## Contents

### First Invited Talk

Computing Discrete Logarithms in $\mathbb{F}_{36^{137}}$ and $\mathbb{F}_{36^{163}}$ Using Magma

_Gora Adj, Alfred Menezes, Thomaz Oliveira, and Francisco Rodríguez-Henríquez_

### Finite Field Arithmetic

Accelerating Iterative SpMV for the Discrete Logarithm Problem

_Use of GPUs_  
_Hamza Jeljeli_

Finding Optimal Chudnovsky-Chudnovsky Multiplication Algorithms

_Matthieu Rambaud_

Reducing the Complexity of Normal Basis Multiplication

_Ömer Eğecioğlu and Çetin Kaya Koç_

### Second Invited Talk

Open Questions on Nonlinearity and on APN Functions

_Claude Carlet_

### Boolean and Vectorial Functions

Some Results on Difference Balanced Functions

_Alexander Pott and Qi Wang_

Affine Equivalency and Nonlinearity Preserving Bijective Mappings over $\mathbb{F}_2$

_İsa Sertkaya, Ali Doğanaksoy, Osmanbey Uzunkol, and Mehmet Sabır Kiraz_

On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions

_Ferruh Özbudak, Ahmet Sinak, and Oğuz Yayla_

On o-Equivalence of Niho Bent Functions

_Lilya Budaghyan, Claude Carlet, Tor Helleseth, and Alexander Kholosha_
Third Invited Talk

L-Polynomials of the Curve $y^{q} - y = \gamma x^{q^{d}+1} - \alpha$ over $F_q$.

Ferruh Özbudak and Zülfükar Saygı

171

Coding Theory and Code-Based Cryptography

Efficient Software Implementations of Code-Based Hash Functions and Stream-Ciphers.

Pierre-Louis Cayrel, Mohammed Meziani, Ousmane Ndiaye, and Quentin Santos

187

Quadratic Residue Codes over $F_p + vF_p + v^2F_p$.

Yan Liu, Minjia Shi, and Patrick Solé

204

Author Index

213