Africacrypt 2008

June 11 – 14, Casablanca, Morocco

Call for Papers

Submission: Nov. 24, 2007 **Notification:** Feb. 12, 2008

Final version: Mar. 13, 2008

– General Information –

Original papers on all technical aspects of cryptology are solicited for submission to Africacrypt 2008. The conference is organized by the Moroccan Association for Cryptography (AMC) in cooperation with IACR. For more information see http://www.africacrypt.org/index_en.htm.

The conference seeks original contributions in any area of cryptology or related fields. We welcome submissions about new cryptographic primitive proposals, cryptanalysis, security models, implementation aspects, and applications. We also consider submissions about cryptographic aspects of network security, complexity theory, information theory, coding theory, number theory, and quantum computing. We intend to have special sessions on security and privacy aspects in wireless technologies (including mobile ad hoc networks and RFID) and biometric access control.

– Instructions for Authors –

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop with formally published proceedings. Information about submissions may be shared with program chairs of other conferences for that purpose. Accepted submissions may not appear in any other conference or workshop with proceedings. The submission must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of key words, and its introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Since the final version of accepted papers will have to follow the LNCS guidelines (see http://www.springeronline.com/lncs) with a total page limit of 18 pages including references and appendices, it is advised to submit in the same format. Committee members are not required to review more than that, so the paper should be intelligible and self-contained within this length.

Papers must be submitted electronically. A detailed description of the electronic submission procedure is available at http://lasecpc11.epfl.ch/iChair. Submissions must conform to this procedure. Late submissions and non-electronic submissions will not be considered.

Authors of accepted papers must guarantee that their paper will be presented at the conference.

– Conference Proceedings –

Proceedings are intended to be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers.

– Program Committee –

Tom Berson *(Anagram, USA)*
Alex Biryukov *(University of Luxembourg, Luxembourg)*
Xavier Boyen *(Voltage Inc, USA)*
Anne Canteaut *(INRIA, France)*
Jean-Marc Couveignes *(Toulouse University, France)*
Mohamed El Marraki *(Faculty of Science Rabat, Morrocco)*
Steven Galbraith *(Royal Holloway University of London, UK)*
Helena Handschuh *(Spansion, France)*
Tetsu Iwata *(Nagoya University, Japan)*
Pascal Junod *(Nagracard, Switzerland)*
Tanja Lange *(TU Eindhoven, The Netherlands)*
Arjen Lenstra *(EPFL, Switzerland)*
Javier Lopez *(University of Malaga, Spain)*
Stefan Lucks *(Bauhaus-University Weimar, Germany)*
Mitsuru Matsui *(Mitsubishi Electric Corp, Japan)*
Alexander May *(Bochum University, Germany)*
Atsuko Miyaji *(JAIST, Japan)*
David Molnar *(Berkeley University, USA)*
Refik Molva *(Eurecom, France)*
Jean Monnerat *(UCSD, USA)*
David Naccache *(ENS, France)*
Raphael Phan *(EPFL, Switzerland)*
Josef Pieprzyk *(Macquarie University, Australia)*
Bart Preneel *(K.U.Leuven, Belgium)*
Jean-Jacques Quisquater *(UCL, Belgium)*
C Pandu Rangan *(University of Madras, India)*
Vincent Rijmen *(Graz University of Technology, Austria)*
Rei Safavi-Naini *(University of Calgary, Canada)*
Louis Salvail *(University of Aarhus, Denmark)*
Ali Aydin Selcuk *(Bilkent University, Turkey)*
Serge Vaudenay (chair) *(EPFL, Switzerland)*
Michael Wiener *(Cryptographic Clarity, Canada)*
Amr Youssef *(Concordia University, Canada)*

– Program Chair

Serge Vaudenay
Ecole Polytechnique Fédérale de Lausanne
I&C - Security and Cryptography Laboratory
INF 241 (INF Building), Station 14
CH-1015 Lausanne
Switzerland
email: Serge.Vaudenay(at)epfl.ch

General Chair –

Abdelhak Azhari
Ecole Normale Supérieure de Casablanca
Department of Mathematics and Data Processing
BP 50069 Casa
Gandhi Casablanca
Morocco
email: aazhari2001(at)yahoo.fr