JOURNAL OF MATHEMATICAL CRYPTOLOGY

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 Celdes • CNKI Scholar (China National Knowledge Infrastucture) • 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 JMCOBY

TYPESETTING Dimler & Albroscheit, Müncheberg

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

Printed in Germany

Contents