BIRKHÄUSER

Volume 3
No. 2
pp. 127–224
2010
ISSN 1661-8270

Mathematics in Computer Science

Symbolic Computation and Cryptography

Editors

Jean-Charles Faugère
Ludovic Perret

Math.Comput.Sci. (2010) 3:127–128
DOI 10.1007/s11786-009-0017-6

Mathematics in Computer Science

Foreword

Jean-Charles Faugère · Ludovic Perret

Published online: 12 January 2010

This special issue of Mathematics in Computer Science is devoted to *Symbolic Computation and Cryptography*. It is a follow-up to SCC'08, the First International Conference on Symbolic Computation and Cryptography,[1] which was held in Beijing, China in April 2008, with 21 papers presented to an audience of more than 100 people. The conference program also featured three invited talks given by Bruno Buchberger, Adi Shamir, and Xiaoyun Wang and one tutorial talk by Claude Carlet. Some of the papers included in this special issue were presented at SCC'08. All the submissions were reviewed by experts in the relevant areas according to the standards of the journal. We thank the reviewers for their timely help in providing informative feedback to the authors.

This special issue, as well as the SCC conference, has been organized in response to the growing interest of applying and developing techniques and software tools of symbolic computation in cryptography. For example, lattice reduction algorithms have become a standard tool of cryptologists. The rapid development of algebraic cryptanalysis—which reduces the problem of evaluating the security of cryptographic primitives to the difficulty of solving algebraic systems—makes Gröbner bases and other algebraic system solving techniques more and more important in cryptography. As the reader may see in this issue, the intersection between Symbolic Computation and Cryptography is not limited to these mentioned tools.

We emphasize that cryptography demands the development of new efficient algorithms to treat basic problems of symbolic computation (e.g., finding "good" bases of lattice/ideals and decomposing polynomials). At least, highly efficient implementations of existing algorithms are required to handle real-life applications. For instance, an attack against HFE—a well-known cryptographic scheme based on polynomials—led to solving a system of 80 equations in 80 variables over $\mathbb{F}_2$ with a specific version of the F_5 algorithm. In contrast, the algebraic cryptanalysis of symmetric ciphers requires solving an algebraic system with more than 1,000 variables. Up to now, this seems to be out of the scope of application of current algorithms. In this issue, two papers present however a new approach for small variants of AES and the stream cipher Trivium. All in all, we think that the practical constraints imposed by cryptography is an inspiring source of algorithmic challenges for symbolic computation.

[1] http://www.cc4cm.org/scc2008/.

J.-C. Faugère (✉) · L. Perret
LIP6/SALSA Project Team, INRIA-UPMC (Paris 6), 104, avenue du Président Kennedy, 75016 Paris, France
e-mail: Jean-Charles.Faugere@inria.fr

L. Perret
e-mail: Ludovic.Perret@lip6.fr

The articles in this issue are related to the following topics.

- Algebraic cryptanalysis: Bulygin and Brickenstein present a new approach for modeling small variants of AES; Eibachn, Völkel, and Pilz consider the stream ciphers Bivium and Trivium.
- Lattice-based cryptanalysis: this is done by Lee and Hahn.
- Coding theory: Otmani, Tillich, and Dallot present a very efficient attack against variants of McEliece's system.
- Curves: Duquesne uses symbolic tools to deduce arithmetic formulas and Minzlaff presents a method for computing zeta functions of curves.
- Other related topics: the non-optimality and chaotic behaviour of some digital expansion are studied by Heuberger.

Mathematics in Computer Science

Volume 3, No. 2 (2010)
Pages 127–224

Contents