Marc Fossorier
Hideki Imai
Shu Lin
Alain Poli (Eds.)

LNCS 3857

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

16th International Symposium, AAECC-16
Las Vegas, NV, USA, February 2006
Proceedings

Springer

Marc Fossorier Hideki Imai
Shu Lin Alain Poli (Eds.)

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

16th International Symposium, AAECC-16
Las Vegas, NV, USA, February 20-24, 2006
Proceedings

Springer

Volume Editors

Marc Fossorier
University of Hawaii, Department of Electrical Engineering
2540 Dole St., Holmes Hall 483, Honolulu, HI 96822, USA
E-mail: marc@spectra.eng.hawaii.edu

Hideki Imai
University of Tokyo, Institute of Industrial Science
Komaba, Meguro-ku, Tokyo 153-8505, Japan
E-mail: imai@iis.u-tokyo.ac.jp

Shu Lin
University of California, Department of Electrical and Computer Engineering
Davis One Shields Avenue, Davis, CA 95615, USA
E-mail: shulin@ece.udavis.edu

Alain Poli
University Paul Sabatier, AAECC/IRIT
118 route de Narbonne, 31067 Toulouse cedex, France
E-mail: poli@cict.fr

Library of Congress Control Number: 2005938816

CR Subject Classification (1998): E.4, I.1, E.3, G.2, F.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-31423-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-31423-3 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11617983 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3857

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Preface

The AAECC symposium was started in June 1983 by Alain Poli (Toulouse), who, together with R. Desq, D. Lazard, and P. Camion, organized the first conference. The meaning of the acronym AAECC changed from "Applied Algebra and Error Correcting Codes" to "Applied Algebra, Algebraic Algorithms, and Error Correcting Codes." One reason was the increasing importance of complexity, particularly for decoding algorithms. During the AAECC-12 symposium the Conference Committee decided to enforce the theory and practice of the coding side as well as the cryptographic aspects. Algebra is conserved as in the past, but slightly more oriented to algebraic geometry codes, finite fields, complexity, polynomials, and graphs.

For AAECC-16 the main subjects covered were:

- Block codes.
- Algebra and codes: rings, fields, AG codes.
- Cryptography.
- Sequences.
- Algorithms, decoding algorithms.
- Iterative decoding: code construction and decoding algorithms.
- Algebra: constructions in algebra, Galois group, differential algebra, polynomials.

Four invited speakers characterize the outlines of AAECC-16:

- C. Carlet ("On Bent and Highly Nonlinear Balanced/Resilient Functions and their Algebraic Immunities").
- S. Gao ("Grobner Bases and Linear Codes").
- R.J. McEliece ("On Generalized Parity Checks").
- T. Okamoto ("Cryptography Based on Bilinear Maps").

Except for AAECC-1 (Discrete Mathematics, 56, 1985) and AAECC-7 (Discrete Mathematics, 33, 1991), the proceedings of all the symposia have been published in Springer's *Lecture Notes in Computer Science* series (vol. 228, 229, 307, 356, 357, 508, 673, 948, 1255, 1719, 2227, 2643). It is a policy of AAECC to maintain a high scientific standard. This has been made possible thanks to the many referees involved. Each submitted paper was evaluated by at least two international researchers.

AAECC-16 received 32 submissions; 25 were selected for publication in these proceedings while 7 additional works contributed to the symposium as oral presentations. In addition to the four invited speakers, five invited papers also contributed to these proceedings.

The symposium was organized by Marc Fossorier, Shu Lin, Hideki Imai and Alain Poli, with the help of the 'Centre Baudis' in Toulouse.

We express our thanks to Springer staff, especially to Alfred Hofmann and Anna Kramer, as well as to the referees.

November 2005

M. Fossorier
S. Lin
H. Imai
A. Poli

Organization

Steering Committee

Conference General Chairman:	Shu Lin (Univ. of Davis, USA)
Conference Co-chairmen:	H. Imai (Univ. of Tokyo, Japan), Alain Poli (Univ. of Toulouse, France)
Publication:	Marc Fossorier (Univ. of Hawaii, USA)
Local Arrangements:	Fay Horie (Univ. of Hawaii, USA)

Conference Committee

J. Calmet
G. Cohen
S.D. Cohen
G.L. Feng
M. Giusti
J. Heintz
T. Hoehold
H. Imai
H. Janwa
J.M. Jensen
R. Kohno
H.W. Lenstra Jr.
S. Lin
O. Moreno
H. Niederreiter
A. Poli
T.R.N. Rao
S. Sakata
P. Sole

Program Committee

T. Berger
E. Biglieri
J. Calmet
C. Carlet
D. Costello
T. Ericson
P. Farrell
M. Fossorier
J. Hagenauer
S. Harari
T. Helleseth
E. Kaltofen
T. Kasami
L.R. Knudsen
S. Lietsyn
R.J. McEliece
R. Morelos-Zaragoza
H. Niederreiter
P. Sole
H. Tilborg

Lecture Notes in Computer Science

For information about Vols. 1–3769

please contact your bookseller or Springer

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3857: M. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 339 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision - ACCV 2006, Part II. XXXI, 977 pages. 2005.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision - ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Sublibrary LNAI).

Vol. 3834: D.G. Feitelson, E. Frachtenberg, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VIII, 283 pages. 2005.

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3832: D. Zhang, A.K. Jain (Eds.), Advances in Biometrics. XX, 796 pages. 2005.

Vol. 3831: J. Wiedermann, G. Tel, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2006: Theory and Practice of Computer Science. XV, 576 pages. 2006.

Vol. 3829: P. Pettersson, W. Yi (Eds.), Formal Modeling and Analysis of Timed Systems. IX, 305 pages. 2005.

Vol. 3828: X. Deng, Y. Ye (Eds.), Internet and Network Economics. XVII, 1106 pages. 2005.

Vol. 3827: X. Deng, D. Du (Eds.), Algorithms and Computation. XX, 1190 pages. 2005.

Vol. 3826: B. Benatallah, F. Casati, P. Traverso (Eds.), Service-Oriented Computing - ICSOC 2005. XVIII, 597 pages. 2005.

Vol. 3824: L.T. Yang, M. Amamiya, Z. Liu, M. Guo, F.J. Rammig (Eds.), Embedded and Ubiquitous Computing – EUC 2005. XXIII, 1204 pages. 2005.

Vol. 3823: T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, L.T. Yang (Eds.), Embedded and Ubiquitous Computing – EUC 2005 Workshops. XXXII, 1317 pages. 2005.

Vol. 3822: D. Feng, D. Lin, M. Yung (Eds.), Information Security and Cryptology. XII, 420 pages. 2005.

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3820: L.T. Yang, X. Zhou, W. Zhao, Z. Wu, Y. Zhu, M. Lin (Eds.), Embedded Software and Systems. XXVIII, 779 pages. 2005.

Vol. 3819: P. Van Hentenryck (Ed.), Practical Aspects of Declarative Languages. X, 231 pages. 2005.

Vol. 3818: S. Grumbach, L. Sui, V. Vianu (Eds.), Advances in Computer Science – ASIAN 2005. XIII, 294 pages. 2005.

Vol. 3817: M. Faundez-Zanuy, L. Janer, A. Esposito, A. Satue-Villar, J. Roure, V. Espinosa-Duro (Eds.), Nonlinear Analyses and Algorithms for Speech Processing. XII, 380 pages. 2006. (Sublibrary LNAI).

Vol. 3816: G. Chakraborty (Ed.), Distributed Computing and Internet Technology. XXI, 606 pages. 2005.

Vol. 3815: E.A. Fox, E.J. Neuhold, P. Premsmit, V. Wuwongse (Eds.), Digital Libraries: Implementing Strategies and Sharing Experiences. XVII, 529 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Sublibrary LNAI).

Vol. 3813: R. Molva, G. Tsudik, D. Westhoff (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. VIII, 219 pages. 2005.

Vol. 3810: Y.G. Desmedt, H. Wang, Y. Mu, Y. Li (Eds.), Cryptology and Network Security. XI, 349 pages. 2005.

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Sublibrary LNAI).

Vol. 3808: C. Bento, A. Cardoso, G. Dias (Eds.), Progress in Artificial Intelligence. XVIII, 704 pages. 2005. (Sublibrary LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3804: G. Bebis, R. Boyle, D. Koracin, B. Parvin (Eds.), Advances in Visual Computing. XX, 755 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3802: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part II. XLII, 1166 pages. 2005. (Sublibrary LNAI).

Vol. 3801: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part I. XLI, 1122 pages. 2005. (Sublibrary LNAI).

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

Vol. 3798: A. Dearle, S. Eisenbach (Eds.), Component Deployment. X, 197 pages. 2005.

Vol. 3797: S. Maitra, C. E. V. Madhavan, R. Venkatesan (Eds.), Progress in Cryptology - INDOCRYPT 2005. XIV, 417 pages. 2005.

Vol. 3796: N.P. Smart (Ed.), Cryptography and Coding. XI, 461 pages. 2005.

Vol. 3795: H. Zhuge, G.C. Fox (Eds.), Grid and Cooperative Computing - GCC 2005. XXI, 1203 pages. 2005.

Vol. 3794: X. Jia, J. Wu, Y. He (Eds.), Mobile Ad-hoc and Sensor Networks. XX, 1136 pages. 2005.

Vol. 3793: T. Conte, N. Navarro, W.-m.W. Hwu, M. Valero, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XIII, 317 pages. 2005.

Vol. 3792: I. Richardson, P. Abrahamsson, R. Messnarz (Eds.), Software Process Improvement. VIII, 215 pages. 2005.

Vol. 3791: A. Adi, S. Stoutenburg, S. Tabet (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 225 pages. 2005.

Vol. 3790: G. Alonso (Ed.), Middleware 2005. XIII, 443 pages. 2005.

Vol. 3789: A. Gelbukh, Á. de Albornoz, H. Terashima-Marín (Eds.), MICAI 2005: Advances in Artificial Intelligence. XXVI, 1198 pages. 2005. (Sublibrary LNAI).

Vol. 3788: B. Roy (Ed.), Advances in Cryptology - ASIACRYPT 2005. XIV, 703 pages. 2005.

Vol. 3787: D. Kratsch (Ed.), Graph-Theoretic Concepts in Computer Science. XIV, 470 pages. 2005.

Vol. 3785: K.-K. Lau, R. Banach (Eds.), Formal Methods and Software Engineering. XIV, 496 pages. 2005.

Vol. 3784: J. Taò, T. Tan, R.W. Picard (Eds.), Affective Computing and Intelligent Interaction. XIX, 1008 pages. 2005.

Vol. 3783: S. Qing, W. Mao, J. Lopez, G. Wang (Eds.), Information and Communications Security. XIV, 492 pages. 2005.

Vol. 3782: K.-D. Althoff, A. Dengel, R. Bergmann, M. Nick, T.R. Roth-Berghofer (Eds.), Professional Knowledge Management. XXIII, 739 pages. 2005. (Sublibrary LNAI).

Vol. 3781: S.Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, D. Zhang (Eds.), Advances in Biometric Person Authentication. XI, 250 pages. 2005.

Vol. 3780: K. Yi (Ed.), Programming Languages and Systems. XI, 435 pages. 2005.

Vol. 3779: H. Jin, D. Reed, W. Jiang (Eds.), Network and Parallel Computing. XV, 513 pages. 2005.

Vol. 3778: C. Atkinson, C. Bunse, H.-G. Gross, C. Peper (Eds.), Component-Based Software Development for Embedded Systems. VIII, 345 pages. 2005.

Vol. 3777: O.B. Lupanov, O.M. Kasim-Zade, A.V. Chaskin, K. Steinhöfel (Eds.), Stochastic Algorithms: Foundations and Applications. VIII, 239 pages. 2005.

Vol. 3776: S.K. Pal, S. Bandyopadhyay, S. Biswas (Eds.), Pattern Recognition and Machine Intelligence. XXIV, 808 pages. 2005.

Vol. 3775: J. Schönwälder, J. Serrat (Eds.), Ambient Networks. XIII, 281 pages. 2005.

Vol. 3774: G. Bierman, C. Koch (Eds.), Database Programming Languages. X, 295 pages. 2005.

Vol. 3773: A. Sanfeliu, M.L. Cortés (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XX, 1094 pages. 2005.

Vol. 3772: M.P. Consens, G. Navarro (Eds.), String Processing and Information Retrieval. XIV, 406 pages. 2005.

Vol. 3771: J.M.T. Romijn, G.P. Smith, J. van de Pol (Eds.), Integrated Formal Methods. XI, 407 pages. 2005.

Vol. 3770: J. Akoka, S.W. Liddle, I.-Y. Song, M. Bertolotto, I. Comyn-Wattiau, W.-J. van den Heuvel, M. Kolp, J. Trujillo, C. Kop, H.C. Mayr (Eds.), Perspectives in Conceptual Modeling. XXII, 476 pages. 2005.

Table of Contents

On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities

Claude Carlet*

INRIA, Projet CODES, BP 105 - 78153, Le Chesnay Cedex, France
claude.carlet@inria.fr

Abstract. Since the introduction of the notions of nonlinearity in the mid-70's (the term has been in fact introduced later), of correlation immunity and resiliency in the mid-80's, and of algebraic immunity recently, the problem of efficiently constructing Boolean functions satisfying, at high levels, one or several of these criteria has received much attention. Only few primary constructions are known, and secondary constructions are also necessary to obtain functions achieving or approaching the best possible cryptographic characteristics. After recalling the background on cryptographic criteria and making some general observations, we try to give a survey of all these constructions and their properties. We then show that a nice and simple property of Boolean functions leads to a general secondary construction building an n-variable function from three known n-variable functions. This construction generalizes secondary constructions recently obtained for Boolean bent functions and also leads to secondary constructions of highly nonlinear balanced or resilient functions, with potentially better algebraic immunities than the three functions used as building blocks.

Keywords: stream cipher, Boolean function, algebraic degree, resiliency, nonlinearity, algebraic attack.

1 Introduction

Boolean functions, that is, F_2-valued functions defined on the vector space F_2^n of all binary words of a given length n, are used in the S-boxes of block ciphers and in the pseudo-random generators of stream ciphers. They play a central role in their security. The generation of the keystream consists, in many stream ciphers, of a linear part, producing a sequence with a large period, usually composed of one or several LFSR's, and a nonlinear combining or filtering function f which produces the output, given the state of the linear part. The main classical cryptographic criteria for designing such function f are balancedness (f is balanced if its Hamming weight equals 2^{n-1}) to prevent the system from leaking statistical information on the plaintext when the ciphertext is known, a high algebraic

* Also member of the University of Paris 8 (MAATICAH).

M. Fossorier et al. (Eds.): AAECC 2006, LNCS 3857, pp. 1–28, 2006.

degree (that is, a high degree of the algebraic normal form of the function) to prevent the system from Massey's attack by the Berlekamp-Massey algorithm, a high order of correlation immunity (and more precisely, of resiliency, since the functions must be balanced) to counter correlation attacks (at least in the case of combining functions), and a high nonlinearity (that is, a large Hamming distance to affine functions) to withstand correlation attacks (again) and linear attacks.

The recent algebraic attacks have led to further characteristics of Boolean functions. These attacks recover the secret key by solving an overdefined system of multivariate algebraic equations. The scenarios found in [26], under which low degree equations can be deduced from the knowledge of the nonlinear combining or filtering function, have led in [48] to a new parameter, the (basic) algebraic immunity, which must be high. This condition is itself not sufficient, since a function can have sufficiently high algebraic immunity and be weak against fast algebraic attacks [25]. A further criterion strengthening the basic notion of algebraic immunity can be defined accordingly.

The problems of designing numerous bent functions (that is, functions with highest possible nonlinearity) and of efficiently constructing highly nonlinear balanced (or, if necessary, resilient) functions with high algebraic degrees have been receiving much attention for several years. They are relevant to several domains: mainly cryptography, but also combinatorics, design theory, coding theory ... Few primary constructions (in which the functions are designed *ex nihilo*) are known, and secondary constructions (which use already defined functions to design new ones) are also necessary to obtain functions, on a sufficient number of variables, achieving or approaching the best possible cryptographic characteristics. We can say that research has obtained limited but non-negligible success in these matters. However, the problem of meeting all of these characteristics at sufficient levels and, also, achieving high algebraic immunities, with functions whose outputs can be fastly computed (this is also a necessary condition for using them in stream ciphers) shows some resistance. The most efficient primary construction in this matter has been obtained in [29] (the authors present their result as a secondary construction, but as they observe themselves, their construction is just a direct sum of a function taken as a building block, with a function that they design and which corresponds to a primary construction). It leads to functions in any even numbers of variables and with optimal algebraic immunities. And as shown in [19], their algebraic degrees are very high and their output can be very fastly computed. They are not balanced, but any function! can be made balanced by adding one variable. The remaining problem is in their insufficient nonlinearities, which makes them unusable in cryptosystems. Used as a secondary construction, their method does not give full satisfaction either, for the same reason. Hence, this secondary construction represents a very nice but still partial step towards a good tradeoff between nonlinearity, resiliency and algebraic immunity.

Most classical primary or secondary constructions of highly nonlinear functions seem to produce insufficient algebraic immunities. For instance, the

10-variable Boolean function used in the LILI keystream generator (a submission to NESSIE European call for cryptographic primitives) is built following [56] by using classical constructions; see [59]. It has algebraic immunity 4 and is responsible for the lack of resistance of LILI to algebraic attacks, see [26].

As shown in [48], taking random balanced functions on sufficiently large numbers of variables could suffice to withstand algebraic attacks on the stream ciphers using them. It would also withstand fast algebraic attacks (this can be checked with the same methods as in [48]). As shown in [49], it would moreover give reasonable nonlinearities. But such solution would imply using functions on large numbers of variables, whose outputs would be computable in much too long time. This would not allow acceptable efficiency of the corresponding stream ciphers. It would not allow nonzero resiliency orders either.

The present paper tries to present the state of the art on Boolean cryptographic functions and to suggest several directions for further research. At the end of the paper, a construction (first presented in [17]) of functions on F_2^n from functions on F_2^n is presented, which combined with the classical primary and secondary constructions can lead to functions achieving high algebraic degrees, high nonlinearities and high resiliency orders, and which also allows attaining potentially high algebraic immunity. The same principle allows constructing bent functions too.

2 Preliminaries and General Observations

In some parts of this paper, we will deal in the same time with sums modulo 2 and with sums computed in $\mathbb{Z}$. We denote by $\oplus$ the addition in F_2 (but we denote by $+$ the addition in the field F_{2^n} and in the vector space F_2^n, since there will be no ambiguity) and by $+$ the addition in $\mathbb{Z}$. We denote by $\bigoplus_{i\in\ldots}$ (resp. $\sum_{i\in\ldots}$) the corresponding multiple sums. Let n be any positive integer. Any Boolean function f on n variables admits a unique algebraic normal form (A.N.F.):

$$f(x_1,\ldots,x_n) = \bigoplus_{I\subseteq\{1,\ldots,n\}} a_I \prod_{i\in I} x_i,$$

where the a_I's are in F_2. The terms $\prod_{i\in I} x_i$ are called *monomials*. The *algebraic degree* $d^\circ f$ of a Boolean function f equals the maximum degree of those monomials with nonzero coefficients in its algebraic normal form. *Affine functions* are those Boolean functions of degrees at most 1.

Another representation of Boolean functions is also very useful. The vector space F_2^n can be endowed with the structure of the field F_{2^n}, since this field is an n-dimensional F_2-vector space. The function $(u,v)\mapsto tr(u\,v)$, where $tr(u) = u + u^2 + u^{2^2} + \cdots + u^{2^{n-1}}$ is the *trace function*, is an inner product in F_{2^n}. Every Boolean function can be written in the form $f(x) = tr(F(x))$ where F is a mapping from F_{2^n} into F_{2^n}, and this leads to the *trace representation*: $f(x) = tr\left(\sum_{i=0}^{2^n-1} \beta_i\, x^i\right)$, where $\beta_i \in F_{2^n}$. Thanks to the fact that $tr(u^2) = tr(u)$ for every $u \in F_{2^n}$, we can restrict the exponents i with nonzero coefficients β_i so that there is at most one such exponent in each cyclotomic class $\{i \times 2^j\ [\bmod\ (2^n-1)]\,;\, j \in N\}$.

The *Hamming weight* $w_H(f)$ of a Boolean function f on n variables is the size of its support $\{x \in F_2^n;\ f(x)=1\}$. The *Hamming distance* $d_H(f,g)$ between two Boolean functions f and g is the Hamming weight of their difference $f \oplus g$. The *nonlinearity* of f is its minimum distance to all affine functions. Functions used in stream or block ciphers must have high nonlinearities to resist the attacks on these ciphers (correlation and linear attacks, see [4, 40, 41, 58]). The nonlinearity of f can be expressed by means of the discrete Fourier transform of the "sign" function $\chi_f(x) = (-1)^{f(x)}$, equal to $\widehat{\chi_f}(s) = \sum_{x\in F_2^n}(-1)^{f(x)\oplus x\cdot s}$ (and which is called the *Walsh transform*, or Walsh-Hadamard transform): the distance $d_H(f,l)$ between f and the affine function $l(x) = s\cdot x \oplus \epsilon$ $(s \in F_2^n;\ \epsilon \in F_2)$ and the number $\widehat{\chi_f}(s)$ are related by:

$$\widehat{\chi_f}(s) = (-1)^\epsilon(2^n - 2d_H(f,l)) \tag{1}$$

and the nonlinearity N_f of any Boolean function on F_2^n is therefore related to the Walsh spectrum of χ_f via the relation:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{s\in F_2^n}|\widehat{\chi_f}(s)|. \tag{2}$$

It is upper bounded by $2^{n-1} - 2^{n/2-1}$ because of the so-called Parseval's relation $\sum_{s\in F_2^n}\widehat{\chi_f}^2(s) = 2^{2n}$.

A Boolean function is called *bent* if its nonlinearity equals $2^{n-1} - 2^{n/2-1}$, where n is necessarily even. Then, its distance to every affine function equals $2^{n-1} \pm 2^{n/2-1}$, according to Parseval's relation again and to (1).

A Boolean function f is bent if and only if all of its *derivatives* $D_af(x) = f(x) \oplus f(x+a)$ are balanced, (see [53]). Hence, f is bent if and only if its support is a *difference set* (cf. [30]).

If f is bent, then the *dual* Boolean function $\widetilde{f}$ defined on F_2^n by $\widehat{\chi_f}(s) = 2^{\frac{n}{2}}\chi_{\widetilde{f}}(s)$ is bent. The dual of $\widetilde{f}$ is f itself. The mapping $f \mapsto \widetilde{f}$ is an isometry (the Hamming distance between two bent functions is equal to that of their duals).

The notion of bent function is invariant under linear equivalence and it is independent of the choice of the inner product in F_2^n (since any other inner product has the form $\langle x, s\rangle = x \cdot L(s)$, where L is an auto-adjoint linear isomorphism).

Rothaus' inequality [53] states that any bent function has algebraic degree at most $n/2$. Algebraic degree being an important complexity parameter, bent functions with high degrees are preferred from cryptographic viewpoint.

The class of bent functions, whose determination or classification is still an open problem, is relevant to cryptography (cf. [47]), to algebraic coding theory (cf. [45]), to sequence theory (cf. [51]) and to design theory (any difference set can be used to construct a symmetric design, cf. [1], pages 274-278). More information on bent functions can be found in the survey paper [10] or in the more recent chapter [18].

The class of bent functions is included in the class of the so-called *plateaued* functions. This notion has been introduced by Zheng and Zhang in [62]. A function is called plateaued if its Walsh transform takes at most three values 0 and $\pm\lambda$ (where λ is some positive integer, that we call the *amplitude* of the plateaued function). Because of Parseval's relation, λ must be of the form 2^r where $r \geq \frac{n}{2}$, and the suppport $\{s \in F_2^n / \widehat{\chi_f}(s) \neq 0\}$ of the Walsh transform of a plateaued function of amplitude 2^r has size 2^{2n-2r}.

Bent functions cannot be *balanced*, i.e. have uniformly distributed output. Hence, they cannot be used without modifications in the pseudo-random generator of a stream cipher, since this would leak statistical information on the plaintext, given the ciphertext[1]. Finding balanced functions with highest known nonlinearities is an important cryptographic task, as well as obtaining the best possible upper bounds on the nonlinearities of balanced functions. A nice way of designing highly nonlinear balanced functions is due to Dobbertin [33]: taking a bent function f which is constant on an $n/2$-dimensional flat A of F_2^n and replacing the values of f on A by the values of a highly nonlinear balanced function on A (identified to a function on $F_2^{n/2}$). The problem of similarly modifying bent functions into resilient functions (see definition below) has been studied in [46].

After the criteria of balancedness, high algebraic degree and high nonlinearity, which are relevant to all stream ciphers, another important cryptographic criterion for Boolean functions is resiliency. It plays a central role in their security, at least in the case of the standard model – the combination generator (cf. [57]). In this model, the vector whose coordinates are the outputs to n linear feedback shift registers is the input to a Boolean function. The output to the function during N clock cycles produces the keystream (of length N, the length of the plaintext), which is then (as in any stream cipher) bitwise xored with the message to produce the cipher. Some divide-and-conquer attacks exist on this method of encryption (cf. [4, 40, 41, 58]). To withstand these *correlation attacks*, the distribution probability of the output to the function must be unaltered when any m of its inputs are fixed [58], with m as large as possible. This property, called *m-th order correlation-immunity* [57], is characterized by the set of zero values in the Walsh spectrum [61]: f is m-th order correlation-immune if and only if $\widehat{\chi_f}(u) = 0$, for all $u \in F_2^n$ such that $1 \leq w_H(u) \leq m$, where $w_H(u)$ denotes the Hamming weight of the n-bit vector u, (the number of its nonzero components). Balanced m-th order correlation-immune functions are called *m-resilient* functions. They are characterized by the fact that $\widehat{\chi_f}(u) = 0$ for all $u \in F_2^n$ such that $0 \leq w_H(u) \leq m$.

The notions of correlation immune and resilient functions are not invariant under linear equivalence; they are invariant under translations $x \mapsto x + a$, since, if $g(x) = f(x + a)$, then $\widehat{\chi_g}(u) = \widehat{\chi_f}(u)(-1)^{a \cdot u}$, under permutations of the input coordinates, and when n is even, under an additional involution (see [38]).

Siegenthaler's inequality [57] states that any m-th order correlation immune function on n variables has degree at most $n - m$, that any m-resilient function

[1] However, as soon as n is large enough (say $n \geq 20$), the bias $\frac{2^{n/2-1}}{2^{n-1}}$ between their weights and the weight of balanced functions is quite small.