Call for Papers

7th International Conference on Cryptology
AFRICACRYPT 2014

May 28–30, 2014, Marrakech, Morocco

https://africacrypt14.di.ens.fr/

Africacrypt is an Annual International Conference on the Theory and Applications of Cryptology. Africacrypt 2014 is organized by the ENSIAS School of Engineering and the University Mohamed V Souissi, Rabat, in cooperation with the International Association for Cryptologic Research (IACR).

The aim of Africacrypt 2014 is to provide an international forum for practitioners and researchers from industry, academia and government from all over the world for a wide ranging discussion of all forms of cryptography and its applications.

The conference seeks original contributions in any area of cryptology or related fields. We welcome submissions about, but not limited to:

- Secret-key cryptography (block ciphers, stream ciphers, hash functions, MAC, etc)
- Secret-key cryptanalysis
- Public-key cryptography (identification protocols, digital signatures, encryption, etc)
- Public-key cryptanalysis
- Cryptographic protocols
- Design of cryptographic schemes
- Security proofs
- Anonymity (electronic commerce and payment, electronic voting, etc)
- Information theory
- Foundations and complexity theory
- Elliptic curves, lattices and coding theory
- Efficient implementations and practical applications

Important Dates

Submission deadline:	**January 15th, 2014** at 16:00 UTC
Acceptance notification:	March 1st, 2014
Proceedings version:	March 17th, 2014
Conference:	May 28th, 2014

Conference Organizers

General chair
Mostafa Belkasmi
ENSIAS, Mohammed V-Souissi University
Rabat, Morocco

Program chairs
David Pointcheval
Damien Vergnaud
(ENS, Paris)

Instructions for Authors

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any journal or other conference or workshop that has proceedings.

Submissions will take place entirely via a web system available from

`https://africacrypt14.di.ens.fr/submissions/`.

All submissions will be blind reviewed. 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 final proceedings version will be a paper of at most 18 pages in the llncs style. The document submitted (excluding appendices) should correspond to what the authors expect to be published if their paper is accepted without modification. We therefore strongly recommend that authors check whether their paper (without appendices) will fit within the above llncs space constraints. Committee members are not required to review more than that, so the paper should be intelligible and self-contained within this length. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Proceedings

The proceedings with revised selected papers will be published in Springer-Verlag's Lecture Notes in Computer Science, and will be available at the conference.

Clear instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Program Committee

Abdelhak Azhari – *Hassan II University in Casablanca, Morocco*
Hussain Benazza – *Ensam-Meknes, Moulay Ismail University, Morocco*
Dario Catalano – *Università di Catania, Italy*
Riaal Domingues – *South African Communications and Security Agency, South Africa*
Dario Fiore – *IMDEA Software Institute, Spain*
Pierre-Alain Fouque – *University of Rennes I, France*
Georg Fuchsbauer – *IST Austria*
Sanjam Garg – *IBM Research, USA*
Essam Ghadafi – *University of Bristol, UK*
Tetsu Iwata – *Nagoya University, Japan*
Seny Kamara – *Microsoft Research, USA*
Fabien Laguillaumie – *University of Lyon I, France*
Benoit Libert – *Technicolor, France*
Mark Manulis – *University of Surrey, UK*
Maria Naya-Plasencia – *INRIA, France*
Abderrahmane Nitaj – *University of Caen, France*
Kaisa Nyberg – *Aalto University School of Science, Finland*
Sami Omar – *Tunis University, Tunisia*
Ayoub Otmani – *University of Rouen, France*
Duong Hieu Phan – *University of Paris 8, France*
Vincent Rijmen – *KU Leuven and iMinds, Belgium*
Magdy Saeb – *Arab Academy of Science, Technology and Maritime Transport, Alexandria, Egypt*
Rei Safavi-Naini – *University of Calgary, Canada*
Palash Sarkar – *Indian Statistical Institute, India*
Peter Schwabe – *Radboud University Nijmegen, The Netherlands*
Francesco Sica – *Nazarbayev University, Kazakhstan*
Djiby Sow – *University of Dakar, Senegal*
Fran cois-Xavier Standaert – *UCL, Belgium*
Christine Swart – *University of Cape Town, South Africa*
Isamu Teranishi – *NEC, Japan*
Mehdi Tibouchi – *NTT Secure Platform Laboratories, Japan*
Ivan Visconti – *Università di Salerno, Italy*
Duncan Wong – *City University of Hong Kong, China*
Amr M. Youssef – *Concordia University, Montreal, Quebec, Canada*