

Contents

Invited Talk I

A Brief History of Pairings	3
<i>Razvan Barbulescu</i>	

Elliptic Curves

Differential Addition on Binary Elliptic Curves.	21
<i>Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini</i>	
Adequate Elliptic Curves for Computing the Product of n Pairings	36
<i>Loubna Ghammam and Emmanuel Fouotsa</i>	
On Pseudorandom Properties of Certain Sequences of Points on Elliptic Curve.	54
<i>László Méri</i>	

Applications

Linear Complexity and Expansion Complexity of Some Number Theoretic Sequences	67
<i>Richard Hofer and Arne Winterhof</i>	

Irreducible Polynomials

On Sets of Irreducible Polynomials Closed by Composition	77
<i>Andrea Ferraguti, Giacomo Micheli, and Reto Schnyder</i>	
A Note on the Brawley-Carlitz Theorem on Irreducibility of Composed Products of Polynomials over Finite Fields.	84
<i>Akihiro Munemasa and Hiroko Nakamura</i>	

Invited Talk II

On Arcs and Quadrics	95
<i>Simeon Ball</i>	

Applications to Cryptography

A Generalised Successive Resultants Algorithm	105
<i>James H. Davenport, Christophe Petit, and Benjamin Pring</i>	

Distribution and Polynomial Interpolation of the Dodis-Yampolskiy Pseudo-Random Function.	125
<i>Thierry Mefenza and Damien Vergnaud</i>	

Boolean Functions

A Conjecture About Gauss Sums and Bentness of Binomial Boolean Functions.	143
<i>Jean-Pierre Flori</i>	

Generalized Bent Functions and Their Gray Images.	160
<i>Thor Martinsen, Wilfried Meidl, and Pantelimon Stănică</i>	

Cryptography

Enhanced Digital Signature Using RNS Digit Exponent Representation	177
<i>Thomas Plantard and Jean-Marc Robert</i>	

Efficient Finite Field Multiplication for Isogeny Based Post Quantum Cryptography	193
<i>Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede</i>	

A Search Strategy to Optimize the Affine Variant Properties of S-Boxes	208
<i>Stjepan Picek, Bohan Yang, and Nele Mentens</i>	

Cryptography and Boolean Functions

A Super-Set of Patterson-Wiedemann Functions – Upper Bounds and Possible Nonlinearities.	227
<i>Selçuk Kavut, Subhamoy Maitra, and Ferruh Özbudak</i>	

A Correction and Improvements of Some Recent Results on Walsh Transforms of Gold Type and Kasami-Welch Type Functions	243
<i>Ayhan Coşgun and Ferruh Özbudak</i>	

A Practical Group Signature Scheme Based on Rank Metric.	258
<i>Quentin Alamélou, Olivier Blazy, Stéphane Cauchie, and Philippe Gaborit</i>	

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