AFRICACRYPT 2019

11th International Conference on the Theory and Application of Cryptographic Techniques

July 9–11, 2019 • Rabat, Morocco

Program chairs

Johannes Buchmann *TU Darmstadt*
Abderrahmane Nitaj *University of Caen*

General chair

Tajjeeddine Rachidi *University of Ifrane*

Program committee

Elena Andreeva *Katholieke Uni. Leuven*
Muhammad Rezal Kamel Ariffin *UPM*
Hatem M. Bahig *Ain Shams Uni., Cairo*
Magali Bardet *University of Rouen*
Lejla Batina *Radboud University*
Hussain Benazza *Uni. Moulay Ismail*
Olivier Blazy *University of Limoges*
Colin Boyd *Norwegian Uni. Sci. Technology*
Sbastien Canard *Orange Labs*
Sherman S. M. Chow *Ch. Uni. Hong Kong*
Nicolas Courtois *Uni. College London*
Joan Daemen *Radboud Uni. Nijmegen*
Luca De Feo *Uni. Versaille*
Nadia El Mrabet *EMSE*
Javier Herranz *Uni. Politècnica Catalunya*
Sorina Ionica *University Picardie, France*
Tetsu Iwata *Nagoya University*
Juliane Krämer *TU Darmstadt, Germany*
Subhamoy Maitra *Indian S. Inst. Kolkata*
Abderrahmane Nitaj *Uni. Caen Normandie*
Yanbin Pan *Chinese Academy of Sci. China*
Christophe Petit *Uni. Birmingham*
Elizabeth A. Quaglia *Uni. London*
Tajje-eddine Rachidi *Al Akhawayn Univ.*
Adeline Roux-Langlois *CNRS,IRISA*
Palash Sarkar *Indian S. Inst. Kolkata*
Alessandra Scafuro *Uni., Raleigh, USA*
Ali Aydin Selçuk *TOBB Uni. Ankara*
Djiby Sow *Uni. Dakar*
Pontelimon Stanica *Monterey, CA, USA*
Noah Stephens-Davidowitz *New York Uni.*
Joseph Tonien *Uni. Wollongong*
Damien Vergnaud *Sorbonne Uni. Paris*
Vanessa Vitse *Uni. Grenoble*
Amr M. Youssef *Concordia Uni.*

Invited Speakers

- Sebastian Faust *TU Darmstadt*
- Martin R. Albrecht *R. Holloway, London*

Important dates

Submission deadline: **April 2, 2019**
Notification: May 2, 2019
Camera-ready version: May 10, 2019
Conference dates: July 9-11, 2019

Africacrypt is an Annual International Conference on the Theory and Application of Cryptology. Africacrypt 2019 is organized by Al Akhawayn University In Ifrane, Ifrane, Morocco, in cooperation with the International Association for Cryptologic Research (IACR). The aim of Africacrypt 2019 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, ...);
- 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 18 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 and must make a full version of their paper available online.

For submission please use easychair at

https://easychair.org/conferences/?conf=africacrypt2019

instructions and further information please point your web-browser to:

http://africacrypt2019.aui.ma/index.php

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