CONTEMPORARY MATHEMATICS

418

Algebraic Methods in Cryptography

AMS/DMV Joint International Meeting
June 16–19, 2005
Mainz, Germany

International Workshop on Algebraic Methods
in Cryptography
November 17–18, 2005
Bochum, Germany

Lothar Gerritzen
Dorian Goldfeld
Martin Kreuzer
Gerhard Rosenberger
Vladimir Shpilrain
Editors

American Mathematical Society

http://dx.doi.org/10.1090/conm/418

Algebraic Methods in Cryptography

CONTEMPORARY
MATHEMATICS

418

Algebraic Methods in Cryptography

AMS/DMV Joint International Meeting
June 16–19, 2005
Mainz, Germany

International Workshop on Algebraic Methods in Cryptography
November 17–18, 2005
Bochum, Germany

Lothar Gerritzen
Dorian Goldfeld
Martin Kreuzer
Gerhard Rosenberger
Vladimir Shpilrain
Editors

American Mathematical Society
Providence, Rhode Island

2000 *Mathematics Subject Classification.* Primary 94A60, 20Fxx, 68P25, 68W20, 68W30, 11T71, 57M05.

Library of Congress Cataloging-in-Publication Data

Special Session on Algebraic Cryptography at the Joint International Meeting of the AMS and the Deutsche Mathematiker-Vereinigung (2005 : Mainz, Germany)

Algebraic methods in cryptography : Special Session on Algebraic Cryptography at the Joint International Meeting of the AMS and the Deutsche Mathematiker-Vereinigung, June 16–19, 2005, Mainz, Germany : International Workshop on Algebraic Methods in Cryptography, November 17–18, 2005, Bochum, Germany / editors, Lothar Gerritzen... [et al.].

p. cm. — (Contemporary mathematics, ISSN 0271-4132 ; v. 418)

ISBN-13: 978-0-8218-4037-5 (alk. paper)

ISBN-10: 0-8218-4037-1 (alk. paper)

1. Algebra. 2. Cryptography. I. Gerritzen, Lothar, 1941– II. American Mathematical Society. III. Deutsche Mathematiker-Vereinigung. IV. International Workshop on Algebraic Methods in Cryptography (2005 : Bochum, Germany) V. Title.

QA150.S64 2005
652′.8—dc22 2006043028

♾ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at http://www.ams.org/

10 9 8 7 6 5 4 3 2 1 11 10 09 08 07 06

Contents

Preface

This volume consists of contributions by speakers at the Special Session on Algebraic Cryptography at the Joint International Meeting of the AMS with the Deutsche Mathematiker-Vereinigung held in Mainz, Germany, on June 16–19, 2005, and at the International Workshop on Algebraic Methods in Cryptography held in Bochum, Germany, on November 17–18, 2005.

The readers will find here a variety of contributions, mostly related to public-key cryptography, including design of new cryptographic primitives as well as cryptanalysis of previously suggested schemes. Most papers are original research papers in the area that can be loosely defined as "Non-commutative cryptography"; this means that groups (or other algebraic structures) which are used as platforms are non-commutative.

We are grateful to the American Mathematical Society for assisting us in publication of this volume. In particular, we thank Christine M. Thivierge for her patient work in putting this volume together.

Lothar Gerritzen
Dorian Goldfeld
Martin Kreuzer
Gerhard Rosenberger
Vladimir Shpilrain

Titles in This Series

418 **Lothar Gerritzen, Dorian Goldfeld, Martin Kreuzer, Gerhard Rosenberger, and Vladimir Shpilrain, Editors,** Algebraic methods in cryptography, 2006

417 **Vadim B. Kuznetsov and Siddhartha Sahi, Editors,** Jack, Hall-Littlewood and Macdonald polynomials, 2006

416 **Toshitake Kohno and Masanori Morishita, Editors,** Primes and Knots, 2006

415 **Gregory Berkolaiko, Robert Carlson, Stephen A. Fulling, and Peter Kuchment, Editors,** Quantum Graphs and Their Applications, 2006

414 **Deguang Han, Palle E. T. Jorgensen, and David Royal Larson, Editors,** Operator theory, operator algebras, and applications, 2006

413 **Georgia M. Benkart, Jens C. Jantzen, Zongzhu Lin, Daniel K. Nakano, and Brian J. Parshall, Editors,** Representations of algebraic groups, quantum groups and Lie algebras, 2006

412 **Nikolai Chernov, Yulia Karpeshina, Ian W. Knowles, Roger T. Lewis, and Rudi Weikard, Editors,** Recent advances in differential equations and mathematical physics, 2006

411 **J. Marshall Ash and Roger L. Jones, Editors,** Harmonic analysis: Calderón-Zygmund and beyond, 2006

410 **Abba Gumel, Carlos Castillo-Chavez, Ronald E. Mickens, and Dominic P. Clemence, Editors,** Mathematical studies on human disease dynamics: Emerging paradigms and challenges, 2006

409 **Juan Luis Vázquez, Xavier Cabré, and José Antonio Carrillo, Editors,** Recent trends in partial differential equations, 2006

408 **Habib Ammari and Hyeonbae Kang, Editors,** Inverse problems, multi-scale analysis and effective medium theory, 2006

407 **Alejandro Ádem, Jesús González, and Guillermo Pastor, Editors,** Recent developments in algebraic topology, 2006

406 **José A. de la Peña and Raymundo Bautista, Editors,** Trends in representation theory of algebras and related topics, 2006

405 **Andrew Markoe and Eric Todd Quinto, Editors,** Integral geometry and tomography, 2006

404 **Alexander Borichev, Håkan Hedenmalm, and Kehe Zhu, Editors,** Bergman spaces and related topics in complex analysis, 2006

403 **Tyler J. Jarvis, Takashi Kimura, and Arkady Vaintrob, Editors,** Gromov-Witten theory of spin curves and orbifolds, 2006

402 **Zvi Arad, Mariagrazia Bianchi, Wolfgang Herfort, Patrizia Longobardi, Mercede Maj, and Carlo Scoppola, Editors,** Ischia group theory 2004, 2006

401 **Katrin Becker, Melanie Becker, Aaron Bertram, Paul S. Green, and Benjamin McKay, Editors,** Snowbird lectures on string geometry, 2006

400 **Shiferaw Berhanu, Hua Chen, Jorge Hounie, Xiaojun Huang, Sheng-Li Tan, and Stephen S.-T. Yau, Editors,** Recent progress on some problems in several complex variables and partial differential equations, 2006

399 **Dominique Arlettaz and Kathryn Hess, Editors,** An Alpine anthology of homotopy theory, 2006

398 **Jay Jorgenson and Lynne Walling, Editors,** The ubiquitous heat kernel, 2006

397 **José M. Muñoz Porras, Sorin Popescu, and Rubí E. Rodríguez, Editors,** The geometry of Riemann surfaces and Abelian varieties, 2006

396 **Robert L. Devaney and Linda Keen, Editors,** Complex dynamics: Twenty-five years after the appearance of the Mandelbrot set, 2006

395 **Gary R. Jensen and Steven G. Krantz, Editors,** 150 Years of Mathematics at Washington University in St. Louis, 2006

TITLES IN THIS SERIES

394 **Rostislav Grigorchuk, Michael Mihalik, Mark Sapir, and Zoran Šuniḱ, Editors,** Topological and asymptotic aspects of group theory, 2006

393 **Alec L. Matheson, Michael I. Stessin, and Richard M. Timoney, Editors,** Recent advances in operator-related function theory, 2006

392 **Stephen Berman, Brian Parshall, Leonard Scott, and Weiqiang Wang, Editors,** Infinite-dimensional aspects of representation theory and applications, 2005

391 **Jürgen Fuchs, Jouko Mickelsson, Grigori Rozenblioum, Alexander Stolin, and Anders Westerberg, Editors,** Noncommutative geometry and representation theory in mathematical physics, 2005

390 **Sudhir Ghorpade, Hema Srinivasan, and Jugal Verma, Editors,** Commutative algebra and algebraic geometry, 2005

389 **James Eells, Etienne Ghys, Mikhail Lyubich, Jacob Palis, and José Seade, Editors,** Geometry and dynamics, 2005

388 **Ravi Vakil, Editor,** Snowbird lectures in algebraic geometry, 2005

387 **Michael Entov, Yehuda Pinchover, and Michah Sageev, Editors,** Geometry, spectral theory, groups, and dynamics, 2005

386 **Yasuyuki Kachi, S. B. Mulay, and Pavlos Tzermias, Editors,** Recent progress in arithmetic and algebraic geometry, 2005

385 **Sergiy Kolyada, Yuri Manin, and Thomas Ward, Editors,** Algebraic and topological dynamics, 2005

384 **B. Diarra, A. Escassut, A. K. Katsaras, and L. Narici, Editors,** Ultrametric functional analysis, 2005

383 **Z.-C. Shi, Z. Chen, T. Tang, and D. Yu, Editors,** Recent advances in adaptive computation, 2005

382 **Mark Agranovsky, Lavi Karp, and David Shoikhet, Editors,** Complex analysis and dynamical systems II, 2005

381 **David Evans, Jeffrey J. Holt, Chris Jones, Karen Klintworth, Brian Parshall, Olivier Pfister, and Harold N. Ward, Editors,** Coding theory and quantum computing, 2005

380 **Andreas Blass and Yi Zhang, Editors,** Logic and its applications, 2005

379 **Dominic P. Clemence and Guoqing Tang, Editors,** Mathematical studies in nonlinear wave propagation, 2005

378 **Alexandre V. Borovik, Editor,** Groups, languages, algorithms, 2005

377 **G. L. Litvinov and V. P. Maslov, Editors,** Idempotent mathematics and mathematical physics, 2005

376 **José A. de la Peña, Ernesto Vallejo, and Natig Atakishiyev, Editors,** Algebraic structures and their representations, 2005

375 **Joseph Lipman, Suresh Nayak, and Pramathanath Sastry,** Variance and duality for cousin complexes on formal schemes, 2005

374 **Alexander Barvinok, Matthias Beck, Christian Haase, Bruce Reznick, and Volkmar Welker, Editors,** Integer points in polyhedra—geometry, number theory, algebra, optimization, 2005

373 **O. Costin, M. D. Kruskal, and A. Macintyre, Editors,** Analyzable functions and applications, 2005

372 **José Burillo, Sean Cleary, Murray Elder, Jennifer Taback, and Enric Ventura, Editors,** Geometric methods in group theory, 2005

For a complete list of titles in this series, visit the
AMS Bookstore at **www.ams.org/bookstore/**.

The book consists of contributions related mostly to public-key cryptography, including the design of new cryptographic primitives as well as cryptanalysis of previously suggested schemes. Most papers are original research papers in the area that can be loosely defined as "non-commutative cryptography"; this means that groups (or other algebraic structures) which are used as platforms are non-commutative.

ISBN 0-8218-4037-1

9 780821 840375

CONM/418

AMS *on the* Web
www.ams.org