Contents

Preface vii

Computational Number Theory

C. Alonso, J. Gutierrez and R. Rubio
On the Dimension and the Number of Parameters of a Unirational Variety 3

A. Conflitti
On Elements of High Order in Finite Fields 11

C. Ding, D.R. Kohel and S. Ling
Counting the Number of Points on Affine Diagonal Curves 15

J. Friedlander, C. Pomerance and I.E. Shparlinski
Small Values of the Carmichael Function and Cryptographic Applications 25

J. von zur Gathen and F. Pappalardi
Density Estimates Related to Gauss Periods 33

W. Han
Distribution of the Coefficients of Primitive Polynomials over Finite Fields 43

J. Hoffstein and D. Lieman
The Distribution of the Quadratic Symbol in Function Fields and a Faster Mathematical Stream Cipher 59

D. Kohel
Rational Groups of Elliptic Curves Suitable for Cryptography 69

K.Y. Lam and F. Sica
Effective Determination of the Proportion of Split Primes in Number Fields 81

P. Mihalescu
Algorithms for Generating, Testing and Proving Primes: A Survey 93

R. Peralta
Elliptic Curve Factorization Using a "Partially Oblivious" Function 123

A.J. van der Poorten
The Hermite-Serret Algorithm and $12^2 + 33^2$ 129

C.P. Xing
Applications of Algebraic Curves to Constructions of Sequences 137

Cryptography

N. Alexandris, M. Burmester, V. Chrissikopoulos and Y. Desmedt
Designated 2-Verifier Proofs and their Application to Electronic Commerce 149

E. Dawson, L. Simpson and J. Golić
Divide and Conquer Attacks on Certain Irregularly Clocked Stream Ciphers 165

A. De Bonis and A. De Santis
New Results on the Randomness of Visual Cryptography Schemes 187

D. Gollmann
Authentication – Myths and Misconceptions 203

M.I. Gonzales Vasco and M. Naslund
A Survey of Bit-security and Hard Core Functions 227

M.I. Gonzales Vasco and I.E. Shparlinski
On the Security of Diffie–Hellman Bits 257

J. Hoffstein and J.H. Silverman
Polynomial Rings and Efficient Public Key Authentication II 269

P. Mihalescu
Security of Biased Sources for Cryptographic Keys 287

M. Naslund and A. Russell
Achieving Optimal Fairness from Biased Coinflips 303

P.Q. Nguyen
The Dark Side of the Hidden Number Problem: Lattice Attacks on DSA 321

P.Q. Nguyen, I.E. Shparlinski and J. Stern
Distribution of Modular Sums and the Security of the Server Aided Exponentiation 331

R. Safavi-Naini and W. Susilo
A General Construction for Fail-Stop Signatures using Authentication Codes 343

R. Safavi-Naini and H. Wang
Robust Additive Secret Sharing Schemes over $\mathbf{Z_m}$ 357

R.D. Silverman
RSA Public Key Validation 369