Call for Papers

4th International Conference on Cryptology
AFRICACRYPT 2011

July 4–8, 2011, Dakar, Senegal

http://www.africacrypt2011.com

Africacrypt is an Annual International Conference on the Theory and Applications of Cryptology. Africacrypt 2011 is organized by Université Cheikh Anta Diop (Dakar University) in cooperation with the International Association for Cryptologic Research (IACR).

The aim of Africacrypt 2011 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
- Multi-party computation
- Quantum cryptography
- Elliptic curves
- Lattices
- Efficient implementations

Important Dates

Submission deadline:	**January 14, 2011**
Acceptance notification:	March 18, 2011
Proceedings version:	April 18, 2011

Conference Organizers

General chairs

Mamadou Sanghare
(LACGAA, Dakar University)
Djiby Sow
(LACGAA, Dakar University)

Program chairs

David Pointcheval
(ENS, Paris)
Abderrahmane Nitaj
(Univ. of Caen)

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://africacrypt2011.di.ens.fr/`.

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 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 (Univ. of Casablanca, Morocco)
Abdelmalek Azizi (Univ. of Oujda, Morocco)
Hatem M. Bahig (Ain Shams Univ., Cairo, Egypt)
Colin Boyd (Queensland Univ. of Tech., Australia)
Anne Canteaut (INRIA, France)
David Cash (UC San Diego, USA)
Dario Catalano (Univ. di Catania, Italy)
Riaal Domingues (South African Communications and Security Agency, South Africa)
Eiichiro Fujisaki (NTT Labs, Japan)
David Galindo (Univ. of Luxembourg, Luxembourg)
Maria Isabel Gonzalez-Vasco (Univ. Rey Juan Carlos, Madrid, Spain)
Aline Gouget (CryptoExperts, France)
Jens Groth (University College London, UK)
Martin Hirt (ETH Zurich, Switzerland)
Tetsu Iwata (Nagoya Univ., Japan)
Stanislaw Jarecki (UC Irvine, California, USA)
Seny Kamara (Microsoft, Redmond, USA)
Fabien Laguillaumie (Univ. of Caen, France)
Mark Manulis (TU Darmstadt & CASED, Germany)
Bruno Martin (I3S, Univ. of Nice-Sophia Antipolis, France)
Keith Martin (Royal Holloway, Univ. of London, UK)
Mitsuru Matsui (Mitsubishi Electric, Japan)
Kaisa Nyberg (Aalto Univ. & Nokia, Finland)
Sami Omar (Tunis Univ., Tunisia)
Ayoub Otmani (Univ. of Caen, France & INRIA, France)
Josef Pieprzyk (Macquarie Univ., Australia)
Vincent Rijmen (K.U. Leuven, Belgium & TU Graz, Austria)
Magdy Saeb (Arab Academy for Science & Technology, Alexandria, Egypt)
Kazue Sako (NEC, Japan)
Palash Sarkar (Indian Statistical Institute, India)
Francesco Sica (Univ. of Calgary, Canada)
Martijn Stam (EPFL, Switzerland)
Christine Swart (Univ. of Cape Town, South Africa)
Damien Vergnaud (ENS, Paris, France)
Ivan Visconti (Univ. of Salerno, Italy)
Bogdan Warinschi (Bristol Univ., UK)
Duncan Wong (City Univ. of Hong Kong, China)
Scott Yilek (Univ. of St. Thomas, USA)
Amr M. Youssef (Concordia Univ., Montreal, Quebec, Canada)