AFRICACRYPT 2018

10th International Conference on the Theory and Application of Cryptographic Techniques

May 7–9, 2018 • Marrakesh, Morocco

http://africacrypt2018.aui.ma/index.php

Program chairs

Antoine Joux *UPMC Paris, France*
Abderrahmane Nitaj *Uni. Caen, France*
Tajje-eddine Rachidi *AUI Ifrane, Morocco*

Program committee

Elena Andreeva *KU Leuven, Belgium*
Hatem M. Bahig *Uni. Cairo, Egypt*
Magali Bardet *Uni. Rouen, France*
Hussain Benazza *Uni. Meknes, Morocco*
Colin Boyd *Uni. Science and Technology, Norway*
Dario Catalano *Uni. Catania, Italy*
Xing Chaoping *Nanyang Tech. Uni., Singapore*
Sherman S.M. Chow *Chinese Uni. Hong Kong*
Nicolas Courtois *Un. College London, U.K.*
Luca De Feo *Uni. Versaille, France*
Milena Djukanovic *Uni. Monteegro, Montenegro*
Nadia EL Mrabet *Mines Saint-Etienne, France*
Pierre-Alain Fouque *Uni. Rennes, France*
Gottfried Herold *Ruhr-Uni. Bochum, Germany*
Javier Herranz *Uni. Catalunya, Spain*
Sorina Ionica *Uni. Picardie, France*
Tetsu Iwata *Nagoya Uni., Japan*
Juliane Kramer *TU Darmstadt, Germany*
Fabien Laguillaumie *Uni. Lyon, France*
Tancrède Lepoint *SRI International, USA*
Ayoub Otmani *Uni. Rouen, France*
Duong Hieu Phan *Uni. Limoges, France*
Elizabeth A. Quaglia *RH, Uni. London, U.K.*
Tajje-eddine Rachidi *AUI Ifrane, Morocco*
Adeline Roux-Langlois *CNRS/IRISA, France*
Magdy Saeb *Arab Aca. Sc., Alexandria, Egypt*
Rei Safavi-Naini *Uni. Calgary, Canada*
Palash Sarkar *Indian Statistical Institute, India*
Alessandra Scafuro *Uni. Raleigh, USA*
Peter Schwabe *Uni. Nijmegen, The Netherlands*
Djiby Sow *Uni. Dakar, Senegal*
Pantelimon Stanica *Naval P. S., Monterey, USA*
Noah Stephens-Davidowitz *New-York Uni., USA*
Willy Susilo *Uni. Wollongong, Australia*
Joseph Tonien *Uni. Wollongong, Australia*
Damien Vergnaud *ENS Paris, France*
Vanessa Vitse *Institut Fourier, Grenoble, France*
Amr M. Youssef *Concordia Uni. Montreal, Canada*

General chair

Tajje-eddine Rachidi *AUI Ifrane, Morocco*

Important dates

Submission deadline: **January 7, 2018**
Notification: February 20, 2018
Camera-ready version: February 27, 2018
Conference dates: May 7–9, 2018

Africacrypt is an Annual International Conference on the Theory and Application of Cryptology. Africacrypt 2018 is organized by Alakhawain University in Ifrane, Morocco, in cooperation with the International Association for Cryptologic Research (IACR). The aim of Africacrypt 2018 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 program committee is seeking original research papers pertaining to all aspects of cryptography as well as tutorials are solicited. Submissions may present theory, techniques, applications and practical experience on topics including, but not limited to:

- Secret-key cryptography (block ciphers, stream ciphers, hash functions, MAC, ...);
- Public-key and Secret-key cryptanalysis;
- Public-key cryptography (identification protocols, digital signatures, encryption, ...);
- Cryptographic protocols;
- Design of cryptographic schemes;
- Security proofs;
- Anonymity (electronic commerce and payment, electronic voting, ...);
- Information theory;
- Foundations and complexity theory;
- Multi-party computation;
- Quantum cryptography;
- Elliptic curves;
- Lattices;
- Code-based cryptography;
- Efficient implementations.

Instructions for authors

Authors are invited to submit papers (PDF format) with novel contributions electronically using the submission form available on the conference web site. Submitted papers must be original, unpublished, ***anonymous***, and not submitted to journals or other conferences/workshops that have proceedings. Submissions must be written in English and should be at most 20 pages in total including bibliography and appendices. Papers not meeting these guidelines risk rejection without consideration. All submissions will be blind-refereed.

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

For submission instructions and further information please point your web-browser to: http://africacrypt2018.aui.ma

Proceedings

The proceedings will be published in the Springer Lecture Notes in Computer Science (LNCS) series. Accepted papers should follow the LNCS default author instructions

https://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0