SCC 2010

2nd International Conference on Symbolic Computation and Cryptography

http://scc2010.rhul.ac.uk/

Royal Holloway, University of London, United Kingdom

CALL FOR PAPERS

SCC 2010 is the second edition of a new series of conferences where research and development in symbolic computation and cryptography may be presented and discussed. It is organised in response to the growing interest in applying and developing methods, techniques, and software tools of symbolic computation for cryptography. The use of Lattice Reduction algorithms in cryptology and the application of Gröbner bases in the context of algebraic attacks are typical examples of explored applications.

SCC 2010 aims at providing an interactive forum for interested researchers to exchange ideas and views, to present research results and progress, and to learn and discuss recent developments and emerging problems on:

- the design, modelling, and analysis of cryptographic systems and protocols for which symbolic computation may be used or needed;
- the design, implementation, and analysis of algorithms and software tools of symbolic computation that may have potential applications in cryptography.

TOPICS

Specific topics for SCC 2010 include, but are not limited to:

- Multivariate cryptography, braid group cryptography, non-commutative cryptography, and quantum cryptography.
- Code-based, factorization-based, and lattice-based cryptography.
- Algebraic attacks for block ciphers, stream ciphers, and hash functions.
- Design and analysis of algebraic, elliptic, and embedded cryptographic systems and protocols.
- Gröbner basis techniques in cryptology, algebraic number theory, and coding theory.
- Triangular sets and new techniques for solving algebraic systems over finite fields.
- Algorithms and software for symbolic computation in cryptography.

INVITED SPEAKERS

- Vladimir Gerdt (Joint Institute for Nuclear Research, Moscow, Russia)
- Alexander May (Ruhr-Universität Bochum, Germany)
- Alexei Miasnikov (McGill University, Montreal, Canada)
- Jacques Stern (ENS - Paris, France)

SUBMISSION

Potential participants of SCC 2010 are invited to submit extended abstracts of 3-5 pages or full papers (with at most 14 pages) describing their work to be presented at the conference. The submitted extended abstracts and full papers will be reviewed by members of the program committee (PC) for soundness and relevance to the conference. Submission of original research papers is encouraged, while published material and work in progress will also be considered for presentation at the conference. We note that there will be no formal proceedings for the SCC 2010 conference; in particular, a paper submitted to SCC 2010 may also be submitted elsewhere after the conference.

Extended abstracts and full papers should be prepared using Springer's LNCS LaTeX style file available on the SCC 2010 webpage and according to the instructions given therein. Submissions must be done preferably electronically via EasyChair at:

http://www.easychair.org/conferences/?conf=scc2010

or sent in PDF format as e-mail attachment to scc2010-pc@easychair.org.

There will be no formal proceedings for SCC 2010 conference. However all accepted extended abstracts and full papers will be printed on the conference records for distribution during the event.

PUBLICATION

Authors of the extended abstracts and full papers accepted for presentation at the conference will be invited to submit their full and/or revised papers for publication in a special issue of a journal (to be specified) after the meeting.

IMPORTANT DATES

Deadline for extended abstract submission:	March 14, 2010
Notification of acceptance or rejection:	April 11, 2010
Conference taking place:	June 23-25, 2010
Deadline for full paper submission:	November 28, 2010

PROGRAMME COMMITTEE

Jean-Charles Faugère, Co-chair (UPMC-INRIA, France)
Carlos Cid, Co-chair (Royal Holloway University of London, United Kingdom)

Daniel Bernstein (University of Illinois at Chicago, USA)
Olivier Billet (Orange Labs, France)
Claude Carlet (University of Paris 8, France)
Pierre-Alain Fouque (ENS - Paris, France)
Joachim von zur Gathen (Universität Paderborn, Germany)
Pierrick Gaudry (CNRS, France)
Jaime Gutierrez (University of Cantabria, Spain)
Antoine Joux (Université de Versailles Saint-Quentin-en-Yvelines, France)
Martin Kreuzer (Universität Passau, Germany)
Dongdai Lin (Institute of Software of Chinese Academy of Sciences, China)
Alexander May (Ruhr-Universität Bochum, Germany)
Ayoub Otmani (GREYC-Ensicaen & University of Caen, France)
Ludovic Perret (LIP6-UPMC Univ Paris 6, France)
Igor Shparlinski (Macquarie University, Australia)
Boaz Tsaban (Bar-Ilan University, Israel)
Maria Isabel González Vasco (Universidad Rey Juan Carlos, Spain)

LOCAL ORGANISATION

Carlos Cid and Martin Albrecht
Information Security Group
Royal Holloway, University of London
Egham, TW20 0EX, United Kingdom
email: scc2010@rhul.ac.uk