

Contents

First Invited Talk

Computing Discrete Logarithms in $\mathbb{F}_{3^{6 \cdot 137}}$ and $\mathbb{F}_{3^{6 \cdot 163}}$ Using Magma	3
<i>Gora Adj, Alfred Menezes, Thomaz Oliveira,</i> <i>and Francisco Rodríguez-Henríquez</i>	

Finite Field Arithmetic

Accelerating Iterative SpMV for the Discrete Logarithm Problem Using GPUs	25
<i>Hamza Jeljeli</i>	
Finding Optimal Chudnovsky-Chudnovsky Multiplication Algorithms	45
<i>Matthieu Rambaud</i>	
Reducing the Complexity of Normal Basis Multiplication	61
<i>Ömer Eğecioğlu and Çetin Kaya Koç</i>	

Second Invited Talk

Open Questions on Nonlinearity and on APN Functions	83
<i>Claude Carlet</i>	

Boolean and Vectorial Functions

Some Results on Difference Balanced Functions	111
<i>Alexander Pott and Qi Wang</i>	
Affine Equivalency and Nonlinearity Preserving Bijective Mappings over \mathbb{F}_2	121
<i>İsa Sertkaya, Ali Doğanaksoy, Osmanbey Uzunkol,</i> <i>and Mehmet Sabır Kiraz</i>	
On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions.	137
<i>Ferruh Özbudak, Ahmet Sınak, and Oğuz Yayla</i>	
On o-Equivalence of Niho Bent Functions	155
<i>Lilya Budaghyan, Claude Carlet, Tor Helleseeth,</i> <i>and Alexander Kholosha</i>	

Third Invited Talk

L-Polynomials of the Curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over \mathbb{F}_{q^m}	171
<i>Ferruh Özbudak and Zülfükar Saygi</i>	

Coding Theory and Code-Based Cryptography

Efficient Software Implementations of Code-Based Hash Functions and Stream-Ciphers	187
<i>Pierre-Louis Cayrel, Mohammed Meziani, Ousmane Ndiaye, and Quentin Santos</i>	

Quadratic Residue Codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$	204
<i>Yan Liu, Minjia Shi, and Patrick Solé</i>	

Author Index	213
-------------------------------	-----

Arithmetic of Finite Fields

5th International Workshop, WAIFI 2014, Gebze, Turkey,

September 27-28, 2014. Revised Selected Papers

Koç, Ç.K.; Mesnager, S.; Savas, E. (Eds.)

2015, X, 213 p. 18 illus., Softcover

ISBN: 978-3-319-16276-8