Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 7 (3): 317-325, 2007
ISSN 1812-5654

Secondary Construction of Resilient Functions and Plateaued Functions: Study Their Algebraic Immunity

[1]Belmeguenaï Aïssa and [2]Doghman Nouredine
[1]Department of Electronics, Faculty of Science and Engineering,
Badji Mokhtar University-Skikda LP 26 El-Hadeik Avenue
[2]Department of Electronics, Faculty of Science and Engineering,
Badji Mokhtar University-Annaba LP 12

Abstract: In this study, we first give a survey of the Siegenthaler's constructions and the general Carlet's construction of resilient functions, permitting to obtain resilient functions achieving the best possible trade-offs between resiliency order, algebraic degree and nonlinearity. Then, we introduce and we study a new secondary construction of resilient functions based on the principal of the siegenthaler's construction. This construction permitted to increase the algebraic immunity, algebraic degree and define many more resilient functions where the degree, algebraic immunity, resiliency and nonlinearity achieving are high. Thus, permits to obtain resilient functions achieving the best possible trade-offs between resiliency order, algebraic degree and nonlinearity (that is, achieving Siegenthaler's and Sarkar, al.'s bounds). We conclude the paper by generalizing our construction to plateaued functions.

Key words: Stream ciphers, boolean function, plateaued function, resiliency, nonlinearity, algebraic degree, Algebraic immunity

INTRODUCTION

In the standard model of stream cipher, the outputs to n Linear Feedback Shift Register (LFSR) are combined by a nonlinear Boolean function to produce the keystream. This keystream is bitwise XORed with the message plantext to produce the ciphertext. The decryption machinery is identical to the encryption machinery. Then it is now well accepted that for a Boolean function to be used in stream cipher systems it must satisfy several properties: balancedness, high nonlinearity, high algebraic degree and high order of correlation immunity to resist different know attacks (Siegenthaler, 1985; Menezes *et al*., 1997; Ding *et al*., 1991).

Each of the above mentioned properties provide protection against a class of attacks. Also it is not possible to get the best possible values for each of these properties spartanly and there are certain trade-offs involved among the above properties. For example, Siegenthaler showed (Siegenthaler, 1984) that for an n-variable Boolean function f cannot at the same time have a high degree and a high order of correlation immunity. If the function f is k-th order correlation immune function ($0 \leq k \prec n$) then f has algebraic degree smaller than or equal to n-k. Moreover, if fis k-resilient with $k \leq n-2$, then $d^{\circ}(f) = n-k-1$. The exact nature of trade-off among algebraic degree, order of correlation immunity and nonlinearity has also been investigated (Sarkar and Maitra, 2000a; Tarannikov, 2000; Zheng and Zhang, 2000; Carlet, 2001; Carlet and Sarkar, 2002). Many papers have approached the construction problem by fixing one or two parameters and trying to design balanced Boolean function with good parameters (Camion *et al*., 1992; Seberry *et al*., 1994; Chee *et al*., 1996; Filiol and Fontaine, 1998; Maitra and Sarkar, 1999; Carlet and Sarkar, 2002; Sarkar and Maitra, 2000b). Thus, only constructions interesting of optimal functions that we know are of secondary constructions type and they are based on the principe introduced by Sarkar and Maitra (2000a). Among these constructions, we can quote, for example, those of Pasalic, Maïtra, Johansson and Sarkar (Paslic *et al*., 2001) or those of Carlet (2004) who generalizes and extends the whole of the secondary constructions presented by Sarkar and Maitra (2000a), Taranikov (2000), (Taranikov (2001), Paslic *et al*. (2001), Maitra and Pasalic (2002), Maitra and Sarkar (2002) and Carlet (2002).

Sarkar and Maitra (2000b) have showed in that a divisibility bound on the Walsh transform values of an

Corresponding Author: Belmeguenaï Aïssa, Department of Electronics, Faculty of Science and Engineering, August 20 University- Skikda LP 26 El-Hadeik Avenue

n-variable k-resilient function, with k≤n-2: these values are divisible by 2^{k+2}, also, this divisibility bound is improved in (Carlet, 2001; Carlet and Sarkar, 2002). Independently obtained by Tarannikov (2000) and by Zheng and Zhang (2001): the nonlinearity of any n-variable, k-resilient function is upper bounded by $2^{n-1}-2^{k+1}$. Tarannikov showed that resilient functions achieving this bound must have degree n-k-1 (that is, achieve Siegenthaler's bound); thus, they achieve best possible trade-offs between algebraic degree, resiliency order and nonlinearity.

Since the introduction, the cryptographic parameters: a high algebraic degree, a high resiliency order and a high nonlinearity were the only requirements needed for constructing the Boolean function used in a stream cipher or in filtering model. The recent algebraic attacks (Courtois and Meier, 2002; Meier *et al*., 2004) have dramatically complicated this situation by adding a new algebraic immunity criterion of considerable importance to this list. Very recently, a new criterion of algebraic immunity has received a lot of attention in cryptographic literature for example (Ars and Fourgère, 2005; Carlet and Gaborit, 2005; Carlet *et al*., 2006). Carlet and Gaborit (2005) showed that it was not hard to construct functions with an optimal AI and that there are strong reasons which indicate that, as soon as n is large enough, almost all random balanced Boolean functions were almost optimal.

In this research, we first study a construction combined by a Siegenthaler's construction and Carlet's general secondary construction permitting to obtain resilient function with best possible trade-off between algebraic degree, resiliency order and nonlinearity. Then, we introduce and we study a new construction of resilient functions on F_2^{n+2} based on the principal of the Siegenthaler's construction. These constructions permitted to increase the cryptographic parameters and to define many more resilient and plateaued functions where the degree, algebraic immunity, resiliency and nonlinearity achieving are high. Thus, permit to obtain resilient functions achieving the best possible trade-offs between resiliency order, algebraic degree and nonlinearity (that is, achieving Siegenthaler's and Sarkar's bounds.

CONCEPT AND DEFINITIONS

In this section, we introduce a few basic concepts and definitions. A Boolean function on n variables may be viewed as a mapping from F_2^n in to F_2. The set of all n-variable Boolean function is denoted by B_n. By $\oplus$ we denote sum modulo 2. The Hamming weight wt (f) of a Boolean function f on F_2^n is the size of its support $\{x \in F_2^n; f(x) = 1\}$ The Hamming distance d (f, g) between two Boolean functions f and g is the Hamming weight of their difference $f \oplus g$, d (f, g) = wt ($f \oplus g$). An n-variable Boolean function f has unique algebraic normal form (A.N.F).

$$f(x_1,x_2,...,x_n) = \bigoplus_{(u)\in F_2^n} a_u\left(\prod_{i=1}^{n} x_i^{u_i}\right) = \bigoplus_{u\in F_2^n} a_u x^u \cdot$$

The algebraic degree of Boolean function f, denoted by d°(f), is defined as the number of variables in the longest term of f. If algebraic degree of f is smaller than or equal to one then f is called affine function. An affine function with a constant term equal to zero is called a linear function.

Definition 1: Let f a function on F_2^n. The Walsh-Hadamard transform (or spectrum) of f is defined as

$$\forall u \in F_2^n, Wf(u) = \sum_{x\in F_2^n} (-1)^{f(x)}(-1)^{u.x} \qquad (1)$$

Where u.x denoted the usual scalar product of vectors u and x.

Definition 2: A Boolean function f on F_2^n is called balanced if wt(f) = wt($f \oplus 1$). Otherwise, f is balanced if and only if wt(f) = 2^{n-1}.

Definition 3: A function is called plateaued if its squared Walsh transform takes at most one nonzero value, that is, if its Walsh transform takes at most three values 0 and $\pm\lambda$ (where λ is some positive integer, that we call the amplitude of the plateaued function).

Proposition 1: Let f a Boolean function on F_2^n.The nonlinearity Nf of f is equal to:

$$Nf = 2^{n-1} - \frac{1}{2}\max_{u\in F_2^n} |Wf(u)| \qquad (2)$$

Proposition 2: (Xiao and Massey, 1988): Let f a Boolean function on F_2^n. Then -f is t-th order correlation-immune if and only if $Wf(u) = 0 \forall u \in F_2^n, 1 \le wt(u) \le t$ .It is t-th resilient if moreover . $Wf(0) = 0 \forall u \in F_2^n, 0 \le wt(u) \le t$.

Definition 3: (Carlet *et al*., 2006) Let $f \in B_n$. The algebraic immunity AI_n (f) of f is the smaller degree of non null function g such that f * g = 0 or (1 + f)* g = 0. Otherwise, the minimum value of d such that f or f + 1 admits an annihilator of degree d.

We denote by (n, k, d, N), we mean an n-variable function, k-resilient function having degree d and

nonlinearity N. In the above notation, we may replace some component by (-) if we do not want to specify it.

SECONDARY CONSTRUCTIONS IN LITERATURE

Siegenthaler's construction: The functions $g \in B_n$ constructed by Siegenthaler are defined by the form

$$g(x_1,...,x_n,x_{n+1}) = (x_{n+1} \oplus 1)f(x_1,...,x_n) \oplus x_{n+1}h(x_1,...,x_n) \quad (3)$$

The Walsh transform of g is

$$Wg(u_1,...,u_{n+1}) = Wf(u_1,...,u_n) + (-1)^{u_{n+1}} Wh(u_1,...,u_n) \quad (4)$$

Proposition 3: Let f and h be two Boolean functions on F_2^n. Then

- If f and h are t-resilient, then function g defined by (3) is t-resilient; moreover, if for every $u \in F_2^n$ of Hamming weight wt (u) = t + 1, we have Wf (u) + Wh (u) = 0, then g is (t + 1)-resilient.
- The nonlinearity of g is: $N_g \geq N_f + N_h$.
  - if f and h achieve maximum possible nonlinearity $2^{n-1} - 2^{t+1}$ and if g is (t + 1)-resilient, then the nonlinearity $2^n - 2^{t+2}$ of g is the best possible;
  - if the supports of the Walsh transforms of f and h are disjoint, then we have $N_g = 2^{n-1} + \min(N_f, N_h)$; thus, if f and h achieve nonlinearity $2^{n-1} - 2^{t+1}$ then g achieves best possible nonlinearity $2^n - 2^{t+1}$.
- If the degree of f and h are not all the same (i.e d° (f) ≠ d° (h)), then we have: d° g = 1 + max (d° f, d° h).

General carlet's construction: In a recent study (Carlet, 2004), Carlet presented secondary constructions generalizing the Tarannikov *et al.*'s construction. The functions $g \in B_{r+s}$ in which Carlet is interested are defined starting from two functions f_1 and f_2 on B_r and two functions h_1 and h_2 on B_s by the form;

$$g(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1 + f_2)(x)(g_1 + g_2)(y) \quad (5)$$

Proposition 4: (Carlet, 2004): Let r, s, t and k be positive integers such that $t \prec r$ and $k \prec s$. Let f_1 and f_2 be two t-resilient functions on F_2^r and let h_1 and h_2 be two k-resilient functions on F_2^s. Let a function g on F_2^{r+s} defined by (5). Then:

- The value of the Walsh transform of g, for every $(u, v) \in F_2^r \times F_2^s$ equals

$$Wg(u,v) = \frac{1}{2}Wf_1(u)\left[Wh_1(v) + Wh_2(v)\right] + \frac{1}{2}Wf_2(u)\left[Wh_1(v) - Wh_2(v)\right] \quad (6)$$

- The function g is (t + k + 1)-resilient.
- The nonlinearity of g is satisfied

$$Ng \geq -2^{r+s-1} + 2^s(Nf_1 + Nf_2) + 2^r(Nh_1 + Nh_2) - (Nf_1 + Nf_2)(Nh_1 + Nh_2) \quad (7)$$

- If the Walsh transform of h_1 and h_2 have disjoint supports, then, we have

$$Ng \geq 2^{s-1}(Nf_1 + Nf_2) + (2^r - (Nf_1 + Nf_2)) \min(Nh_1, Nh_2) \quad (8)$$

- If the Walsh transforms of f_1 and f_2 have disjoint supports, as well as of h_1 and h_2, then

$$Ng = \min_{i,j\in\{1,2\}} (2^{r+s-2} + 2^{s-1}Nf_i + 2^{r-1}Nh_j - Nf_iNh_j) \quad (9)$$

- If f_1 and f_2 are distinct and if h_1 and h_2 are distinct, then algebraic degree of g equals:

$$d°g = \max(d°f_1, d°h_1, d°(f_1 + f_2) + d°(h_1 + h_2)) \quad (10)$$

- If f_1 and f_2 are two r-variables t-resilient having disjoint spectra, achieving a $2^{r-1} - 2^{t+1}$ nonlinearity, if h_1 and h_2 are two s-variables k-resilient having disjoint spectra, achieving a $2^{s-1}-2^{k+1}$ nonlinearity and such that d° $(f_1 + f_2)$ = r-t-1, d° $(h_1 + h_2)$ = s-k-1, then g is a (r + s)-variable and (t + k+ 1)-resilient with a r+s-t-k-2 degree achieving a $2^{r+s-1} - 2^{t+k+2}$ nonlinearity. Hence, it achieves a Siegenthaler's and Sarkar *et al*'s bounds.

Combination between the siegenthaler's construction and the general carlet's construction: Let r, s, t and k be positive integers such that $t \prec r$ and $k \prec s$. Let f_1, f_2, f_3 and f_4 be four t-resilient functions on F_2^r and let h_1, h_2, h_3, h_1 and h_4 be four k-resilient functions on F_2^s. Consider the function

$$g(x,y,z) = (1 \oplus z)g_1(x,y) \oplus zg_2(x,y) \text{ on } F_2^{r+s+1} \quad (11)$$

Where $(x,y) \in F_2^r \times F_2^s$ and $z \in F_2$, such that g_1 and g_2 be two functions on F_2^{r+s} defined as follows:

$g_1(x,y) = f_1(x) \oplus h_1(y) \oplus (f_1 + f_2)(x)(h_1 + h_2)(y)$ and
$g_2(x,y) = f_3(x) \oplus h_3(y) \oplus (f_3 + f_4)(x)(h_3 + h_4)(y)$.

Proposition 5: Let a function $g \in B_{r+s+1}$ defined by (11). Then, if f_1, f_2, f_3 and f_4 are t-resilient and if h_1, h_2, h_3 and h_4 be four k-resilient, then g is $(t+k+1)$-resilient. Moreover, if for every $(u,v) \in F_2^r \times F_2^s$ of Hamming weight $(t+k+1)$, we have $Wg_1(u, v) + Wg_2(u, v) = 0$, then g is $(t + k + 2)$-resilient. The Walsh transform of g at $(u,v) \in F_2^r \times F_2^s$ $w \in F_2$ takes Value

$$\begin{aligned} Wg(u,v,w) = {} & \frac{1}{2} Wf_1(u)\left[Wh_1(v) + Wh_2(v)\right] + \\ & \frac{1}{2} Wf_2(u)\left[Wh_1(v) - Wh_2(v)\right] + (-1)^w \\ & \left[\begin{array}{l} \frac{1}{2} Wf_3(u)\left[Wh_3(v) + Wh_4(v)\right] + \\ \frac{1}{2} Wf_4\left[Wh_3(v) - Wh_4(v)\right] \end{array}\right] \end{aligned} \quad (12)$$

Proof: For every $(u,v) \in F_2^r \times F_2^s$, $w \in F_2$ and from relations 4, we have $Wg(u, v, w) = Wg_1(u, v) + (-1)^w Wg_2(u, v)$, hence from Relations 6, we deduced

$$\begin{aligned} Wg(u,v,w) = {} & \frac{1}{2} Wf_1(u)\left[Wh_1(v) + Wh_2(v)\right] + \\ & \frac{1}{2} Wf_2(u)\left[Wh_1(v) - Wh_2(v)\right] + (-1)^w \\ & \left[\begin{array}{l} \frac{1}{2} Wf_3(u)\left[Wh_3(v) + Wh_4(v)\right] \\ + \frac{1}{2} Wf_4\left[Wh_3(v) - Wh_4(v)\right] \end{array}\right] \end{aligned}$$

that is relation (12)

If f_1, f_2, f_3, f_4 are t-resilient and if h_1, h_2, h_3, h_4 are k-resilient, then, we have, from item (ii) of proposition 4, the functions g_1 and g_2 are $(t+k+1)$-resilient. This implies for every $(u,v) \in F_2^r \times F_2^s$ of Hamming weight smaller than or equal to $t + k + 1$ the values of $Wg_1(u, v)$ and $Wg_2(u, v)$ are null, which implies the value of $Wg(u, v, w) = Wg_1(u, v) + (-1)^w Wg_2(u, v)$ is null for every $w \in F_2$. Moreover, if for every $(u,v) \in F_2^r \times F_2^s$ of Hamming weight $(t + k + 2)$, the values of $Wg_1(u, v)$ and $Wg_2(u, v)$ satisfy the relation

$Wg_1(u, v) = - Wg_2(u, v)$. This implies
$Wf_1(u)\left[Wh_1(v) + Wh_2(v)\right] + Wf_2(u)\left[Wh_1(v) - Wh_2(v)\right]$
$= - [Wf_3(u)[Wh_3(v) + Wh_4(v)] + Wf_4[Wh_3(v) - Wh_4(v)]]$, the for $w = 0$, we deduce that $Wg(u, v, w) = Wf_1(u)[Wh_1(v) + Wh_2(v)] + Wf_2(u)[Wh_1(v) - Wh_2(v)] = (-1)^0 Wf_3(u)[Wh_3(v) + Wh_4(v)] + Wf_4(u)[Wh_3(v) - Wh_4(v)]]$. Therefore, g is $(t + k + 2)$-resilient.

Theorem 1: Let a function $g \in B_{r+s+1}$ defined by (11). Then

- The nonlinearity of g is:

$$\begin{aligned} Ng \geq {} & -2^{r+s} + 2^s \sum_{i=1}^{4} Nf_i + 2^r \sum_{j=1}^{4} Nh_j - \sum_{i=1}^{2} Nf_i \\ & \times \sum_{j=1}^{2} Nh_j - \sum_{i=3}^{4} Nf_i \times \sum_{j=3}^{4} Nh_j \end{aligned} \quad (13)$$

- If the supports of the Walsh transform of h_1 and h_2 are disjoint, as well as those of h_3 and h_4 then we have:

$$\begin{aligned} Ng \geq {} & 2^{s-1} \times \sum_{i=1}^{4} Nf_i + (2^r - \sum_{i=1}^{2} Nf_i) \min_{j \in \{1,2\}} \\ & Nh_j + (2^r - \sum_{i=3}^{4} Nf_i) \min_{j \in \{3,4\}} Nh_j \end{aligned} \quad (14)$$

- If the Walsh transforms of f_1 and f_2 have disjoint supports, as well as of f_3 and f_4 and if the supports of the Walsh transform of h_1 and h_2 are disjoint, as well as those of h_3 and h_4, then we have:

$$\begin{aligned} Ng \geq {} & 2^{r+s-1} + \min_{i,j \in \{1,2\}} (2^{r-1} Nh_j + 2^{s-1} Nf_i - Nf_i Nh_j) + \\ & \min_{i,j \in \{3,4\}} (2^{r-1} Nh_j + 2^{s-1} Nf_i - Nf_i Nh_j) \end{aligned} \quad (15)$$

- If f_1, f_2 are distinct, if f_3, f_4 are distinct, if h_1, h_2 are distinct and if h_3, h_4 are distinct then the algebraic degree of g takes:
  $d^\circ g = 1 + \max (d^\circ f_1, d^\circ h_1, d^\circ f_3, d^\circ (f_1 + f_2) + d^\circ (h_1 + h_2), d^\circ (f_3 + f_4) + d^\circ (h_3 + h_4))$.
  Otherwise, it takes:
  $1 + \max (d^\circ f_1, d^\circ h_1, d^\circ f_3, d^\circ h_3)$.

Proof:

- Relation (12) implies

$$\begin{aligned} & \max_{(u,v,w) \in F_2^r \times F_2^s \times F_2} \left|Wg(u,v,w)\right| \leq \\ & \frac{1}{2}\left(\max_{u \in F_2^r} \left|Wf_1(u)\right| + \max_{u \in F_2^r} \left|Wf_2(u)\right|\right) \\ & \times \left(\max_{v \in F_2^s} \left|Wh_1(v)\right| + \max_{v \in F_2^s} \left|Wh_2(v)\right|\right) \\ & + \left(\max_{u \in F_2^r} \left|Wf_3(u)\right| + \max_{u \in F_2^r} \left|Wf_4(u)\right|\right) \\ & \times \left(\max_{v \in F_2^s} \left|Wh_3(v)\right| + \max_{v \in F_2^s} \left|Wh_4(v)\right|\right) \end{aligned}.$$

Using relation (2)

$$2^{r+s+1}-2Ng \le \frac{1}{2}\left((2^r-2Nf_1)+(2^r-2Nf_2)\right)$$
$$\times\left((2^s-2Nh_1)+(2^s-2Nh_2)\right)$$

$$+\frac{1}{2}\left((2^r-2Nf_3)+(2^r-2Nf_4)\right)$$
$$\times\left((2^s-2Nh_3)+(2^s-2Nh_4)\right)$$

is equivalent to (13).

- If the supports of the Walsh transform of h_1, h_2 are disjoint and if the Walsh transform of h_3, h_4 have disjoint supports then relation (12) can take:

$$Wg(u,v,w)=\frac{1}{2}Wh_1(v)\left[Wf_1(u)+Wf_2(u)\right]$$
$$+\frac{1}{2}Wh_3\left[Wf_3(u)+Wf_4(u)\right]$$
$$+\frac{1}{2}Wh_2(v)\left[Wf_1(u)-Wf_2(u)\right]$$
$$+\frac{1}{2}Wh_4\left[Wf_3(u)-Wf_4(u)\right]$$

which implies that

$$\max_{(u,v,w)\in F_2^r\times F_2^s\times F_2}\left|Wg(u,v,w)\right| \le \frac{1}{2}$$
$$\left(\max_{u\in F_2^r}\left|Wf_1(u)\right|+\max_{u\in F_2^r}\left|Wf_2(u)\right|\right)\times$$
$$\max_{i\in\{1,2\}}\left(\max_{v\in F_2^s}\left|Wh_i(v)\right|\right)$$

$$+\frac{1}{2}\left(\max_{u\in F_2^r}\left|Wf_3(u)\right|+\max_{u\in F_2^r}\left|Wf_4(u)\right|\right)\times$$
$$\max_{i\in\{3,4\}}\left(\max_{v\in F_2^s}\left|Wh_i(v)\right|\right).$$

Using (2) we deduce

$$2^{r+s+1}-2Ng \le \frac{1}{2}(2^r-2Nf_1+2^r-2Nf_2)$$
$$\times\max_{i\in\{1,2\}}(2^s-2Nh_i)$$

$$+\frac{1}{2}(2^r-2Nf_3+2^r-2Nf_4)\times\max_{i\in\{3,4\}}(2^s-2Nh_i)$$

Which is equivolent (14)

- If the Walsh transforms of f_1 and f_2 have disjoint supports, as well as those of f_3, f_4 and if the Walsh transforms of h_1 and h_2 have disjoint supports, as well as those of h_3 and h_4, we deduce from (12) that:

$$\max_{(u,v,w)\in F_2^r\times F_2^s\times F_2}\left|Wg(u,v,w)\right| \le \frac{1}{2}$$
$$\max_{i,j\in\{1,2\}}\left(\max_{u\in F_2^r}\left|Wf_i(u)\right|\max_{v\in F_2^s}\left|Wh_j(v)\right|\right)$$
$$+\frac{1}{2}\max_{i,j\in\{3,4\}}\left(\max_{u\in F_2^r}\left|Wf_i(u)\right|\max_{v\in F_2^s}\left|Wh_j(v)\right|\right)$$

which, using (2)

$$2^{r+s+1}-2Ng \le \frac{1}{2}\max_{i,j\in\{1,2\}}\left((2^r-2Nf_i)(2^s-2Nh_j)\right)$$
$$+\frac{1}{2}\max_{i,j\in\{3,4\}}\left((2^r-2Nf_i)(2^s-2Nh_j)\right)$$

is equivalent to (15).

- It is obvious that if f_1, f_2 are distinct, if f_3, f_4 are distinct, if h_1, h_2 are distinct and if h_3, h_4 are distinct the terms of highest degree is in $(f_1 + f_2)$ (x) $(h_1 + h_2)$ (y) or in $(f_3 + f_4)$ (x) $(h_3 + h_4)$ (y).

Corollary 1: Let f_1, f_2, f_3 and f_4 be four (r, t, -, $2^{r-1} - 2^{t+1}$) functions and if the Walsh transforms of f_1, f_2 have disjoint supports, as well as those of f_3, f_4 and such that $f_1 + f_2$ and $f_3 + f_4$ have the same degree r−t−1. Let h_1, h_2, h_3 and h_4 be four (s, k, -, $2^{s-1} - 2^{k+1}$) functions and if the Walsh transforms of h_1, h_2 have disjoint supports, as well as those of h_3, h_4 and such that $h_1 + h_2$ and h_3, h_4 have the same degree s−k−1, then the function $g \in B_{r+s+1}$ defined by 11 is (t+ k + 2)-resilient has degree r + s − t − k − 2 and nonlinearity $2^{r+s} - 2^{t+k+3}$ and thus, achieves Siegenthaler's and Sarkar *et al.*'s bounds.

Construction of plateaued functions: We consider now the same construction as in the section 4, but applied to plateaued functions instead of resilient functions.

Lemma 1: Let r, s be two positive integers. Let f_1, f_2, f_3 and f_4 be four r-variable plateaued functions that have the same amplitude 2^m. Let h_1, h_2, h_3 and h_4 be four s-variable plateaued functions that have the same amplitude 2^l. Let the function g (r + s + 1)-variable defined by (11).

- If for every $u \in F_2^r$, the values of Wf_1 (u), Wf_2 (u), Wf_3 (u) and Wf (u) and if for every $v \in F_2^s$, the values of Wh_1 (v), Wh_2 (v), Wh_3 (v) and Wh_4 (v) are simultaneously null, or simultaneously non null, then g is a plateaued function with amplitude 2^{m+l+1}.

- If the Walsh transforms of f_1 and f_2 have disjoint supports, as well as of f_3 and f_4 and if the supports of the Walsh transform of h_1 and h_2 are disjoint, as well as those of h_3 and h_4, then g is a plateaued function with amplitude 2^{m+1}.

Proof:

- From relation (10), we deduced if the functions Wf_1, Wf_2, Wf_3, Wf_4, Wh_1, Wh_2, Wh_3 and Wh_4 are simultaneously null (resp. Simultaneously non null), then Wg (u, v, w) is null (resp. equal
$$\frac{1}{2}\times\pm 2^m\left(\pm 2^l \pm 2^l\right)+\frac{1}{2}\times\pm 2^m\left(\pm 2^l \pm 2^l\right)=\pm 2^{m+l+1}$$
because f_1, f_2, f_3, f_4, are plateaued functions with the same amplitude 2^m and h_1, h_2, h_3, h_4, are plateaued functions having the same amplitude 2^l: then, g is a plateaued function with amplitude 2^{m+l+1}.
- If the Walsh transforms of f_1 and f_2 have disjoint supports, as well as of f_3 and f_4 and if the supports of the Walsh transform of h_1 and h_2 are disjoint, as well as those of h_3 and h_4, then, from relation (10), we have Wg (u, v, w) is equal 0 or equal:
$$\frac{1}{2}\times\pm 2^m\times\pm 2^l+\frac{1}{2}\times 2^m\times\pm 2^l=\pm 2^{m+l}$$
then, we deduced that g is a plateaued function with amplitude 2^{m+l}.

A new secondary construction of resilient functions: In this section, we present a new secondary construction of resilient functions on F_2^{n+2} based on the Siegenthaler's construction principle, permitting to obtain resilient functions achieving the best possible trade-offs between resiliency order, algebraic degree, immunity algebraic degree and nonlinearity (that is, achieving Siegenthaler's and Sarkar's *et al.* bound).

Let n, t be positive integers such that $t \prec n$ and let f and h be two n-variable t-resilient functions. Consider the functions $g \in B_{n+2}$ such that

$$g(x, y_1, y_2) = (1 \oplus y_1 y_2) f(x) \oplus (y_1 y_2) h(x) \qquad (16)$$

Where $x \in F_2^n$ and $y_1, y_2 \in F_2$. Note that the truth-table of g can be obtained by concatenating the truth-table of f and h. We have truth-tables:

y1	y2	g (x, y_1, y_2)
0	0	f (×)
0	1	f (×)
1	0	f (×)
1	1	h (×)

The Walsh transforms of g is equal:

$$\begin{aligned} Wg(u, v_1, v_2) &= \sum_{x\in F_2^n / y_1=y_2=0} (-1)^{f(x)+ux} + \\ &\sum_{x\in F_2^n / y_1=0, y_2=1} (-1)^{f(x)+ux+v_2} + \sum_{x\in F_2^n / y_1=1, y_2=0} (-1)^{f(x)+ux+v_1} \\ &+ \sum_{x\in F_2^n / y_1=y_2=1} (-1)^{h(x)+ux+v_2} = Wf(u) + (-1)^{v_1} Wf(u) \\ &+(-1)^{v_2} Wf(u) + (-1)^{v_1+v_2} Wh(u) \\ &= \left(1+(-1)^{v_1}+(-1)^{v_2}\right) Wf(u) + (-1)^{v_1+v_2}) Wh(u) \end{aligned} \qquad (17)$$

Where $u \in F_2^n$ and $v_1, v_2 \in F_2$.

Truth-tables of Walsh transform g is:

v_1	v_2	Wg (u, v_1, v_2)
0	0	3Wf (u) + Wh (u)
0	1	Wf (u) – Wh (u)
1	0	Wf (u) – Wh (u)
1	1	Wh (u) – Wf (u)

The goal of proposition 6 and theorem 2 are to show, while being based on relation 17, how the resiliency and non linearity of g are related to the comportment of the functions f and h.

Proposition 6: Let $g \in B_{n+2}$ be a function defined by 16. Then, if f and h be two functions t-resilient, then the function g is t-resilient. Moreover, if for every $u \in F_2^n$ of Hamming weight t + 1, we have Wf (u) = Wh (u) or Wh (u) = – 3Wf (u), then the function g is a t + 1-resilient.

Proof: If f and h be two functions t-resilient, then for every $u \in F_2^n$ of Hamming weight smaller than or equal to t, the values of Wf (u), Wh (u) are null and it is deduced that the value Wg (u, v1, v2) = $\left(1+(-1)^{v_1}+(-1)^{v_2}\right) Wf(u) + (-1)^{v_1+v_2}) Wh(u)$

is null for every $(v_1, v_2) \in F_2^2$: The functions g is t-resilient. Moreover, if for every $u \in F_2^n$ of Hamming weight t+1, we have the values Wf (u), Wh (u) satisfy, respectively the relations Wh (u) – Wf (u) = 0, then for $v_1 \neq v_2 = 1$, or 3Wf (u)+Wh (u) = 0, then for $v_1 = v_2 = 0$. We have Wg (u, v_1, v_2) = 0 it is deduced that the functions g is a t+1-resilient.

Theorem 2: Let $g \in B_{n+2}$ be a function defined by 16.

- If for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 = v_2 = 0$, then the non linearity of g is obtained from those of f and h in the following way:

(18) $Ng \geq 3NF + Nh$. Moreover, if f and h achieve a maximum possible $2^{n-1} - 2^{t+2}$ nonlinearity and if g is t + 1-resilient, then the nonlinearity $2^{n+1} - 2^{t+2}$ of g is the best possible. If the support of the Walsh transform of f and h are disjoint, then we have

(19) $Ng = 2^{n-1} + \min(3Nf, 2^n + Nh)$; thus, if f and h achieve a maximum possible $2^{n-1} - 2^{t+2}$ nonlinearity, then g achieves a maximum possible $2^{n+1} - 3\times 2^{t+1}$ nonlinearity.

- If for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 \neq v_2$ or $v_1 = v_2 = 1$, we have

(20) $Ng \geq 2^n + Nf + Nh$. Moreover, if f and h achieve a maximum possible $2^{n-1} - 2^{t+2}$ nonlinearity and if g is t + 1-resilient, then the nonlinearity $2^{n+1} - 2^{t+2}$ of g is the best possible. If the support of the Walsh transform of f and h are disjoint, then we have

(21) $Ng = 3\times 2^{n-1} + \min(nf, Nh)$; thus, if f and h achieve a maximum possible $2^{n-1} - 2^{t+1}$ nonlinearity, then g achieves maximum possible nonlinearity $2^{n+1} - 2^{t+1}$.

- If the monomials of highest degree in the algebraic normal forms of f and h are not all the same (i.e. d° f ≠ d° h), then d° g = 2 + max (d° f, d° h).

Proof:

- If for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 = v_2 = 0$, then we deduced from relation (17) the number $\max_{u_1,\ldots,u_{n+2}\in F_2} |Wg(u_1,\ldots,u_{n+2})|$ is clearly upper bounded by $3\max_{u_1,\ldots,u_n\in F_2} |Wf(u_1,\ldots,u_n)| + \max_{u_1,\ldots,u_n\in F_2} |Wh(u_1,\ldots,u_n)|$ using relation (2): This implies the inequality $2^{n+2} - 2Ng \leq 3 \times (2^n - 2Nf) + 2^n - 2Nh$. We deduce that $Ng \geq 3Nf + Nh$. Moreover if $Nf = Nh = 2^{n-1} - 2^{t+1}$, then from relation (18), we have $Ng \geq 2^{n-1} - 2^{t+3}$ and if g is a t + 1-resilient, then from we have $Ng \leq 2^{n+1} - 2^{t+2}$: we deduce that the $2^{n+1} - 2^{t+2}$ nonlinearity of g is the best possible. If the support of the Walsh transform of f and h are disjoint, we deduce also, from the relation (17), that the number $\max_{u_1,\ldots,u_{n+2}\in F_2} |Wg(u_1,\ldots,u_{n+2})|$ is equal to

$$\max(3\max_{u_1,\ldots,u_n\in F_2} |Wf(u_1,\ldots,u_n)|; \max_{u_1,\ldots,u_n\in F_2} |Wh(u_1,\ldots,u_n)|)$$

Using relation (2), we have also $2^{n+2} - 2Ng = \min(3 \times (2^n - 2Nf), 2^n - 2Nh)$ and Ng are equals. Therefore $Ng = 2^{n-1} + \min(3Nf, 2^n + Nh)$. Thus, if f and h achieve a $2^{n-1} - 2^{t+1}$ nonlinearity then from the relation (19), it is clearly that g achieves a maximum possible $2^{n-1} - 3 \times 2^{t+1}$ nonlinearity.

- If for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 \neq v_2$ or $v_1 = v_2 = 1$, then we deduce from relation (17) that $\max_{u_1,\ldots,u_{n+2}\in F_2} |Wg(u_1,\ldots,u_{n+2})| \leq \max_{u\in F_2^n} |Wf(u)| + \max_{u\in F_2^n} |Wh(u)|$

Using relation (2), we have $Ng \geq 2^n + Nf + Nh$. Moreover if f and h achieve a $2^{n-1} - 2^{t+1}$ nonlinearity, then from the relation (20), we deduce $Ng \geq 2^{n+1} - 2^{t+2}$ and if g is a t + 1-resilient, then from we have $Ng \geq 2^{n+1} - 2^{t+2}$: we deduce then that the $2^{n+1} - 2^{t+2}$ nonlinearity of g is the best possible. If the support of the Walsh transform of f and h are disjoint, we deduce also from relation (17) that $\max_{u_1,\ldots,u_{n+2}\in F_2} |Wg(u_1,\ldots,u_{n+2})| = \max\left(\max_{u\in F_2^n} |Wf(u)|, \max_{u\in F_2^n} |Wh(u|\right)$

Using relation (2), we have $2^{n+2} - 2Ng = \text{Min}(2^n - 2Nf, 2^n - 2Nh)$ if f and h achieve a maximum possible $2^{n-1} - 2^{t+1}$ nonlinearity and then from the relation (20) we have $2^{n+1} - 2^{t+1}$

- It is obvious that it d° g = 2 + max (d° f, d° h).

Corollary 2: Let f and h be two n-variable t-resilient functions with disjoint Walsh supports achieving a $2^{n-1} - 2^{t+1}$ nonlinearity such that d° (f + h) = n − t − 1 and if for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 \neq v_2$ or $v_1 = v_2 = 1$. Then the function defined by 16 is n + 2-variable t-resilient function has a n − t + 1 degree and having a $2^{n+1} - 2^{t+1}$ nonlinearity that is achieving Siegenthaler's and Sarkar *et al*'s bounds; note that this construction increases by 2 the degree.

Construction of plateaued functions: We consider now the same construction 16, but applied to plateaued functions instead of resilient functions.

Lemma 2: Let n be positive integer. Let f and h be two plateaued functions having the same amplitude 2^r on F_2^n. Let $g \in B_{n+2}$ be function given by 16 then:

- If for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 = v_2 = 0$ and if for every $u \in F_2^n$ the values of Wf (u) and Wh (u) are simultaneously null, or simultaneously non null, then g is plateaued function with amplitude 2^{r+2} on F_2^{n+2}.
- If for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 \neq v_2$ or $v_1 = v_2 = 1$ and if at least one of the values Wf (u) and Wf (u) is null, then g is a plateaued function with an amplitude 2^r on F_2^{n+2}.

Proof:

- For every $u \in F_2^n$ and for all pair $(v_1, v_2) \in F_2 \times F_2$ we have $Wg(u, v_1, v_2) =$
  $\left(1+(-1)^{v_1}+(-1)^{v_2}\right)Wf(u)+(-1)^{v_1+v_2})Wh(u)$
  If $v_1 = v_2 = 0$ and if f and h are simultaneously null (resp. Simultaneously non null), we deduce that Wg (u, v_1, v_2) is equal to $3 \times (\pm 2^r) + \pm 2^{r+2}$ because f and h are plateaued functions with amplitude 2^r: g is a plateaued function with amplitude 2^{r+2}.
- If for every all pair $(v_1, v_2) \in F_2 \times F_2$ such that $v_1 \neq v_2$ or $v_1 = v_2 = 1$ and if at least one of the values Wf (u) and Wf (u) is null, then also from the relation (17) we have $(u, v_1, v_2) = \pm 2^r$ because f and h are plateaued functions with an amplitude 2^r.

Proposition 7: Let f and h be two n-variable functions with algebraic immunity $AI_n(f) = d_1$ and $AI_n(h) = d_2$. Let $g \in B_{n+2}$ be function given by 16 Then:

- If $d_1 \neq d_2$ the $Ai_{n+2}(g) = 2 + \min\{d_1, d_2\}$.
- If $d_1 = d_2 = d$ then $d \leq AI_{n+2}(g) \leq d + 2$, and $AI_{n+2}(g) = d$ if only if there exist f_1 and $h_1 \in B_n$with algebraic degree d such that $\{f * f_1 = 0, h * h_1 = o\}$ or $\{(1 + f) * f_1 = 0, (1 + h) * h_1 = 0\}$ and $d^\circ g(f_1 + h_1) \leq d - 2$.

Proof: Let $\varphi \in B_n$, by $LDA_n(\varphi)$ we denoted the set of a non null function $\varphi_1 \in B_n$ with lowest possible degree such that $\varphi * \varphi_1 = 0$ or $(1 + \varphi) * \varphi_1 = 0$.

- First time we prove item i. Let us write $\varphi = (1 + y_1y_2)\varphi_1 + y_1y_2\varphi_2 \in LDA_{n+2}(g)$. We first consider the case $g * \varphi = 0$. This implies $(1 + y_1y_2) f * \varphi_1 + y_1y_2 h*\varphi_2 = 0$. So $f * \varphi_1$ and $h * \varphi_1 = 0$. Similarly for the case with $(1 + g) * \varphi = 0$. Thus, we have $(1 + y_1y_2) * (1 + f) * \varphi_1 + y_1y_2 *(1 = h) * \varphi_2 = 0$. We deduce that $(1 + y_1y_2) * (1 + f) * \varphi_1 = 0$ and $y_1y_2 *(1 + h) * \varphi_2 = 0$. Now there can be three cases in both scenarios:
  - φ_1 is zero and φ_2 is non zero. So $d^\circ(\varphi_2) \geq d_2$. This implies $d^\circ(g) \geq d_2 + 2$
  - φ_1 is non zero and φ_2 is zero. So $d^\circ(\varphi_1) \geq d_1$. This implies $d^\circ(g) \geq d_1 + 2$
  - φ_1 and φ_2 are non zero. So $d^\circ(\varphi_1) \geq d_1$ and $d^\circ(\varphi_2) \geq d_2$. This implies $d^\circ(g) \geq 2 + \max\{d_1, d_2\}$. when $d_1 \neq d_2$

  So for $d_1 \neq d_2$, we get $AI_{n+2}(g) \geq 2 + \min\{Ai_n(f), AI_n(h)\}$. (I)

Let $f_1 \in LDA_n(f)$, $h \in LDA_n(h)$. If $f * f = 0$ then we have $(1 + y_1y_2) f_1 * g = 0$.

If $h * h_1 = 0$ then $y_1y_2h_1 * g = 0$. Thus if $(1 + f) * f_1 = 0$ then we have $(1 + y_1y_2) f_1 * (1+g) = 0$. If $(1 + h) * h = 0$ then $y_1y_2 * h_1 * (1 + g) = 0$. We deduce that

$$Ai_{n+2}(g) \leq 2 + \min\{Ai_n(f), Ai_n(h)\}. \quad (II)$$

From equation (I) and (II) we deduce that $Ai_{n+2}(g) \leq 2 + \min\{d_1, d_2\}$.

Let $\varphi = f_1 + y_1y_2(f_1 + h_2) \in LDA_{n+2}(g)$. It is clearly that φ has at least a degree d because f, h has at least a degree d. So $d \leq Ai_{n+2}(g) \leq d + 2$.

If $Ai_{n+2}(g) = d$, then the highest degree term of f_1 and h_1 must be the same which gives $d^\circ(f_1 + h_2) \leq d - 2$. Note that we have $\{f * f = 0, h * h = 0\}$ or $\{(1 + f) * f = 0, (1 + h) * h = 0\}$ and $d^\circ g(f_1 + h_1) \leq d - 2$. Then clearly $Ai_{n+2}(g) = d$.

CONCLUSIONS

We have given a new secondary construction of resilient functions based on the Siegenthaler's construction principal. These constructions permit to increase the cryptographic parameters (algebraic immunity, algebraic degree, resiliency and nonlinearity) and to define many more resilient and plateaued functions where the achieved degree, algebraic immunity, resiliency and nonlinearity are high. Thus, it permits to build resilient functions achieving the best possible trade-offs between resiliency order, algebraic degree and nonlinearity (that is, achieving Siegenthaler's bound and Sarkar *et al.*'s bounds).

REFERENCES

Ars, G. and J.C. Faugère, 2005. Algebraic immunity of functions over finite fields. Workshop on Boolean Functions: Cryptotography and Aapplication. LIFAR, University of Rouen, March 7-8.

Camion, P., C. Carlet, P. Charpin and N. Sendrier, 1992. On correlation immune functions, Advances in Cryptology-CRYPTO 91, 86-100. Springer-Verlag.

Carlet, C., 2001. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. Discrete Mathematics and Theoretical Compu. Sci., pp: 131-144.

Carlet, C. and P. Sarkar, 2002. Spectral domain analysis of correlation and resilient Boolean functions. Finite Fields and Applications, 8: 120-130.

Carlet, C., 2002. A larger class of cryptographic Boolean functions via a study of the Maiorana-Mc Farland construction. Cryptology-CRYPTO 2002, Lecture Notes in Computer Sci., Springer-Verlag, pp: 549- 564.

Carlet, C., 2004. On the secondary constructions of resilient and bent functions. Coding, Cryptography and Combinatorics, Progress in Computer Science and Applied Logic, 23: 3-28.

Carlet, C. and P. Gaborit, 2005. On the construction of balanced Boolean functions with a goode algebraic immunity. Workshop on Boolean Functions: Cryptotography and Application 2005, LIFAR, University of Rouen, March 7-8.

Carlet, C, D.K. Dalai, K.C. Gupta and S. Maitra, 2006. Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction. IEEE Trans. Inform. Theory, (In Press).

Chee, L.S., D. Lee and S.H. Sung, 1996. On the correlation immune functions and their nonlinearity. Advances in Cryptology, Asiacrypt 96, N° 1163, Lecture Notes in Computer Sci., pp: 232 -243, Springer-Verlag.

Courtois, N. and W. Meier, 2002. Algebraic Attacks on Stream Ciphers with Linear Feedback. Advances in cryptology-EUROCRYPT 2003, Lecture Notes in Computer Sci., 2656: 346-359, Springer.

Ding, C., G. Xiao and W. Shan, 1991. The stability theory of stream ciphers, N° 561, Lecture Note in Computer Sci., Springer-Verlag.

Filiol, E. and C. Fontaine, 1998. Highly nonlinear balanced Boolean functions with a good correlation-immunity. Advances in Cryptology-EUROCRYPT 98. Springer-Verlag.

Maitra, S. and P. Sarkar, 1999. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. Advances in Cryptology-CRYPTO 99, N° 1666, Lecture Notes in Computer Sci., pp: 198-215. Springer Verlag.

Maitra, S. and E. Pasalic, 2002. Further constructions of resilient functions with very high nonlinearity. IEEE Trans. Inform. Theory, 48: 1825-1834.

Maitra, S. and P. Sarkar, 2002. Modifications of patterson-wideman Functions for cryptographic applications. IEEE Trans. Inform. Theory, 48: 278-284.

Meier, W., E. Pasalic and C. Carlet, 2004. Algebraic attacks and decomposition of Boolean functions. Advances in Cryptology-EUROCRYPT 2004, Lecture Notes in Computer Sci., Springer Verlag, 3027: 474-491.

Menezes, A., P.V. Oorschot and S. Vanstone, 1997. Handbook of Applied Cryptography, CRC Press.

Pasalic, E., T. Johansson, S. Maitra and P. Sarkar, 2001. New construction of resilient and correlation-immune Boolean functions achieving upper bounds on nonlinearity. Workshop on Coding and Cryptography. Electronic Notes in Discrete Mathematics Elsevier.

Sarkar, P. and S. Maitra, 2000a. Construction of nonlinearity Boolean function with important cryptographic properties. Advences in Cryptology-EUROCRYPT 2000, N° 1807, Lecture Note in Computer Sci., pp: 485-506, Springer-Verlag.

Sarkar, P. and S. Maitra, 2000b. Nonlinearity bounds and construction of résilient Boolean functions. Advances in Cryptology-EUROCRYPT 2000, 1880, Lecture Notes in Computer Sci., pp: 515-532. Springer Verlag.

Seberry, J., X.M. Zhang and Y. Zheng, 1994. On Constructions and nonlinearity of correlation immune Boolean functions. Advances in Cryptology EUROCRYPT 93, pp: 181-199, Springer-Verlag.

Siegenthaler, T., 1984. Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, IT-30: 776-780, September.

Siegenthaler, T., 1985. Decrypting a class of stream ciphers using ciphertext only. IEEE Trans. Computers, C-34: 81-85, January.

Tarannikov, Y.V., 2000. On resilient Boolean functions with maxim um possible nonlinearity. Proceedings of INDOCRYPT 2000, Lecture Notes in Computer Sci., 1977: 19-30.

Tarannikov, Y.V., 2001. New construction of resilient Boolean functions with maximum nonlinearity. Fast Software Encryption, 2355, Lecture Notes in Computer Sci., pp: 66-77.

Xiao, G.Z. and J.L. Massey, 1988. A spectral characterization of correlation-immune combining function. IEEE Trans. Theory Inform., It-34 NR.3: 569-571.

Zheng, Y. and X.M. Zhang, 2000. Improving upper bound cryptographic properties. Advences in Cryptology-EUROCRYPT 2000, N° 1807, Lecture Note in Computer Sci., Springer-Verlag, pp: 485-506.