

CALL FOR PAPERS

RSA Conference 2007, Cryptographers' Track

February 5–9, 2007, Moscone Center, San Francisco, USA

The RSA Conference is the largest, regularly-staged computer security event. The Cryptographers' Track (CT-RSA) is a research conference within the RSA Conference. 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, symmetric-key encryption, digital signatures, hash functions, cryptographic protocols, tamper-resistance, fast implementations, elliptic-curve cryptography, quantum cryptography, formal security models, network security, e-commerce.

Important Dates

Submission deadline: **July 10, 2006 - 13:00 GMT** (9:00 EDT, 22:00 JST)
Acceptance notification: September 8, 2006
Proceedings version: October 10, 2006

Instructions for Authors

Submissions must not substantially duplicate work that has been published in, or submitted in parallel to, any journal, 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, a short abstract, and a list of keywords. 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. Submissions will take place entirely via a web system:

<https://s1.iacr.org/websubrev/rsa07/>

The proceedings will be published in Springer-Verlag's LNCS series and should be available at the conference. The 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 the speakers.**)

Program Committee

Masayuki Abe (<i>NTT, Japan</i>) – PC Chair	Arjen K. Lenstra (<i>EPFL, Switzerland</i>)
Kazumaro Aoki (<i>NTT, Japan</i>)	Helger Lipmaa (<i>Cybernetica AS/Univ. Tartu, Estonia</i>)
John Black (<i>University of Colorado at Boulder, USA</i>)	Stefan Lucks (<i>University of Mannheim, Germany</i>)
Colin Boyd (<i>QUT, Australia</i>)	Bart Preneel (<i>Katholieke Univ. Leuven, Belgium</i>)
Jung Hee Cheon (<i>Seoul National University, Korea</i>)	Vincent Rijmen (<i>Graz Univ. of Technology, Austria</i>)
Alexander W. Dent (<i>Royal Holloway, UK</i>)	Kazue Sako (<i>NEC, Japan</i>)
Serge Fehr (<i>CWI, The Netherlands</i>)	Adam Smith (<i>Weizmann Institute of Science, Israel</i>)
Stuart Haber (<i>HP Labs, USA</i>)	Douglas Stinson (<i>University of Waterloo, Canada</i>)
Shai Halevi (<i>IBM T. J. Watson Research, USA</i>)	Brent Waters (<i>SRI International, USA</i>)
Goichiro Hanaoka (<i>AIST, Japan</i>)	Susanne Wetzel (<i>Stevens Institute of Technology, USA</i>)
Marc Joye (<i>Gemplus, France</i>)	Yiqun Lisa Yin (<i>Independent Consultant, USA</i>)
Jonathan Katz (<i>University of Maryland, USA</i>)	Adam Young (<i>MITRE Corporation, USA</i>)

Steering Committee

Alfred Menezes (<i>University of Waterloo, Canada</i>)	Ron Rivest (<i>MIT, USA</i>)
Tatsuaki Okamoto (<i>NTT, Japan</i>)	Moti Yung (<i>RSA Labs and Columbia Univ., USA</i>)
David Pointcheval (<i>CNRS/ENS, France</i>)	