

RSA Conference 2009, Cryptographers' Track (CT-RSA 2009)

April 20-24, 2009, Moscone Center, San Francisco, CA, USA

Call for Papers

www.minicrypt.de → CT-RSA 2009

Background:

The RSA Conference is the largest, regularly-staged computer security event, with over 350 vendors and thousands of attendees. The Cryptographers' Track (CT-RSA) is a research conference within the RSA Conference. CT-RSA has begun in 2001 and has become an established venue for presenting cryptographic research papers. The conference proceedings will be published in Springer's Lecture Notes in Computer Science (LNCS) series and should be available at the conference.

Topics of Interest:

Original research papers pertaining to all aspects of cryptography are solicited. Submissions may present applications, techniques, theory, and practical experience on topics including, but not limited to: public-key encryption, private-key encryption, digital signatures, message authentication, hash functions, pseudorandomness, cryptographic protocols, tamper-resistance, fast implementations, elliptic-curve cryptography, quantum cryptography, formal security models.

Important Dates:

Submission Deadline	October 13, 2008, 12:00 UTC October 21, 2008, 12:00 UTC
Notification of Authors	December 22, 2008
Deadline for Proceedings Version	January 19, 2009
Conference	April 20-24, 2009

Instructions for Authors:

Submissions must not substantially duplicate work that was published elsewhere, or work that any of the authors has submitted in parallel to any other conference or workshop that has proceedings. The paper must be **anonymous** with no author names, affiliations, acknowledgements, or obvious references. It should begin with a title and a short abstract. The paper should be **at most 12 pages** excluding the bibliography and clearly marked appendices using reasonable font size and margins. (A total page limit will be applied to those papers accepted for publication in the proceedings.) The main body of the paper should be intelligible and self-contained as the committee members are not required to read the appendices. Submissions not meeting these guidelines risk rejection without consideration of their merits. Program Committee members are allowed to submit at most one paper.

Submissions will take place via a **web system**. Electronic submissions must conform to the procedure described in the submission server and must be received by the deadline indicated above. Electronic submission via the described interface is the only form of submission considered.

Notification of acceptance or rejection will be sent to authors by December 22, 2008. Authors of accepted papers must guarantee that at least one of the co-authors will attend the conference and deliver the talk. Registration fees will be waived for speakers.

Program Committee:

Michel Abdalla (ENS & CNRS, France)
Zuzana Beerliova-Trubiniová (ETH Zurich, Switzerland)
Alex Biryukov (University of Luxembourg, Luxembourg)
Melissa Chase (Microsoft Research, USA)
Alex Dent (Royal Holloway, UK)
Nelly Fazio (City University of New York, USA)
Marc Fischlin (Darmstadt University, Germany) - Program Chair
Juan Garay (AT&T Labs - Research, USA)
Amir Herzberg (Bar-Ilan University, Israel)
Dennis Hofheinz (CWI, Netherlands)
Nick Howgrave-Graham (NTRU Cryptosystems, USA)
Stanislaw Jarecki (UC Irvine, USA)
Marc Joye (Thomson, France)
Alexander May (Bochum University, Germany)
Jesper Buus Nielsen (University of Aarhus, Denmark)
Giuseppe Persiano (University of Salerno, Italy)
Josef Pieprzyk (Macquarie University, Australia)
Vincent Rijmen (K.U.Leuven, Belgium, and Graz University of Technology, Austria)
Kazuo Sako (NEC, Japan)
Christian Schaffner (CWI, Netherlands)
Berry Schoenmakers (TU Eindhoven, Netherlands)
Willy Susilo (University of Wollongong, Australia)
Pim Tuyls (Philips, Netherlands)
Jorge Villar (UPC Barcelona, Spain)
Bogdan Warinschi (University of Bristol, UK)

Program Chair and Contact:

Marc Fischlin, Department of Computer Science, Darmstadt University of Technology, Germany.
Tel: +49-(0)6151-163337. E-mail: marc.fischlin@gmail.com (please include CT-RSA 2009 in the subject line).

Steering Committee:

Masayuki Abe, Tal Malkin, David Pointcheval, Ron Rivest, Moti Yung.