AFRICACRYPT 2017

9th International Conference on the Theory and Application of Cryptographic Techniques

May 24–26, 2017 • Dakar, Senegal

Program chairs

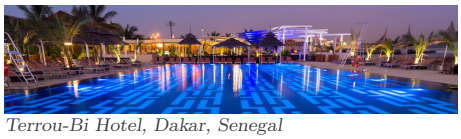
Marc Joye *NXP Semiconductors*
Abderrahmane Nitaj *Université de Caen*

Program committee

Riham Altawy *Concordia University*
Abdelhak Azhari *Université de Casablanca*
Hussain Benazza *Université Moulay Ismail*
Dario Catalano *Universita di Catania*
Pierre-Louis Cayrel *Univ. Saint Etienne*
Sherman S.M. Chow *CU Hong Kong*
Nadia El Mrabet *EMSE*
Pierre-Alain Fouque *Université Rennes I*
Jens Groth *University College London*
Javier Herranz *U. Politècnica de Catalunya*
Tetsu Iwata *Nagoya University*
Saqib Kakvi *University of Bristol*
Seny Kamara *Brown University*
Fabien Laguillaumie *Université de Lyon I*
Benoît Libert *ENS Lyon*
Mark Manulis *University of Surrey*
Tarik Moataz *Colorado State University*
Ayoub Otmani *Université de Rouen*
Vanishree Rao *PARC*
Tajje-eddine Rachidi *Al Akhawayn Univ.*
Magdy Saeb *Arab Academy for Science*
Rei Safavi-Naini *University of Calgary*
Kazue Sako *NEC*
Palash Sarkar *Indian Statistical Institute*
Peter Schwabe *Radboud Universiteit*
Francesco Sica *Nazarbayev University*
Djiby Sow *Université de Dakar*
Willy Susilo *University of Wollongong*
Christine Swart *Univ. Cape Town*
François-Xavier Standaert *UCL*
Joseph Tonien *University of Wollongong*
Amr M. Youssef *Concordia University*

General chairs

Mamadou Sangharé *Université de Dakar*
Djiby Sow *Université de Dakar*
Abdoul Aziz Ciss *Polytechnique Thies*


Terrou-Bi Hotel, Dakar, Senegal

Important dates

Submission deadline: **January 15, 2017**
Notification: February 28, 2017
Camera-ready version: March 10, 2017
Conference dates: May 24–26, 2017

Africacrypt is an Annual International Conference on the Theory and Application of Cryptology. Africacrypt 2017 is organized by Cheikh Anta Diop University, Dakar, Senegal, in cooperation with the International Association for Cryptologic Research (IACR). The aim of Africacrypt 2017 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, ...);
- Secret-key cryptanalysis;
- Public-key cryptography (identification protocols, digital signatures, encryption, ...);
- Public-key cryptanalysis;
- 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 instructions and further information please point your web-browser to:

`https://sites.google.com/site/africacrypt2017/`

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.