A New Class of Correlation Immune Functions with High Nonlinearity and Growing Algebraic Immunity

Anton BOTEV
Moscow State Lomonosov University, Russia

Abstract. We present a new large family of correlation immune Boolean functions having high nonlinearity. This family includes some known classes of highly nonlinear m-resilient functions as particular cases. We state that functions of this family have a growing algebraic immunity (together with the growth of inputs). Velocity of such a growth is at least $\Omega(\sqrt{n})$.

Keywords. Boolean functions, correlation immunity, algebraic immunity, nonlinearity

Introduction

In this paper we give consideration to certain tradeoffs between some important cryptographical parameters of balanced Boolean functions, namely: nonlinearity, correlation immunity and algebraic immunity. Such a parameters are considered as crucial when using Boolean functions as generating functions in Linear Feedback Shift Registers. They have complex tradeoffs between each another, so there is no function having even two optimal parameters at the same time. So, the general approach in learning cryptographically 'good' functions is to fix some of the parameters and try to tune up the others.

Historically the first tradeoff of such a kind was the tradeoff between nonlinearity and correlation immunity. Three groups of researchers, Sarkar and Maitra [10], Tarannikov [11], Zheng and Zhang [13], had proven that For an n-variable mth order correlation immune Boolean function f, $n - m \geq 1$, the inequality $nl(f) \leq 2^{n-1} - 2^m$ holds. Moreover, if f is balanced (i. e. m-resilient), $n - m \geq 2$, then $nl(f) \leq 2^{n-1} - 2^{m+1}$. Moreover, Tarannikov had built ([12]) a recursive (growing with respect to n sequence of m-resilient functions having best possible nonlinearity ($0.6n - 1 \leq m \leq n - 2$). Further we propose a family of functions having Tarannikov's construction as a particular case.

After that Pasalic, Maitra, Johansson and Sarkar had proposed ([9]) another recursive construction of functions with maximal nonlinearity based on Tarannikov's functions. These functions are the particular case of our construction, too.

Then, fixing both nonlinearity and correlation immunity we can check up the value of a relatively new ([8]) concept of algebraic immunity. The notion of algebraic immunity was emerged with appearance of algebraic attack proposed in 2005 ([2]). High algebraic immunity may conflict with other criteria. Existing examples ([4], [1]) have not good enough other cryptographically important parameters, or they are not controlled.

It turned out, however, that for a new family of Boolean functions the value of algebraic immunity is growing together with the growth of inputs n (and, accordingly, of nonlinearity and of correlation immunity), with velocity not less than $\Omega(\sqrt{n})$.

1. Basic Definitions and Background

We consider the binary vector space of n-variable Boolean functions, i.e. the space of functions from F_2^n to F_2. Every Boolean function can be written in an unique way as an n-variable polynomial over F_2^n where the degree of each variable is at most 1 using Algebraic Normal Form (ANF):

$$f(x_1, \ldots, x_n) = \bigoplus_{a_1, \ldots, a_n \in F_2^n} g(a_1, \ldots, a_n) x_1^{a_1} \cdots x_n^{a_n},$$

where g is also function over F_2^n. Algebraic degree of f ($degf$ is the number of variables in the longest component of ANF. Function is said to be Affine iff $degf \leq 1$. Weight of Boolean function f (or $wt(f)$)is a number of vectors x over F_2^n such that $f(x) = 1$. Distance between functions f and g is a weight of $f \oplus g$. Function f is said to be balanced if $wt(f) = wt(f \oplus 1) = 2^{n-1}$.

Nonlinearity of f is a minimal distance between f and a set of all the affine functions.

Boolean function f is said to be correlation immune of order m if output and every m inputs of f are statistically independent. If in addition f is balanced then it is said to be m-resilient. Correlation immunity of f is the maximal value of m holding m-immunity of f.

Finally, algebraic immunity of f is the minimal degree of nontrivial annihilator either of f or of $f + 1$, i.e. the minimal degree of a function g such that either $f \cdot g = 0$ or $(f + 1) \cdot g = 0$).

1.1. Known Tradeoffs between Cryptographically Significant Properties

1.1.1. Correlation Immunity vs Nonlinearity

Sarkar, Maitra [10], *Tarannikov* [11], *Zheng, Zhang* [13], 2000:

For an n-variable mth order correlation immune Boolean function f, $n - m \geq 1$, the inequality $nl(f) \leq 2^{n-1} - 2^m$ holds. Moreover, if f is balanced (i. e. m-resilient), $n - m \geq 2$, then $nl(f) \leq 2^{n-1} - 2^{m+1}$.

Tarannikov, Fyodorova, 2000 [6]:

Constructions of n-variable m-resilient Boolean functions with the maximum possible nonlinearity $2^{n-1} - 2^{m+1}$ for $m \geq 0.5902...n(1 + o(1)$.

1.1.2. Correlation Immunity vs Algebraic Immunity

No certain tradeoffs so far.

1.1.3. Nonlinearity vs Algebraic Immunity

Dalai, Gupta, Maitra, 2004 [3]:

$$nl(f) \geq \sum_{i=0}^{AI(f)-2} \binom{n}{i}.$$

Lobanov, 2005 [7]:

$$nl(f) \geq 2^{n-1} - \sum_{i=AI(f)-1}^{n-AI(f)} \binom{n-1}{i} = 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}.$$

Lobanov's bound is tight for all possible pairs of n and $AI(f)$.

1.2. Other known results

Courtois, Meier, 2003 [2]:
For any Boolean function f of n variables $AI(f) \leq \lceil \frac{n}{2} \rceil$.

Didier, 2006 [5]:
"Almost all" balanced Boolean functions f of n variables have algebraic immunity approximately $n/2$.

1.3. Constructions of Functions with High Immunity

Here we give examples of functions having high correlation immunity or high algebraic immunity. Note that there is no construction having both good algebraic immunity and good correlation immunity so far.

1.3.1. Algebraic Immunity

Dalai, Gupta, Maitra, 2005 [4]:
Functions with maximum possible algebraic immunity $\lceil \frac{n}{2} \rceil$ — recursive and direct constructions.
Nonlinearity is not quite good, however, most of other cryptographically important parameters are not controlled.

Braeken, Preenel, 2005 [1]:
Algebraic immunity of some classes of symmetric functions.

1.3.2. Correlation Immunity — Tarannikov's Construction [12]

Let $f_{n,1} \in F_2^n$ be m-resilient function and $f_{n+1,2} \in F_2^{n+1}$ be $(m+1)$-resilient function $(m \leq n-2)$, and $\mathrm{nl}(f_{n,1}) = 2^{n-1} - 2^{m+1}$, $\mathrm{nl}(f_{n+1,2}) = 2^n - 2^{m+2}$ (both nonlinearities are maximal). Moreover, let $f_{n+1,2}$ have some cryptographic property (existence of a pair of quasilinear variables).

Then there exist $f_{n+3,1} \in F_2^{n+3}$ and $f_{n+4,2} \in F_2^{n+4}$ so that $f_{n+3,1}$ is $(m+2)$-resilient and $f_{n+4,2}$ is $(m+3)$-resilient, and nonlinearities of $f_{n+3,1}$ and $f_{n+4,2}$ are maximal, too, and $f_{n+4,2}$ has a pair of quasilinear variables.

Construction takes place for $0.6n - 1 \leq m \leq n - 2$.

1.3.3. Correlation Immunity — Pasalic et al's Construction [9]

Let $H^0 \in F_2^n$ be the *initial function* (having some cryptographic property) and H^i be the ith function (after i iterations). Let H^0 be m-resilient and have a maximal nonlinearity.

Then let $H^{i'}$ be H^i with x_{n+3i} having changed to $x_{n+3i+1} + x_{n+3i+2}$. Further, let F^{i+1} be $H^i + x_{n+3i+1} + x_{n+3i+2}$ and let G^{i+1} be $H^{i'} + x_{n+3i} + x_{n+3i+2}$.

Then H^{i+1} is the concatenation of F^{i+1} and G^{i+1}. Moreover, H^{i+1} is $(m+2i)$-resilient and have a maximal possible nonlinearity, and H^{i+1} has the same needed cryptographic property what has H^0.

2. Generalization of Tarannikov and Pasalic *et al*'s Constructions

Here we present a generalization of known recursive constructions of functions with maximal nonlinearity and announce that this generalization has maximal nonlinearity indeed and that this construction provides nonlinearity at least $\Omega(\sqrt{n})$.

2.1. Constructing

Let $0.6n - 1 \leq m \leq n - 2$. Let $f_{n,0}$ and $f_{n,1}$ are m-resilient Boolean functions on ${F_2}^n$ having maximal nonlinearities $2^{n-1} - 2^{m+1}$ both. Let they have a pair of variables (linear for $f_{n,0}$ and quasilinear for $f_{n,1}$; definition of quasilinearity one can find in [12]).

Then $f_{n+3,0}$ and $f_{n+3,1}$ are $m+2$-resilient Boolean functions on ${F_2}^{n+3}$ having maximal nonlinearities $2^{n+2} - 2^{m+3}$ both. Moreover, they have a pair of variables which linear for $f_{n+3,0}$ and quasilinear for $f_{n+3,1}$. These functions are definited as follows:

$$f_{n+3,0} = x_{n+1}(f_{n,0} + f_{n,1}) + \sigma_{n,0} + x_{n+2} + x_{n+3} + h_{n,0},$$
$$f_{n+3,1} = x_{n+1} + x_{n+2}(f_{n,0} + f_{n,1} + \sigma_{n,1}) + x_{n+3}(f_{n,0} + f_{n,1} + \sigma_{n,1} + 1) + h_{n,1},$$

where $h_{n,0}, h_{n,1} \in \{f_{n,0}, f_{n,1}, 1 + f_{n,0}, 1 + f_{n,1}\}$ and $\sigma_{n,0}, \sigma_{n,1} \in \{0, 1\}$.

Constructions of Tarannikov and of Pasalic *et al* are the particular cases of this construction. Particular values of $h_{n,0}, h_{n,1}, \sigma_{n,0}, \sigma_{n,1}$ are as follows:

- Tarannikov's construction:
  $h_{n,0} = f_{n,1}$,
  $h_{n,1} = f_{n,1}$,
  $\sigma_{n,0} = 0$,
  $\sigma_{n,1} = 1$.
- Pasalic *et al*'s construction:
  $h_{n,0} = f_{n,0}$,
  $h_{n,1} = f_{n,0}$,
  $\sigma_{n,0} = 1$,
  $\sigma_{n,1} = 1$

It's easy to see that the number of possible functions after ith iteration is 64^i.

2.2. Nonlinearity and Algebraic immunity

Here we announce some properties of given construction. The next theorem shows that functions obtained from the construction have a maximal possible nonlinearity:

Theorem. *Let $f^{(i)}$ be an m-resilient Boolean function obtained from $f_{n,0}$ and $f_{n,1}$ after i iterations. Then* $\mathrm{nl}(f^{(i)}) = 2^{n-1} - 2^{m+1}$.

The next theorem states that an algebraic immunity of functions are growing with the velocity not less than $\Omega(\sqrt{n})$.

Theorem. *Let $f_{n,0}$ and $f_{n,1}$ be initial functions of construction, and $k = \max\{AI(f_{n,0}, AI(f_{n,1})\}$. Then after at most i iterations $f^{(i)}_{n,0}$ and $f^{(i)}_{n,1}$ have algebraic immunities strictly greater than k.*

Corollary. *This recursive construction provides Algebraic immunity at least $\Omega(\sqrt{n})$.*

Conclusion

Thus, wide class of recursive m-resilient ($0.6n - 1 \leq m \leq n - 2$) functions is obtained. Functions from this class have the best possible tradeoff between correlation immunity and nonlinearity and growing algebraic immunity.

References

[1] Braeken A., Preneel B., On the algebraic immunity of symmetric Boolean functions, Paper 2005/245 in http://eprint.iacr.org/.

[2] Courtois N., Meier W., Algebraic attacks on stream ciphers with linear feedback, Advanced in Cryptology: Eurocrypt 2003, Warsaw, Poland, May 4–8, 2003, Proceedings, Lecture Notes in Computer Science, V. 2656, pp. 345–357, Springer-Verlag, 2003.

[3] Dalai D.K., Gupta K.C., Maitra S., Results on Algebraic immunity for cryptographically significant Boolean functions, Indocrypt 2004, Lecture Notes in Computer Science, V. 3348, pp. 92–106, Springer-Verlag, 2004.

[4] Dalai D.K., Gupta K.C., Maitra S., Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity, FSE 2005, Lecture Notes in Computer Science, V. 3557, pp. 98–111, Springer-Verlag, 2005.

[5] Didier F., Tillich J.-P., Computing the Algebraic Immunity Efficiently, FSE 2006, Lecture Notes in Computer Science, V. 4047, pp. 359–374, Springer-Verlag, 2006.

[6] Fedorova M., Tarannikov Yu., On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Lecture Notes in Computer Science, V. 2247, pp. 254–266, Springer-Verlag, 2001.

[7] Lobanov M., Tight Bound between Nonlinearity and Algebraic Immunity, Paper 2005/441 in http://eprint.iacr.org/.

[8] Meier W., Pasalic E., Carlet C., Algebraic attack and decomposition of Boolean functions, Proceedings of Eurocrypt 2004, Interlaken, Switzerland, May 2–6, 2004, Lecture Notes in Computer Science, V. 3027, pp. 474–491, Springer-Verlag, 2004.

[9] Pasalic E., Maitra S., Johansson T, Sarkar P., New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity, Workshop on Coding and Cryptography - WCC 2001, Paris, January 8–12, 2001, Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

[10] Sarkar P., Maitra S., Nonlinearity bounds and constructions of resilient boolean functions, In Advanced in Cryptology: Crypto 2000, Proceedings, Lecture Notes in Computer Science, V. 1880, pp. 515–532, Springer-Verlag, 2000.

[11] Tarannikov Yu., On resilient Boolean functions with maximal possible nonlinearity, Proceedings of Indocrypt 2000, Calcutta, India, December 10–13, 2000, Lecture Notes in Computer Science, V. 1977, pp. 19–30, Springer-Verlag, 2000.

[12] Tarannikov Yu., New constructions of resilient Boolean functions with maximal nonlinearity // Fast Software Encryption. 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001. Revised Papers, Lecture Notes in Computer Science, V. 2355, 2002, pp. 66-77.

[13] Zheng Y., Zhang X.-M., Improved upper bound on nonlinearity of high order correlation immune functions, Lecture Notes in Computer Science, V. 2012, pp. 264–274, Springer Verlag, 2001. (Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptography (SAC (2000), pp. 258–269, August 2000).