A Resilient Functions For Stream Cipher Applications: Modified Tarrannikov's Construction And Analysis Of Their Algebraic Immunity

Aissa Belmeguenai, (PhD)
Khaled Mansouri, (PhD)
Rafik Djemili, (PhD)
August 20 University- Skikda LP 26 El-hadeik, Algeria

Abstract

Boolean functions with good cryptographic properties (high algebraic degree, balancedness, high order of correlation immunity and high nonlinearity) have an important significance in stream cipher (combiner model or filter model) since these functions allow to construct stream cipher resistant to various attacks. In this work the modified Tarannikov's construction method is considered. This construction permits to obtain functions achieving all necessary criteria for being used in the pseudo-random generators in stream ciphers. Thus, this allows constructing recursively the resilient function achieving Siegenthaler's bound and Sarkar, et al.'s bound using a resilient function in a smaller number of variables. Finally, we used the modified Tarannikov's construction for designing keystream generators for digital images encryption.

Keywords: Algebraic Immunity, Image Encryption, Nonlinearity, Stream Ciphers, Resilient Function

Introduction

Boolean functions are crucial cryptographic primitives in stream cipher and cryptography in general. In the case of stream cipher (the combiner model or filter model) the Boolean functions are required to have good cryptographic properties: high algebraic degree, balanced, high order correlation immunity, high nonlinearity, and high algebraic immunity degree to counter certain attacks (Berlekamp 1968) - (Armknecht 2004).

Unfortunately, during a research involving construction of Boolean functions in cryptography, we come immediately to the following problem: It is impossible for a Boolean function to satisfy simultaneously and optimally all criteria: high algebraic degree, balancedness, order correlation

immunity highest possible and high nonlinearity. This means a cryptographer to seek compromise.

Siegenthaler showed in (Siegenthaler 1984) that any n-variable Boolean function f used in a stream cipher can both have a high algebraic degree and high order correlations immunity, since its degree is upper bounded by $n-t$. If f is t-th order correlation immune function ($0 \le t \le n$) has algebraic degree smaller than or equal to $n-t$. Moreover, if f is a t-resilient function ($0 \le t \le n$) it has algebraic degree smaller than or equal to $n-t-1$ if $t \le n-2$ and equal to 1 if $t = n-1$.

Sarkar and Maitra proved in (Sarkar 2000) divisibility bound on the Walsh transform values of an *n*-variable, t*-th* order correlation immune (resp. t-resilient) function, with $t \le n-2$: these values are divisible by 2^{t+1} (resp. by 2^{t+2}). This provides a nontrivial upper bound on the nonlinearity of resilient functions (and also of correlation immune functions, but non-balanced functions present less cryptographic interest), independently obtained by Tarannikov (Tarannikov 2000) and by Zheng and Zhang (Zheng 2001): the nonlinearity of any *n*-variable, t-resilient function is upper bounded by $2^{n-1} - 2^{t+1}$. Tarannikov proved that resilient functions achieving this bound must have degree $n-t-1$ (that is, achieve Siegenthaler's bound); thus, they achieve the best possible trade-offs between resiliency order, degree and nonlinearity.

In this paper, the modified Tarannikov's construction method is introduced. This construction permits to increase the cryptographic parameters: algebraic degree, resiliency and nonlinearity and to define many more resilient functions where the degree, resiliency and nonlinearity achieved are high. Thus, to allow obtaining 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).

Preliminaries

In this section, few basic concepts and results are introduced. A Boolean function on n-variable may be viewed as a mapping from F_2^n in to F_2. By $\oplus$ we denote the sum modulo 2. The Hamming weight $wt(f)$ of a Boolean function f on F_2^n is the size of its *support* $\{x \in F_2^n; f(x) = 1\}$.

By (n, t, d, N), we mean an n-variable function, t-resilient function having degree d and nonlinearity N. In the above notation, we may replace some components by $(-)$ if we do not want to specify it.

An n-variable Boolean function f has a unique algebraic normal form (A.N.F): $f(x_1,...,x_n) = a_0 + \sum_{i=0}^{n} a_i x_i + \sum_{1\le i<j\le n} a_{i,j} x_i x_j + ... + a_{1,2,...,n} x_1 x_2 ... x_n$, where the coefficients a_0, a_i, $a_{i,j}$,..., $a_{1,2,...,n}$ belong to F_2.

The Walsh transform of an n-variable Boolean function f defined by

$$Wf(u) = \sum_{x\in F_2^n} (-1)^{f(x)\oplus u\cdot x}, \forall u \in F_2^n \quad (2.1)$$

where $x.u = x_1.u_1 + ... + x_n.u_n$ denotes the usual scalar product of vectors u and x.

The algebraic degree, $\deg(f)$, of a Boolean function f is the number of variables in the highest order term with non zero coefficient. If the 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.

A Boolean function f on F_2^n is balanced if $wt(f) = wt(f \oplus 1)$. In other words, f is balanced if and only if $wt(f) = 2^{n-1}$. Correlation immune functions and resilient functions are two important classes of Boolean functions. Xiao and Massey (Xiao 88) provided a spectral characterization of correlation immunity. A function f is t-th order correlation immune if and only if its Walsh transform satisfies: $Wf(u) = 0$, for $1 \le wt(u) \le t$, where $wt(u)$ denotes the Hamming weight of u, and function f is balanced if moreover $Wf(0) = 0$, $\forall u \in F_2^n$, $0 \le wt(u) \le t$. A balanced t-th order correlation immune function is called t-resilient.

The Boolean functions used in a nonlinear combiner must have high correlation immunity. If the combiner function is not correlation immune then the attacker can find correlations between the keystream and the contents of one of the LFSRs. This allows the attacker to mount a divide and conquer attack in which internal state of each LFSR is recovered independently of the other LFSRs.

Nonlinearity of a Boolean function f measures the distance of the Boolean function from the set of all affine functions. The nonlinearity Nf of an n-variable Boolean function f, can be written as

$$Nf = 2^{n-1} - \frac{1}{2}\max_{u\in F_2^n} |Wf(u)|. \quad (2.2)$$

It is upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$ (we shall call this bound the universal bound), due to Parseval's relation $\sum_{u \in F_2^n} Wf^2(u) = 2^{2n}$.

(2.3)

Boolean functions used in stream ciphers must have high nonlinearity. A high nonlinearity weakens the correlation between the input and output and prevents the attacker from using linear approximations of the function.

The algebraic immunity $AI_n(f)$ of a Boolean function f is the smaller degree of non null function g such that $f * g = 0$ or $(1 \oplus f) * g = 0$. In other words, the minimum value of d such that f or $1 \oplus f$ admits an annihilator of degree d. It has been proven in (Meier 2003) that the algebraic immunity of any *n*-variable Boolean function is upper bounded by $\lceil \frac{n}{2} \rceil$. Hence, if the degree is greater than $\lceil \frac{n}{2} \rceil$, the best possible algebraic immunity is $\lceil \frac{n}{2} \rceil$.

Proposition 1: *(Dalai 2006) Let f be a functions on n variables with an algebraic immunity $AI_n(f) = d$. Let l be an affine function with any of the following properties:*

1. *l is a function on $x_1,...,x_n$*
2. *l is a function on $x_1,...,x_n$ and some other variables.*
3. *l is a function on variable other than $x_1,...,x_n$. Let $f \oplus l$ be a function on r variable. Then $d - 1 \le AI_r(f \oplus l) \le d + 1$ for case 1and 2, and $d \le AI_r(f \oplus l) \le d + 1$ for case 3.*

Tarannikov's Construction

In (Tarannikov 2000), Tarannikov has proposed an important construction of resilient functions. Let g_1 and g_2 be two Boolean functions on F_2^n such that $Ng_1 = Ng_2 = \sigma$, besides g_1 depends on the variables x_i and x_j linearly and g_2 depends on a pair of the variables (x_i, x_j) quasi-linearly. Consider the function
$g(x_1,...,x_{n+2}) = (1 + x_{n+2} \oplus x_{n+1}) g_1(x_1,...,x_n) \oplus (x_{n+2} \oplus x_{n+1}) g_2(x_1,...,x_n) \oplus x_{n+1}$ on F_2^{n+2}. Then, we have:

1. If g_1 and g_2 are t-resilient, then g is (t+1) – resilient. Moreover, g depends on the variables x_{n+1} and x_{n+2} quasi-linearly.

2. $Ng = 2^n + 2\sigma$

- If g_1 and g_2 achieve the maximum possible nonlinearity $2^{n-1} - 2^{t+1}$, then the nonlinearity $2^{n+1} - 2^{t+2}$ of g is the best possible;

Modification of Tarannikov's Construction:

We will propose a modification of Tarannikov's construction. Let us first present the construction.

Construction 1: *Let n, t be positive integers such that $t \prec n$. Let g (n, t, d, Ng). Let $f = x_{n+2} \oplus x_{n+1} \oplus g$ and $h = x_{n+2} \oplus x_n \oplus g^*$ be two $n+2$-variable functions, where $g^*(x_1, x_2, ..., x_{n-1}, x_{n+1}, x_{n+2}) = g(x_1, x_2, ..., x_{n-1}, x_{n+1} \oplus x_{n+2})$ is the function generated from g by replacing the variable x_n by $(x_{n+2} \oplus x_{n+1})$. We construct a function G in $n+4$ variables in the following way, $G = (1 \oplus x_{n+4} \oplus x_{n+3}) f \oplus (x_{n+4} \oplus x_{n+3}) h \oplus x_{n+3}$. Then the following important result is obtained.*

Lemma 1: *Let G be a function of $n+4$ variables as described in Construction 1. Then G is (t+3) – resilient with nonlinearity $NG = 2^{n+2} + 8Ng$. Moreover, G depends on the variables x_{n+3} and x_{n+4} quasilinearly. If g achieves a maximal possible nonlinearity $2^{n-1} - 2^{t+1}$, then nonlinearity $NG = 2^{n+3} - 2^{t+4}$ of G is the best possible and $\deg(G) = 1 + \deg(g)$.*

Proof:

By lemma 4.2 and 4.4 of (Tarannikov 2000) the functions f and h are t+2-resilient functions on F_2^{n+2}, $Nf = Nh = 4Ng = \alpha$. Moreover, the function f depends on the variables x_{n+1}, x_{n+2} linearly, and the function h depends on the variables x_{n+1}, x_{n+2} quasilinearly.

$\deg(f) = \deg(h) = \deg(g)$.

By lemma 5.1 of (Tarannikov 2000) the function G is a t+3-resilient function on F_2^{n+4} with nonlinearity $NG = 2^{n+2} + 2\alpha = 2^{n+2} + 2 \times 4Ng = 2^{n+2} + 8Ng$. Moreover, G depends on the variables x_{n+3} and x_{n+4} quasi-linearly. If g achieves a maximal possible nonlinearity $2^{n-1} - 2^{t+1}$, then. We have $NG = 2^{n+2} + 8Ng = 2^{n+2} + 8(2^{n-1} - 2^{t+1}) = 2^{n+3} - 2^{t+4}$ is the best possible nonlinearity of G.

The construction 1 can be applied iteratively.

Construction 2: *Let G_0 be the initial function of n variables and G_k the constructed function after k-th iteration. Let us denote by G_k^* the function*

generated from G_k *by replacing the variable* x_{n+4k} *by* $(x_{n+4k+2} \oplus x_{n+4k+1})$. *Let* $f_{k+1} = x_{n+4k+2} \oplus x_{n+4k+1} \oplus G_k$ *and* $h_{k+1} = x_{n+4k+2} \oplus x_{n+4k} \oplus G_k^*$. *Then the constructed function at* $k+1$*-th step,* $G_{k+1} = (1 \oplus x_{n+4k+4} \oplus x_{n+4k+3}) f_{k+1} \oplus (x_{n+4k+4} \oplus x_{n+4k+3}) h_{k+1} \oplus x_{n+4k+3}$.

We have following results.

Proposition 2: For $k \succ 0$, $G_k = (1 \oplus F_k) G_0 \oplus F_k G_0^* \oplus H_k$ where $\deg(F_k) = k$ and $\deg(H_k) = k+1$.

Proof:

$G_1 = (1 \oplus x_{n+4} \oplus x_{n+3}) f_1 \oplus (x_{n+4} \oplus x_{n+3}) h_1 \oplus x_{n+3}$

$= (1 \oplus x_{n+4} \oplus x_{n+3}) G_0 \oplus (x_{n+4} \oplus x_{n+3}) G_0^* \oplus (1 \oplus x_{n+4} \oplus x_{n+3})(x_{n+2} \oplus x_{n+1})$

$\oplus (x_{n+4} \oplus x_{n+3})(x_{n+2} \oplus x_n) \oplus x_{n+3}$

$= (1 \oplus F_1) G_0 \oplus F_1 G_0^* \oplus (1 \oplus F_1)(x_{n+2} \oplus x_{n+1}) \oplus F_1 (x_{n+2} \oplus x_n) \oplus x_{n+3}$

$= (1 \oplus F_1) G_0 \oplus F_1 G_0^* \oplus H_1$

where F_1 and H_1 are 1 and 2 degree polynomials respectively.

Let us assume that this is true for some $i \geq 1$, i.e., $G_i = (1 \oplus F_i) G_0 \oplus F_i G_0^* \oplus H_i$, where F_i is a *i*-degree polynomial and H_i is a *i+1*-degree polynomial. We have

$G_{i+1} = (1 \oplus x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i+1} \oplus G_i) \oplus$

$(x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i} \oplus G_i^*) \oplus x_{n+4i+3}$

$= (1 \oplus x_{n+4i+4} \oplus x_{n+4i+3}) G_i \oplus (x_{n+4i+4} \oplus x_{n+4i+3}) G_i^* \oplus (1 \oplus x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i+1}) \oplus$

$(x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i}) \oplus x_{n+4i+3}$

$= (1 \oplus x_{n+4i+4} \oplus x_{n+4i+3})((1 \oplus F_i) G_0 \oplus F_i G_0^* \oplus H_i) \oplus (x_{n+4i+4} \oplus x_{n+4i+3})((1 \oplus F_i^*) G_0 \oplus F_i^* G_0^* \oplus H_i^*)$

$\oplus (1 \oplus x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i+1}) \oplus (x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i}) \oplus x_{n+4i+3}$

Where F_i^* and H_i^* are generated by replacing the variable x_{n+4i} by $(x_{n+4i+2} \oplus x_{n+4i+1})$ in F_i and H_i respectively. Thus,

$G_{i+1} = (1 \oplus F_i \oplus F_i(x_{n+4i+4} \oplus x_{n+4i+3}) \oplus F_i^*(x_{n+4i+4} \oplus x_{n+4i+3})) G_0 \oplus$

$(F_i \oplus F_i(x_{n+4i+4} \oplus x_{n+4i+3}) \oplus F_i^*(x_{n+4i+4} \oplus x_{n+4i+3})) G_0^* \oplus (1 \oplus x_{n+4i+4} \oplus x_{n+4i+3}) H_i \oplus$

$(x_{n+4i+4} \oplus x_{n+4i+3}) H_i^* \oplus (1 \oplus x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i+1}) \oplus$

$(x_{n+4i+4} \oplus x_{n+4i+3})(x_{n+4i+2} \oplus x_{n+4i}) \oplus x_{n+4i+3}$

This implies

$G_{i+1} = (1 \oplus F_{i+1}) G_0 \oplus F_{i+1} G_0^* \oplus H_{i+1}$, where F_{i+1} and H_{i+1} are *i+1* and *i+2* degree polynomials respectively.

Proposition 3*: *Let g be a n-variable function with an algebraic immunity $AI_n(g) = d$. *Let* G *be a function on* $n+4$ *variables a described by construction 1. If* f *and* h *have one of the following properties:*

1. $AI_{n+2}(f) = AI_{n+2}(h) = d$
2. $AI_{n+2}(f) = AI_{n+2}(h) = d+1$
3. $AI_{n+2}(f) \neq AI_{n+2}(h)$

Then $d-1 \leq AI_{n+4}(G) \leq d+3$ *for case 1,* $d \leq AI_{n+4}(G) \leq d+3$ *for case 2 and 3.*

Proof:

First we prove the upper bound. Let φ be a non null function with lowest degree such that $g * \varphi = 0$ or $(1 \oplus g) * \varphi = 0$. Let $g = \alpha \oplus \beta * x_n$ where α, β are functions on $n-1$ variable, free from the variable x_n. According to proposition 2, we get $G = (1 \oplus F_1)g \oplus F_1 g^* \oplus H_1$ where F_1 and H_1 are degree 1 and degree 2 polynomials respectively. So,
$(1 \oplus F_1)g \oplus F_1 g^* = (1 \oplus F_1)(\alpha \oplus \beta * x_n) \oplus F_1(\alpha \oplus \beta * (x_{n+1} \oplus x_{n+2}))$
$= \alpha \oplus \beta * x_n \oplus F_1 * \beta(x_n \oplus x_{n+1} \oplus x_{n+2}) = g \oplus F_1 * \beta * (x_n \oplus x_{n+1} \oplus x_{n+2})$.
If $g * \varphi = 0$, then $G * \varphi * (1 \oplus H_1) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) =$
$((1 \oplus F_1)g \oplus F_1 g^* \oplus H_1) * \varphi * (1 \oplus H_1) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) =$
$(g \oplus F_1 * \beta(x_n \oplus x_{n+1} \oplus x_{n+2}) \oplus H_1) * \varphi * (1 \oplus H_1) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) = 0$.
If $(1 \oplus g) * \varphi = 0$, then $(1 \oplus G) * \varphi * (1 \oplus H_1) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) = 0$.
Hence, $AI_{n+4}(G) \leq d + 2 + 1$.

Now we prove the lower bound. Let $h_1 = x_{n+2} \oplus g(x_1, x_2, ..., x_{n-1}, x_{n+1} \oplus x_{n+2})$, according to proposition 1 case 1, we have $d-1 \leq AI_{n+1}(h_1) \leq d+1$. According to proposition 1 case 3, we have $d \leq AI_{n+2}(f) \leq d+1$ and $d \leq AI_{n+2}(h) \leq d+1$.

If $AI_{n+2}(f) = AI_{n+2}(h) = d$. Following proposition 2 of (Belmeguenai 2009) case 2 and following proposition 1 case 1 we have $AI_{n+4}(G) \geq d-1$.

If $AI_{n+2}(f) = AI_{n+2}(h) = d+1$. Following proposition 2 of (Belmeguenai 2009) case 2 and following proposition 1 case 1 we have $AI_{n+4}(G) \geq d$.

If $AI_{n+2}(f) \neq AI_{n+2}(h)$. Following proposition 2 of (Belmeguenai 2009) case 1 and following proposition 1 case 1 we have $AI_{n+4}(G) \geq d$.

In the following theorem, we present the lower and upper bound on algebraic immunity of G_k in terms of the algebraic immunity of G_0.

Theorem 1: *Let G_0 be the initial function of n variables and G_k the constructed function after k-th iteration described by construction 2. Then:* $AI_n(G_0)-1 \le AI_{n+4k}(G_k) \le AI_n(G_0)+k+2$.

Proof:

Following proposition 3 we have $AI_{n+4k}(G_k) \ge AI_n(G_0)-1$.

Let Φ be a non null function with lowest degree d such that $G_0 * \Phi = 0$ or $(1 \oplus G_0) * \Phi = 0$. Let $G_0 = \mathrm{Y} \oplus \mathrm{Z} * x_n$ where Y, Z are functions on $n-1$ variable, free from the variable x_n. According the proposition 2, we get the function $G_k = (1 \oplus F_k)G_0 \oplus F_k G_0^* \oplus H_k$ where F_k and H_k are degree k and degree $k+1$ polynomials respectively. So,

$(1 \oplus F_k)G_0 \oplus F_k G_0^* = (1 \oplus F_k)(\mathrm{Y} \oplus \mathrm{Z} * x_n) \oplus F_k(\mathrm{Y} \oplus \mathrm{Z} * (x_{n+1} \oplus x_{n+2}))$

$= \mathrm{Y} \oplus \mathrm{Z} * x_n \oplus F_k * \mathrm{Z}(x_n \oplus x_{n+1} \oplus x_{n+2}) = G_0 \oplus F_k * \mathrm{Z} * (x_n \oplus x_{n+1} \oplus x_{n+2})$.

If $G_0 * \Phi = 0$, then $G_k * \Phi * (1 \oplus H_k) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) =$

$((1 \oplus F_k)G_0 \oplus F_k G_0^* \oplus H_k) * \Phi * (1 \oplus H_k) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) =$

$(G_0 \oplus F_k * Z(x_n \oplus x_{n+1} \oplus x_{n+2}) \oplus H_k) * \Phi * (1 \oplus H_k) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) = 0$

.

If $(1 \oplus G_0) * \Phi = 0$, then $(1 \oplus G_k) * \Phi * (1 \oplus H_k) * (1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) = 0$.

Hence, $AI_{n+4}(G_k) \le d + k + 2$.

Improved Resilient Functions used in Previous Keystream Generators:

Example 1: *Let us consider an* $(8,3,4,2^7 - 2^4)$ *initial function*

$G_0 = (x_5 \oplus x_8x_5 \oplus x_8x_6 \oplus x_8x_7)(x_1x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_2x_3) \oplus x_7 \oplus x_6 \oplus x_8x_5$

$\oplus x_8x_6 \oplus x_1x_4 \oplus x_3x_4 \oplus x_2 \oplus x_1$,

this function is optimized considering order of resiliency, nonlinear, algebraic degree. The constructed functions G_1, G_2, G_3 and G_4 are respectively an $(12,6,5,2^{11} - 2^7)$, $(16,9,6,2^{15} - 2^{10})$, $(20,12,7,2^{19} - 2^{13})$ and $(24,15,8,2^{23} - 2^{16})$. These function all are optimized considering order of resiliency, nonlinear, algebraic degree, i.e. the functions that achieve Siegenthaler's and Sarkar, al.'s bounds.

Example 2: *Four $n = 11$, we consider an $(11,6,4,2^{10} - 2^7)$ initial function G_0, the function G_0 used in this example is proposed for ACHTERBAHN-80* (Gammel 2005)*, this function is optimal, i.e. that achieve Siegenthaler's and Sarkar, al.'s bounds. The functions G_1 is an $(15,9,5,2^{14} - 2^{10})$ function. Next*

function G_2 *is an* $(19,12,6,2^{18}-2^{13})$ *function. The function* G_3 *is an* $(23,15,7,2^{22}-2^{16})$ *function. At the next step we have* G_4 *is an* $(27,18,8,2^{26}-2^{19})$ *function. All the functions* G_1, G_2, G_3 *and* G_4 *are achieve Siegenthaler's and Sarkar, al.'s bounds.*

Example 3: *Let us start with an initial* $(13,8,4,2^{12}-2^{9})$ *function* G_0 *proposed for Achterbahn-128/80* (Gammel 2006)*, this function achieve Siegenthaler's and Sarkar, al.'s bounds. The functions* G_1 *an* $(17,11,5,2^{16}-2^{12})$*. The function* G_2 *is an* $(21,14,6,2^{20}-2^{15})$*. The function* G_3 *is an* $(25,17,7,2^{24}-2^{18})$*. The function* G_4 *is an* $(29,20,8,2^{28}-2^{21})$*. The functions* G_1, G_2, G_3 *and* G_4 *all achieve Siegenthaler's and Sarkar, al.'s bounds.*

Conclusion

A modified Tarannikov's construction method is presented. This construction can be applied iteratively, therefore permitting to increase the cryptographic parameters: algebraic degree, resiliency, nonlinearity and algebraic immunity, and to define many more resilient functions where the algebraic degree, resiliency and nonlinearity achieving are high. Thus, the construction permits to design: from any optimal resilient functions achieving Siegenthaler's bound and Sarkar, al.'s bounds a large class of optimal function achieving Siegenthaler's bound and Sarkar, al.'s bounds.

References:

E.R Berlekamp. (1968). *Algebraic Coding Theory*, Mc Grow- Hill, New-York.

C. Carlet. (2010). *Boolean functions for cryptography and error-correcting codes. In Y. Crama and P. Hammer, editors, Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010.* The chapter is downloadable from http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf.

J.Dj. Golic. (1994). *Linear cryptanalysis of stream ciphers. In Fast Software Encryption 1994, Lecture Notes in Computer Science*, N° 1008, pp 154–169. Springer-Verlag, 1994.

T. Siegenthaler. (1985). *Decrypting a class of stream ciphers using cipher text only*, *IEEE Transactions on Computers, C-34*, N°1 pp 81–85, January 1985.

W. Meier and O. Staffelbach. (1988). *Fast correlation attacks on Stream chiper,* In *: Advances in cryptology- EUROCRYPT' 88,* ed. by GÜNTHER (C.G), Lectures Notes in Computer science N° 430, pp 301-314, Springer Verlag, 1988.

R. Forré. (1989). *A fast correlation attack on nonlinearly feedforward _ltered shift-register sequences. In J-J Quisquater and J. Vandewalle, editors, Advances in Cryptology - Eurocrypt '89,* vol 434 of Lecture Notes in Computer Science, pp 586-595. IACR, Springer, April 1989.

A. Canteaut and M. Trabbia. (2000). *Improved fast correlation attacks using parity-check equations of weight 4 and 5. In B. Preneel, editor, Advances in Cryptology - Eurocrypt 2000, vol 1807 of Lecture Notes in Computer Science,* pp 573-588. IACR, Springer, May 2000.

C. Carlet and K. Feng. (2008). *An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In J. Pieprzyk, editor, Advances in Cryptology - Asiacrypt 2008,* vol 5350 of Lecture Notes in Computer Science, pp 425-440.IACR, Springer.

N. Courtois and W. Meier. (2003). *Algebraic Attacks on Stream Ciphers with Linear Feedback, Advances in cryptology– EUROCRYPT 2003, Lecture Notes in Computer Science 2656*, pp. 345-359, Springer,2003.

N. Courtois. (2003). *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback, advances in cryptology–CRYPTO 2003, Lecture Notes in Computer Science 2729*, pp. 177-194, Springer, 2003.

F. Armknecht. (2004). *Improving Fast algebraic Attacks, In FSE 2004*, N° 3017 In Lecture Notes in Computer Science, pp 65-82. Springer Verlag.

T. Siegenthaler. (1984). *Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Transactions on Information Theory*, IT-30, N°5, pp 776–780.

P. Sarkar and S. Maitra. (2000). *Nonlinearity bounds and construction of resilient Boolean functions, In: Advances in Cryptology - EUROCRYPT 2000*, vol. 1880 in Lecture Notes in Computer Science, pp 515–532. Springer Verlag.

Y. V. Tarannikov. (2000). *On resilient Boolean functions with maximum possible nonlinearity, Proceedings of INDOCRYPT 2000,* Lecture Notes in Computer Science 1977, pp 19-30.

Y. Zheng and X. M. Zhang. (2001). *Improving upper bound on the non linearity of high order correlation immune functions, Proceedings of Selected Areas in Cryptography 2000,* Lecture Notes in computer Science 2012, pp 262- 274.

G. Z. Xiao, J. L. Massey. (1988). *A spectral characterization of correlation-immune combining functions, IEEE Trans, Inf. Theory, Vol IT 34, N° 3*, pp. 569-571.

D. K. Dalai. (2006). *On Some Necessary Conditions of Boolean Functions to Resist Algebraic Attacks, Thesis. Applied Statistics Unit Indian Statistical Institute Kolkata*, India.

A. Belmeguenaï, M. Kaddeche, K. Mansouri and N. Derouiche. (2009). *Construction of Resilient Functions by Modified Siegenthaler's Construction, International Review on Computers and Software (IRCOS),* Vol 4, N°4, pp 465-469.

B. M. Gammel, R. Gottfert, O. Kniffler. (2005). *The Achterbahn stream cipher, eSTREAM, ECRYPT Stream Cipher Project,* Report 2005/002, 29 April 2005. http://www.ecrypt.eu.org/stream/papers.html.

B. M. Gammel, R. Gottfert, O. Kniffler. (2006). Achterbahn-128/80, *eSTREAM, ECRYPT Stream Cipher Project,* Report 2006/001. http://www.ecrypt.eu.org/stream/p2ciphers/achterbahn/achterbahn_p2.pdf.