Contents

Invited Talk I

A Brief History of Pairings .................................................. 3
  Razvan Barbulescu

Elliptic Curves

Differential Addition on Binary Elliptic Curves ......................... 21
  Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini

Adequate Elliptic Curves for Computing the Product of n Pairings .... 36
  Loubna Ghammam and Emmanuel Fouotsa

On Pseudorandom Properties of Certain Sequences of Points on Elliptic Curve ............................................................... 54
  László Mérai

Applications

Linear Complexity and Expansion Complexity of Some Number Theoretic Sequences ............................................................. 67
  Richard Hofer and Arne Winterhof

Irreducible Polynomials

On Sets of Irreducible Polynomials Closed by Composition ............ 77
  Andrea Ferraguti, Giacomo Micheli, and Reto Schnyder

A Note on the Brawley-Carlitz Theorem on Irreducibility of Composed Products of Polynomials over Finite Fields ...................... 84
  Akihiro Munemasa and Hiroko Nakamura

Invited Talk II

On Arcs and Quadrics ............................................................. 95
  Simeon Ball

Applications to Cryptography

A Generalised Successive Resultants Algorithm .......................... 105
  James H. Davenport, Christophe Petit, and Benjamin Pring
Distribution and Polynomial Interpolation of the Dodis-Yampolskiy Pseudo-Random Function ................................................................. 125

Thierry Mefenza and Damien Vergnaud

Boolean Functions

A Conjecture About Gauss Sums and Bentness of Binomial Boolean Functions ................................................................. 143

Jean-Pierre Flori

Generalized Bent Functions and Their Gray Images. ................. 160

Thor Martinsen, Wilfried Meidl, and Pantelimon Stănică

Cryptography

Enhanced Digital Signature Using RNS Digit Exponent Representation . . . . 177

Thomas Plantard and Jean-Marc Robert

Efficient Finite Field Multiplication for Isogeny Based Post Quantum Cryptography ...................................................... 193

Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede

A Search Strategy to Optimize the Affine Variant Properties of S-Boxes . . . . 208

Stjepan Picek, Bohan Yang, and Nele Mentens

Cryptography and Boolean Functions

A Super-Set of Patterson-Wiedemann Functions – Upper Bounds and Possible Nonlinearities. .................................................. 227

Selçuk Kavut, Subhamoy Maitra, and Ferruh Özbudak

A Correction and Improvements of Some Recent Results on Walsh Transforms of Gold Type and Kasami-Welch Type Functions ................. 243

Ayhan Coşgun and Ferruh Özbudak

A Practical Group Signature Scheme Based on Rank Metric. ................. 258

Quentin Alamélo, Olivier Blazy, Stéphane Cauchie, and Philippe Gaborit

Author Index ............................................................................. 277
Arithmetic of Finite Fields
6th International Workshop, WAIFI 2016, Ghent, Belgium, July 13-15, 2016, Revised Selected Papers
duquesne, S.; Nikova, S. (Eds.)
2016, XII, 277 p. 12 illus., Softcover
ISBN: 978-3-319-55226-2