Paper

Random generation of Boolean functions with high degree of correlation immunity

Anna Grocholewska-Czuryło

Abstract—In recent years a cryptographic community is paying a lot of attention to the constructions of so called resilient functions for use mainly in stream cipher systems. Very little work however has been devoted to random generation of such functions. This paper tries to fill that gap and presents an algorithm that can generate at random highly nonlinear resilient functions. Generated functions are analyzed and compared to the results obtained from the best know constructions and some upper bounds on nonlinearity and resiliency. It is shown that randomly generated functions achieve in most cases results equal to the best known designs, while in other cases fall just behind such constructs. It is argued that the algorithm can perhaps be used to prove the existence of some resilient functions for which no mathematical prove has been given so far.

Keywords—cryptography, ciphers, Boolean functions, correlation immunity, reslilience, random generation.

1. Introduction

Boolean functions play an important role in virtually any modern cryptographic system – be it block or stream ciphers, private or public key systems, authentication algorithms, etc. As security of these systems relies on Boolean functions these functions should posses some specific criteria that would protect a cryptographic system from any existing cryptanalytic attacks, and preferably make it also immune against any attacks that might be designed in the future. These criteria are called cryptographic criteria.

It is widely accepted among cryptologists that most important criteria are balancedness, high nonlinearity, propagation criteria, correlation immunity, high algebraic degree. Unfortunately no Boolean function exists that would fulfil all of these criteria to the maximum, so finding a cryptographically strong Boolean functions is always a trade-off between these criteria and is not a trivial task.

In particular, a functions whose output leaks no information about its input values is of great importance. Such functions are called correlation immune Boolean functions and were introduced by T. Siegenthaler in 1984 [32] and ever since then have been a topic of active research. A balanced correlation immune function is called a resilient function. As balancedness is one criterion that should be fulfilled under any circumstances, resilience is a criterion most often mentioned in the scientific literature when one talks about correlation immunity.

Most of the cryptographic criteria is in one way or another related to nonlinearity of the Boolean function. Highest nonlinearity is very desirable so most of the research concentrates on fulfilling the cryptographic criteria while maintaining a highest possible nonlinearity, which very often (virtually always) has to be sacrificed to some extent.

The approach to finding a good cryptographic functions is most often based on specific algebraic constructions of Boolean functions with desirable properties – like highly nonlinear Boolean function with high order of resiliency. Or constructing bent functions (functions with highest possible nonlinearity) and then modifying them to fulfil other cryptographic criteria.

In the article the author argues that the use of randomly chosen Boolean functions with good cryptographic properties (if we are able to find such functions) is probably better than the use of functions with similar parameters which are obtained by explicit constructions. The main reason is that explicit constructions usually lead to functions which have very particular (algebraic or combinatorial) structures, which may induce weaknesses regarding existing or future attacks. Therefore, author considered finding and studying randomly generated Boolean functions (at least with a few inputs and outputs) with good cryptographic properties, to be of high interest.

Based on a algorithm designed by the author which can generate highly nonlinear functions at random, some comparative results are presented that give an insight to differences between constructed and generated Boolean function with good cryptographic properties.

Particular emphasis of the paper is on resiliency of highly nonlinear functions. The random generation algorithm manages to output balanced functions which in some cases have the highest achievable nonlinearity for a particular number of variables and/or have higher nonlinearity then some of the modern methods for obtaining cryptographically strong Boolean functions.

The paper is organized as follows. Section 2 provides some basic definitions and notations that are used throughout the remainder of the article. In Section 3 a random function generator is described, which is used as a foundation for obtaining highly nonlinear resilient functions. Experimental results and comparisons to other research are given in Section 4. Then conclusions follow in Section 5.

2. Preliminaries

We use square brackets to denote vectors like $[a_1,\ldots,a_n]$ and round brackets to denote functions like $f(x_1,\ldots,x_n)$.

2.1. Boolean function

Let $GF(2)=\langle\sum,\oplus,\bullet\rangle$ be two-element Galois field, where $\sum=\{0,1\}$, $\oplus$ and $\bullet$ denotes the sum and multiplication mod 2, respectively. A function $f:\sum^n\mapsto\sum$ is an n-argument Boolean function. Let $z=x_1\cdot 2^{n-1}+x_2\cdot 2^{n-2}+\ldots+x_n\cdot 2^0$ be the decimal representation of arguments $(x_1,x_2,\ldots,x_n)$ of the function f. Let us denote $f(x_1,x_2,\ldots,x_n)$ as y_z. Then $[y_0,y_1,\ldots,y_{2^n-1}]$ is called a truth table of the function f.

2.2. Linear and nonlinear Boolean functions

An n-argument Boolean function f is linear if it can be represented in the following form: $f(x_1,x_2,\ldots,x_n)=a_1x_1\oplus a_2x_2\oplus\ldots\oplus a_nx_n$. Let L_n be a set of all n-argument linear Boolean functions. Let $M_n=\{g:\sum^n\mapsto\sum\mid g(x_1,x_2,\ldots,x_n)=1\oplus f(x_1,x_2,\ldots,x_n)$ and $f\in L_n\}$. A set $A_n=L_n\cup M_n$ is called a set of n-argument affine Boolean functions. A Boolean function $f:\sum^n\mapsto\sum$ that is not affine is called a nonlinear Boolean function.

2.3. Balance

Let $N_0[y_0,y_1,\ldots,y_{2^n-1}]$ be a number of zeros (0's) in the truth table $[y_0,y_1,\ldots,y_{2^n-1}]$ of function f, and $N_1[y_0,y_1,\ldots,y_{2^n-1}]$ be a number of ones (1's). A Boolean function is balanced if

$$N_0[y_0,y_1,\ldots,y_{2^n-1}]=N_1[y_0,y_1,\ldots,y_{2^n-1}].$$

2.4. Algebraic normal form

A Boolean function can also be represented as a maximum of 2^n coefficients of the algebraic normal form (ANF). These coefficients provide a formula for the evaluation of the function for any given input $x=[x_1,x_2,\ldots,x_n]$:

$$f(x)=a_0\oplus\sum_{i=1}^{n}a_ix_i\oplus\sum_{1\le i<j\le n}a_{ij}x_ix_j\oplus\ldots\oplus a_{12\ldots n}x_1x_2\ldots x_n,$$

where $\sum$, $\oplus$ denote modulo 2 summation.

The order of nonlinearity of a Boolean function $f(x)$ is a maximum number of variables in a product term with non-zero coefficient a_J, where J is a subset of $\{1,2,3,\ldots,n\}$. In the case where J is an empty set the coefficient is denoted as a_0 and is called a zero order coefficient. Coefficients of order 1 are $a_1,a_2,\ldots,a_n$, coefficients of order 2 are $a_{12},a_{13},\ldots,a_{(n-1)n}$, coefficient of order n is $a_{12\ldots n}$. The number of all ANF coefficients equals 2^n.

Let us denote the number of all (zero and non-zero) coefficients of order i of function f as $\sigma_i(f)$. For n-argument function f there are as many coefficients of a given order as there are i-element combinations in n-element set, i.e., $\sigma_i(f)=\binom{n}{i}$.

2.5. Hamming distance

Hamming weight of a binary vector $x\in\sum^n$, denoted as $hwt(x)$, is the number of ones in that vector.

Hamming distance between two Boolean functions $f,g:\sum^n\mapsto\sum$ is denoted by $d(f,g)$ and is defined as follows:

$$d(f,g)=\sum_{x\in\sum^n}f(x)\oplus g(x).$$

The distance of a Boolean function f from a set of n-argument Boolean functions X_n is defined as follows:

$$\delta(f)=\min_{g\in X_n}d(f,g),$$

where $d(f,g)$ is the Hamming distance between functions f and g. The distance of a function f a set of affine functions A_n is the distance of function f from the nearest function $g\in A_n$.

The distance of function f from a set of all affine functions is called the nonlinearity of function f and is denoted by N_f.

2.6. Bent functions

A Boolean function $f:\sum^n\mapsto\sum$ is perfectly nonlinear if and only if $f(x)\oplus f(x\oplus\alpha)$ is balanced for any $\alpha\in\sum^n$ such that $1\le hwt(\alpha)\le n$.

For a perfectly nonlinear Boolean function, any change of inputs causes the change of the output with probability of 0.5.

Meier and Staffelbach [24] proved that the set of perfectly nonlinear Boolean functions is the same as the set of Boolean bent functions defined by Rothaus [29].

Perfectly nonlinear functions (or bent functions) have the same, and the maximum possible distance to all affine functions.

Bent functions are not balanced. Hamming weight of a bent function equals $2^{n-1}\pm 2^{\frac{n}{2}-1}$.

2.7. Walsh transform

Let $x=(x_1,x_2,\ldots,x_n)$ and $\omega=(\omega_1,\omega_2,\ldots,\omega_n)$ both belong to $\{0,1\}^n$ and $x\bullet\omega=x_1\omega_1,x_2\omega_2,\ldots,x_n\omega_n$. Let $f(x)$ be a Boolean functions on n variables. Then the Walsh transform of $f(x)$ is a real valued function over $\{0,1\}^n$ that can be defined as:

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

The Walsh transform is sometimes called the spectral distribution or simply the spectra of a Boolean function. It is an important tool for the analysis of Boolean function.

2.8. Correlation immunity and resilience

Guo-Zhen and Massey [13] have provided a spectral characterisation of correlation immune functions using Walsh

transform. We can use that as a definition of correlation immunity:

A function $f(x_1, x_2, \ldots, x_n)$ is m-order correlation immune (CI) iff its Walsh transform W_f satisfies $W_f = 0$, for $1 \leq hwt(\omega) \leq m$. Note that balanced m-order correlation immune functions are called m-resilient functions and if f is balanced then $W_f(0) = 0$. Thus, a function $f(x_1, x_2, \ldots, x_n)$ is m-resilient iff its Walsh transform W_f satisfies $W_f(\omega) = 0$, for $0 \leq hwt(\omega) \leq m$.

By an (n, m, d, x) function we mean an n-variable, m-resilient (balanced m-order CI) function with degree d and nonlinearity x. In the above notation the degree component is replaced by a '-' (i.e., $(n, m, -, x)$), if we do not want to specify a degree.

3. Random generation of highly nonlinear functions

As already mentioned earlier, so called bent Boolean functions achieve the highest possible nonlinearity. There exist a number of algorithms for constructing bent Boolean functions. Such constructions have been given by Rothaus [29], Kam and Davida [15], Maiorana [17], Adams and Tavares [1], and others.

Most of the known bent function constructions take bent functions of n arguments as their input and generate bent functions of $n+2$ arguments. One major drawback of these methods is the fact that they are deterministic. Only short bent functions ($n = 4$ or 6) are selected at random and the resulting function is obtained using the same, deterministic formula every time. The possible drawback of such approach (constructions) were stated in the beginning of this paper.

Drawing bent functions at random is not feasible already for small number of arguments ($n > 6$). To make such generation possible, an algorithm was designed that generates random Boolean functions in algebraic normal form thus making use of some basic properties of bent functions to considerably narrow the search space. This makes the generation of bent functions feasible for $n > 6$.

The algorithm for the generation of bent functions in ANF domain takes as its input the minimum and maximum number of ANF coefficients of every order that the resulting functions are allowed to have. Since the nonlinear order of bent functions is less or equal to $n/2$, clearly in ANF of a bent function can not be any ANF coefficient of order higher then $n/2$. This restriction is the major reason for random generation feasibility, since it considerably reduces the possible search space.

However the fact that bent functions are not balanced prohibits their direct application in the cipher system. Still, as bent functions achieve maximum possible nonlinearity they are often used as a foundation for constructing highly nonlinear balanced functions. In recent years some methods have been proposed that transform bent functions to balanced Boolean functions with minimal loss in nonlinearity. Examples of such methods are given in [18] and [19]. Still, balancing bent function can lead to low order of resiliency. In a quest for a randomly generated, highly nonlinear function with higher order resiliency the above mentioned random bent function generation algorithm has been modified to generate such functions. Here again some specific properties of resilient functions are crucial.

As already stated there are certain trade-offs involved among the parameters of a cryptographically sound Boolean function. As it has been showed by Siegenthaler [32] for an n-variable function, of degree d and order of correlation immunity m the following holds: $m + d \leq n$. Further, if the function is balanced then $m + d \leq n - 1$.

The generating algorithm is used basically in the same way as when generating bent functions. Still it operates in the ANF domain and it takes as its input the number minimal and maximal number of coefficients of every order. Nonlinear order is restricted according to Siegenthalter's findings and some more precise upper bounds on resilient order given by Sarkar and Maitra in [30].

Sarkar and Maitra in [30] present some construction methods for highly nonlinear resilient functions and give upper bounds on nonlinearity of resilient functions.

For the sake of completeness a Maiorana-McFarland like construction technique will now be briefly discussed. This technique is perhaps the most important of all resilient Boolean functions construction methods and has been investigated in a number of papers [2, 3, 5, 31]. This construction has been used by Maitra and Sarkar as a basis for their work.

Let π be a map from $\{0,1\}^r$ to $\{0,1\}^k$, where for any $x \in \{0,1\}^r$, $hwt(\pi(x)) \geq m+1$. Let $f : \{0,1\}^{r+k} \mapsto \{0,1\}$ be a Boolean function defined as $f(x,y) = y \bullet \pi(x) \oplus g(x)$, where $x \in \{0,1\}^r$, $y \in \{0,1\}^k$ and $y \bullet \pi(x)$ is the inner product of y and $\pi(x)$. Then f is m-resilient.

Table 1
Upper bounds on nonlinearity of resilient functions

	5	*6*	*7*	*8*	*9*	*10*
1	12	24	56	116*	244*	492*
2	8	24	56*	112	240	480
3	0	16	48	112	240*	480
4		0	32	96	224	480*
5			0	64	192	448
6				0	128	384
7					0	256
8						0

Table 1 summarises the results obtained in [30] and gives upper bounds on nonlinearity of resilient functions for number of arguments ranging from 5 to 10. The rows represent the resiliency and the columns represent the number of variables. Entries with * indicate bounds which have not yet been achieved. Functions can be constructed with parameters satisfying the other entries.

Table 1 can be used as a benchmark for assessing the efficacy of resilient functions construction methods.

4. Experimental results

Now let's see the results from above mentioned random resilient function generator against the upper bounds presented in Table 1.
The maximum nonlinearity is known for all Boolean functions on even number of variables – it is achieved by bent functions. The maximum nonlinearity for odd variable Boolean functions is known for $n \leq 7$. Also, maximum nonlinearity question is solved for balanced and resilient functions on n variables for $n \leq 5$ (which is easy to do by exhaustive computer search). Let's consider cases for $6 \leq n \leq 10$.

- $n = 6$: Maximum nonlinearity for $n = 6$ is 28 (for bent functions). Maximum nonlinearity of a balanced function is 26 and construction of such functions is known. Maximum nonlinearities for 1, 2 and 3-resilient functions were shown (be computer search) to be 24, 24 and 16. Random resilient function generator presented in this paper is able to generate 1, 2 and 3-resilient functions.

- $n = 7$: Maximum nonlinearity of a balanced Boolean functions for $n = 7$ is 56. As shown in [30] the maximum nonlinearities for 1, 2, 3 and 4-resilient functions are respectively 56, 56, 48, 32. However 2-resilient function with nonlinearity of 56 is not known. Random generator is able to generate all these resilient functions except that (7,2,-,56).

- $n = 8$: Nonlinearity of 8 argument bent function is 120. Maximum (theoretical) nonlinearity for a balanced function is 118, however such function if not known. Maximum possible nonlinearities for 1, 2, 3, 4 and 5-resilient functions are 116, 112, 112, 96, and 64. The existence of (8,1,-,116) function is an open problem. Constructions for other functions are known. Random generator can output all the functions except the not known (8,1,-,116) and (8,3,-,112).

- $n = 9$: Maximum nonlinearity of such functions as an open problem. The known upper bound if 244. It is easy to construct a function with nonlinearity of 240. Maximum nonlinearities of resilient functions are 244, 240, 240, 224, 192, 128 for 1, 2, 3, 4, 5, 6-resilient functions respectively. The generator is capable of generating (9,1,-,240), (9,2,-,224), (9,5,-,192) and (9,6,-,128) functions.

- $n = 10$: The nonlinearity of a bent function is 496. Maximum nonlinearity of a balanced function is 494, best know function has linearity of 492. 492, 488, 480, 480, 448, 384, 256 are the nonlinearities of 1,2, 3, 4, 5, 6, 7-resilient function. Constructions of the following functions are not known: (10,1,-,492), (10,1,-,488), (10,2,-,488), (10,4,-,480). Random generator can generate the following: (10,1,-,480), (10,3,-,448), (10,5,-,384), (10,7,-,256).

5. Conclusions

As shown in the previous paragraph, the random resilient function generator is capable of generating Boolean functions having some very promising cryptographic qualities. In many cases these functions are on par with the best known constructions. In other cases they fall slightly short of best achievable results. In any case they have the advantage of being truly random and not being restricted by specific constraints associated with each specific design. One can suspect that such constraints may render the function (or a cipher system based on it) vulnerable to some future cryptographic attack.
Also, results presented in this article are the very first results from the resilient function generator. It's output relies heavily on parameter setting, mainly on the number of higher order ANF coefficients in the resulting function. As this dependencies are investigated we might expect still better results from the generator.
As with generated bent functions, also generated resilient functions can have a very compact (small) algebraic normal form which can be utilized for efficient storage and fast cryptographic routines.

Acknowledgements

This scientific paper has been financed as a research project from Polish State Committee For Scientific Research funds in the years 2004–2006.

References

[1] C. M. Adams and S. E. Tavares, "Generating and counting binary bent sequences", *IEEE Trans. Inform. Theory*, vol. IT-36, pp. 1170–1173, 1990.

[2] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation immune functions", in *Adv. Crypt. CRYPTO 1991*, Santa Barbara, USA, 1991, pp. 86–100.

[3] C. Carlet, "More correlation immune and resilient functions over Galois fields and Galois rings", in *Adv. Crypt. EUROCRYPT 1997*, Konstanz, Germany, 1997, pp. 422–433.

[4] C. Carlet, "On the coset weight divisibility and nonlinearity of resilient and correlation immune functions", in *SETA 2001*, Bergen, Norway, 2001.

[5] S. Chee, S. Lee, D. Lee, and S. H. Sung, "On the correlation immune functions and their nonlinearity", in *Advances in Cryptology ASIACRYPT 1996*, *LNCS*. Berlin: Springer, 1996, vol. 1163, pp. 232–243.

[6] J. A. Clark and J. L. Jacob, "Two stage optimisation in the design of Boolean functions", in *5th Australasian Conference on Information Security and Privacy, ACISP 2000*, E. Dawson, A. Clark, and C. Boyd, Eds., *LNCS*. Berlin: Springer, 2000, vol. 1841, pp. 242–254.

[7] J. A. Clark, J. L. Jacob, and S. Stepney, "The design of S-boxes by simulated annealing", in *Int. Conf. Evol. Comput. CEC 2004*, Portland, USA, 2004.

[8] J. A. Clark, J. L. Jacob, and S. Stepney, "Secret agents leave big footprints: how to plant a cryptographic trapdoor, and why you might not get away with it", in *Genetic and Evolutionary Computation Conference GECCO 2003*, *LNCS*. Berlin: Springer, 2003, vol. 2724, pp. 2022–2033.

[9] J. A. Clark, J. L. Jacob, and S. Stepney, "Functions satisfying multiple criteria", in *Progress in Cryptology INDOCRYPT 2002*, *LNCS*. Berlin: Springer, 2002, vol. 2551, pp. 246–259.

[10] J. A. Clark, J. L. Jacob, and S. Stepney, "Searching for cost functions", in *Int. Conf. Evol. Comput. CEC 2004*, Portland, USA, 2004, pp. 1517–1524.

[11] H. Dobbertin, "Construction of bent functions and balanced functions with high nonlinearity", in *Fast Software Encryption, 1994 Leuven Workshop*, *LNCS*. Berlin: Springer, 1994, vol. 1008, pp. 61–74.

[12] R. Forré, "The strict avalanche criterion: spectral properties of Boolean functions with high nonlinearity", in *Advances in Cryptology: CRYPTO 1988*, *LNCS*. Berlin: Springer, 1990, vol. 403, pp. 450–468.

[13] X. Guo-Zhen and J. Massey, "A spectral characterization of correlation immune combining functions", *IEEE Trans. Inform. Theory*, vol. 34, no. 3, pp. 569–571, 1988.

[14] X. D. Hou, "On the norm and covering radius of first-order Reed-Muller codes", *IEEE Trans. Inform. Theory*, vol. 43, no. 3, pp. 1025–1027, 1997.

[15] J. B. Kam and G. Davida, "Structured design of substitution-permutation encryption networks", *IEEE Trans. Comput.*, vol. C-28, pp. 747–753, 1979.

[16] K. Kurosawa and T. Satoh, "Generalization of higher order SAC to vector output Boolean functions", *IEICE Trans.*, vol. E90, no. 1, 1998.

[17] J. A. Maiorana, "A class of bent functions", R41 Tech. Paper, 1971.

[18] S. Maity and T. Johansson, "Construction of cryptographically important Boolean functions", in *INDOCRYPT 2002*, Hyderabad, India, 2002, pp. 234–245.

[19] S. Maity and S. Maitra, "Minimum distance between bent and 1-resilient Boolean functions", in *FSE 2004*, New Delhi, India, 2004, pp. 143–160.

[20] S. Maitra, "Highly nonlinear balanced Boolean functions with very good autocorrelation property", Tech. Rep. 2000/047, Indian Statistical Institute, Calcutta, 2000.

[21] S. Maitra, "Autocorrelation properties of correlation immune Boolean functions", in *INDOCRYPT 2001*, Chennai, India, 2001, pp. 242–253.

[22] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity", in *SETA 2001*, Bergen, Norway, 2001.

[23] M. Matsui, "Linear cryptanalysis method for DES cipher (abstracts)", in *EUROCRYPT 1993*, Lofthus, Norway, 1993.

[24] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions", in *Advances in Cryptology: EUROCRYPT 1989*, J. J. Quisquater, J. Vandewalle, Eds., *LNCS*. Berlin: Springer, 1989, vol. 434, pp. 549–562.

[25] W. Millan, A. Clark, and E. Dawson, "Heuristic design of cryptographically strong balanced Boolean functions", in *Advances in Cryptology: EUROCRYPT 1998*, *LNCS*. Berlin: Springer, 1998, vol. 1403, pp. 489–499.

[26] K. Nyberg, "Perfect nonlinear S-boxes", in *Advances of Cryptology: EUROCRYPT 1991*, *LNCS*. Berlin: Springer, 1991, vol. 547, pp. 378–386.

[27] E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar, "New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity", in *Workshop on Coding Theory, Electronic Notes in Discrete Mathematics*, Elsevier, 2001.

[28] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions", in *Advances in Cryptology: EUROCRYPT 1990*, *LNCS*. Berlin: Springer, 1991, vol. 473, pp. 161–173.

[29] O. S. Rothaus, "On bent functions", *J. Combin. Theory: Ser. A*, vol. 20, pp. 300–305, 1976.

[30] P. Sarkar and S. Maitra, "New directions in design of resilient Boolean functions", Tech. Rep. ASD/2000/04, Indian Statistical Institute, 2000.

[31] J. Seberry, X. M. Zhang, and Y. Zheng, "On constructions and nonlinearity of correlation immune Boolean functions", in *Advances in Cryptology: EUROCRYPT 1993*, Lofthus, Norway, 1994, pp. 181–199.

[32] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications", *IEEE Trans. Inform. Theory*, vol. IT-30, no. 5, pp. 776–780, 1984.

[33] J. J. Son, J. I. Lim, S. Chee, and S. H. Sung, "Global avalanche characteristics and nonlinearity of balanced Boolean functions", *Inform. Proces. Lett.*, vol. 65, no. 3, pp. 139–144, 1998.

[34] S. H. Sung, S. Chee, and C. Park, "Global avalanche characteristics and propagation criterion of balanced Boolean functions", *Inform. Proces. Lett.*, vol. 69, no. 1, pp. 21–24, 1999.

[35] Y. Tarannikov, "On resilient Boolean functions with maximal possible nonlinearity", Tech. Rep. 2000/005, Mech. & Math. Department, Moscow State University, 2000.

[36] X. M. Zhang and Y. Zheng, "GAC – the criterion for global avalanche characteristics of cryptographic functions", *J. Univ. Comput. Sci.*, vol. 1, no. 5, pp. 316–333, 1995.

Anna Grocholewska-Czuryło is an adjunct at the Poznań University of Technology. She has studied and published papers on a range of topics like natural language processing, cellular automata, neural networks and has finally focused on data security and cryptology, especially methods of designing Boolean functions and s-box design. She has earned her Ph.D. degree entitled: "Pseudobalanced and Bent Boolean Functions and Algorithms of their Generating Methods" in 2001.

e-mail: czurylo@sk-kari.put.poznan.pl
Institute of Control and Information Engineering
Poznań University of Technology
Marii Skłodowskiej-Curie Sq. 5
60-965 Poznań, Poland