Table of Contents

Personal Tributes

Laudatio in Honour of Professor Dr. Johannes Buchmann on the Occasion of His 60th Birthday 1
Hugh C. Williams

Have a Break – Have a Security Centre: From DZI to CASED 3
Harald Baier

Computational Number Theory

Operating Degrees for XL vs. F_4/F_5 for Generic $\mathcal{MQ}$ with Number of Equations Linear in That of Variables 19
Jenny Yuan-Chun Yeh, Chen-Mou Cheng, and Bo-Yin Yang

Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields 34
Jintai Ding and Dieter Schmidt

Shorter Compact Representations in Real Quadratic Fields 50
Alan K. Silvester, Michael J. Jacobson Jr., and Hugh C. Williams

Hardness of Cryptographic Assumptions

Factoring Integers by CVP Algorithms 73
Claus Peter Schnorr

Solving the Elliptic Curve Discrete Logarithm Problem Using Semaev Polynomials, Weil Descent and Gröbner Basis Methods – An Experimental Study 94
Michael Shantz and Edlyn Teske

An Experiment of Number Field Sieve for Discrete Logarithm Problem over GF(p^{12}) 108
Kenichiro Hayasaka, Kazumaro Aoki, Tetsutaro Kobayashi, and Tsuyoshi Takagi

Universal Security: From Bits and Mips to Pools, Lakes – and Beyond 121
Arjen K. Lenstra, Thorsten Kleinjung, and Emmanuel Thomé

Hardware Security

Identities for Embedded Systems Enabled by Physical Unclonable Functions 125
Dominik Merli, Georg Sigl, and Claudia Eckert

When Should an Implementation Attack Be Viewed as Successful? 139
Werner Schindler

AMASIVE: An Adaptable and Modular Autonomous Side-Channel Vulnerability Evaluation Framework 151
Sorin A. Huss, Marc Stöttinger, and Michael Zohner

A Performance Boost for Hash-Based Signatures 166
Thomas Eisenbarth, Ingo von Maurich, Christof Paar, and Xin Ye

Privacy and Security

Privacy-Preserving Reconciliation Protocols: From Theory to Practice 183
Ulrike Meyer and Susanne Wetzel

Defining Privacy Based on Distributions of Privacy Breaches 211
Matthias Huber, Jörn Müller-Quade, and Tobias Nilges

A Constructive Perspective on Key Encapsulation 226
Sandro Coretti, Ueli Maurer, and Björn Tackmann

Application Security

Why Are Business Processes Not Secure? 240
Günter Müller and Rafael Accorsi

Mental Models – General Introduction and Review of Their Application to Human-Centred Security 255
Melanie Volkamer and Karen Renaud

Author Index 281