

2014 • VOLUME 8 • NUMBER 3

JOURNAL OF MATHEMATICAL CRYPTOLOGY

MANAGING EDITORS

Spyros S. Magliveras, Boca Raton

Rainer Steinwandt, Boca Raton

Tran van Trung, Essen

EDITORIAL BOARD

Simon R. Blackburn, London

Ernie Brickell, Hillsboro

Mike Burmester, Tallahassee

Ronald Cramer, Amsterdam/Leiden

Ed Dawson, Brisbane

Robert Gilman, Hoboken

María Isabel González Vasco, Madrid

Otokar Grosek, Bratislava

Kwangjo Kim, Daejeon

Neal Koblitz, Seattle

Kaoru Kurosawa, Ibaraki

Alfred Menezes, Waterloo

Ron Mullin, Waterloo/Boca Raton

Phong Q. Nguyen, Paris

Josef Pieprzyk, Sydney

Rei Safavi-Naini, Calgary

Igor Shparlinski, Sydney

Doug Stinson, Waterloo

Hugh Williams, Calgary

Moti Yung, New York

DE GRUYTER

JOURNAL OF MATHEMATICAL CRYPTOLOGY is a forum for original research articles in the area of mathematical cryptology. Works in the theory of cryptology and articles linking mathematics with cryptology are welcome. Submissions from all areas of mathematics significant for cryptology are invited, including but not limited to, algebra, algebraic geometry, coding theory, combinatorics, number theory, probability and stochastic processes. The scope includes mathematical results of algorithmic or computational nature that are of interest to cryptology. While the journal does not cover information security as a whole, the submission of manuscripts on information security with a strong mathematical emphasis is explicitly encouraged.

All information regarding notes for contributors, subscriptions, Open access, back volumes and orders is available online at www.degruyter.com/jmc.

ABSTRACTED/INDEXED IN Celdes • CNKI Scholar (China National Knowledge Infrastructure) • CNPIEC • DBLP Computer Science Bibliography • EBSCO: Academic Search; TOC Premier; Discovery Service • Elsevier: SCOPUS • Gale Cengage: Academic One File • Google Scholar • Inspec • J-Gate • Mathematical Reviews (MathSciNet) • Naviga (Softweco) • Primo Central (ExLibris) • ProQuest: Computer and Information Systems Abstracts; Deep Indexing: Computing, Math & Statistics, Science Journals; Engineering Research Database; High Tech Research Database; Illustrata: Technology; Technology Research Database • SCImago (SJR) • Summon (Serials Solutions/ProQuest) • TDOne (TDNet) • WorldCat (OCLC) • Zentralblatt Math.

ISSN 1862-2976 • e-ISSN 1862-2984 • CODEN JMCOPY

RESPONSIBLE EDITORS Spyros S. Magliveras, Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA.
Email: spyros@fau.edu

Rainer Steinwandt, Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA.
Email: rsteinwa@fau.edu

Tran van Trung, Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Ellernstr. 29, 45326 Essen, Germany.
Email: trung@iem.uni-due.de

JOURNAL MANAGER Katharina Kaupen, De Gruyter, Genthiner Straße 13, 10785 Berlin, Germany.
Tel.: +49 (0)30 260 05-385, Fax: +49 (0)30 260 05-250
Email: katharina.kaupen@degruyter.com

RESPONSIBLE FOR ADVERTISEMENTS Claudia Neumann, De Gruyter, Genthiner Straße 13, 10785 Berlin, Germany. Tel.: +49 (0)30 260 05-226, Fax: +49 (0)30 260 05-322
Email: anzeigen@degruyter.com

© 2014 Walter de Gruyter GmbH, Berlin/Boston

TYPESETTING Dimler & Albroscheit, Müncheberg

PRINTING Franz X. Stückle Druck und Verlag e.K., Ettenheim

Printed in Germany



L. DE FEO, D. JAO, J. PLÛT Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies	209
C. CARLET, J.-L. DANGER, S. GUILLEY, H. MAGHREBI Leakage squeezing: Optimal implementation and security evaluation	249
D. HARIDAS, S. VENKATRAMAN, G. VARADAN Security analysis of Modified Rivest Scheme	297
M. YASUDA, K. YOKOYAMA, T. SHIMOYAMA, J. KOGURE, T. KOSHIBA On the exact decryption range for Gentry–Halevi’s implementation of fully homomorphic encryption	305

