

# Table of Contents

## Invited Talk 1

|                                                                  |   |
|------------------------------------------------------------------|---|
| Recursive Towers of Function Fields over Finite Fields . . . . . | 1 |
| <i>Henning Stichtenoth</i>                                       |   |

## Efficient Finite Field Arithmetic

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| High-Performance Modular Multiplication on the Cell Processor . . . . .             | 7  |
| <i>Joppe W. Bos</i>                                                                 |    |
| A Modified Low Complexity Digit-Level Gaussian Normal Basis<br>Multiplier . . . . . | 25 |
| <i>Reza Azarderakhsh and Arash Reyhani-Masoleh</i>                                  |    |
| Type-II Optimal Polynomial Bases . . . . .                                          | 41 |
| <i>Daniel J. Bernstein and Tanja Lange</i>                                          |    |

## Pseudo-random Numbers and Sequences

|                                                                                                                 |    |
|-----------------------------------------------------------------------------------------------------------------|----|
| Pseudorandom Vector Sequences Derived from Triangular Polynomial<br>Systems with Constant Multipliers . . . . . | 62 |
| <i>Alina Ostafe</i>                                                                                             |    |
| Structure of Pseudorandom Numbers Derived from Fermat Quotients . . .                                           | 73 |
| <i>Zhizhong Chen, Alina Ostafe, and Arne Winterhof</i>                                                          |    |

## Boolean Functions

|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| Distribution of Boolean Functions According to the Second-Order<br>Nonlinearity . . . . . | 86 |
| <i>Stéphanie Dib</i>                                                                      |    |
| Hyper-bent Boolean Functions with Multiple Trace Terms . . . . .                          | 97 |
| <i>Sihem Mesnager</i>                                                                     |    |

## Invited Talk 2

|                                                                                                          |     |
|----------------------------------------------------------------------------------------------------------|-----|
| On the Efficiency and Security of Pairing-Based Protocols in the<br>Type 1 and Type 4 Settings . . . . . | 114 |
| <i>Sanjit Chatterjee, Darrel Hankerson, and Alfred Menezes</i>                                           |     |

## Functions, Equations and Modular Multiplication

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| Switching Construction of Planar Functions on Finite Fields.....       | 135 |
| <i>Alexander Pott and Yue Zhou</i>                                     |     |
| Solving Equation Systems by Agreeing and Learning .....                | 151 |
| <i>Thorsten Ernst Schilling and Håvard Raddum</i>                      |     |
| Speeding Up Bipartite Modular Multiplication.....                      | 166 |
| <i>Miroslav Knežević, Frederik Vercauteren, and Ingrid Verbauwhede</i> |     |

## Finite Field Arithmetic for Pairing Based Cryptography

|                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------|-----|
| Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography ..... | 180 |
| <i>Naomi Benger and Michael Scott</i>                                                                 |     |
| Delaying Mismatched Field Multiplications in Pairing Computations ...                                 | 196 |
| <i>Craig Costello, Colin Boyd, Juan Manuel Gonzalez Nieto, and Kenneth Koon-Ho Wong</i>               |     |

## Invited Talk 3

|                                                                           |     |
|---------------------------------------------------------------------------|-----|
| Regenerating Codes for Distributed Storage Networks .....                 | 215 |
| <i>Nihar B. Shah, K.V. Rashmi, P. Vijay Kumar, and Kannan Ramchandran</i> |     |

## Finite Fields, Cryptography and Coding

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| On Rationality of the Intersection Points of a Line with a Plane Quartic ..... | 224 |
| <i>Roger Oyono and Christophe Ritzenthaler</i>                                 |     |
| Reflections about a Single Checksum .....                                      | 238 |
| <i>Ulrich Tamm</i>                                                             |     |
| Efficient Time-Area Scalable ECC Processor Using $\mu$ -Coding Technique.....  | 250 |
| <i>Mohamed N. Hassan and Mohammed Benaïssa</i>                                 |     |

|                   |     |
|-------------------|-----|
| Author Index..... | 269 |
|-------------------|-----|