# Table of Contents

## Coding Theory

Subspace Codes ..... 1
*Azadeh Khaleghi, Danilo Silva, and Frank R. Kschischang*

On Linear Programming Decoding on a Quantized Additive White Gaussian Noise Channel ..... 22
*Eirik Rosnes*

Codes as Modules over Skew Polynomial Rings ..... 38
*Delphine Boucher and Felix Ulmer*

On Higher Weights and Code Existence ..... 56
*Hans Georg Schaathun*

Mass Formula for Even Codes over $\mathbb{Z}_8$ ..... 65
*Koichi Betsumiya, Rowena Alma L. Betty, and Akihiro Munemasa*

On the Classification of Self-dual $\mathbb{Z}_k$-Codes ..... 78
*Masaaki Harada and Akihiro Munemasa*

On Linear Codes from Maximal Curves ..... 91
*Stefania Fanali*

## Symmetric Cryptography

On Linear Cryptanalysis with Many Linear Approximations ..... 112
*Benoît Gérard and Jean-Pierre Tillich*

Bivium as a Mixed-Integer Linear Programming Problem ..... 133
*Julia Borghoff, Lars R. Knudsen, and Mathias Stolpe*

Security of Cyclic Double Block Length Hash Functions ..... 153
*Ewan Fleischmann, Michael Gorski, and Stefan Lucks*

Another Glance at Double-Length Hashing ..... 176
*Onur Özen and Martijn Stam*

Geometric Ideas for Cryptographic Equation Solving in Even Characteristic ..... 202
*Sean Murphy and Maura B. Paterson*

## Security Protocols

Provably Secure Code-Based Threshold Ring Signatures ..... 222
*Léonard Dallot and Damien Vergnaud*

A New Protocol for the Nearby Friend Problem ..... 236
*Sanjit Chatterjee, Koray Karabina, and Alfred Menezes*

Distributing the Key Distribution Centre in Sakai Kasahara Based Systems ..... 252
*Martin Geisler and Nigel P. Smart*

Key Predistribution Schemes and One-Time Broadcast Encryption Schemes from Algebraic Geometry Codes ..... 263
*Hao Chen, San Ling, Carles Padró, Huaxiong Wang, and Chaoping Xing*

Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes ..... 278
*Nuttapong Attrapadung and Hideki Imai*

Certificate-Free Attribute Authentication ..... 301
*Dalia Khader, Liqun Chen, and James H. Davenport*

## Asymmetric Cryptography

Comparing with RSA ..... 326
*Julien Cathalo, David Naccache, and Jean-Jacques Quisquater*

Double-Exponentiation in Factor-4 Groups and Its Applications ..... 336
*Koray Karabina*

Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms ..... 351
*Antoine Joux, Reynald Lercier, David Naccache, and Emmanuel Thomé*

An Improvement to the Gaudry-Schost Algorithm for Multidimensional Discrete Logarithm Problems ..... 368
*Steven Galbraith and Raminder S. Ruprai*

## Boolean Functions

On Designs and Multiplier Groups Constructed from Almost Perfect Nonlinear Functions ..... 383
*Yves Edel and Alexander Pott*

A New Family of Hyper-Bent Boolean Functions in Polynomial Form ... 402
*Sihem Mesnager*

The Rayleigh Quotient of Bent Functions ..... 418
*Lars Eirik Danielsen, Matthew G. Parker, and Patrick Solé*

## Side Channels and Implementations

Cache Timing Analysis of LFSR-Based Stream Ciphers ..... 433
*Gregor Leander, Erik Zenner, and Philip Hawkes*

Optimal Recovery of Secret Keys from Weak Side Channel Traces ..... 446
*Werner Schindler and Colin D. Walter*

Practical Zero-Knowledge Proofs for Circuit Evaluation ..... 469
*Essam Ghadafi, Nigel P. Smart, and Bogdan Warinschi*

**Author Index** ..... 495