

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

Carlo Blundo, Salerno

Mike Burmester, Tallahassee

Ronald Cramer, Amsterdam/Leiden

Ed Dawson, Brisbane

Robert Gilman, Hoboken

María Isabel González Vasco, Madrid

Otokar Grosek, Bratislava

Tor Helleseeth, Bergen

Kwangjo Kim, Daejeon

Neal Koblitz, Seattle

Kaoru Kurosawa, Ibaraki

Tanja Lange, Eindhoven

Kristin Lauter, Redmond

Alfred Menezes, Waterloo

Ron Mullin, Waterloo/Boca Raton

Phong Q. Nguyen, Paris

Josef Pieprzyk, Sydney

Martin Rötteler, Redmond

Rei Safavi-Naini, Calgary

Igor Shparlinski, Sydney

Doug Stinson, Waterloo

Tsuyoshi Takagi, Fukuoka

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/journals/jmc.

ABSTRACTED/INDEXED IN Baidu Scholar · Celdes · CNKI Scholar (China National Knowledge Infrastructure) · CNPIEC · DBLP Computer Science Bibliography · EBSCO (relevant databases) · EBSCO Discovery Service · Elsevier: Reaxys; SCOPUS · Gale/Cengage · Genamics JournalSeek · Google Scholar · Inspec · J-Gate · JournalTOCs · KESLI-NDSL (Korean National Discovery for Science Leaders) · Mathematical Reviews (MathSciNet) · Naviga (Softweco) · Primo Central (ExLibris) · ProQuest (relevant databases) · ReadCube · ResearchGate · SCImago (SJR) · Summon (Serials Solutions/ProQuest) · TDNet · Ulrich's Periodicals Directory/ulrichsweb · WanFang Data · WorldCat (OCLC) · Zentralblatt Math (zbMATH).

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, Fakultät für Mathematik, Universität Duisburg-Essen, Thea-Leymann-Straße 9, 45127 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 05-264
Email: anzeigen@degruyter.com

© 2018 Walter de Gruyter GmbH, Berlin/Boston

TYPESETTING Dimler & Albroscheit, Münchenberg

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

Printed in Germany



Offenlegung der Inhaber und Beteiligungsverhältnisse gem. § 7a Abs. 1 Ziff. 1, Abs. 2 Ziff. 3 des Berliner Pressegesetzes: Die Gesellschafter der Walter de Gruyter GmbH sind: Cram, Gisela, Rentnerin, Berlin; Cram, Elsbeth, Pensionärin, Rosengarten-Alvesen; Cram, Dr. Georg-Martin, Unternehmens-Systemberater, Stadtbergen; Cram, Maike, Wien (Österreich); Cram, Jens, Mannheim; Cram, Ingrid, Betriebsleiterin, Tuxpan/Michoacan (Mexiko); Cram, Sabina, Mexico, DF (Mexiko); Cram, Silke, Wissenschaftlerin, Mexico DF (Mexiko); Cram, Björn, Aachen; Cram, Berit, Hamm; Cram-Gomez, Susana, Mexico DF (Mexiko); Cram-Heydrich, Walter, Mexico DF (Mexiko); Cram-Heydrich, Kurt, Angestellter, Mexico DF (Mexiko); Duvenbeck, Birgitta, Oberstudienrätin i.R., Bad Homburg; Gädeke, Gudula, M.A., Atemtherapeutin/Lehrerin, Tübingen; Gädeke, Martin, Einzelunternehmer, Ingolstadt; Lubasch, Dr. Annette, Ärztin, Berlin; Schütz, Dr. Christa, Ärztin, Mannheim; Schütz, Sonja, Berlin; Schütz, Julianne, Berlin; Schütz, Antje, Berlin; Schütz, Valentin, Mannheim; Seils, Dorothee, Apothekerin, Stuttgart; Seils, Dr. Ernst-Albert, Pensionär, Reppenstedt; Seils, Gabriele, Dozentin, Berlin; Seils, Christoph, Journalist, Berlin; Siebert, John-Walter, Pfarrer, Oberstenfeld; Tran, Renate, Mediatorin, Zürich (Schweiz).

Contents

Juha Partala

Algebraic generalization of Diffie–Hellman key exchange — 1

Tran van Trung

Construction of strongly aperiodic logarithmic signatures — 23

Hassan Qahur Al Mahri, Leonie Simpson,
Harry Bartlett, Ed Dawson, Kenneth Koon-Ho Wong

A fundamental flaw in the ++AE authenticated encryption mode — 37

Sabyasachi Dey, Santanu Sarkar

Generalization of Roos bias in RC4 and some results on key-keystream relations — 43

Thalia M. Laing, Douglas R. Stinson

A survey and refinement of repairable threshold schemes — 57

