Construction of Cryptographically Important Boolean Functions

Soumen Maity[1] and Thomas Johansson[2]

[1] Theoretical Statistics and Mathematics Unit, Indian Statistical Institute, 203 B. T. Road, Calcutta-700108, INDIA, E-mail: soumenmaity@hotmail.com
[2] Department of Information Technology, Lund University, P.O. Box 118, S-221 00 Lund, SWEDEN, E-mail: thomas@it.lth.se

Abstract. Boolean functions are used as nonlinear combining functions in certain stream ciphers. A Boolean function is said to be correlation immune if its output leaks no information about its input values. Balanced correlation immune functions are called resilient functions. Finding methods for easy construction of resilient functions with additional properties is an active research area. Maitra and Pasalic [3] have constructed 8-variable 1-resilient Boolean functions with nonlinearity 116. Their technique interlinks mathematical results with classical computer search. In this paper we describe a new technique to construct 8-variable 1-resilient Boolean functions with the same nonlinearity. Using a similar technique, we directly construct 10-variable (resp. 12-variable), 1-resilient functions with nonlinearity 488 (resp. 1996). Finally, we describe some results on the construction of n-variable t-resilient functions with maximum nonlinearity.

Keywords: Boolean function; Balancedness; Nonlinearity; Perfectly nonlinear function; Bent function; Algebraic degree; Correlation immunity; Resiliency; Stream cipher; Combinatorial problems

1 Introduction

Boolean functions have many applications in computer security practices including the construction of keystream generators based on a set of shift registers. Such a function should possess certain desirable properties to withstand known cryptanalytic attacks. Four such important properties are balancedness, correlation immunity, algebraic degree and nonlinearity. The maximum possible nonlinearity for n-variable functions is known only for even n and equals $2^{n-1} - 2^{\frac{n}{2}-1}$. Functions achieving this nonlinearity are called bent and were introduced by Rothaus [6]. Correlation immune functions were introduced by Siegenthaler [8], to withstand a class of "divide and conquer" attacks on certain models of stream ciphers. He also investigated the properties of Boolean functions with correlation immunity. Recently, a nontrivial upper bound on the nonlinearity of resilient functions was obtained by Sarkar and Maitra [7]. They proved that the

* This research was supported by ReX program of Stichting Nlnet, Netherlands.

nonlinearity of n-variable (n even) t-resilient function is less then or equal to $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{t+1}$ (resp. $2^{n-1} - 2^{t+1}$) if $t+1 \leq \frac{n}{2} - 1$ (resp. $t+1 > \frac{n}{2} - 1$). A similar kind of result has been presented independently by Tarannikov [9] and Zheng and Zhang [11]. Construction of resilient Boolean functions achieving the upper bound on nonlinearity is an important research area. Maitra and Pasalic [3] have constructed 8-variable 1-resilient Boolean functions with nonlinearity 116. In this paper, we describe a new technique to construct other 8-variable 1-resilient Boolean functions with nonlinearity 116. We start with an 8-variable bent function f and suitably change some bits in the output column of the truth table of f to get our 8-variable 1-resilient function with nonlinearity 116. Furthermore, using a similar technique, we directly construct 10-variable (resp. 12-variable), 1-resilient functions with nonlinearity 488 (resp. 1996). Finally we provide some results on the construction of n-variable t-resilient functions with maximum nonlinearity.

2 Preliminaries

Let n be any positive integer. An n-variable Boolean function is a map $f: \{0,1\}^n \rightarrow \{0,1\}$. These functions play a major role in stream cipher cryptosystems. Boolean functions are used in many different binary keystream generators based on LFSRs. Their purpose in the keystream generators is often to destroy the linearity introduced by the LFSRs. An n-variable Boolean function $f(x_1, x_2, \ldots, x_n)$ can be represented as multivariate polynomial over $GF(2)$. That is, $f(x_1, x_2, \ldots, x_n)$ can be written as

$$a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \ldots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in GF(2)$ and the addition and multiplication operations are in $GF(2)$. A truth table lists the function output value for all possible inputs.

In the cryptographic applications there are several properties of Boolean functions that are interesting to investigate. We now discuss some important properties of Boolean functions for stream cipher application.

Definition 1. An n-variable Boolean function $f(X)$ is *balanced* if the output column in the truth table contains an equal number of 0's and 1's.

Definition 2. The *algebraic degree*, or simply *degree*, of a Boolean function $f(X)$ is defined to be the number of variables in the highest order product of $f(X)$, when $f(X)$ is written in algebraic normal form. The algebraic degree of $f(X)$ is denoted by $deg(f)$.

Let $\mathcal{F}_n$ be the set of all Boolean functions in n variables. Let $F_2 = GF(2)$. The *Hamming distance* between two functions $f(X), g(X) \in \mathcal{F}_n$ is defined as,

$$d_H(f,g) = |\{X \mid f(X) \neq g(X),\ X \in F_2^n\}|.$$

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. Let $\mathcal{A}_n$ be the set of all affine functions in n variables.

Definition 3. We define the *nonlinearity* of a Boolean function $f(X)$, denoted by N_f, as the Hamming distance to the nearest affine function, i.e.,

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

This measure of nonlinearity is related to linear cryptanalysis [4].

In most of the cryptographic applications, we would like that the correlation between an individual input variable and an output variable is small. Siegenthaler [8] introduced the concept of correlation immunity of combining functions for nonlinear combined stream ciphers, and investigated the properties of Boolean functions with correlation immunity. The purpose of introducing correlation-immune functions as nonlinear functions for stream cipher is to spare them from the "divide and conquer" attack.

Definition 4. An n-variable Boolean function is defined to be t-th order *correlation immune*, if for any t-tuple of independent identically distributed binary random variables $X_{i_1}, X_{i_2}, \ldots, X_{i_t}$, we have

$$I(X_{i_1}, X_{i_2}, \ldots, X_{i_t}; Y) = 0, \quad 1 \leq i_1 < i_2 < \ldots < i_t \leq n,$$

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

A Boolean function that is both balanced and t-th order correlation immune is called a *t-resilient* function.
The properties above are often investigated through the Walsh transform.

Definition 5. Let $f(X)$ be an n-variable Boolean function. Let us consider $X = (x_1, x_2, \ldots, x_n)$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$ both belonging to $\{0,1\}^n$ and $X \cdot \omega = x_1\omega_1 \oplus x_2\omega_2 \oplus \ldots \oplus x_n\omega_n$. Then the *Walsh transform* of $f(X)$ is a real valued function over $\{0,1\}^n$, which is defined as

$$W_f(\omega) = \sum_{X \in \{0,1\}^n} (-1)^{f(X) \oplus X \cdot \omega}$$

The Walsh transform is sometimes called the spectral distribution or simply the spectrum of a Boolean function.

The Hamming distance between a Boolean function $f(X)$ and an affine function $g(X) = X \cdot \omega + b$, where $b \in F_2$, can be calculated with the Walsh transform as

$$d_H(f, g) = 2^{n-1} - \frac{(-1)^b W_f(\omega)}{2}.$$

Thus, the nonlinearity of $f(X)$ can be obtained from the Walsh transform as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega} |W_f(\omega)|.$$

A function f of n variables is called bent if $W_f(\omega) = \pm 2^{\frac{n}{2}}$ for all $\omega \in \{0,1\}^n$. In other words, an n-variable function is called bent if $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. These functions are important in both cryptography and coding theory since they achieve the maximum possible nonlinearity.

Xiao and Massey [10] gave a spectral characterization of Boolean function with correlation immunity. Here we state this characterization as a definition of correlation immunity.

Definition 6. A Boolean function f is t-th order correlation immune (CI) iff its Walsh transform W satisfies

$$W_f(\omega) = 0 \quad \text{for all} \quad \omega \in F_2^n; \quad 1 \leq wt(\omega) \leq t,$$

where $wt(\omega)$ is the Hamming weight of the binary string ω. Furthermore, if f is balanced then $W_f(\mathbf{0}) = 0$. Balanced t-th order correlation immune functions are called t-resilient functions.
Thus, a Boolean function f is t-resilient iff its Walsh transform W satisfies

$$W_f(\omega) = 0 \quad \text{for all} \quad \omega \in F_2^n; \quad 0 \leq wt(\omega) \leq t.$$

We now recall the definition and some properties of perfectly nonlinear functions for later use. Let f be a function from abelian group $(A,+)$ of order n to another abelian group $(B,+)$ of order m. A robust measure [5] of the nonlinearity of functions is related to differential cryptanalysis [1] and uses the derivatives $D_a f(x) = f(x+a) - f(x)$. It may be defined by

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \Pr(D_a f(x) = b),$$

where $\Pr(E)$ denotes the probability of the occurrence of event E. The smaller the value of P_f, the higher the corresponding nonlinearity of f (if f is linear, then $P_f = 1$).

Definition 7. A function $f : A \to B$ has perfect nonlinearity if $P_f = \frac{1}{|B|}$.

Definition 8. A function $g : A \to B$ is balanced if the size of $g^{-1}(b)$ is same for every $b \in B$.

Theorem 1. A function $f : A \to B$ has perfect nonlinearity if and only if, for every $a \in A^* = A - \{0\}$, the derivative $D_a f$ is balanced.

Theorem 2. (Carlet and Ding [2]) Let $f : (A,+) \to (B,+)$ have perfect nonlinearity, and let $l : (B,+) \to (C,+)$ be a linear onto function. Then the composition $l \circ f$ is a function from $(A,+)$ to $(C,+)$ with perfect nonlinearity.

In the case of Boolean functions, perfect nonlinear functions are called bent. For a general survey of perfectly nonlinear functions one can refer to Carlet and Ding [2].

3 Construction of Bent Functions

In this section, we describe a method to construct n-variable (n even) bent function.

Lemma 1. Let n and m be any positive integers, where m divides n. Let

$$g : F_{2^m}^{\frac{n}{m}} \rightarrow F_{2^m}$$

and

$$f = Tr(g) : F_{2^m}^{\frac{n}{m}} \rightarrow F_2$$

where Tr is the trace function from F_{2^m} to F_2. If g is perfectly nonlinear, then f is an n-variable bent function.

Proof: Since $g : F_{2^m}^{\frac{n}{m}} \rightarrow F_{2^m}$ is perfectly nonlinear function and $Tr : F_{2^m} \rightarrow F_2$ is a linear onto function, the composition $Tr(g)$ is a bent function from $F_{2^m}^{\frac{n}{m}}$ to F_2. It follows from Theorem 2.

The bent functions we will use in Theorem 3 and Theorem 4 can be obtained using Lemma 1.

Example 1. Let $n = 8$, $m = 4$ and $g(X_1, X_2) = X_1X_2$ where $X_i \in F_{2^4}$. It is known that g is a perfectly nonlinear function. For detail see Carlet and Ding [2]. We use primitive polynomial $x^4 + x + 1$ to generate all the elements of the field F_{2^4}. By using Lemma 1, we get an 8-variable bent function $f(X_1, X_2) = Tr(g(X_1, X_2))$ as follows:
00000000000000000101010110101010000011110000111101011010101001010011001100110011001101100110100110010011110000111100011010011001011001010101010101010100000000111111110101101001011010000011111111100000110011001100110001100111110011000110100101101001001111001100000111001100110001100111110011000110100101101001001111001100000111.
It has nonlinearity 120 and weight 120.

Example 2. Let $n = 10$, $m = 5$ and $g(X_1, X_2) = X_1X_2$ where $X_i \in F_{2^5}$. Here we consider primitive polynomial $1 + x^3 + x^5$ to generate all the elements of the field F_{2^5}. Then, by Lemma 1, we get a 10-variable bent function f as follows:
0000000033CC33CC5A5A5A5A6996699633333333300FF00FF696969695AA55AA55555555566
9966990F0F0F0F3CC33CC36666666655AA55AA3C3C3C3C0FF00FF00000FFFF33CCCC33
5A5A5A5699696693333CCCC00FFFF00696996965AA5A55A5555AAAA669999660F0FF0F0
3CC3C33C6666999955AAAA553C3CC3C30FF0F00F. To save space we represent f in hexadecimal format. Note that, f has nonlinearity 496 and $wt(f) = 496$.

Later we will use bent functions of this type to construct our resilient functions.

4 Construction of 1-resilient Functions

4.1 Construction of 8-variable 1-resilient Functions with Nonlinearity 116

We now show how to construct an 8-variable 1-resilient function with nonlinearity 116 using an 8-variable bent function f.

Theorem 3. Let $S_1 = \{(0,0,0,0,0,0,0,1),(0,0,0,0,0,0,1,0),(0,0,0,0,0,1,0,0),$ $(0,0,0,0,1,0,0,0),(0,0,0,1,0,0,0,0),(0,0,1,0,0,0,0,0),(0,1,0,0,0,0,0,0),$ $(1,0,0,0,0,0,0,0)\}$ and $S_2 = \{(0,0,0,0,0,0,0,0),(1,1,1,1,1,1,1,1)\}$. Let f be an 8-variable bent function such that $f(X) = 0$ for all $X \in S_1 \cup \{(0,0,0,0,0,0,0,0)\}$ and $f(1,1,1,1,1,1,1,1) = 1$. Let us construct f' as follows:

$$f'(X) = \begin{cases} f(X) \oplus 1 & \text{if } X \in S_1 \cup S_2 \\ f(X) & \text{otherwise} \end{cases}$$

Then f' is an 8-variable 1-resilient function with nonlinearity 116.

Proof. Let $h : \{0,1\}^n \to \{0,1\}$ be a Boolean function and $C \subseteq \{0,1\}^n$. Then we define $\rho_1^C(h) = |\{X \in C \ ; \ h(X) = 1\}|$ and $\rho_0^C(h) = |\{X \in C \ ; \ h(X) = 0\}|$. Let $A = \{0,1\}^8$, $S = S_1 \cup S_2$ and $\bar{S} = \{0,1\}^8 - S$. It may be noted that, $\rho_1^{\bar{S}}(f \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f' \oplus X \cdot \omega)$ and $\rho_0^{\bar{S}}(f \oplus X \cdot \omega) = \rho_0^{\bar{S}}(f' \oplus X \cdot \omega)$ for all $\omega \in \{0,1\}^8$.

Let $wt(\omega) \in \{0,1\}$. We verify from Table 2, that $\rho_1^S(f \oplus X \cdot \omega) = 1$ and $\rho_1^S(f' \oplus X \cdot \omega) = 9$. So, $wt(f \oplus X \cdot \omega) = \rho_1^A(f \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f \oplus X \cdot \omega) + \rho_1^S(f \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f \oplus X \cdot \omega) + 1 = 120$ implies $\rho_1^{\bar{S}}(f \oplus X \cdot \omega) = 119$. Thus $wt(f' \oplus X \cdot \omega) = \rho_1^A(f' \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f' \oplus X \cdot \omega) + \rho_1^S(f' \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f \oplus X \cdot \omega) + 9 = 128$. Hence f' is 1-resilient. It only remains to prove that f' has nonlinearity 116. The nonlinearity of f' can be obtained from the Walsh transform as

$$N_{f'} = 2^7 - \frac{1}{2} \max_{\omega} |W_{f'}(\omega)|.$$

We now recall Definition 5 and write $W_f(\omega) = \rho_0^A(f \oplus X \cdot \omega) - \rho_1^A(f \oplus X \cdot \omega)$ where $A = \{0,1\}^8$. To find $\max_\omega |W_{f'}(\omega)|$, we consider the following cases:

Case 1: Let $wt(\omega) \in \{0,1\}$. Since f' is 1-resilient, $f' \oplus X \cdot \omega$ is balanced. Hence $W_{f'}(\omega) = 0$.

S.N.	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	$f(X)$	$f'(X)$
0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	0	1
2	0	0	0	0	0	0	1	0	0	1
4	0	0	0	0	0	1	0	0	0	1
8	0	0	0	0	1	0	0	0	0	1
16	0	0	0	1	0	0	0	0	0	1
32	0	0	1	0	0	0	0	0	0	1
64	0	1	0	0	0	0	0	0	0	1
128	1	0	0	0	0	0	0	0	0	1
255	1	1	1	1	1	1	1	1	1	0

Table 2: Table shows the values of $f(X)$ and $f'(X)$ for $X \in S$.

Case 2: Let $wt(\omega) \in \{2,3\}$. It is know that, We verify from Table 2, that $\rho_1^S(f \oplus X \cdot \omega) = 3$ and $\rho_1^S(f' \oplus X \cdot \omega) = 7$. and $\rho_1^S(f' \oplus X \cdot \omega) = 7$. The Walsh transform of f, $W_f(\omega) = \rho_0^A(f \oplus X \cdot \omega) - \rho_1^A(f \oplus X \cdot \omega) = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) + \rho_0^S(f \oplus X \cdot \omega)] - [\rho_1^{\bar{S}}(f \oplus X \cdot \omega) + \rho_1^S(f \oplus X \cdot \omega)] = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) + 7] - [\rho_1^{\bar{S}}(f \oplus X \cdot \omega) + 3] = \pm 16$. Hence $[\rho_0^{\bar{S}}(f \oplus X \cdot \omega) - \rho_1^{\bar{S}}(f \oplus X \cdot \omega)] \in \{-20, +12\}$. Thus, the Walsh transform of f', $W_{f'}(\omega) = [\rho_0^{\bar{S}}(f' \oplus X \cdot \omega) + \rho_0^S(f' \oplus X \cdot \omega)] - [\rho_1^{\bar{S}}(f' \oplus X \cdot \omega) + \rho_1^S(f' \oplus X \cdot \omega)] = [\rho_0^{\bar{S}}(f' \oplus X \cdot \omega) + 3] - [\rho_1^{\bar{S}}(f' \oplus X \cdot \omega) + 7] = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) - \rho_1^{\bar{S}}(f \oplus X \cdot \omega)] - 4 \in \{-24, +8\}$.

Case 3: Let $wt(\omega) \in \{4,5\}$. Here $\rho_1^S(f \oplus X \cdot \omega) = 5$ and $\rho_1^S(f' \oplus X \cdot \omega) = 5$. Thus the Walsh transform of f', $W_{f'}(\omega) = \pm 16$.

Case 4: Let $wt(\omega) \in \{6,7\}$. Note that, $\rho_1^S(f \oplus X \cdot \omega) = 7$ and $\rho_1^S(f' \oplus X \cdot \omega) = 3$. So, the Walsh transform values of f', $W_{f'}(\omega) \in \{-8, +24\}$.

Case 5: Let $wt(\omega) = 8$. It's easy to check that the Walsh transform value is -16 and, $\rho_1^S(f \oplus X \cdot \omega) = 9$ and $\rho_1^S(f' \oplus X \cdot \omega) = 1$. So, $W_f(\omega) = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) + 1] - [\rho_1^{\bar{S}}(f \oplus X \cdot \omega) + 9] = -16$ implies $[\rho_0^{\bar{S}}(f \oplus X \cdot \omega) - \rho_1^{\bar{S}}(f \oplus X \cdot \omega)] = -8$. Thus, the Walsh transform of f', $W_{f'}(\omega) = [\rho_0^{\bar{S}}(f' \oplus X \cdot \omega) + 9] - [\rho_1^{\bar{S}}(f' \oplus X \cdot \omega) + 1] = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) - \rho_1^{\bar{S}}(f \oplus X \cdot \omega)] + 8 = 0$.

So $\max_\omega |W_{f'}(\omega)| = 24$ and $N_{f'} = 2^7 - 12 = 116$. Hence the theorem follows.

We now indicate our basis for the choice of the elements of S in Theorem 3. We choose the elements of S in two steps. First we select the set S_1 and construct

$$f_1(X) = \begin{cases} f(X) \oplus 1 & \text{if } X \in S_1 \\ f(X) & \text{otherwise} \end{cases}$$

Note that f_1 is balanced but $wt(f_1 \oplus X_i) = 126$ for all i. To make $wt(f_1 \oplus X_i) = 128$, keeping balancedness property unaffected, we finally choose the set S_2 and construct

$$f'(X) = \begin{cases} f_1(X) \oplus 1 & \text{if } X \in S_2 \\ f_1(X) & \text{otherwise} \end{cases}.$$

Note that f' is balanced as well as $wt(f' + X_i) = 128$ for all i. We mention that the bent function of Example 1 can be used in Theorem 3.

4.2 Construction of 10-variable (resp. 12-variable) 1-resilient Functions with Nonlinearity 488 (resp. 1996)

In this section, we construct a 10-variable 1-resilient function with nonlinearity 488, by using the same technique as in the construction of 8-variable 1-resilient functions with nonlinearity 116.

Theorem 4. Let $S_1 = \{(0,0,0,0,0,0,0,0,0,0), (0,0,0,0,0,0,0,0,0,1),$
$(0,0,0,0,0,0,0,0,1,0), (0,0,0,0,0,0,0,1,0,0), (0,0,0,0,0,0,1,0,0,0), (0,0,0,0,0,1,0,0,0,0),$

$(0,0,0,0,1,0,0,0,0,0)$, $(0,0,0,1,0,0,0,0,0,0)$, $(0,0,1,0,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0,0,0,0)$, $(1,0,0,0,0,0,0,0,0,0)$, $(0,0,0,0,0,0,0,0,1,1)$, $(0,0,0,0,0,0,0,1,1,0)$, $(0,0,0,0,0,0,1,1,0,0)$, $(0,0,0,0,0,1,1,0,0,0)$, $(0,0,0,0,0,1,0,0,0,1)$, $(0,0,0,1,1,0,0,0,0,0)$, $(0,0,1,1,0,0,0,0,0,0)$, $(0,1,1,0,0,0,0,0,0,0)$, $(1,1,0,0,0,0,0,0,0,0)$, $(1,0,0,0,1,0,0,0,0,0)$, $(1,1,1,1,1,1,1,1,1,1)\}$ and $S_2 = \{(0,0,0,0,1,0,1,0,0,1)$, $(1,1,1,1,0,1,0,1,1,0)$, $(0,1,0,0,1,0,0,0,0,1)$, $(1,0,1,1,0,1,1,1,1,0)\}$. Let f be a 10-variable bent function such that $f(X) = 0$ for all $X \in S_1 - \{(1,1,1,1,1,1,1,1,1,1)\}$ and $f(X) = 1$ for all $X \in S_2 \cup \{(1,1,1,1,1,1,1,1,1,1)\}$. Let us construct f' as follows:

$$f'(X) = \begin{cases} f(X) \oplus 1 & \text{if } X \in S_1 \cup S_2 \\ f(X) & \text{otherwise} \end{cases}$$

Then f' is a 10-variable 1-resilient function with nonlinearity 488.

Proof: The proof of the present theorem is similar to that of Theorem 3. Note that $wt(f \oplus X \cdot \omega) = 496$ for all ω such that $wt(\omega) \in \{0,1\}$. Table 3 shows the values of $f(X)$ and $f'(X)$ for all $X \in S$. Let $A = F_2^{10}$, $S = S_1 \cup S_2$ and $\bar{S} = A - S$.

Let $wt(\omega) \in \{0,1\}$. We see from Table 3, that $\rho_1^S(f \oplus X \cdot \omega) = 5$ and $\rho_1^S(f' \oplus X \cdot \omega) = 21$. Then $wt(f \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f \oplus X \cdot \omega) + \rho_1^S(f \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f \oplus X \cdot \omega) + 5 = 496$ implies $\rho_1^{\bar{S}}(f \oplus X \cdot \omega) = 491$. Moreover, $\rho_1^{\bar{S}}(f \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f' \oplus X \cdot \omega)$ for all $\omega \in \{0,1\}^{10}$. Thus $wt(f' \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f' \oplus X \cdot \omega) + \rho_1^S(f' \oplus X \cdot \omega) = \rho_1^{\bar{S}}(f) + 21 = 512$. Hence f' is 1-resilient.

The nonlinearity of f' can be obtained from the Walsh transform as

$$N_{f'} = 2^9 - \frac{1}{2} \max_{\omega} |W_{f'}(\omega)|.$$

It is known that, $W_f(\omega) = \pm 32$ for all $\omega \in \{0,1\}^{10}$. To find $\max_\omega |W_{f'}(\omega)|$, we consider the following cases:
Case 1: Let $wt(\omega) \in \{0,1\}$. Since f' is 1-resilient, $f' \oplus X \cdot \omega$ is balanced. Hence $W_{f'}(\omega) = 0$.

Case 2: Let $wt(\omega) \in \{2,3,\ldots,10\}$. We verify from Table 3, that $\rho_1^S(f \oplus X \cdot \omega) \in \{5,7,9,11,13,15,17,19\}$. Let $\Omega_1 = \{\omega \ ; \ \rho_1^S(f \oplus X \cdot \omega) = 5,7\}$ and $\Omega_2 = \{\omega \ ; \ \rho_1^S(f \oplus X \cdot \omega) = 19\}$. It can be verified that $W_f(\omega) = +32$ for $\omega \in \Omega_1$ and $W_f(\omega) = -32$ for $\omega \in \Omega_2$. If $\rho_1^S(f \oplus X \cdot \omega) = 5$, then $W_f(\omega) = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) + \rho_0^S(f \oplus X \cdot \omega)] - [\rho_1^{\bar{S}}(f \oplus X \cdot \omega) + \rho_1^S(f \oplus X \cdot \omega)] = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) + 21] - [\rho_1^{\bar{S}}(f \oplus X \cdot \omega) + 5] = +32$. Hence $[\rho_0^{\bar{S}}(f \oplus X \cdot \omega) - \rho_1^{\bar{S}}(f \oplus X \cdot \omega)] = +16$ and the Walsh transform of f', $W_{f'}(\omega) = [\rho_0^{\bar{S}}(f' \oplus X \cdot \omega) + 5] - [\rho_1^{\bar{S}}(f' \oplus X \cdot \omega) + 21] = [\rho_0^{\bar{S}}(f \oplus X \cdot \omega) - \rho_1^{\bar{S}}(f \oplus X \cdot \omega)] - 16 = 0$. Similarly, if $\rho_1^S(f \oplus X \cdot \omega) = 7$ (resp. 19), then $W_{f'}(\omega) = +8$ (resp. -8). Otherwise, if $\rho_1^S(f \oplus X \cdot \omega) \in \{9,11,13,15,17\}$, then the Walsh transform of f', $W_{f'}(\omega) \in \{\pm 16, \pm 24, \pm 32, \pm 40, \pm 48\}$.
So $\max_\omega |W_{f'}(\omega)| = 48$ and $N_{f'} = 2^9 - 24 = 488$. Hence the theorem follows.

S.N.	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	$f(X)$	$f'(X)$
0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	0	0	1	0	1
2	0	0	0	0	0	0	0	0	1	0	0	1
4	0	0	0	0	0	0	0	1	0	0	0	1
8	0	0	0	0	0	0	1	0	0	0	0	1
16	0	0	0	0	0	1	0	0	0	0	0	1
32	0	0	0	0	1	0	0	0	0	0	0	1
64	0	0	0	1	0	0	0	0	0	0	0	1
128	0	0	1	0	0	0	0	0	0	0	0	1
256	0	1	0	0	0	0	0	0	0	0	0	1
512	1	0	0	0	0	0	0	0	0	0	0	1
1023	1	1	1	1	1	1	1	1	1	1	1	0
3	0	0	0	0	0	0	0	0	1	1	0	1
6	0	0	0	0	0	0	0	1	1	0	0	1
12	0	0	0	0	0	0	1	1	0	0	0	1
24	0	0	0	0	0	1	1	0	0	0	0	1
17	0	0	0	0	0	1	0	0	0	1	0	1
96	0	0	0	1	1	0	0	0	0	0	0	1
192	0	0	1	1	0	0	0	0	0	0	0	1
384	0	1	1	0	0	0	0	0	0	0	0	1
768	1	1	0	0	0	0	0	0	0	0	0	1
544	1	0	0	0	1	0	0	0	0	0	0	1
41	0	0	0	0	1	0	1	0	0	1	1	0
982	1	1	1	1	0	1	0	1	1	0	1	0
289	0	1	0	0	1	0	0	0	0	1	1	0
734	1	0	1	1	0	1	1	1	1	0	1	0

Table 3: Table shows the values of $f(X)$ and $f'(X)$ for $X \in S$.

We now indicate our basis for the choice of the elements of S in Theorem 4. First we select the set S_1 and construct

$$f_1(X) = \begin{cases} f(X) \oplus 1 & \text{if } X \in S_1 \\ f(X) & \text{otherwise} \end{cases}$$

It may be noted that f_1 is 1-resilient but $wt(f_1) = 516$. Now to make f_1 balanced, keeping the resiliency property unaffected, we choose the elements of S_2 by computer search and construct

$$f'(X) = \begin{cases} f_1(X) \oplus 1 & \text{if } X \in S_2 \\ f_1(X) & \text{otherwise} \end{cases} .$$

The bent function of Example 2 can be used in Theorem 4. If we list the elements of S as the rows of a matrix M, then in each column of M, 1 occurs the same number of times. The M matrix necessarily satisfies this condition to get a 1-resilient function.

We construct a 12-variable 1-resilient function with nonlinearity 1996, by using the same technique as in the construction of 8-variable and 10-variable

resilient functions. Let $n = 12$, $m = 6$ and $g(X_1, X_2) = X_1 X_2$ where $X_i \in F_{2^6}$. We use primitive polynomial $1 + x + x^6$ to generate the elements of the field F_{2^6}. Then, by Lemma 1, we get a 12-variable bent function f with $f(1, 1, 1, \ldots, 1) = 1$. Here, we consider $S = \{(000), (001), (002), (004), (008), (010), (020), (040), (080), (100), (200), (400), (800), (FFF), (003), (005), (006), (009), (00A), (00C), (011), (012), (014), (018), (021), (022), (024), (028), (030), (0C0), (140), (180), (240), (280), (300), (440), (480), (500), (600), (840), (880), (900), (A00), (C00), (043), (FBC), (045), (FBA), (049), (FB6), (060), (F9F), (066), (F99)\}$. To save space we present the elements of S in hexadecimal format.

Maitra and Pasalic [3] have constructed a 10-variable (resp. 12-variable) 1-resilient function with nonlinearity 488 (resp. 1996) by suitably concatenating 8-variable 1-resilient functions with nonlinearity 116. But our construction is not based on concatenation and we believe one can construct 10-variable (resp. 12-variable) 1-resilient functions with maximum nonlinearity 492 (resp. 2012) by choosing an appropriate S. In the following section, we focus on selection of the elements of S.

5 Some General Results

Lemma 2. Let f be an n-variable (n even) bent function, and let $S \subseteq \{0,1\}^n$, such that

(i) $\rho_0^S(f \oplus X \cdot \omega) - \rho_1^S(f \oplus X \cdot \omega) = 2^{\frac{n}{2}-1}$ for all ω such that $0 \leq wt(\omega) \leq 1$,
(ii) $-2^2 \leq \rho_0^S(f \oplus X \cdot \omega) - \rho_1^S(f \oplus X \cdot \omega) \leq +2^{\frac{n}{2}} + 2^2$ for all ω whenever $2 \leq wt(\omega) \leq n$ and $W_f(\omega) = +2^{\frac{n}{2}}$ and
(iii) $-(2^{\frac{n}{2}} + 2^2) \leq \rho_0^S(f \oplus X \cdot \omega) - \rho_1^S(f \oplus X \cdot \omega) \leq +2^2$ for all ω whenever $2 \leq wt(\omega) \leq n$ and $W_f(\omega) = -2^{\frac{n}{2}}$.

Then

$$f'(X) = \begin{cases} f(X) \oplus 1 & \text{if } X \in S \\ f(X) & \text{otherwise} \end{cases}$$

is an n-variable 1-resilient function with nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1} - 2^2$.

We shall illustrate Lemma 2 by Theorem 3 and Theorem 4. It is easy to verify that, in Theorem 3, S satisfies conditions (i), (ii) and (iii) of Lemma 2. So f' of Theorem 3 is an 8-variable 1-resilient function with maximum nonlinearity. Let us consider Theorem 4. It can be verified that, $\rho_1^S(f \oplus X \cdot \omega) = 9$ (resp. 17) for some ω such that $2 \leq wt(\omega) \leq 10$ and $W_f(\omega) = -32$ (resp. $W_f(\omega) = +32$). That is, $\rho_0^S(f \oplus X \cdot \omega) - \rho_1^S(f \oplus X \cdot \omega) = +8$ (resp. -8) for some ω such that $2 \leq wt(\omega) \leq 10$ and $W_f(\omega) = -32$ (resp. $W_f(\omega) = +32$). Which violates condition (iii) (resp. condition (ii)) of Lemma 2. It may be noted that, f' of Theorem 4 is a 10-variable 1-resilient function but not with maximum nonlinearity. In general we have the following lemma.

Lemma 3. Let f be an n-variable (n even) bent function, and let $S \subseteq \{0,1\}^n$, such that

(i) $\rho_0^S(f \oplus \omega.X) - \rho_1^S(f \oplus \omega.X) = 2^{\frac{n}{2}-1}$ for ω such that $0 \leq wt(\omega) \leq t$,
(ii) $-2^{t+1} \leq \rho_0^S(f \oplus X \cdot \omega) - \rho_1^S(f \oplus X \cdot \omega) \leq +2^{\frac{n}{2}} + 2^{t+1}$ for all ω such that $t+1 \leq wt(\omega) \leq n$ and $W_f(\omega) = +2^{\frac{n}{2}}$ and
(iii) $-(2^{\frac{n}{2}} + 2^{t+1}) \leq \rho_0^S(f \oplus X \cdot \omega) - \rho_1^S(f \oplus X \cdot \omega) \leq +2^{t+1}$ for all ω such that $t+1 \leq wt(\omega) \leq n$ and $W_f(\omega) = -2^{\frac{n}{2}}$.

Then

$$f'(X) = \begin{cases} f(X) \oplus 1 & \text{if } X \in S \\ f(X) & \text{otherwise} \end{cases}$$

is an n-variable t-resilient function with nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{t+1}$ if $t+1 \leq \frac{n}{2} - 1$.

6 Conclusions

We have considered the construction of 1-resilient functions with maximum nonlinearity. We have constructed 8-variable 1-resilient functions with maximum nonlinearity. Moreover, we have constructed 10-variable (resp. 12-variable), 1-resilient functions with nonlinearity 488 (resp. 1996). The new construction is based on selecting a number of elements S. However we mention that we do not have any good algorithm to generate the elements of S. The method mentioned to construct the three Boolean functions may be generalized and that is our future course of research. It is also interesting to investigate the propagation characteristics of these functions.

Acknowledgement
The authors are grateful to Stichting Nlnet, Netherlands for supporting this research work.

References

1. Biham, E. and Shamir, A., Differential cryptanalysis of DES-like cryptosystems., *Journal of Cryptology* Vol 4, No. 1, 1991, 3-72.
2. Carlet, C. and Ding, C., Highly nonlinear mappings. Email: Claude.Carlet@inria.fr (C. Carlet), cding@cs.ust.hk (C. Ding)
3. Maitra, S. and Pasalic, E., Further construction of resilient Boolean functions with very high nonlinearity. *IEEE Trans. on Information Theory*, Vol 48, No. 7, July 2002, 1825-1834.
4. Matsui, M., Linear cryptanalysis method for DES cipher. *Advances in Cryptology-EUROCRYPT 1993,* LNCS 765, 1994, pp. 386-397.
5. Nyberg, K., Perfect non-linear S-boxes. *Advances in Cryptology-EUROCRYPT 1991,* LNCS 547, 1992, pp. 378-386.
6. Rothaus, O. S., On bent functions, *J. Combin. Theory*, Ser. A 20, 1976, 300-305.
7. Sarkar, P. and Maitra, S., Nonlinearity bounds and constructions of resilient Boolean functions. *CRYPTO 2000*, LNCS 1880, 2000, pp. 515-532.
8. Siegenthaler, T., Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. on Information Theory*, IT-30(5), September 1984, 776-780.

9. Tarannikov, Y. V., On resilient Boolean functions with maximum possible nonlinearity. In *Progress in Cryptology-INDOCRYPT 2000*, LNCS 1977, Springer Verlag, 2000, pp. 19-30.
10. Xiao, G. and Massey, J.L., A spectral characterization of correlation-immune functions. *IEEE Trans. on Information Theory*, 34(3), 1988, 569-571.
11. Zheng, Y. and Zhang, X. M., Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography-SAC 2000*, LNCS 2012, 2000, pp. 264-274.