An Alternative Method of Construction of Resilient Functions

Aissa Belmeguenai
Laboratoire de Recherche
en Electronique de Skikda
Université 20 Août 1955- Skikda
BP 26 Route d'El-hadaeik
Skikda 21000, Algeria
Email: belmeguenaiaissa@yahoo.fr

Salim Ouchtati
Laboratoire de Recherche
en Electronique de Skikda
Université 20 Août 1955- Skikda
BP 26 Route d'El-hadaeik
Skikda 21000, Algeria
Email: ouchtatisalim@yahoo.fr

Youcef ZENNIR
Laboratoire d'automatique de Skikda
Université 20 Août 1955- Skikda
BP 26 Route d'El-hadaeik
Skikda 21000, Algeria
Email: y.zennir@univ-skikda.dz

***Abstract*—In this paper, we present the modified Tarannikov's construction. This method allows improving the cryptographic criteria: algebraic degree, resiliency, nonlinearity and algebraic immunity. Thus, we can use this iteratively construction to build: from any optimal resilient functions achieving Siegenthaler's bound and Sarkar et al.'s bound, a large class of optimal function achieving Siegenthaler's bound and Sarkar et al.'s bound.**

***Index Terms*—Resilient Function, Stream Cipher, Siegenthaler's construction, Tarannikov's construction.**

I. Introduction

The Boolean functions are crucial cryptographic primitives in stream cipher and cryptography in general. In the case of the combination of several registers by nonlinear Boolean, these functions must satisfy certain cryptographic properties such as: high algebraic degree, balanced, high order of correlation immunity, high nonlinearity and high algebraic immunity degree to resist different attacks: Berlekamp-Massey algorithm [1] and [2], correlation attack [3], [4], linear attack [5] and algebraic attack[6], [7], [8], [9], [10].

Unfortunately, when searching the constructions of Boolean functions intervening in cryptography, we are immediately faced to the following problem: is it impossible for a Boolean function to satisfy simultaneously and optimally the following criteria: high algebraic degree, balanced, the highest possible order of correlation immunity and high nonlinearity. This means a cryptographer to seek compromise. Most often, in the phase of construction the algorithm.

A. Bent function and algebraic degree

An n-variable Boolean function f is bent, then we have:

- If $n \geq 4$, then we have $deg(f) \leq \frac{n}{2}$;
- If $n = 2$, then we have $deg(f) = 1$;

Where n is even.

An n-variable Boolean function f is bent, then its algebraic degree is upper bounded by $\frac{n}{2}$.

B. Bent Function and Balanced

An n-variable Boolean function f is called balanced if and only if $Wf(u) = 0$. Where Wf is Walsh-Hadamard transform of f. An n -variable Boolean function f is bent if and only if $Wf(u) = 2^{\frac{n}{2}}$, for every $u \in F_2^n$. These two criteria are incompatible. A bent function cannot be balanced.

C. Order of Correlation Immunity and Algebraic Degree

Siegenthaler proved in [11] that any n-variable t-resilient function used in a stream cipher cannot both have a high algebraic degree and high order of correlations immunity, since its degree is upper bounded by $n - t$. If f is t-th order correlation immune function ($0 \leq t \leq n$) has an algebraic degree smaller than or equal to $n - t$. Moreover, if f is t-resilient function ($0 \leq t \leq n$) has an algebraic degree smaller than or equal to $n - t - 1$ if $t \leq n - 2$ and equal to 1 if $t = n - 1$.

D. High Nonlinearity and Correlation Immunity

Sarkar and Maitra demonstrated in [12] that the divisibility bound on the Walsh transform values of an n-variable, t-th order correlation immune (resp. t-resilient) function, with $t \leq n - 2$: these values are divisible by $2^{n-1} - 2^{t+1}$(resp by $2^{n-1} - 2^{t+2}$). This will provide a nontrivial upper bound on the nonlinearity of resilient functions (and also of correlation immune functions, but non-balanced functions present less cryptographic interest). The nonlinearity of any n-variable, t-resilient function is upper bounded by $2^{n-1} - 2^{t+1}$, this is independently obtained by Tarannikov [13] and by Zheng and Zhang [14]. Tarannikov demonstrated that resilient functions achieving this bound must have degree $n - t - 1$ (which is achieving Siegenthaler's bound); thus, they achieve best possible trade-offs between resiliency order, algebraic degree and nonlinearity.

This paper gives a secondary construction of resilient function. The paper is organized as follows. In section two we recall the basic notions and concepts of Boolean functions. In section three we introduce the proposed construction. Finally section four concludes the paper.

II. Preliminaries

A Boolean function on n-variable may be viewed as a mapping from the vector space F_2^n in to F_2. 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 $support\{x \in F_2^n; f(x) = 1\}$. An n-variable Boolean function f has unique algebraic normal form (ANF):

$f(x_1, \cdots, x_n) = a_0 \oplus \sum_{1 \le i \le n} a_i x_i \oplus \sum_{1 \le i \prec j \le n} a_{ij} x_i x_j \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n$.

Where the coefficients $a_0, a_i, a_{ij}, a_{12\cdots n}$ belong to F_2.

The algebraic degree $deg(f)$ of a Boolean function f is defined as the number of variables in the longest term of f. If the algebraic degree of f is smaller than or equal to one then f is called affine function. An affined function with a constant term equal to zero is called a linear function. Let f be Boolean function on F_2^n. Then the Walsh-Hadamard transform of f is defined as:

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

Where $u \cdot x = u_1 x_1 \oplus \cdots \oplus u_n x_n$, denotes the usual scalar product of vectors u and x.

The nonlinearity Nf of an n-variable function f is the minimum distance from the set of all n-variable affine function, it is equal to:

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

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.

A Boolean function f on F_2^n is balanced if $wt(f) = wt(1 \oplus f)$. 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 [15] provided a spectral characterization of correlation immune. A function f is $t-th$-order correlation immune if and only if its Walsh transform satisfies: $Wf(u) = 0$, for all $\forall u \in F_2^n$, such that $1 \le wt(u) \le t$, where $wt(u)$ denotes the Hamming weight of u, and function f is balanced if moreover $Wf(0) = 0$. A balanced $t-th$ order correlation immune functions are called t-resilient functions. They are characterized by the fact that $Wf(u) = 0$ for all $\forall u \in F_2^n$, such that $0 \le wt(u) \le t$.

A Boolean function f on F_2^{n+m} depends on the variables $x_{n+1}, ..., x_{n+m}$ linearly if f can be represented in the form :

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

A Boolean function f on F_2^n depends on the variables x_i and x_j quasilinearly if we can represent f in the following form:

$$f(x) = h(y) \oplus x_i \quad (4)$$

Where $y = (x_1, ..., x_{i-1}, x_{i+1}, ..., x_{j-1}, x_{j+1}, ..., x_n, x_i \oplus x_j)$.

By (N, t, d, N) , we denote a 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.

Proposition 1: [11] Let f be a Boolean function on F_2^{n+m}. Then if f depends on the variables $x_{n+1}, ..., x_{n+m}$ linearly, then f is a $(t + m)$-resilient function with nonlinearity $Nf = 2^m Nh$, where h is a t-resilient function used in the representation of f in the form 3;

Proposition 2: [13] Let f be a boolean function on F_2^n. Then if f depends on the variables x_i and x_j quasilinearly, then f is a $t + 1$-resilient function with nonlinearity $Nf = 2Nh$, where h is a t-resilient function used in the representation of f in the form 4.

Proposition 3: [13] Let f_1 and f_2 be two t-resilient Boolean functions on F_2^n such that $Nf_1 = Nf_2 = N_0$. Moreover assume f_1 depends on the variables x_i and x_j linearly and f_2 depends on a pair of the variables (x_i, x_j) quasilinearly. Then the function $f(x_1, ..., x_{n+1}) = (1 \oplus x_{n+1}) f_1(x_1, ..., x_n) \oplus x_{n+1} f_2(x_1, ..., x_n)$ is a t-resilient function on F_2^{n+1} with nonlinearity $Nf = 2^{n-1} + N_0$.

Proposition 4: [16] Let g be Boolean function on F_2^n and l be a affine function on F_2^m. Let $g + L$ be a function on s variables. If l is a function on $x_{n+2}, ..., x_{n+m}$ and x_n, then, we have

$AI_n(g) - 1 \le AI_s(g + l) \le AI_n(g) + 1$.

If l is a function on $x_{n+1}, x_{n+2}, ..., x_{n+m}$, then, we have

$AI_n(g) \le AI_s(g + l) \le AI_n(g) + 1$.

Proposition 5: [17] Let f_1 and f_2 be two n-variable functions with $AI_n(f_1) = d_1$ and $AI_n(f_2) = d_2$. Let $f(x_1, ..., x_{n+1}) =$

$(1 \oplus x_{n+1}) f_1(x_1, ..., x_n) \oplus x_{n+1} f_2(x_1, ..., x_n)$ be function on F_2^{n+1}. Then:

If $d_1 = d_2 = d$, then $d \le AI_{n+1}(f) \le d + 1$.

If $d_1 \ne d_2$, then $AI_{n+1}(f) = min(d_1, d_2) + 1$.

III. Proposed Construction

In [11] Siegenthaler proposed a construction of resilient functions. Tarannikov has proposed in [13] an important construction of resilient functions. In this section, we will propose a construction of resilient function based on the combination between the Siegenthaler's construction and Tarannikov's construction. Let us first present the construction.

Construction 1: Let n, m and t be positive integers such that $t \prec n$ and $2 \le m$. Let g_0 be (n, t, d, N_0) the Boolean function. Let g_0^* be boolean function generated from g_0 by replacing the variable x_n with $(x_{n+1} \oplus x_{n+2})$. Let $f_1 = l_1 \oplus g_0$ and $f_2 = l_2 \oplus g_0^*$ be two Boolean functions on F_2^{n+m} . Where l_1 and l_2 are two affine functions on F_2^m defined respectively by $l_1 = x_{n+1} \oplus x_{n+2} \oplus ... \oplus x_{n+m}$ and $l_2 = x_n \oplus x_{n+2} \oplus ... \oplus x_{n+m}$. We construct the function g_1 in $(n + m + 1)$-variable in the following way: $g_1 = (1 \oplus x_{n+m+1}) f_1 \oplus x_{n+m+1} f_2$. Then the following important results are obtained.

Theorem 1: Let g_1 be a function defined by construction 1. Then g_1 is an $(n+m+1)$-variale $(t+m)$-resilient function has algebraic degree $d + 1$. Moreover: $Ng_1 = 2^{n+m-1} + 2^m N_0$.

Proof :

By proposition 1 the function f_1 is $(t+m)$-resilient function on F_2^{n+m} with nonlinearity $Nf_1 = 2^m N_0$. Moreover, f_1 depends on the variables $x_{n+1}, ..., x_{n+m}$ linearly.

Let $h = x_n \oplus x_{n+2} \oplus g_0^*$. By proposition 2 the function h is $(t+2)$-resilient function on F_2^{n+2} has nonlinearity $Nh = 4N_0$. Moreover, h depends on the variables x_{n+1} and x_{n+2} quasilinearly.

By proposition 1 the function $f_2 = x_{n+3} \oplus ...x_{n+m} \oplus h$ is $(t+m)$-resilient function on F_2^{n+m} with nonlinearity $Nf_2 = 2^{m-2}Nh = 2^m N_0$.

By proposition 3 the function g_1 is an $(n+m+1)$-variable $(n+m)$-resilient function has nonlinearity $Ng_1 = 2^{n+m-1} + 2^m N_0$.

It is obvious that it $deg\,(g_1) = deg\,(g_0) + 1$.

Corollary 1: In the construction 1, if g_0 is a $\left(n, t, d, 2^{n-1} - 2^{t+1}\right)$ function. Then the function g_1 defined by construction 1 is an

$\left(n+m+1, t+m, d+1, 2^{n+m-1} - 2^{t+m+1}\right)$.

Lemma 1: Let g_1 be a function defined by construction 1. Then

$AI_n(g_0) \leq AI_{n+m+1}(g_1) \leq AI_n(g_0) + 3$.

Proof :

First we prove the lower bound. Let algebraic immunity of g_0 be d, so $AI_n(g_0^*) = d$. By proposition 4 we have $AI_{n+m}(f_1) \geq d$ and by proposition 4 we have $AI_{n+m}(f_2) \geq d-1$. Then by proposition 5, we have $AI_{n+m+1}(g_1) \geq d$.

Now we prove the upper bound. Let $g_1 = (1 \oplus x_{n+m+1})\, f_1 \oplus x_{n+m+1} f_2 = (1 \oplus x_{n+m+1})(l_1 \oplus g_0) \oplus x_{n+m+1}(l_2 \oplus g_0^*) = (1 \oplus x_{n+m+1})g_0 \oplus x_{n+m+1}g_0^* \oplus (1 \oplus x_{n+m+1})l_1 \oplus x_{n+m+1}l_2 = (1 \oplus x_{n+m+1})g_0 \oplus x_{n+m+1}g_0^* \oplus \alpha$, where $\alpha = (1 \oplus x_{n+m+1})l_1 \oplus x_{n+m+1}l_2$ has degree 2.

Let $h \neq 0$ be boolean function such that $g_0 * h = 0$ or $(1 \oplus g_0) * h = 0$. Let $g_0 = \varphi \oplus \phi x_n$, where φ and ϕ are functions on $n-1$ variables, free from the variable x_n. So $(1 \oplus x_{n+m+1})g_0 \oplus x_{n+m+1}g_0^* = (1 \oplus x_{n+m+1})(\varphi \oplus \phi x_n) \oplus x_{n+m+1}(\varphi \oplus \phi(x_{n+1} \oplus x_{n+2})) = x_{n+m+1}\phi(x_n \oplus x_{n+1} \oplus x_{n+2}) \oplus g_0$.

If $g_0 * h = 0$ then $g_1 * (1 \oplus \alpha)(1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) * h = = x_{n+m+1}\phi(x_n \oplus x_{n+1} \oplus x_{n+2}) \oplus g_0 \oplus \alpha) * (1 \oplus \alpha)(1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) * h = 0$.

If $(1 \oplus g_0) * h = 0$ then $(1 \oplus g_1) * (1 \oplus \alpha)(1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) * h = 1 \oplus x_{n+m+1}\phi(x_n \oplus x_{n+1} \oplus x_{n+2}) \oplus g_0 \oplus \alpha) * (1 \oplus \alpha)(1 \oplus x_n \oplus x_{n+1} \oplus x_{n+2}) * h = 0$. Thus $AI_{n+m+1}(g_1) \leq d+3$.

The construction 1 can be applied iteratively.

IV. Conclusion

In this work a modified Tarannikov's construction method with extended number of variables is presented. The construction permitted to increase the cryptographic parameters such as: algebraic degree, resiliency order, nonlinearity and algebraic immunity degree, it enables also to define many resilient functions having interesting cryptographic properties. Thus, we can use this iteratively construction to build: from any optimal resilient functions achieving Siegenthaler's bound and Sarkar et al.'s bound, a large class of optimal functions achieving Siegenthaler's bound and Sarkar et al.'s bound.

References

[1] E.R Berlekamp, Algebraic Coding Theory, Mc Grow- Hill, New- York, 1968.

[2] J.L Massey, Shift-Register synthesis and BCH decoding, IEEE Transactions on Information Theory, Volume IT-15, p 122-127, 1969.

[3] T. Siegenthaler, Decrypting a class of stream ciphers using cipher text only, IEEE Transactions on Computers, C-34, N 1, p 81-85, January 1985.

[4] W. Meier and O. Staffelbach, Fast correlation attacks on Stream chiper, In Advances in cryptology- EUROCRYPT'88, éd. Par GÜNTHER (C.G), Lectures Notes in Computer science N 430, p 301-314, Springer Verlag, 1988.

[5] J.Dj. Golic, Linear cryptanalysis of stream ciphers, In Fast Software Encryption 1994, Lecture Notes in Computer Science, N 1008, pp 154-169. Springer-Verlag, 1994.

[6] N. Courtois, J. Pieprzyk, Cryptanalysis of block ciphers with overde-fined systems of equations, In Advances in Cryptology ASIACRYPT 2002, N 2501 in Lecture Notes in Computer Science, p 267-287. Springer Verlag, 2002.

[7] N. Courtois and W. Meier, Algebraic Attacks on Stream Ciphers with Linear Feedback, Advances in cryptology EUROCRYPT 2003, Lecture Notes in Computer Science 2656, p 346-359, Springer,2003.

[8] N. Courtois, Fast Algebraic Attacks on Stream Ciphers with Linear Feedback, Advances in cryptology CRYPTO 2003, Lecture Notes in Computer Science 2729, p 177-194, Springer, 2003.

[9] D. H. Lee et al, *Algebraic Attacks on Summation Generators*, In FSE 2004, N 3017 in Lecture Notes in Computer Science, p 34-48, Springer Verlag, 2004.

[10] W. Meier, E. Pasalic, C. Carlet, Algebraic attacks and decomposition of Boolean functions, In Advances in Cryptology - EUROCRYPT 2004, N 3027 in Lecture Notes in Computer Science, p 474-491, Springer Verlag, 2004.

[11] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Transactions on Information Theory, IT-30, N 5 p 776-780, September 1984.

[12] P. Sarkar and S. Maitra, Nonlinearity bounds and construction of resilient Boolean functions, In Advances in Cryptology EUROCRYPT 2000, vol 1880 in Lecture Notes in Computer Science, p 515-532, Springer Verlag, 2000.

[13] Y. V. Tarannikov, On resilient Boolean functions with maximum possible nonlinearity, Proceedings of INDOCRYPT 2000, Lecture Notes in Computer Science 1977, p 19-30, 2000.

[14] Y. Zheng and X. M. Zhang, 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, p 262-274, 2001.

[15] G. Z. Xiao, J. L. Massey, A spectral characterization of correlation-immune combining functions, IEEE Trans, Inf. Theory, Vol IT 34, N 3, p 569-571, 1988.

[16] D. K. Dalai, K. C. Gupta et S. Maitra, Results on Algebraic Immunity for Cryptographically Significant Boolean Functions, Indocrypt 2004, Chennai, India, December 20-22, p 92-106, N 3348 in Lecture Notes in Computer Science, Springer Verlag, 2004.

[17] C. Carletet et al, Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction, IEEE Transactions on Information Theory 52 (2006) p 3105-3121, 2006.