

Contents

Préface

Baha GÜCLÜ DÜNDAR, Faruk GÖLOĞLU, Ali DOĞANAKSOY, Zülfiükar SAYGI

A method of constructing highly nonlinear balanced Boolean functions

Joel RATSABY

Complexity of constrained Boolean function classes Of VC-dimension

Sumanta SARKAR, Subhamoy MAITRA

Efficient search for symmetric Boolean functions Under constraints on Walsh spectra values

Éric FÉRARD, François RODIER

Nonlinearity of some Boolean functions

Anna GROCHOLEWSKA-CZURYŁO

Random generation of highly nonlinear resilient Boolean functions

Selçuk KAVUT, Subhamoy MAITRA, Melek D. YÜCEL

Autocorrelation spectra of balanced Boolean functions On an odd number of input variables

Nils Gregor LEANDER

Another class of non-normal bent functions

Ali DOĞANAKSOY, Serhat SAĞDIÇOĞLU, Zülfiükar SAYGI, Muhiddin UĞUZ

A note on linearity and homomorphism

Deepak KUMAR DALAI, Kishan CHAND GUPTA, Subhamoy MAITRA

Notion of algebraic immunity and its evaluation related to fast algebraic attacks

Philippe LANGEVIN, Patrice RABIZZONI, Pascal VÉRON, Jean-Pierre ZANOTTI

On the number of bent functions with 8 variables

Deepak KUMAR DALAI, Subhamoy MAITRA, Sumanta SARKAR

Results on rotation symmetric bent functions

Miguel COUCEIRO, Maurice POUZET

On a quasi-ordering on Boolean functions

Faruk GÖLOĞLU, Melek D. YÜCEL

Necessary conditions on balanced Boolean functions With maximum nonlinearity

Olga MASNYK HANSEN, Jean-Francis MICHON

Boolean Gröbner Basis

.....

In « Fonctions booléennes / Boolean Functions » volume 1

Claude Carlet, Philippe Gaborit

On the Construction of Balanced Boolean Functions with a good Algebraic Immunity

Gwénoél Ars, Jean-Charles Faugère

Algebraic Immunities of Functions over Finite Fields

Elif Yildirim Saygi, Zülfiükar Saygi, Meltem Sönmez Turan, Ali Doğanaksoy

A Statistical Approach on the Number of Functions Satisfying Strict Avalanche Criteria

François Rodier

Asymptotic Distribution for the Nonlinearity of Boolean Functions

Claude Carlet, Sihem Mesnager

On the Supports of the Walsh Transforms of Boolean Functions

Alexander Maximov, Martin Hell, Subhamoy Maitra

Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables

Qingshu Meng, Min Yang, Huanguo Zhang, Yuzhen Liu

Analysis of Affinely Equivalent Boolean Functions

Gérard Duchamp, Hatem Hadj Kacem, Eric Laugerotte

On the Decomposition of Boolean Functions

Vincent Carlier, Hervé Chabanne, Emmanuelle Dottax

Grey-Box Implementation of Block Ciphers Preserving the Confidentiality of their Design

Philippe Guillot

Cryptographical Boolean Functions Construction from Linear Codes

Zu-Ling Chang, Fang-Wei Fu, Qiao-Yan Wen

Generalized Constructions of Highly Non-Linear Multi-Output Boolean Functions

Julien Bringer, Valérie Gillot, Philippe Langevin

Exponential Sums and Boolean Functions

Anna Grochowska-Czuryło

Randomly Generated Bent Boolean Functions