Synopsis of the thesis entitled

# Cryptographic and Combinatorial Properties of Boolean Functions and S-boxes

*by*

Kishan Chand Gupta
Applied Statistics Unit
Indian Statistical Institute

2004

*under the supervision of*

Dr. Palash Sarkar
Applied Statistics Unit
Indian Statistical Institute

# 1 Introduction

In this thesis we study combinatorial aspects of Boolean functions and S-boxes with important cryptographic properties and construct new functions possesing such properties. These have possible applications in the design of private key (symmetric key) cryptosystems.

Symmetric key cryptosystems are broadly divided into two classes.

1. Stream Ciphers,
2. Block Ciphers.

Some recent proposals of stream ciphers are SNOW [37], SCREAM [52], TURING [98], MUGI [117], HBB [102], RABBIT [9], HELIX [38] and some proposals of block ciphers are DES, AES, RC6 [97], MARS [12], SERPENT [6], TWOFISH [104].

In *stream cipher cryptography* a pseudorandom sequence of bits of length equal to the message length is generated. This sequence is then bitwise XOR-ed (addition modulo 2) with the message sequence and the resulting sequence is transmitted. At the receiving end, deciphering is done by generating the same pseudorandom sequence and again bitwise XORing the cipher bits with the random bits. The seed of the pseudorandom bit generator is obtained from the secret key.

Linear Feedback Shift Registers (LFSRs) are important building blocks in stream cipher systems. A standard model (see Figure 1) of stream cipher [109, 110, 34] combines the outputs of several independent LFSR sequences using a nonlinear Boolean function to produce the keystream. Design and analysis of practical stream cipher was kept confidential for a long time. An important boost occurred in the 1970's, when several research papers on the design of LFSR-based stream cipher occurred. As LFSRs are linear, some form of nonlinearity is introduced by using nonlinear Boolean functions (see [100]).

Properties of the nonlinear combining Boolean function received a lot of attention in literature for the last two decades and it is now possible to get good Boolean functions which resist many of the known attacks. In this thesis we have not considered algebraic attacks as this class of attacks have become known only very recently. We consider *balancedness, nonlinearity, algebraic degree, correlation immunity and resiliency* of Boolean functions and S-boxes for use in stream ciphers model based on Figure 1.

A Boolean function used in stream cipher should be balanced, which is required for the pseudorandomness of generated keystream. In the stream cipher model, the combining

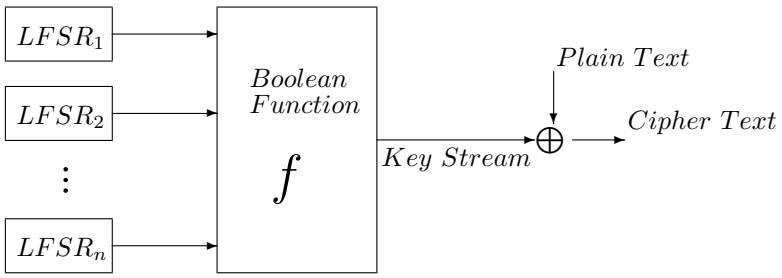


Figure 1: LFSR based encryption scheme

Boolean function is so chosen that it increases the linear complexity [100] of the resulting key stream. High algebraic degree provides high linear complexity [101, 34]. Therefore high algebraic degree is desirable in stream ciphers. A Boolean function should have high nonlinearity to be used in stream ciphers. A function with low nonlinearity is prone to linear approximation attack. Linear approximation means approximating the combining function by a linear function. To resist *divide-and-conquer* attack a Boolean function in stream cipher should be correlation immune of higher order [109, 110].

We can not achieve all the desirable properties of our liking, so there will be some trade of between these properties. Depending on the application we have to decide which properties are more important.

In *block cipher cryptography*, the message bits are divided into blocks and each block is separately enciphered using the same key and transmitted. Most of the modern day block ciphers are iterated ciphers and use substitution boxes (S-boxes) as the nonlinear part in the scheme. The security of the block ciphers greatly depends on the strength of the substitution boxes.

Matsui [76] introduced linear cryptanalysis method for block cipher. Linear cryptanalysis means approximating a linear combination of the component functions of an S-box, used in a block cipher by a linear function of the input variables. To resist linear cryptanalysis S-boxes should have higher nonlinearity.

Differential cryptanalysis [7] is a chosen-plaintext attack and involves comparing the XOR of two inputs to the XOR of corresponding two outputs. A nonuniform output distribution will be the basis for a successful differential attack.

Webster and Tavares [118] introduced the concept of strict avalanche criteria (SAC).

Propagation Characteristic (PC) and SAC are two important cryptographic properties for S-boxes to resist differential cryptanalysis. To get uniform output distribution, S-boxes in block ciphers should have PC($l$) of higher order for $l \geq 1$. SAC($k$) is PC(1) of order $k$. S-boxes having PC($l$) of order $k$ with large $l$ and with very high nonlinearity and algebraic degree are hard to find. Therefore sometimes we may have to be satisfied with S-boxes of higher order SAC.

Jakobsen and Knudsen [58] identified interpolation attack on block ciphers with S-boxes having small algebraic degree. Later Canteaut and Videau [15] provided higher order differential attack on block ciphers using S-boxes with low algebraic degree. So algebraic degree of S-boxes should be high to resist such attacks.

Again, as stated for Boolean functions used in stream ciphers, we can not achieve all the desirable properties for S-boxes used in block ciphers. We have to decide which properties are more important depending on the application.

In writing this introduction, we have benefitted from Willi Meier's tutorial in National Workshop on Cryptology 2003 organized at Anna University, India.

# 2 Definitions

We provide some definitions and their importance in brief. Let $\mathbb{F}_2 = GF(2)$. We consider the domain of a Boolean function to be the vector space $(\mathbb{F}_2^n, \oplus)$ over $\mathbb{F}_2$, where $\oplus$ is used to denote the addition operator over both $\mathbb{F}_2$ and the vector space $\mathbb{F}_2^n$. The inner product of two vectors $u, v \in \mathbb{F}_2^n$ will be denoted by $\langle u, v \rangle$. The weight of an $n$-bit vector $u$ is the number of ones in $u$ and will be denoted by $\mathtt{wt}(u)$. The (Hamming) distance between two vectors $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ is the number of places where they differ and is denoted by $d(x, y)$. Let $g : \{0,1\}^n \to \{0,1\}^m$ be an S-box and $f : \{0,1\}^m \to \{0,1\}$ be an $m$-variable Boolean function. The composition of $f$ and $g$, denoted by $f \circ g$ is an $n$-variable Boolean function defined by $(f \circ g)(x) = f(g(x))$.

A truth table is a tabulation of all possible combinations of input values and their corresponding outputs. The following provides an example of a 3-variable Boolean function. Note that the input variables $x_3, x_2, x_1$ are tabulated in each row. The function is represented in the rightmost column. For an $n$-variable Boolean function the truth table contains $n$ columns for inputs, 1 column for output and $2^n$ rows for all the enumerations of the input variables.

| $x_3$ | $x_2$ | $x_1$ | $f$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 0 |

A function $f$ is said to be balanced if its output column in the truth table contains equal number of 0's and 1's (i.e. $\mathsf{wt}(f) = 2^{n-1}$). An $(n, m)$ S-box $g$, is said to be balanced if $l \circ g$ is balanced for every non-constant $m$-variable linear function $l$.

An important tool for the analysis of a Boolean function is its Walsh transform (WT). The WT of an $n$-variable Boolean function $f$ is an integer valued function $W_f : \{0,1\}^n \to [-2^n, 2^n]$ defined by (see [73, page 414])

$$W_f(u) = \sum_{w \in \mathbb{F}_2^n} (-1)^{f(w) \oplus \langle u, w \rangle}.$$

An $n$-variable function is called *correlation immune* of order $t$ ($t$-CI) if $W_f(u) = 0$ for all $u$ with $1 \leq \mathsf{wt}(u) \leq t$ [109, 119]. Further the function is balanced if and only if $W_f(0) = 0$. A balanced $t$-CI function is called *$t$-resilient*. An $(n, m)$ S-box $g$ is said to be $t$-CI, if $l \circ g$ is $t$-CI for every non-constant $m$-variable linear function $l$ (see [122]). Further, if $g$ is balanced then $g$ is called $t$-resilient.

A parameter of fundamental importance in cryptography is the nonlinearity of a function (see [73]). This is defined to be the distance from the set of all affine functions. It is more convenient to define it in terms of the spectrum of a Boolean function. The nonlinearity $\mathsf{nl}(f)$ of an $n$-variable Boolean function $f$, is defined as

$$\mathsf{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} |W_f(u)|.$$

For an $(n, m)$ S-box $g$,

$$\mathsf{nl}(g) = \min\{\mathsf{nl}(l \circ g) : l \text{ is a non-constant } m\text{-variable linear function }\}.$$

For even $n$, an $n$-variable function $f$ is called *bent* if $W_f(u) = \pm 2^{\frac{n}{2}}$, for all $u \in \mathbb{F}_2^n$ (see [99]). This class of functions is important in both cryptography and coding theory. For even $n$, bent functions achieve the maximum possible nonlinearity.

An $n$-variable Boolean function $f$ satisfies strict avalanche criteria (SAC) if $f(x) \oplus f(x \oplus \alpha)$ is balanced for any $\alpha \in \mathbb{F}_2^n$ with $\mathsf{wt}(\alpha) = 1$. A function $f$ satisfies SAC($k$) if every subfunction obtained from $f(x_1, \cdots, x_n)$ by keeping at most $k$ input bits constant satisfies SAC. An $(n, m)$ S-box $g$ is said to be SAC($k$), if $l \circ g$ is SAC($k$) for every non-constant $m$-variable linear function $l$.

A Boolean function $f$ can be uniquely represented by a multivariate polynomial over $\mathbb{F}_2$. This representation is called the algebraic normal form (ANF). The degree of the polynomial is called the algebraic degree or simply the degree of $f$. For an $(n, m)$ S-box $g$,

$$deg(g) = \min\{deg(l \circ g) : l \text{ is a non-constant } m\text{-variable linear function }\}.$$

# 3 Thesis Plan

This thesis is based on six papers [46, 47, 48, 49, 50, 51]. We provide a brief summary of the chapters which appear in the thesis. *Chapter 1* contains the introduction. In *Chapter 2* we provide the necessary preliminary material required in the later chapters.

In *Chapter 3,* we consider the problem of computing Walsh transform (WT) of a Boolean function from its algebraic normal form (ANF). Two standard ways of representing a Boolean function are its truth table representation and ANF representation. Given a truth table we can compute WT by using the fast WT [73] which has complexity $O(m2^m)$, where $m$ is the number of input variables. Hence it is useful if $m$ is around 40 or less. Some Boolean functions have very compact ANF. An example is $g(x_1, \cdots x_{2k}) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2k-1}x_{2k}$ which is a bent function. In general nothing can be said about the WT of a 50-variable Boolean function using the fast WT. We try to provide some answers to this problem. Clearly, it is not possible to compute the WT at all $2^m$ points. Suppose we want to compute WT at a small set of points. We show that this is possible in certain cases where the Boolean function has a compact ANF.

We obtain a formula for the WT of a Boolean function at a certain point in terms of parameters derived from the ANF. We simplify this formula and develop an algorithm to evaluate it to compute the WT at any point. In certain cases, It is possible to run our algorithm for 50 to 100 variable functions having a few hundred terms in their ANF. For such functions it is possible to compute the WT for a small set of points. This provides some useful information about the function such as the size of its support and an estimate of its nonlinearity. Note that for small number of variables, the fast WT is faster than our

algorithm. Hence we do not provide a substitute for the fast WT; rather we provide a tool to analyse a Boolean function in situations where the fast WT cannot be used.

An important cryptanalytic method for the DES algorithm is the linear cryptanalysis method presented by Matsui in [76], which makes use of correlations between the input and output of the round functions of DES. Nyberg [86] presented three correlation theorems and applied them to partial cryptanalysis of several symmetric ciphers.

In *Chapter 4,* we continue the work of Nyberg [86] in a more theoretical direction. We consider a general functional form and obtain its WT. Two of Nyberg's correlation theorems are seen to be special cases of our general functional form. S-box look-up, addition modulo $2^{2k}$ and X-OR are three frequently occurring operations in the design of symmetric ciphers. We consider two methods of combining these operations and in each case apply our main result to obtain the WT. Our result have possible applications to analysis of reduced round block ciphers.

In *Chapter 5,* we construct perfect nonlinear multi-output Boolean functions satisfying higher order SAC. Our first construction is an infinite family of 2-output perfect nonlinear functions satisfying higher order SAC. This construction is achieved using the theory of bilinear forms and symplectic matrices. Next we build on a known connection between 1-factorization of a complete graph and SAC to construct more examples of 2 and 3-output perfect nonlinear functions. In certain cases, the constructed S-boxes have optimal trade-off between the following parameters: numbers of input and output variables, nonlinearity and order of SAC. In case the number of input variables is odd, we modify the construction for perfect nonlinear S-boxes to obtain a construction for maximally nonlinear S-boxes satisfying higher order SAC. Our constructions present the first examples of perfect nonlinear and maximally nonlinear multioutput S-boxes satisfying higher order SAC. Lastly, we present a simple method for improving the degree of the constructed functions with a small sacrifice in nonlinearity and the SAC property. This yields functions which have possible applications in the design of block ciphers.

The next three chapters consider construction of resilient S-boxes and their implementation. We briefly describe each of them below.

In *Chapter 6,* we describe two constructions. In the first construction we describe a simple method using $[n-d-1, m, t+1]$ linear binary code to construct an $n$-input, $m$-output, $t$-resilient function with degree $d > m$ and nonlinearity $2^{n-1} - 2^{n-\lceil (d+1)/2 \rceil} - (m+1)2^{n-d-1}$. For any fixed values of parameters $n, m, t$ and $d$, with $d > m$, the nonlinearity obtained by our construction is higher than the nonlinearity obtained by the only previously

known construction which provides $d > m$ (due to Cheon [24]). The second method is a simple modification of a construction due to Zhang and Zheng [122] and constructs $n$-input, $m$-output resilient S-boxes with degree $d > m$. We prove by an application of the Griesmer bound for linear error correcting codes that the modified Zhang-Zheng construction is superior to the method of [24].

In *Chapter 7,* we use a sharpened version of the Maiorana-McFarland technique to construct nonlinear resilient S-boxes. The nonlinearity obtained by our construction is better than previously known construction methods. The idea is to use affine functions on small number of variables to construct nonlinear resilient functions on larger number of variables. For Boolean functions, the Maiorana-McFarland technique to construct resilient functions was introduced by Camion et al [14]. Nonlinearity calculation for the construction was first performed by Seberry, Zhang and Zheng [107]. This technique was later sharpened by Chee et al [23] and Sarkar-Maitra [103]. For S-boxes, this technique has been used by [63] and [89]. Here we develop and sharpen the technique of affine function concatenation to construct nonlinear resilient S-boxes. This leads to significant improvement in nonlinearity over that obtained in [89] and provides S-boxes with currently best known nonlinearity.

In *Chapter 8,* we consider implementation aspects of resilient S-boxes. We first discuss the applicability of resilient S-boxes to the nonlinear combiner model of stream ciphers. Next we consider the software implementation of Maiorana-McFarland resilient S-boxes. Most papers on construction of resilient Maiorana-McFarland Boolean functions and S-boxes provide mathematical descriptions which are not sufficient for implementation purposes. Moreover, the mathematical description do not bring out the fact that in most cases such S-boxes can be efficiently implemented using a small amount of memory. Our work shows that these S-boxes can be implemented using a small amount of memory and the output of an S-box can be evaluated using very little computation.

# References


[1] K. Beauchamp. *Applications of Walsh and Related Functions.* Academic Press, 1984.

[2] C. Bennett, G. Brassard and J. Robert. Privacy Amplification by Public Discussion. *SIAM Journal of Computing*, volume 17, pages 210–229, 1988.

[3] E. R. Berlekamp. *Algebraic Coding Theory.* McGraw Hill, New York, 1968.

[4] E. R. Berlekamp and L. R. Welch. Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code. *IEEE Transactions on Information Theory*, IT-18(1):203–207, January 1972.

[5] J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. Bounds on resilient functions and orthogonal arrays. In *Advances in Cryptology – CRYPTO'94*, number 839 in Lecture Notes in Computer Science, pages 247–256. Springer Verlag, 1994.

[6] E. Biham, R. J. Anderson and L. R. Knudsen. Serpent: A New Block Cipher Proposal. In *Fast Software Encryption, FSE 1998*, pages 222–238. Springer-Verlag, 1998.

[7] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In *Advances in Cryptology - CRYPTO'90*, Lecture Notes in Computer Science, pages 2–21. Springer-Verlag, 1991.

[8] L. Blum, M. Blum, and M. Shub. A simple unpredictable random number generator. *SIAM Journal on Computing*, 15:364–383, 1986.

[9] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen and O. Scavenius. Rabbit: A New High-Performance Stream Cipher. In *Fast Software Encryption, FSE 2003*, pages 307–329. Springer-Verlag, 2003.

[10] J. A. Bondy and U. S. R. Murthy. *Graph Theory with Applications*. London, Macmillan Press, 1977.

[11] E. F. Brickell, J. H. Moore, and M. R. Purtill. Structures in the S-boxes of the DES. In *Advances in Cryptology – CRYPTO'86*, Lecture Notes in Computer Science, pages 3–8. Springer-Verlag, 1987.

[12] C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S.M. Matyas, L. O'Connor, M. Peyravian, D. Safford, and N. Zunic. "MARS - A Candidate Cipher for AES," *NIST AES Proposal, Jun 98.* http://citeseer.nj.nec.com/burwick99mars.html.

[13] P. Camion and A. Canteaut. Construction of t-Resilient Functions over a Finite Alphabet. *In Advances in Cryptology - EUROCRYP 1996*, pages 283–293, Lecture Notes in Computer Science, Springer-Verlag, 1996.

[14] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation immune functions. In *Advances in Cryptology – CRYPTO'91*, pages 86–100. Springer-Verlag, 1992.

[15] A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. *Advances in Cryptology – Eurocrypt 2002*, LNCS 2332, pages 518–533.

[16] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. In *Advances in Cryptology – Eurocrypt 2000*, pages 507–522, Lecture Notes in Computer Science, Springer-Verlag, 2000.

[17] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity checks equations of weight 4 and 5. In *Advances in Cryptology – Eurocrypt 2000*, pages 573–588, Lecture Notes in Computer Science, Springer-Verlag, 2000.

[18] C. Carlet. On cryptographic propagation criteria for Boolean functions. *Information and Computation*, 151:32–56, 1999.

[19] C. Carlet and P. Guillot. A new representation of Boolean functions. *Proceedings of AAECC'13*, Lecture Notes in Computer Science, 1719, pp 94–103, 1999.

[20] C. Carlet and P. Sarkar. Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions. *Finite Fields and their Applications*, Volume 8, Number 1, January 2002, Pages 120–130.

[21] F. Chabaud, S. Vaudenay. Links Between Differential and Linear Cryptoanalysis. *In Advances in Cryptology - EUROCRYPT 1994*, pages 356–365, Lecture Notes in Computer Science, Springer-Verlag, 1995.

[22] S. Chee, S. Lee, and K. Kim. Semi-bent functions. In *Advances in Cryptology, Asiacrypt'94*, number 917 in Lecture Notes in Computer Science, pages 107–118. Springer-Verlag, 1995.

[23] S. Chee, S. Lee, D. Lee, and S. H. Sung. On the correlation immune functions and their nonlinearity. In *Advances in Cryptology, Asiacrypt 96*, number 1163 in Lecture Notes in Computer Science, pages 232–243. Springer-Verlag, 1996.

[24] J. H. Cheon. Nonlinear Vector Resilient Functions. In *Advances in Cryptology – CRYPTO 2001*, pages 458–469, Lecture Notes in Computer Science, Springer-Verlag, 2001.

[25] V. Chepyzhov and B. Smeets. On a fast correlation attack on certain stream ciphers. In *Advances in Cryptology – EUROCRYPT'91*, volume 547, pages 176–185. Springer-Verlag, 1991.

[26] V. Chepyzhov, T. Johansson and B. Smeets. A simple algorithm for fast correlation attacks on stream ciphers. In *Fast Software Encryption – FSE 2000*, pp 181 –195, Lecture Notes in Computer Science, Springer-Verlag, 2000.

[27] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, and R. Smolensky. The bit extraction problem or t-resilient functions. In *26th IEEE Symposium on Foundations of Computer Science*, pages 396–407, 1985.

[28] N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback, *In Advances in Cryptology – EUROCRYPT 2003*, 345–359.

[29] N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback, Extended version, available at http://www.cryptosystem.net/stream/,2003.

[30] T. W. Cusick. Boolean functions satisfying higher order strict avalanche criterion. In *Advances in Cryptology – EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 102–117. Springer-Verlag, 1994.

[31] J. Daemen and V. Rijmen. *The Design of Rijndael: AES* - The Advanced Encryption Standard (Information Security and Cryptography). Spriner-Verlag 2002.

[32] E. Dawson and C. K. Wu. Construction of correlation immune Boolean functions. In *Information and Communications Security*, Lecture Notes in Computer Science, pages 170–180. Springer-Verlag, 1997.

[33] W. Diffe and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(5):644–654, 1976.

[34] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers*. Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[35] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption*, number 1008 in Lecture Notes in Computer Science, pages 61–74. Springer-Verlag, 1994.

[36] H. Dobbertin, Almost Perfect Nonlinear Power Functions on $GF(2^n)$: The Welch Case. *IEEE Transactions on Information Theory*, Vol 45 , No 4, pp. 1271–1275 , 1999.

[37] P. Ekdahl and T. Johansson. A New Version of the Stream Cipher SNOW. In *Selected Areas in Cryptography, SAC 2003*, pages 47–61.

[38] N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks and T. Kohno. Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive. In *Fast Software Encryption, FSE 2003*, pages 330–346. Springer-Verlag, 2003.

[39] E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology – EUROCRYPT'98*. Springer-Verlag, 1998.

[40] C. Fontaine. On some cosets of the first-order Reed-Muller code with high minimum weight. *IEEE Transactions on Information Theory*, 45(4):1237–1243, 1999.

[41] R. Forré. The strict avalanche criterion : Spectral properties of Boolean functions and an extended definition. In *Advances in Cryptology – CRYPTO'88*, Lecture Notes in Computer Science, pages 450–468. Springer-Verlag, 1990.

[42] J. Friedman. On the bit extraction problem. In *33rd IEEE Symposium on Foundations of Computer Science*, pages 314–319, 1982.

[43] J. Dj. Golic, M. Salmasizadeh, L. Simpson, and E. Dawson. Fast correlation attacks on nonlinear filter generators. *Information Processing Letters*, 64(1):37–42, 1997.

[44] S. W. Golomb. *Shift Register Sequences*. San Fransisco, CA, Holden-Day, 1967.

[45] K. Gopalakrisnan and D. R. Stinson. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography*, 5:241–251, 1995.

[46] K. C. Gupta and P. Sarkar. Improved Construction of Nonlinear S-Boxes. *In Advances in Cryptology – Asiacrypt 2002*, pp 466–483, Lecture Notes in Computer Science, Springer-Verlag, 2002.

[47] K. C. Gupta and P. Sarkar. Construction of Perfect Nonlinear and Maximally Nonlinear Multi-output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria. In *Progress in Cryptology – Indoocrypt 2003*, pp 107–120, Lecture Notes in Computer Science, Springer-Verlag, 2003.

[48] K. C. Gupta and P. Sarkar. Computing Partial Walsh Transform from the Algebraic Normal Form of a Boolean Function. *Electronic Notes in Discrete Mathematics, Volume*

*15*, *http://www.elsevier.nl/gej-ng/31/29/24/75/23/show/Products/notes/index.htt.* Full version of the paper accepted for the special R. C. Bose issue of Discrete Mathematics.

[49] K. C. Gupta and P. Sarkar. A General Correlation Theorem. *Cryptology ePrint Archive: Report 2003/124*, *http://eprint.iacr.org/2003/124.*

[50] K. C. Gupta and P. Sarkar. Software Implementation of Resilient Maiorana-McFarland S-Boxes, preprint.

[51] K. C. Gupta and P. Sarkar. Construction of High Degree Resilient S-Boxes With Improved Nonlinearity. *Indian Statistical Institute, Technical Report No. ASD/2003/4.*

[52] S. Halevi, D. Coppersmith and C. S. Jutla. Scream: A Software-Efficient Stream Cipher. In *Fast Software Encryption – FSE 2002*, pp 195 –209, Lecture Notes in Computer Science, Springer-Verlag, 2002.

[53] R. W. Hamming. *Coding And Information Theory.* Prentice Hall Inc., 1980.

[54] C. Harpes, G. G. Kramer and J. L. Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma. In *Advances in Cryptology – EUROCRYPT 1995*, pages 24–38, Lecture Notes in Computer Science, Springer-Verlag, 1995.

[55] M. Hermelin and K. Nyberg. Correlation Properties of the Bluetooth Combiner Generator. *The Second International Conference on Information Security and Cryptology of ICISC '99*, pages 17–29, Lecture Notes in Computer Science, Springer-Verlag, 2000.

[56] T. Honda, T. Satoh, T. Iwata, and K. Kurosawa. Balanced Boolean functions satisfying PC(2) and very large degree. In *SAC'97*, pages 64–72, January 1997.

[57] E. Horowitz and S. Sahni. *Fundamentals of Data Structures*, W. H. Freeman and Co., 1983.

[58] T. Jakobsen and L. R. Knudsen. The interpolation attack on block ciphers. In *SAC'97*, pages 28–40, January 1997.

[59] T. Johansson. Reduced complexity correlation attacks on twoclock-controlled generators. In *Advances in Cryptology – ASIACRYPT'98*, Lecture Notes in Computer Science. Springer-Verlag, 1998.

[60] T. Johansson. A simple algorithm for fast correlation attacks on stream ciphers. In *Fast Software Encryption'2000*, Lecture Notes in Computer Science. Springer-Verlag, 2000.

[61] T. Johansson and F. Jonsson. Fast correlation attacks based on turbo code techniques. In *Advances in Cryptology – CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 181–197. Springer-Verlag, August 1999.

[62] T. Johansson and F. Jonsson. Improved fast correlation attacks on stream ciphers via convolutional codes. In *Advances in Cryptology – EUROCRYPT'99*, number 1592 in Lecture Notes in Computer Science, pages 347–362. Springer-Verlag, May 1999.

[63] T. Johansson and E. Pasalic. A construction of resilient functions with high nonlinearity. *International Symposium on Information Theory*, 2000.

[64] L. R. Knudsen. Truncated and Higher Order Differentials. In *Fast Software Encryption'1995*, Lecture Notes in Computer Science, pages 196–211, Springer-Verlag, 1995.

[65] D. E. Knuth. *The Art of Computer Programming*, volume 2. Addison Wesley, 1969.

[66] I. Krasikov. On integral zeros of Krawtchouk polynomials. *Journal of Combinatorial Theory, Series A*, 74:71–99, 1996.

[67] K. Kurosawa. Almost security of cryptographic Boolean functions. Cryptology e-print archive, http://eprint.iacr.org/2003/075.

[68] K. Kurosawa and T. Satoh. Generalization of higher order SAC to vector output Boolean functions. In *Advances in Cryptology – ASIACRYPT'96*, Lecture Notes in Computer Science, pages 218–231. Springer-Verlag, 1996.

[69] K. Kurosawa and T. Satoh. Design of SAC/PC($l$) of order $k$ Boolean functions and three other cryptographic criteria. In *Advances in Cryptology – EUROCRYPT'97*, Lecture Notes in Computer Science, pages 434–449. Springer-Verlag, 1997.

[70] K. Kurosawa, T. Satoh and K. Yamamoto. Highly nonlinear $t$-resilient functions . Journal of Universal Computer Science, vol.3, no. 6, pp. 721–729, Springer Publishing Company, 1997.

[71] X. Lai. Higher Order Derivative and Differential Cryptanalysis. In *Communication and Cryptography'1994*, Kluwer Academic Publisher, 1994.

[72] N. Linial, Y. Mansour and N. Nisan. Constant Depth Circuits, Fourier Transform, and Learnability. *Journal of the ACM*, 40(3): 607–620 (1993).

[73] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North Holland, 1977.

[74] S. Maitra and P. Sarkar. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. In *Advances in Cryptology – CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 198–215. Springer Verlag, August 1999.

[75] J. L. Massey. Shift register synthesis and bch decoding. *IEEE Transactions on Information Theory*, IT-15:122–127, January 1969.

[76] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology – EUROCRYPT'93*, Lecture Notes in Computer Science, pages 386–397. Springer-Verlag, 1994.

[77] W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean Functions. To be published In *Advances in Cryptology – EUROCRYPT'04*.

[78] W. Meier and O. Staffelbach. Fast correlation attack on stream ciphers. In *Advances in Cryptology – EUROCRYPT'88*, volume 330, pages 301–314. Springer-Verlag, May 1988.

[79] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology – EUROCRYPT'89*, pages 549–562. Springer-Verlag, 1990.

[80] W. Meier and O. Stafflebach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, 1:159–176, 1989.

[81] W. Meier and O. Staffelbach. Correlation Properties of Combiners with Memory in Stream Cipher. J. Cryptology. 5 (1) (1992) 67–86.

[82] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[83] K. Nyberg. Perfect Nonlinear S-boxes. In *Advances in Cryptology – EUROCRYPT 1991*, pages 378–386, Lecture Notes in Computer Science, Springer-Verlag, 1991.

[84] K. Nyberg. Differentially uniform mapping for cryptography. In *Advances in Cryptology – EUROCRYPT 1993*, pages 55–65, Lecture Notes in Computer Science, Springer-Verlag, 1994.

[85] K. Nyberg. Linear Approximation of Block Ciphers. In *Advances in Cryptology – EUROCRYPT 1994*, pages 439–444, Lecture Notes in Computer Science, Springer-Verlag, 1995.

[86] K. Nyberg. Correlation Theorems in Cryptanalysis. Discrete Applied Mathematics 111 (2001) 177–188.

[87] S. Palit and B. K. Roy. Cryptanalysis of LFSR-encrypted codes with unknown combining functions. In *Advances in Cryptology – ASIACRYPT'99*, number 1716 in Lecture Notes in Computer Science, pages 306–320. Springer Verlag, November 1999.

[88] E. Pasalic and T. Johansson. Further results on the relation between nonlinearity and resiliency of Boolean functions. In *IMA Conference on Cryptography and Coding*, number 1746 in Lecture Notes in Computer Science, pages 35–45. Springer-Verlag, 1999.

[89] E. Pasalic and S. Maitra. Linear Codes in Generalized Construction of Resilient Functions with Very High Nonlinearity. *IEEE Transactions on Information Theory*, Vol 48, No 8, pp. 2182–2191, August 2002.

[90] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983.

[91] N. J. Patterson and D. H. Wiedemann. Correction to - the covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-36(2):443, 1990.

[92] W. Penzhorn. Correlation attacks on stream ciphers : Computing low weight parity checks based on error correcting codes. In *Fast Software Encryption, FSE'96*, volume 1039, pages 159–172. Springer-Verlag, 1996.

[93] B. Preneel. Analysis and design of cryptographic hash functions, doctoral dissertation, K.U. Leuven, 1993.

[94] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, Lecture Notes in Computer Science, pages 161–173. Springer-Verlag, 1991.

[95] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Advances in Cryptology – EUROCRYPT'91*, Lecture Notes in Computer Science, pages 141–152. Springer-Verlag, 1991.

[96] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology – EUROCRYPT'90*, Lecture Notes in Computer Science, pages 161–173. Springer-Verlag, 1991.

[97] R. L. Rivest, M. J. B. Robshaw and Y. L. Yin. RC6 as the AES. In *AES Candidate Conference 2000*, pp 337–342.

[98] G. G. Rose and P. Hawkes. Turing: A Fast Stream Cipher. In *Fast Software Encryption, FSE 2003*, pages 290–306. Springer-Verlag, 2003.

[99] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.

[100] R. A. Rueppel. *Analysis and Design of Stream Ciphers*. Springer Verlag, 1986.

[101] R. A. Rueppel and O. J. Staffelbach. Products of linear recurring sequences with maximum complexity. *IEEE Transactions on Information Theory*, IT-33:124–131, January 1987.

[102] P. Sarkar. Hiji-bij-bij: A New Stream Cipher with a Self-Synchronizing Mode of Operation. In *Progress in Cryptology – Indoocrypt 2003*, pp 36–51, Lecture Notes in Computer Science, Springer-Verlag, 2003.

[103] P. Sarkar and S. Maitra. Construction of Nonlinear Boolean Functions with Important Cryptographic Properties. *In Advances in Cryptology – EUROCRYPT 2000*, pages 485–506, Lecture Notes in Computer Science, Springer-Verlag, 2000.

[104] B. Schneier, J. Kelsey, D. Whiting, D. Wagner and N. Ferguson. Comments on Twofish as an AES Candidate. In *AES Candidate Conference 2000*, pages 355–356.

[105] J. Seberry and X. M. Zhang. Highly nonlinear 0-1 balanced Boolean functions satisfying strict avalanche criterion. In *Advances in Cryptology, Auscrypt'92*, number 718 in Lecture Notes in Computer Science. Springer-Verlag, 1993.

[106] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearly balanced Boolean functions and their propagation characteristics. In *Advances in Cryptology – CRYPTO'93*, pages 49–60. Springer-Verlag, 1994.

[107] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune Boolean functions. In *Advances in Cryptology – EUROCRYPT'93*, pages 181–199. Springer-Verlag, 1994.

[108] J. Seberry, X. M. Zhang, and Y. Zheng. Structures of cryptographic functions with strong avalanche characteristics. In *Advances in Cryptology, Asiacrypt 94*, number 917 in Lecture Notes in Computer Science, pages 119–132. Springer-Verlag, 1995.

[109] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.

[110] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C-34(1):81–85, January 1985.

[111] O. Staffelbach and W. Meier. Cryptographic Significance of the Carry for Ciphers Based on Integer Addition. In *Advances in Cryptology – CRYPT0 1990*, pages 601–615, Lecture Notes in Computer Science, Springer-Verlag, 1991.

[112] D. R. Stinson. Resilient functions and large sets of orthogonal arrays. *Congressus Numerantium*, 92:105–110, 1993.

[113] D. R. Stinson. *Cryptography , Theory and Practice*. CRC Press, 1995.

[114] D. R. Stinson. *Cryptography , Theory and Practice, Second Edition*. CRC Press, 2002.

[115] D. R. Stinson and J. L. Massey. An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. *Journal of Cryptology*, 8(3):167–173, 1995.

[116] J Wallén. Linear Approximation of Addition Modulo $2^n$. *Tenth Annual Workshop on Fast Software Encryption* , February 24–26, 2003, AF-Borgen, Lund, Sweden, pages 277–290, Pre-proceedings.

[117] D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi and B. Preneel. A New Keystream Generator MUGI. In *Fast Software Encryption, FSE 2002*, pages 179–194. Springer-Verlag, 2002.

[118] A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology – CRYPTO'85*, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, 1986.

[119] G. Xiao and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, pages 569–571, 1988.

[120] M. Zhang. Maximum Correlation Analysis of Nonlinear Combining Functions in Stream Ciphers. *Journal of Cryptology*, 13(3): 301–314, 2000.

[121] M. Zhang and A. H. Chan. Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers. In *Advances in Cryptology – CRYPTO 2000*, Lecture Notes in Computer Science, pages 501–514. Springer-Verlag, 2000.

[122] X. M. Zhang and Y. Zheng. Cryptographically resilient functions. *IEEE Transactions on Information Theory*, 43(5):1740–1747, 1997.