8], in terms of disjoint linear codes.

Lemma 4: Let $f \in \mathcal{B}_n$ with $n = 2e$. Let $\mathcal{C} = \{C_0, C_1, \ldots, C_{2^e}\}$ be a set of $[n, n/2, 1]$ disjoint linear codes with $\bigcup_{i=0}^{2^e} C_i = \mathbb{F}_2^n$. Then f is a $\mathcal{PS}^-$ (resp. $\mathcal{PS}^+$) bent function when it satisfies (i) (resp. (ii)):

(i) $supp(f) = \bigcup_{i=0}^{2^{e-1}-1} C_i{}^*$, where $C_i^* = C_i \backslash \{\mathbf{0}\}$,

(ii)$supp(f) = \bigcup_{i=0}^{2^{e-1}} C_i$.

A method of constructing $(n, n/2)$ perfect nonlinear S-boxes, based on the use of $\mathcal{PS}$ class bent functions, was first proposed by Nyberg [23], and is redescribed below.

Lemma 5: Let n be even, and let

$$\mathcal{C} = \{C_0, C_1, \cdots, C_{2^{n/2}-1}, C_{2^{n/2}}\} \quad (35)$$

be a set of $[n, n/2, 1]$ disjoint linear codes of cardinality $2^{n/2}+1$. For $i = 1, \ldots, m$, with $2 \leq m \leq n/2$, let $h_i \in \mathcal{B}_{n/2}$ be

TABLE II
(n, m, t) S-BOXES WITH IMPROVED NONLINEARITY

t	n	m	Construction 1	Construction 2
0	20	2	$2^{19}-2^9-2^5$	$2^{19}-2^9-2^4-2^3$
	24	2	$2^{23}-2^{11}-2^8$	$2^{23}-2^{11}-2^5-2^3$
	28	2	$2^{27}-2^{13}-2^7$	$2^{27}-2^{13}-2^6-2^4$
	32	2	$2^{31}-2^{15}-2^8$	$2^{31}-2^{15}-2^7-2^4$
	36	2	$2^{35}-2^{17}-2^9$	$2^{35}-2^{17}-2^8-2^5$
	40	2	$2^{39}-2^{19}-2^{10}$	$2^{39}-2^{19}-2^9-2^4-2^3$
	26	3	$2^{25}-2^{12}-2^8$	$2^{25}-2^{12}-2^7-2^6$
	36	3	$2^{35}-2^{17}-2^9$	$2^{35}-2^{17}-2^8-2^5$
	38	3	$2^{37}-2^{18}-2^{11}$	$2^{37}-2^{18}-2^{10}-2^9$
	40	4	$2^{39}-2^{19}-2^{10}$	$2^{39}-2^{19}-2^9-2^7$
1	20	2	$2^{19}-2^9-2^7$	$2^{19}-2^9-2^6-2^5$
	24	2	$2^{23}-2^{11}-2^8$	$2^{23}-2^{11}-2^7-2^6-2^4$
	30	3	$2^{29}-2^{14}-2^{10}$	$2^{29}-2^{14}-2^9-2^8$
	22	4	$2^{21}-2^{10}-2^9$	$2^{21}-2^{10}-2^8-2^7$
	30	4	$2^{29}-2^{14}-2^{11}$	$2^{29}-2^{14}-2^{10}-2^9$
	32	4	$2^{31}-2^{15}-2^{11}$	$2^{31}-2^{15}-2^{10}-2^8$
	38	4	$2^{37}-2^{18}-2^{13}$	$2^{37}-2^{18}-2^{12}-2^{11}$
	40	4	$2^{39}-2^{19}-2^{13}$	$2^{39}-2^{19}-2^{12}-2^{11}$
	34	5	$2^{33}-2^{16}-2^{12}$	$2^{33}-2^{16}-2^{11}-2^{10}-2^9$
	36	5	$2^{35}-2^{17}-2^{13}$	$2^{35}-2^{17}-2^{12}-2^{11}$
	38	5	$2^{37}-2^{18}-2^{14}$	$2^{37}-2^{18}-2^{13}-2^{12}$
	32	6	$2^{31}-2^{15}-2^{13}$	$2^{31}-2^{15}-2^{12}-2^{11}$
	34	6	$2^{33}-2^{16}-2^{14}$	$2^{33}-2^{16}-2^{13}-2^{11}$
	40	6	$2^{39}-2^{19}-2^{14}$	$2^{39}-2^{19}-2^{13}-2^{12}$
2	26	2	$2^{25}-2^{12}-2^{10}$	$2^{25}-2^{12}-2^9-2^8$
	36	2	$2^{35}-2^{17}-2^{13}$	$2^{35}-2^{17}-2^{10}-2^9$
	40	2	$2^{39}-2^{19}-2^{14}$	$2^{39}-2^{19}-2^{13}-2^{12}-2^{11}$
	28	3	$2^{27}-2^{13}-2^{11}$	$2^{27}-2^{13}-2^{10}-2^9$
	30	4	$2^{29}-2^{14}-2^{12}$	$2^{29}-2^{14}-2^{11}-2^9-2^8$
	34	4	$2^{33}-2^{16}-2^{13}$	$2^{33}-2^{16}-2^{12}-2^{11}-2^{10}$
	28	5	$2^{27}-2^{13}-2^{12}$	$2^{27}-2^{13}-2^{11}-2^9$
	36	5	$2^{35}-2^{17}-2^{14}$	$2^{35}-2^{17}-2^{13}-2^{12}-2^{10}-2^9$
	38	6	$2^{37}-2^{18}-2^{15}$	$2^{37}-2^{18}-2^{14}-2^{13}$
	36	7	$2^{35}-2^{17}-2^{15}$	$2^{35}-2^{17}-2^{14}-2^{13}$
3	38	2	$2^{37}-2^{18}-2^{15}$	$2^{37}-2^{18}-2^{14}-2^{11}$
	40	3	$2^{39}-2^{19}-2^{16}$	$2^{39}-2^{19}-2^{15}-2^{14}$
	32	4	$2^{31}-2^{15}-2^{14}$	$2^{31}-2^{15}-2^{13}-2^{12}$
	34	5	$2^{33}-2^{16}-2^{15}$	$2^{33}-2^{16}-2^{14}-2^{13}$
	36	6	$2^{35}-2^{17}-2^{16}$	$2^{35}-2^{17}-2^{15}-2^{14}$
	38	7	$2^{37}-2^{18}-2^{17}$	$2^{37}-2^{18}-2^{16}-2^{15}$
4	32	2	$2^{31}-2^{15}-2^{14}$	$2^{31}-2^{15}-2^{13}-2^{12}-2^{11}$
	38	2	$2^{37}-2^{18}-2^{16}$	$2^{37}-2^{18}-2^{15}-2^{14}$
	40	3	$2^{39}-2^{19}-2^{17}$	$2^{39}-2^{19}-2^{16}-2^{15}$
	40	7	-	$2^{39}-2^{19}-2^{18}-2^{16}-2^{15}$
5	20	2	-	$2^{19}-2^{10}-2^9$
	30	5	-	$2^{29}-2^{15}-2^{14}$
	38	2	$2^{37}-2^{18}-2^{17}$	$2^{37}-2^{18}-2^{16}-2^{14}$
	40	3	$2^{39}-2^{19}-2^{18}$	$2^{39}-2^{19}-2^{17}-2^{16}-2^{15}$
	40	5	-	$2^{39}-2^{19}-2^{18}-2^{17}$

such that $H = (h_1, \ldots, h_m)$ is a balanced $(n/2, m)$ S-box. Define the functions $f_i \in \mathcal{B}_n$ by,

$$supp(f_i) = \bigcup_{[j] \in supp(h_i)} C_j^*, \tag{36}$$

where $C_j^* = C_j \backslash \{\mathbf{0}\}$ and $[j]$ denote the binary representation of j. Then, the (n, m) S-box, $F = (f_1, \ldots, f_m)$, is perfect nonlinear.

Proof: By Lemma 4, for $i = 1, \ldots, m$, f_i is obviously a $\mathcal{PS}^-$ type bent function. Since H is a balanced $(n/2, m)$ S-box, then $h_c = c_1h_1 \oplus \cdots \oplus c_mh_m$ is a balanced Boolean function, i.e., $\#supp(h_c) = 2^{n/2-1}$, where $c = (c_1, \ldots, c_m) \in \mathbb{F}_2^{m*}$. Let $f_c = c_1f_1 \oplus \cdots \oplus c_mf_m$ be a nonzero linear combination of $f_1, \ldots, f_m$. Notice that

$$supp(f_c) = \bigcup_{[j] \in supp(h_c)} C_j^*. \tag{37}$$

By Lemma 4, f_c is also a $\mathcal{PS}^-$ type bent function, and therefore $F = (f_1, \ldots, f_m)$ is perfect nonlinear. ■

Example 4: We consider the construction of a $(12, 6)$ perfect nonlinear S-box. Thanks to Theorem 1, a set of $[12, 6, 1]$ disjoint linear codes $\mathcal{C} = \{C_0, C_1, \ldots, C_{64}\}$ can be obtained. Let $y = (y_1, \ldots, y_6) \in \mathbb{F}_2^6$, and let $H = (h_1(y), \ldots, h_6(y))$ be the identity permutation on $\mathbb{F}_2^6$, that is, $h_i(y) = y_i$, $i = 1, \ldots, 6$. We construct a $(12, 6)$ S-box, $F = (f_1, \ldots, f_6)$, by defining $f_i \in \mathcal{B}_6$ as,

$$supp(f_i) = \bigcup_{\substack{0 \le j \le 63 \\ [j] \in \{y \in \mathbb{F}_2^6 : y_i = 1\}}} C_j^*, \quad 1 \le i \le 6.$$

Let $f_c = c_1f_1 \oplus \ldots \oplus c_6f_6$, where $c = (c_1, \ldots, c_m) \in \mathbb{F}_2^{m*}$. Then,

$$supp(f_c) = \bigcup_{\substack{0 \le j \le 63 \\ [j] \in \mathcal{S}}} C_j^*,$$

where $\mathcal{S} = \{y \in \mathbb{F}_2^6 : \sum_{i=1}^m c_iy_i = 1\}$. Note that $\#\mathcal{S} = 2^{n/2-1}$, and by Lemma 4 f_c is a $\mathcal{PS}^-$ bent function. Thus, F is a $(12, 6)$ perfect nonlinear S-box.

Notice that in Lemma 5, the code $E = C_{2^{n/2}}$ is not a part of $supp(f_c)$ for any $c \in \mathbb{F}_2^{m*}$, and hereinafter it will be called a "free code". In the above example, C_{64} is a free code. Without loss of generality, we may assume that an $[n, n/2]$ free code E in Lemma 5 is always of the form: $E = \{\mathbf{0}_{n/2}\} \times \mathbb{F}_2^{n/2}$, where $\mathbf{0}_{n/2} = (0, \ldots, 0) \in \mathbb{F}_2^{n/2}$. Apparently, a function whose support is defined on E can be identified to a Boolean function in $\mathcal{B}_{n/2}$.

The following construction method employs the above result and the recursive process of generating a highly nonlinear balanced Boolean function from a bent function, as originally used in [10], [26].

Construction 3: Let $n \ge 2m$, and furthermore assume $n = 2^r \cdot n_0$ is even satisfying,

$$n_0 \in \{j \mid j \ge m \quad \text{and } j \text{ is odd}\} \cup \{j \mid m \le j < 2m \text{ and } j \text{ is even}\}. \tag{38}$$

By Lemma 5, for $s = 0, \ldots, r-1$, we can obtain an $(\frac{n}{2^s}, m)$ perfect nonlinear S-box

$$F_s = \left(f_1^{(s)}, \ldots, f_m^{(s)}\right).$$

For $s = r$, the goal is to design an $(n_0, m, 0)$ S-box, $F_r = (f_1^{(r)}, \ldots, f_m^{(r)})$, with nonlinearity N_{F_r} as large as possible. Then, using the constructed S-boxes, an (n, m) S-box, $F = (f_1, \ldots, f_m)$, is defined as,

$$supp(f_i) = \bigcup_{s=0}^{r} \widehat{supp(f_i^{(s)})}, \quad i = 1, \ldots, m, \tag{39}$$

where $\widehat{supp(f_i^{(s)})} = \{\mathbf{0}_e\} \times supp(f_i^{(s)})$, and $e = n - \frac{n}{2^s}$.

Remark 2: Note that the condition on n_0 given by (38) implies that for $m = n/2$ only a single step of the recursion

is used. That is, in this case $r = 1$ and it is sufficient to find a suitable highly nonlinear permutation on $\mathbb{F}_2^{n/2}$ for the construction to work.

Theorem 4: Let $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ be as in Construction 3 with $m \leq n_0 < 2m$. Then, F is an $(n, m, 0)$ S-box with strictly almost optimal nonlinearity

$$N_F \quad \geq \quad 2^{n-1} - \sum_{s=1}^{r} 2^{\frac{n}{2^s}-1} - 2^{\lfloor \frac{n_0}{2} \rfloor}. \tag{40}$$

Proof: For any $c = (c_1, \ldots, c_m) \in \mathbb{F}_2^{m*}$, let $f_c = \sum_{i=1}^m c_i f_i$. Since $\#supp(f_c) = 2^{n-1}$, it follows that F is an $(n, m, 0)$ S-box. By noting that, for $s = 0, \ldots, r-1$, $f_c^{(s)}$ is a $\mathcal{PS}^-$ bent function on $\mathbb{F}_2^{\frac{n}{2^s}}$, we get $W_{f_c^{(s)}}(\omega) = \pm 2^{\frac{n}{2^{s+1}}}$. Thus,

$$\mathcal{L}(f_c) = \max_{\omega \in \mathbb{F}_2^n} |W_{f_c}(\omega)| \leq \sum_{s=1}^{r} 2^{\frac{n}{2^s}} + \mathcal{L}(f_c^{(r)}),$$

where

$$W_{f_c}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_c(x)+\omega \cdot x} = \sum_{s=0}^{r} W_{f_c^{(s)}}(\omega).$$

By Remark 1, $\Lambda(F_r) \leq 2^{\lfloor \frac{n_0}{2} \rfloor + 1}$. We have

$$\Lambda(F) \leq \sum_{s=1}^{r} 2^{\frac{n}{2^s}} + \Lambda(F_r) \leq \sum_{s=1}^{r} 2^{\frac{n}{2^s}} + 2^{\lfloor \frac{n_0}{2} \rfloor + 1}.$$

Using (4) for computing N_F, the assertion is proved. ∎

In Example 3, we discussed a construction of a $(12, 2, 0)$ S-box with nonlinearity $N_F = 2008$. To illustrate the improvements gained by the above approach, we notice that this method gives a $(12, 3, 0)$ S-box with even higher nonlinearity, namely $N_F = 2010$. Remark that along with nonlinearity the output space is also increased, hence there is no trade-off of the parameters.

Example 5: Let us consider the construction of a $(12, 3, 0)$ S-box with nonlinearity 2010 using the above approach. Note that in this case $12 = 2^2 \cdot 3$, $r = 2$, $n_0 = 3$. From Lemma 5, by using a set of [12,6,1] disjoint linear codes $\mathcal{C}_0$ whose free code is $E_0 = \{\mathbf{0}_6\} \times \mathbb{F}_2^6$, we can obtain a $(12, 3)$ perfect nonlinear S-box, $F_0 = (f_1^{(0)}, f_2^{(0)}, f_3^{(0)})$. Similarly, by employing a set of [6,3,1] disjoint linear codes $\mathcal{C}_1$, whose free code is $E_1 = \{\mathbf{0}_3\} \times \mathbb{F}_2^3$, we can obtain a $(6, 3)$ perfect nonlinear S-box, $F_1 = (f_1^{(1)}, f_2^{(1)}, f_3^{(1)})$. The next step is to build a permutation F_2 over $\mathbb{F}_2^3$, for instance given by,

$$f_1^{(2)} = x_1 \oplus x_2 x_3,$$
$$f_2^{(2)} = x_2 \oplus x_1 x_3 \oplus x_2 x_3,$$
$$f_3^{(2)} = x_1 \oplus x_2 \oplus x_3 \oplus x_1 x_2,$$

so that $F_2 = (f_1^{(2)}, f_2^{(2)}, f_3^{(2)})$. It is easily verified that $\Lambda(F_2) = 4$. Finally, a $(12, 3, 0)$ S-box, $F = (f_1, f_2, f_3)$, is constructed by defining the support of f_i as,

$$supp(f_i) = supp(f_i^{(0)}) \cup \widehat{supp(f_i^{(1)})} \cup \widehat{supp(f_i^{(2)})}, \ \ i = 1, 2, 3.$$

From the proof of Theorem 4, $\Lambda(F) = 2^6 + 2^3 + 4 = 76$. Therefore, $N_F = 2^{11} - \frac{1}{2} \cdot 76 = 2010$.

We now consider a particular case of our approach where only one step of the recursion is performed as remarked above. The reader should notice that the method proposed by Nyberg [23] is used in the construction of perfect nonlinear (unbalanced) $(n, n/2)$ S-boxes, as opposed to our approach where balanced $(n, n/2, 0)$ S-boxes are constructed.

Corollary 3: Let $n \geq 6$ be even. Then, there exists a balanced function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^{n/2}$, that is, an $(n, n/2, 0)$ S-box with strictly almost optimal nonlinearity

$$N_F = 2^{n-1} - 2^{n/2-1} - 2^{\lfloor n/4 \rfloor}. \tag{41}$$

Proof: Note that $n \equiv 2 \mod 4$ implies that $n/2$ is odd. We may take $G(x) = x^3$, $x \in \mathbb{F}_{2^{n/2}}$, which is a maximally nonlinear permutation on $\mathbb{F}_{n/2}$ i.e., $\Lambda(G) = 2^{\frac{n+2}{4}}$. In this case $r = 1$, so that $G = F_1$, and therefore the nonlinearity equals to $N_F = 2^{n-1} - 2^{n/2-1} - 2^{(n-2)/4}$. Otherwise, if $n \equiv 0 \pmod 4$, then $n/2$ is even and for instance we can take the inverse function $G(x) = x^{-1}$, $x \in \mathbb{F}_{2^{n/2}}$, which is a permutation on $\mathbb{F}_{n/2}$. Since in this case $\Lambda(G) = 2^{\frac{n}{4}+1}$, it follows that $N_F = 2^{n-1} - 2^{n/2-1} - 2^{n/4}$. ∎

Example 6: Let us consider the design of a $(10, 5, 0)$ S-box using the above approach. Since $n \equiv 2 \mod 4$, and $n/2 = 5$ is odd, there exist maximally nonlinear functions on $\mathbb{F}_2^5$. Thus, let $F_1(x) = G(x) = x^3$ again implying that a balanced $(10, 5, 0)$ S-box with nonlinearity 492 can be constructed. If we consider the construction of a $(12, 6, 0)$ S-box, using instead $F_1(x) = G(x) = x^{-1}$ as a permutation on $\mathbb{F}_{2^6}$, a balanced $(12, 6)$ S-box with nonlinearity 2008 can be designed. Note that $N_G = 24$ in this case.

VI. Algebraic properties of our S-boxes

To estimate the algebraic degree of the functions we need some easy technical results.

Lemma 6: Let A^* be a matrix of size $\lambda \times m$ obtained from matrix A in Lemma 2 by deleting the last $2^m - 1 - \lambda$ rows, where $1 \leq \lambda < 2^m - 1$. That is,

$$A^* = \begin{pmatrix} \phi(1) & \phi(\beta) & \ldots & \phi(\beta^{m-1}) \\ \phi(\beta) & \phi(\beta^2) & \ldots & \phi(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(\beta^{\lambda-1}) & \phi(\beta^{\lambda)}) & \ldots & \phi(\beta^{\lambda+m-2}) \end{pmatrix}. \tag{42}$$

Then, for any nonzero linear combinations of the columns of A^*, the sum of the elements in the resulting column is different from the all-zero vector.

Proof: Since $\phi : \mathbb{F}_{2^m} \mapsto C$ defined by

$$\phi(a_0 + a_1\beta + \cdots a_{m-1}\beta^{m-1}) = a_0 c_0 + a_1 c_1 + \cdots a_{m-1} c_{m-1},$$

is an isomorphism it is sufficient to consider linear combinations of the matrix,

$$\begin{pmatrix} 1 & \beta & \ldots & \beta^{m-1} \\ \beta & \beta^2 & \ldots & \beta^m \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{\lambda-1} & \beta^{\lambda} & \ldots & \beta^{\lambda+m-2} \end{pmatrix}. \tag{43}$$

Any nonzero linear combination of columns can be written as

$$(d_0 + d_1\beta + \cdots + d_{m-1}\beta^{m-1}) \begin{pmatrix} 1 \\ \beta \\ \vdots \\ \beta^{\lambda-1} \end{pmatrix},$$

for some $d_0, d_1 \ldots, d_{m-1} \in \mathbb{F}_2$. Since $d_0 + d_1\beta + \cdots + d_{m-1}\beta^{m-1} \neq 0$, it remains to show that $\sum_{i=0}^{\lambda-1} \beta^i \neq 0$ for a primitive element $\beta \in \mathbb{F}^{2^m}$. But $\sum_{i=0}^{\lambda-1} \beta^i = \frac{1+\beta^\lambda}{1+\beta} \neq 0$, for $\lambda < 2^m - 1$. This completes the proof. ∎

We note that in Construction 1 we have used two sets of disjoint linear codes of different length, and it was shown that the parameter $\lambda \neq 2^m - 1$. Along the same lines of reasoning we can deduce that $\lambda \neq 2^m - 1$ is also true for the codes used in Construction 2. Indeed, denoting by k' the minimum length of any linear code used in the construction, the condition similar to (21) is given by,

$$N(n/2) \cdot(2^m-1)\cdot 2^{n/2} + \sum_{j=k'+1}^{n/2-1} \Big(a_j N(j)\cdot(2^m-1)\cdot 2^j\Big) + (N(k')-1)\cdot 2^{k'}\cdot(2^m-1) + \lambda\cdot 2^{k'} = 2^n,$$

where the a_js are binary constants indicating whether some codes of length $k'+1 \leq j \leq n/2-1$ are used. Assuming that $\lambda = 2^m - 1$ the above equation again gives,

$$(2^m-1)\big[N(n/2)\cdot 2^{n/2} + \sum_{j=k'+1}^{n/2-1} (a_j N(j)\cdot 2^j) + N(k')\cdot 2^{k'}\big] = 2^n,$$

which is clearly impossible.

Theorem 5: Let $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ be an (n, m) S-box constructed by means of either Construction 1 or Construction 2. Then, the algebraic degree of F can achieve $n-k'+1$, where k' is the minimal length of the codes used in the construction.

Proof: Let $f_b(X_n) = \sum_{i=1}^m b_i f_i(X_n)$, where not all $b_i \in \mathbb{F}_2$ are equal to zero. We only consider Construction 1, as the same reasoning applies to Construction 2. We have to show the existence of the term of degree $n-k+1$ in the ANF of f_b, for f_i defined by (28). f_b can be viewed as a concatenation of linear functions corresponding to the codewords of $\mathscr{C}$ and $\mathscr{C}'$, of respective length $n/2$ and k. Using the notation of Construction 1, the ANF of f_b is then,

$$f_b(X_n) = f_b(X'_n, X''_n) = \bigoplus_{\sigma\in E_0} \prod_{i=1}^{n/2} (x_i \oplus \sigma_i \oplus 1) l_b^\sigma(X''_n) + \bigoplus_{\delta\in E_1} \prod_{i=1}^{n-k} (x_i \oplus \delta_i \oplus 1) l_b^\delta(x_{n-k+1}, \ldots, x_n),$$

where $l_b^\sigma(X''_n)$ are linear resilient functions in $n/2$ variables obtained from the function matrix A, and similarly l_b^δ are k-variable linear functions obtained from B. It is enough to show that $\sum_{\delta\in E_1} \prod_{i=1}^{n-k}(x_i \oplus \delta_i \oplus 1) l_b^\delta(x_{n-k+1}, \ldots, x_n)$ contains a term of degree $n-k+1$. By Lemma 6, $l_b^*(x_{n-k+1}, \ldots, x_n) = \sum_{\delta\in E_1} l_b^\delta(x_{n-k+1}, \ldots, x_n) \neq 0$, hence the term(s) $x_1 \cdots x_{n-k} \cdot l_b^*(x_{n-k+1}, \ldots, x_n)$ of degree $n-k+1$ is (are) in the ANF of f_b. The result follows by noting that Lemma 6 applies whenever $\lambda < 2^m - 1$, which is by Lemma 3 always the case. ∎

TABLE III
RELEVANT CRYPTOGRAPHIC PARAMETERS OF SOME SMALL (n, m, t)-RESILIENT S-BOXES

Method	(n, m, t)	$deg(F)$	$AI(F)$	N_F
Construction 1	(10,2,0)	7	5	488
Construction 1	(12,2,0)	9	5	2008
Construction 1	(12,2,1)	8	5	2000
Construction 1	(14,3,1)	9	6	8096
Construction 3	(10,5,0)	8	5	**492**
Construction 3	(12,3,0)	11	6	**2010**
Construction 3	(12,6,0)	11	6	2008
Construction 3	(14,7,0)	11	7	**8120**

It is easy to verify that our (n, m, t) S-boxes can reach Siegenthaler's bound given by $deg(F) \leq n - t - 1$, only in those cases when the codes of minimum length used in the construction meet the Singleton bound. This bound states that for any $[n, m, d]$ linear code we necessarily have $m + d \leq n + 1$. Thus, to construct an (n, m, t) S-box that meets the Siegenthaler bound, the smallest length k' of our codes must satisfy $k' = t + 2$, so that $deg(F) = n - k' + 1 = n - t - 1$. Therefore, we need $[k' = t+2, m, t+1]$ linear codes and this implies that only for $m = 2$ there is a possibility of using the codes meeting the Singleton bound.

Remark 3: Let F be a balanced (n, m) S-box constructed by means of Construction 3. Then $deg(F) = n - n_0 + deg(F_r)$. Obviously, F reach Siegenthaler's bound $n - 1$ if $deg(F_r) = n_0 - 1$.

In Table III, we list the most important parameters for some relatively small S-boxes constructed by our methods. The algebraic immunity is either optimal or slightly suboptimal, and the algebraic degree of these functions is in accordance with the result of Theorem 5 and Remark 3. The bold face entries denote the instances for which, to the best of our knowledge, the nonlinearity of our S-boxes is comparable to currently best known nonlinearity values of balanced Boolean functions. Actually, the only construction of balanced Boolean functions that in certain cases compares favourably to the nonlinearity of our S-boxes is the method of Dobbertin [10] and Seberry *et al.* [26].

Theorem 6: [10], [26] For even n, $n \geq 4$ it is possible to construct a balanced Boolean function f^* with nonlinearity

$$N_{f^*} \geq \begin{cases} 2^{2^m-1} - \frac{1}{2}(2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2\cdot 2^2), \\ \qquad\qquad \text{for } n = 2^m \\ 2^{2^s(2t+1)-1} - \frac{1}{2}(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \cdots \\ \quad + 2^{2(2t+1)}2^{2t+1} + 2^{t+1}), \quad \text{for } n = 2^s(2t+1). \end{cases}$$

For instance, the best known nonlinearity for $n = 12$ is currently 2010, and for $n = 14$ this value is 8120 [10], [26]. Apparently, our S-boxes (almost) reach these best known nonlinearities.

Remark 4: It can be verified that provided the existence of a single $[k' = t + 2, 2, t + 1]$ linear code meeting the Singleton bound, a degree optimized $(n, 2, t)$ S-box can be constructed. Nevertheless, the nonlinearity of such an S-box may decrease by the value 2^{t+1} when compared to the values listed in Table V.

VII. Conclusions and an open problem

In this paper, we have presented a construction method to obtain strictly almost optimal resilient functions with a nonlinearity higher than that attainable by any previously known construction method. The following problem is left for future work.

Conjecture 1: Let $n \geq 12$ be even and $t \leq n/2 - 2$. If $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is a strictly almost optimal t-resilient S-box, then $m + t < n/2$.

References

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

[2] A. Canteaut, P. Charpin, and H. Dobbertin, "Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^n}$, and crosscorrelation of maximum-length sequences" SIAM Journal on Discrete Mathematics, vol. 13, no.1, pp. 105-138, 2000.

[3] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in Advances in Cryptology–EUROCRYPTO'94 (Lecture Notes in Computer Sceince). Berlin, Germany: Springer-Verlag, 1995, vol. 950, pp. 356-365.

[4] P. Charpin and E. Pasalic, "Highly nonlinear resilient functions through disjoint codes in projective spaces," Designs, Codes and Cryptography, vol. 37, pp. 319-346, 2005.

[5] L. Chen and F.-W. Fu, "On the construction of new resilient functions from old ones," IEEE Transactions on Information Theory, vol. 45, pp. 2077-2082, 1999.

[6] J. H. Cheon, "Nonlinear vector resilient functions," in Advances in Cryptology–CRYPTO 2001 (Lecture Notes in Computer Science). Berlin, Germany: Springer Verlag, 2001, vol. 2139, pp. 485-469.

[7] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, and R. Smolensky, "The bit extraction problem or t-resilient functions," in IEEE Symposium on Foundations of Computer Science, 1985, vol. 26, pp. 396-407.

[8] J. Dillon, "Elementary Hadamard difference sets," Ph.D dissertation, University of Maryland, College Park, 1974.

[9] C. Ding, G. Xiao, and W. Shan, The Stability Theory of Stream Ciphers (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 561, 1991.

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

[11] K. C. Gupta, and P. Sarkar, "Improved construction of nonlinear resilient S-boxes," IEEE Transactions on Information Theory, vol.51, no.1, pp.339-348, 2005.

[12] T. Johansson and E. Pasalic, "A construction of resilient functions with high nonlinearity," IEEE Transactions on Information Theory, vol. 49, no.2, pp.494-501, 2003.

[13] J. W. Hirschfeld, Projective geometry over finite fields, Oxford University, New York, 1979.

[14] K. Kurosawa, T. Satoh, and K. Yamamoto, "Highly nonlinear t-resilient functions," Journal of Universal Computer Science, vol. 3, no. 6, pp. 721-729, 1997.

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

[16] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. on Inform. Theory*, IT-15(1):122–127, 1969.

[17] M. Matsui, "Linear cryptanalysis method for DES cipher," in Advances in Cryptology–EUROCRYPTO'93 (Lecture Notes in Computer Sceince). Berlin, Germany: Springer-Verlag, 1994, vol. 765, pp. 386-397.

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

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

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

[21] H. Niederreiter and C. Xing, "Disjoint linear codes from algebraic function fields," IEEE Transactions on Information Theory, vol.50, no.9, pp.2174-2177, 2004.

[22] K. Nyberg, "Differentially uniform mappings for cryptography," in Advances in Cryptology - EUROCRYPT 93 (Lecture Notes in Computer Sceince), Berlin, Germany: Springer-Verlag, 1994, vol. 765, pp. 55-64.

[23] K. Nyberg, "Perfect nonlinear S-boxes," in Advances in Cryptology–EUROCRYPT'91 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1991, vol. 547, pp. 378-386.

[24] E. Pasalic and S. Maitra, "Linear codes in generalized construction of resilient functions with very high nonlinearity," IEEE Transactions on Information Theory, vol.48, no.8, pp. 2182-2191, 2002.

[25] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," IEEE Transactions on Information Theory, vol. 30, no.5, pp. 776-780, 1984.

[26] J. Seberry, X. M. Zhang, and Y. Zheng, "Nonlinearly balanced Boolean functions and their propagation characteristics," in Advances in Cryptology–CRYPTO'93, (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1993, vol. 773, pp. 49-60.

[27] D. R. Stinson and J. L. Massey,"An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions," Journal of Cryptology, vol. 8, no. 3, pp. 168-173, 1995.

[28] G. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," IEEE Transactions on Information Theory, vol. 34, no. 3, pp. 569-571, 1988.

[29] X.-M. Zhang and Y. Zheng, "Cryptographically resilient functions," IEEE Transactions on Information Theory, vol. 43, no. 5, pp. 1740-1747, 1997.

Wei-Guo Zhang (张卫国) received the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2007. Since July 2007, he joined ISN Laboratory at Xidian University. His research interests include symmetric cryptography, sequence design, and algebraic coding theory.

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

Appendix

TABLE IV

$M(u, m, d)$ - THE CURRENTLY KNOWN MAXIMAL NUMBER OF $[u, m, d]$ DISJOINT LINEAR CODES

m	$u \setminus d$	1	2	3	4	5	6	7	8	9	10	11	12	13
	4	5	3	-	-	-	-	-	-	-	-	-	-	-
	5	9	8	3	-	-	-	-	-	-	-	-	-	-
	6	21	18	10	1	-	-	-	-	-	-	-	-	-
	7	41	39	28	9	-	-	-	-	-	-	-	-	-
	8	85	81	66	35	10	-	-	-	-	-	-	-	-
	9	169	166	147	98	44	4	-	-	-	-	-	-	-
	10	341	336	312	239	136	31	-	-	-	-	-	-	-
	11	681	677	648	548	381	159	32	-	-	-	-	-	-
2	12	1365	1359	1324	1189	926	504	181	15	-	-	-	-	-
	13	2729	2724	2683	2510	2124	1406	692	146	-	-	-	-	-
	14	5461	5454	5406	5182	4614	3398	1968	643	73	-	-	-	-
	15	10921	10915	10860	10585	9809	7989	5421	2463	648	56	-	-	-
	16	21845	21837	21774	21433	20377	17648	13301	7503	2949	524	-	-	-
	17	43689	43682	43611	43206	41845	38083	31325	20989	11087	3355	462	-	-
	18	87381	87372	87292	86800	85007	79566	68797	50335	30020	11744	2530	210	-
	19	174761	174753	174664	174092	171871	164754	149353	120245	83502	42473	15551	2486	-
	20	349525	349515	349416	348738	345920	336217	313518	267020	201783	120447	56033	14791	1568
	6	9	7	2	-	-	-	-	-	-	-	-	-	-
	7	17	16	9	-	-	-	-	-	-	-	-	-	-
	8	33	32	24	5	-	-	-	-	-	-	-	-	-
	9	73	70	57	26	-	-	-	-	-	-	-	-	-
	10	145	143	127	80	24	-	-	-	-	-	-	-	-
	11	289	287	269	193	86	4	-	-	-	-	-	-	-
	12	585	581	557	461	286	70	-	-	-	-	-	-	-
3	13	1169	1166	1138	1011	748	316	35	-	-	-	-	-	-
	14	2337	2334	2303	2139	1750	1028	322	9	-	-	-	-	-
	15	4681	4676	4638	4429	3849	2504	1029	106	-	-	-	-	-
	16	9361	9357	9314	9060	8297	6333	3605	831	-	-	-	-	-
	17	18721	18717	18670	18362	17350	14540	9938	3894	515	-	-	-	-
	18	37449	37443	37388	37024	35727	31818	24868	14023	4681	144	-	-	-
	19	74897	74892	74831	74396	72707	67063	55454	35166	14825	1970	-	-	-
	20	149793	149788	149722	149215	147149	139893	123695	91644	52646	15683	1156	-	-
	8	17	15	8	-	-	-	-	-	-	-	-	-	-
	9	33	32	23	3	-	-	-	-	-	-	-	-	-
	10	65	64	54	21	-	-	-	-	-	-	-	-	-
	11	129	128	118	71	5	-	-	-	-	-	-	-	-
	12	273	270	252	172	50	-	-	-	-	-	-	-	-
	13	545	543	522	421	221	12	-	-	-	-	-	-	-
4	14	1089	1087	1064	938	652	175	9	-	-	-	-	-	-
	15	2177	2175	2151	1998	1578	747	151	-	-	-	-	-	-
	16	4369	4365	4332	4117	3467	1951	404	8	-	-	-	-	-
	17	8737	8734	8697	8446	7616	5428	2372	151	-	-	-	-	-
	18	17473	17470	17430	17132	16068	12882	7487	1448	-	-	-	-	-
	19	34945	34942	34900	34566	33268	29160	21215	8649	751	-	-	-	-
	20	69905	69900	69848	69423	67629	61369	59822	24946	5146	82	-	-	-
	10	33	31	22	-	-	-	-	-	-	-	-	-	-
	11	65	64	53	12	-	-	-	-	-	-	-	-	-
	12	129	128	116	64	-	-	-	-	-	-	-	-	-
	13	257	256	243	153	15	-	-	-	-	-	-	-	-
	14	513	512	499	408	168	-	-	-	-	-	-	-	-
5	15	1057	1054	1031	899	561	61	-	-	-	-	-	-	-
	16	2113	2111	2085	1921	1469	506	4	-	-	-	-	-	-
	17	4225	4223	4195	3987	3259	1472	97	-	-	-	-	-	-
	18	8449	8447	8417	8151	7222	4679	1233	10	-	-	-	-	-
	19	16897	16895	16864	16572	15366	11711	5219	282	-	-	-	-	-
	20	33825	33821	33779	33439	32034	27355	17748	4133	21	-	-	-	-
	21	67649	67646	67600	67194	65354	58276	42435	15400	799	-	-	-	-
	12	65	63	52	8	-	-	-	-	-	-	-	-	-
	13	129	128	115	48	-	-	-	-	-	-	-	-	-
	14	257	256	242	141	5	-	-	-	-	-	-	-	-
	15	513	512	497	400	129	-	-	-	-	-	-	-	-
6	16	1025	1024	1009	886	480	23	-	-	-	-	-	-	-
	17	2049	2048	2032	1891	1323	256	1	-	-	-	-	-	-
	18	4161	4158	4130	3905	3075	1052	8	-	-	-	-	-	-
	19	8321	8319	8288	8018	6986	3853	413	-	-	-	-	-	-
	20	16641	16639	16606	16274	14946	10522	3133	29	-	-	-	-	-
	21	34281	33279	33244	32911	31346	25956	14034	1338	-	-	-	-	-
	14	129	127	114	42	-	-	-	-	-	-	-	-	-
	15	257	256	241	124	-	-	-	-	-	-	-	-	-
	16	513	512	496	383	100	-	-	-	-	-	-	-	-
7	17	1025	1024	1007	869	396	3	-	-	-	-	-	-	-
	18	2049	2048	2031	1868	1215	124	-	-	-	-	-	-	-
	19	4097	4096	4078	3871	2880	714	-	-	-	-	-	-	-
	20	8193	8192	8172	7941	6764	3122	98	-	-	-	-	-	-
	21	16513	16510	16477	16143	14676	9359	1639	-	-	-	-	-	-
	16	257	255	240	106	-	-	-	-	-	-	-	-	-
	17	513	512	495	365	66	-	-	-	-	-	-	-	-
8	18	1025	1024	1006	859	350	2	-	-	-	-	-	-	-
	19	2049	2048	2029	1846	1099	46	-	-	-	-	-	-	-
	20	4097	4096	4076	3842	2637	394	-	-	-	-	-	-	-
	21	8193	8192	8172	7912	6501	2404	14	-	-	-	-	-	-
	18	513	511	494	350	38	-	-	-	-	-	-	-	-
9	19	1025	1024	1005	839	270	-	-	-	-	-	-	-	-
	20	2049	2048	2028	1823	961	13	-	-	-	-	-	-	-

TABLE V
ACHIEVED NONLINEARITY FOR (n, m, t) S-BOXES

m	$n \setminus t$	0	1	2	3	4	5
2	8	$2^7 - 2^4$	$2^7 - 2^4$	$2^7 - 2^4$	$2^7 - 2^5$	-	-
	10	$2^9 - 2^4 - 2^3$	$2^9 - 2^5$	$2^9 - 2^5$	$2^9 - 2^6$	$2^9 - 2^7$	$2^9 - 2^8$
	12	$2^{11} - 2^5 - 2^3$	$2^{11} - 2^5 - 2^4$	$2^{11} - 2^6$	$2^{11} - 2^7$	$2^{11} - 2^7$	$2^{11} - 2^8$
	14	$2^{13} - 2^6 - 2^4$	$2^{13} - 2^6 - 2^5$	$2^{13} - 2^7$	$2^{13} - 2^7$	$2^{13} - 2^8$	$2^{13} - 2^9$
	16	$2^{15} - 2^7 - 2^4$	$2^{15} - 2^7 - 2^5$	$2^{15} - 2^8$	$2^{15} - 2^8$	$2^{15} - 2^8$	$2^{15} - 2^9$
	18	$2^{17} - 2^8 - 2^5$	$2^{17} - 2^8 - 2^6$	$2^{17} - 2^8 - 2^7$	$2^{17} - 2^9$	$2^{17} - 2^9$	$2^{17} - 2^{10}$
	20	$2^{19} - 2^9 - 2^5$	$2^{19} - 2^9 - 2^7$	$2^{19} - 2^9 - 2^8$	$2^{19} - 2^{10}$	$2^{19} - 2^{10}$	$2^{19} - 2^{11}$
	22	$2^{21} - 2^{10} - 2^6$	$2^{21} - 2^{10} - 2^7$	$2^{21} - 2^{10} - 2^8$	$2^{21} - 2^{11}$	$2^{21} - 2^{11}$	$2^{21} - 2^{11}$
	24	$2^{23} - 2^{11} - 2^6$	$2^{23} - 2^{11} - 2^8$	$2^{23} - 2^{11} - 2^9$	$2^{23} - 2^{11} - 2^{10}$	$2^{23} - 2^{12}$	$2^{23} - 2^{12}$
	26	$2^{25} - 2^{12} - 2^7$	$2^{25} - 2^{12} - 2^8$	$2^{25} - 2^{12} - 2^{10}$	$2^{25} - 2^{12} - 2^{11}$	$2^{25} - 2^{13}$	$2^{25} - 2^{13}$
	28	$2^{27} - 2^{13} - 2^7$	$2^{27} - 2^{13} - 2^9$	$2^{27} - 2^{13} - 2^{10}$	$2^{27} - 2^{13} - 2^{11}$	$2^{27} - 2^{13} - 2^{12}$	$2^{27} - 2^{14}$
	30	$2^{29} - 2^{14} - 2^8$	$2^{29} - 2^{14} - 2^9$	$2^{29} - 2^{14} - 2^{11}$	$2^{29} - 2^{14} - 2^{12}$	$2^{29} - 2^{14} - 2^{13}$	$2^{29} - 2^{15}$
	32	$2^{31} - 2^{15} - 2^8$	$2^{31} - 2^{15} - 2^{10}$	$2^{31} - 2^{15} - 2^{11}$	$2^{31} - 2^{15} - 2^{13}$	$2^{31} - 2^{15} - 2^{14}$	$2^{31} - 2^{15}$
	34	$2^{33} - 2^{16} - 2^9$	$2^{33} - 2^{16} - 2^{10}$	$2^{33} - 2^{16} - 2^{12}$	$2^{33} - 2^{16} - 2^{13}$	$2^{33} - 2^{16} - 2^{14}$	$2^{33} - 2^{16} - 2^{15}$
	36	$2^{35} - 2^{17} - 2^9$	$2^{35} - 2^{17} - 2^{11}$	$2^{35} - 2^{17} - 2^{13}$	$2^{35} - 2^{17} - 2^{14}$	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{16}$
	38	$2^{37} - 2^{18} - 2^{10}$	$2^{37} - 2^{18} - 2^{11}$	$2^{37} - 2^{18} - 2^{13}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{16}$	$2^{37} - 2^{18} - 2^{17}$
	40	$2^{39} - 2^{19} - 2^{10}$	$2^{39} - 2^{19} - 2^{12}$	$2^{39} - 2^{19} - 2^{14}$	$2^{39} - 2^{19} - 2^{15}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{17}$
3	12	$2^{11} - 2^6$	$2^{11} - 2^6$	$2^{11} - 2^6$	$2^{11} - 2^7$	$2^{11} - 2^9$	$2^{11} - 2^{10}$
	14	$2^{13} - 2^6 - 2^5$	$2^{13} - 2^6 - 2^5$	$2^{13} - 2^7$	$2^{13} - 2^8$	$2^{13} - 2^9$	$2^{13} - 2^{10}$
	16	$2^{15} - 2^7 - 2^6$	$2^{15} - 2^7 - 2^6$	$2^{15} - 2^8$	$2^{15} - 2^8$	$2^{15} - 2^9$	$2^{15} - 2^{11}$
	18	$2^{17} - 2^8 - 2^5$	$2^{17} - 2^8 - 2^6$	$2^{17} - 2^9$	$2^{17} - 2^9$	$2^{17} - 2^{10}$	$2^{17} - 2^{11}$
	20	$2^{19} - 2^9 - 2^6$	$2^{19} - 2^9 - 2^7$	$2^{19} - 2^9 - 2^8$	$2^{19} - 2^{10}$	$2^{19} - 2^{10}$	$2^{19} - 2^{11}$
	22	$2^{21} - 2^{10} - 2^7$	$2^{21} - 2^{10} - 2^8$	$2^{21} - 2^{10} - 2^9$	$2^{21} - 2^{11}$	$2^{21} - 2^{11}$	$2^{21} - 2^{12}$
	24	$2^{23} - 2^{11} - 2^6$	$2^{23} - 2^{11} - 2^8$	$2^{23} - 2^{11} - 2^9$	$2^{23} - 2^{12}$	$2^{23} - 2^{12}$	$2^{23} - 2^{12}$
	26	$2^{25} - 2^{12} - 2^8$	$2^{25} - 2^{12} - 2^8$	$2^{25} - 2^{12} - 2^{10}$	$2^{25} - 2^{12} - 2^{11}$	$2^{25} - 2^{13}$	$2^{25} - 2^{13}$
	28	$2^{27} - 2^{13} - 2^9$	$2^{27} - 2^{13} - 2^9$	$2^{27} - 2^{13} - 2^{11}$	$2^{27} - 2^{13} - 2^{12}$	$2^{27} - 2^{14}$	$2^{27} - 2^{14}$
	30	$2^{29} - 2^{14} - 2^7$	$2^{29} - 2^{14} - 2^{10}$	$2^{29} - 2^{14} - 2^{11}$	$2^{29} - 2^{14} - 2^{12}$	$2^{29} - 2^{14} - 2^{13}$	$2^{29} - 2^{15}$
	32	$2^{31} - 2^{15} - 2^9$	$2^{31} - 2^{15} - 2^{10}$	$2^{31} - 2^{15} - 2^{12}$	$2^{31} - 2^{15} - 2^{13}$	$2^{31} - 2^{15} - 2^{14}$	$2^{31} - 2^{16}$
	34	$2^{33} - 2^{16} - 2^{10}$	$2^{33} - 2^{16} - 2^{11}$	$2^{33} - 2^{16} - 2^{12}$	$2^{33} - 2^{16} - 2^{14}$	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{17}$
	36	$2^{35} - 2^{17} - 2^9$	$2^{35} - 2^{17} - 2^{11}$	$2^{35} - 2^{17} - 2^{13}$	$2^{35} - 2^{17} - 2^{14}$	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{16}$
	38	$2^{37} - 2^{18} - 2^{11}$	$2^{37} - 2^{18} - 2^{12}$	$2^{37} - 2^{18} - 2^{13}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{16}$	$2^{37} - 2^{18} - 2^{17}$
	40	$2^{39} - 2^{19} - 2^{12}$	$2^{39} - 2^{19} - 2^{12}$	$2^{39} - 2^{19} - 2^{14}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{17}$	$2^{39} - 2^{19} - 2^{18}$
4	16	$2^{15} - 2^8$	$2^{15} - 2^8$	$2^{15} - 2^8$	$2^{15} - 2^8$	$2^{15} - 2^{10}$	$2^{15} - 2^{12}$
	18	$2^{17} - 2^8 - 2^7$	$2^{17} - 2^9$	$2^{17} - 2^9$	$2^{17} - 2^9$	$2^{17} - 2^{11}$	$2^{17} - 2^{12}$
	20	$2^{19} - 2^9 - 2^7$	$2^{19} - 2^9 - 2^8$	$2^{19} - 2^{10}$	$2^{19} - 2^{10}$	$2^{19} - 2^{11}$	$2^{19} - 2^{12}$
	22	$2^{21} - 2^{10} - 2^8$	$2^{21} - 2^{10} - 2^9$	$2^{21} - 2^{10} - 2^9$	$2^{21} - 2^{11}$	$2^{21} - 2^{12}$	$2^{21} - 2^{13}$
	24	$2^{23} - 2^{11} - 2^7$	$2^{23} - 2^{11} - 2^8$	$2^{23} - 2^{11} - 2^{10}$	$2^{23} - 2^{12}$	$2^{23} - 2^{12}$	$2^{23} - 2^{13}$
	26	$2^{25} - 2^{12} - 2^8$	$2^{25} - 2^{12} - 2^9$	$2^{25} - 2^{12} - 2^{10}$	$2^{25} - 2^{13}$	$2^{25} - 2^{13}$	$2^{25} - 2^{14}$
	28	$2^{27} - 2^{13} - 2^9$	$2^{27} - 2^{13} - 2^{10}$	$2^{27} - 2^{13} - 2^{11}$	$2^{27} - 2^{13} - 2^{12}$	$2^{27} - 2^{14}$	$2^{27} - 2^{14}$
	30	$2^{29} - 2^{14} - 2^{10}$	$2^{29} - 2^{14} - 2^{11}$	$2^{29} - 2^{14} - 2^{12}$	$2^{29} - 2^{14} - 2^{13}$	$2^{29} - 2^{15}$	$2^{29} - 2^{15}$
	32	$2^{31} - 2^{15} - 2^8$	$2^{31} - 2^{15} - 2^{11}$	$2^{31} - 2^{15} - 2^{12}$	$2^{31} - 2^{15} - 2^{14}$	$2^{31} - 2^{16}$	$2^{31} - 2^{16}$
	34	$2^{33} - 2^{16} - 2^{10}$	$2^{33} - 2^{16} - 2^{11}$	$2^{33} - 2^{16} - 2^{13}$	$2^{33} - 2^{16} - 2^{14}$	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{17}$
	36	$2^{35} - 2^{17} - 2^{11}$	$2^{35} - 2^{17} - 2^{12}$	$2^{35} - 2^{17} - 2^{13}$	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{16}$	$2^{35} - 2^{18}$
	38	$2^{37} - 2^{18} - 2^{12}$	$2^{37} - 2^{18} - 2^{13}$	$2^{37} - 2^{18} - 2^{14}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{16}$	$2^{37} - 2^{18} - 2^{17}$
	40	$2^{39} - 2^{19} - 2^{10}$	$2^{39} - 2^{19} - 2^{13}$	$2^{39} - 2^{19} - 2^{14}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{17}$	$2^{39} - 2^{19} - 2^{18}$
5	20	$2^{19} - 2^{10}$	$2^{19} - 2^{10}$	$2^{19} - 2^{10}$	$2^{19} - 2^{11}$	$2^{19} - 2^{12}$	$2^{19} - 2^{14}$
	22	$2^{21} - 2^{10} - 2^9$	$2^{21} - 2^{10} - 2^9$	$2^{21} - 2^{11}$	$2^{21} - 2^{11}$	$2^{21} - 2^{13}$	$2^{21} - 2^{14}$
	24	$2^{23} - 2^{11} - 2^9$	$2^{23} - 2^{11} - 2^9$	$2^{23} - 2^{11} - 2^{10}$	$2^{23} - 2^{12}$	$2^{23} - 2^{13}$	$2^{23} - 2^{14}$
	26	$2^{25} - 2^{12} - 2^{10}$	$2^{25} - 2^{12} - 2^{10}$	$2^{25} - 2^{12} - 2^{11}$	$2^{25} - 2^{13}$	$2^{25} - 2^{13}$	$2^{25} - 2^{15}$
	28	$2^{27} - 2^{13} - 2^{11}$	$2^{27} - 2^{13} - 2^{11}$	$2^{27} - 2^{13} - 2^{12}$	$2^{27} - 2^{14}$	$2^{27} - 2^{14}$	$2^{27} - 2^{15}$
	30	$2^{29} - 2^{14} - 2^9$	$2^{29} - 2^{14} - 2^{10}$	$2^{29} - 2^{14} - 2^{12}$	$2^{29} - 2^{14} - 2^{13}$	$2^{29} - 2^{15}$	$2^{29} - 2^{16}$
	32	$2^{31} - 2^{15} - 2^{10}$	$2^{31} - 2^{15} - 2^{11}$	$2^{31} - 2^{15} - 2^{12}$	$2^{31} - 2^{15} - 2^{14}$	$2^{31} - 2^{16}$	$2^{31} - 2^{16}$
	34	$2^{33} - 2^{16} - 2^{11}$	$2^{33} - 2^{16} - 2^{12}$	$2^{33} - 2^{16} - 2^{13}$	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{17}$	$2^{33} - 2^{17}$
	36	$2^{35} - 2^{17} - 2^{12}$	$2^{35} - 2^{17} - 2^{13}$	$2^{35} - 2^{17} - 2^{14}$	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{16}$	$2^{35} - 2^{18}$
	38	$2^{37} - 2^{18} - 2^{13}$	$2^{37} - 2^{18} - 2^{14}$	$2^{37} - 2^{18} - 2^{14}$	$2^{37} - 2^{18} - 2^{16}$	$2^{37} - 2^{18} - 2^{17}$	$2^{37} - 2^{19}$
	40	$2^{39} - 2^{19} - 2^{10}$	$2^{39} - 2^{19} - 2^{13}$	$2^{39} - 2^{19} - 2^{15}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{17}$	$2^{39} - 2^{20}$
6	24	$2^{23} - 2^{12}$	$2^{23} - 2^{12}$	$2^{23} - 2^{12}$	$2^{23} - 2^{12}$	$2^{23} - 2^{14}$	$2^{23} - 2^{15}$
	26	$2^{25} - 2^{12} - 2^{11}$	$2^{25} - 2^{12} - 2^{11}$	$2^{25} - 2^{12} - 2^{11}$	$2^{25} - 2^{13}$	$2^{25} - 2^{14}$	$2^{25} - 2^{15}$
	28	$2^{27} - 2^{13} - 2^{11}$	$2^{27} - 2^{13} - 2^{11}$	$2^{27} - 2^{13} - 2^{12}$	$2^{27} - 2^{14}$	$2^{27} - 2^{15}$	$2^{27} - 2^{16}$
	30	$2^{29} - 2^{14} - 2^{11}$	$2^{29} - 2^{14} - 2^{12}$	$2^{29} - 2^{14} - 2^{12}$	$2^{29} - 2^{15}$	$2^{29} - 2^{15}$	$2^{29} - 2^{16}$
	32	$2^{31} - 2^{15} - 2^{12}$	$2^{31} - 2^{15} - 2^{13}$	$2^{31} - 2^{15} - 2^{13}$	$2^{31} - 2^{15} - 2^{14}$	$2^{31} - 2^{16}$	$2^{31} - 2^{17}$
	34	$2^{33} - 2^{16} - 2^{13}$	$2^{33} - 2^{16} - 2^{14}$	$2^{33} - 2^{16} - 2^{14}$	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{17}$	$2^{33} - 2^{17}$
	36	$2^{35} - 2^{17} - 2^{11}$	$2^{35} - 2^{17} - 2^{12}$	$2^{35} - 2^{17} - 2^{14}$	$2^{35} - 2^{17} - 2^{16}$	$2^{35} - 2^{18}$	$2^{35} - 2^{18}$
	38	$2^{37} - 2^{18} - 2^{12}$	$2^{37} - 2^{18} - 2^{13}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{16}$	$2^{37} - 2^{18} - 2^{17}$	$2^{37} - 2^{19}$
	40	$2^{39} - 2^{19} - 2^{13}$	$2^{39} - 2^{19} - 2^{14}$	$2^{39} - 2^{19} - 2^{15}$	$2^{39} - 2^{19} - 2^{17}$	$2^{39} - 2^{19} - 2^{18}$	$2^{39} - 2^{20}$
7	28	$2^{27} - 2^{14}$	$2^{27} - 2^{14}$	$2^{27} - 2^{14}$	$2^{27} - 2^{14}$	$2^{27} - 2^{15}$	$2^{27} - 2^{17}$
	30	$2^{29} - 2^{14} - 2^{13}$	$2^{29} - 2^{14} - 2^{13}$	$2^{29} - 2^{14} - 2^{13}$	$2^{29} - 2^{15}$	$2^{29} - 2^{16}$	$2^{29} - 2^{17}$
	32	$2^{31} - 2^{15} - 2^{13}$	$2^{31} - 2^{15} - 2^{13}$	$2^{31} - 2^{15} - 2^{13}$	$2^{31} - 2^{16}$	$2^{31} - 2^{16}$	$2^{31} - 2^{18}$
	34	$2^{33} - 2^{16} - 2^{13}$	$2^{33} - 2^{16} - 2^{13}$	$2^{33} - 2^{16} - 2^{14}$	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{17}$	$2^{33} - 2^{18}$
	36	$2^{35} - 2^{17} - 2^{14}$	$2^{35} - 2^{17} - 2^{14}$	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{16}$	$2^{35} - 2^{18}$	$2^{35} - 2^{19}$
	38	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{17}$	$2^{37} - 2^{19}$	$2^{37} - 2^{19}$
	40	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{17}$	$2^{39} - 2^{20}$	$2^{39} - 2^{20}$
8	32	$2^{31} - 2^{16}$	$2^{31} - 2^{16}$	$2^{31} - 2^{16}$	$2^{31} - 2^{16}$	$2^{31} - 2^{17}$	$2^{31} - 2^{18}$
	34	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{16} - 2^{15}$	$2^{33} - 2^{17}$	$2^{33} - 2^{17}$	$2^{33} - 2^{19}$
	36	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{15}$	$2^{35} - 2^{17} - 2^{16}$	$2^{35} - 2^{18}$	$2^{35} - 2^{19}$
	38	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{15}$	$2^{37} - 2^{18} - 2^{17}$	$2^{37} - 2^{19}$	$2^{37} - 2^{20}$
	40	$2^{39} - 2^{19} - 2^{15}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{16}$	$2^{39} - 2^{19} - 2^{18}$	$2^{39} - 2^{20}$	$2^{39} - 2^{20}$