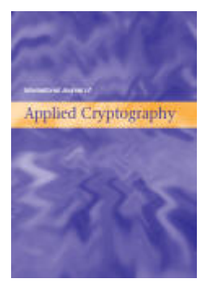
Call for Papers

8^{th} International Conference on Cryptology
AFRICACRYPT 2016

April 13–15, 2016, Fes, Morocco

Organized by AlAkhawyn University in Ifrane



http://africacrypt2016.aui.ma

Africacrypt is an Annual International Conference on the Theory and Applications of Cryptology. Africacrypt is a major scientific event that seeks to advance and promote the field of cryptology on the African continent. The conference has systematically drawn some excellent contributions to the field, and has seen many renown researchers deliver keynote presentations. The conference has always been organized *In cooperation with the International Association for Cryptologic Research* (IACR).
Africacrypt 2016 will be no exception to other past Africacrypt conferences. It will seek excellent contributions to the field, and attract position keynotes. In addition to providing an international forum for researchers and academics from all over the world for presenting and discussing recent advances in cryptology and its applications, Africacrypt 2016 ambitions to attract practionners from governemnt, industry and private sector interested in cryptology and its applications. The 2016 edition of Africacrypt will feature keynote speakers from leading software editors and hardware manufacturers, as well as exposition booths.

Conference topics

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, MAC, etc.)
- Secret-key cryptanalysis
- Cryptographic hash functions
- Public-key cryptography (identification protocols, digital signatures, encryption, etc.)
- Public-key cryptanalysis
- Cryptographic protocols
- Anonymity (electronic commerce and payment, electronic voting, etc)
- Security proofs
- Foundations and complexity theory
- Information theory
- Number theory, elliptic curves, lattices and coding theory
- Efficient implementations and practical applications

Proceedings and presentations

The proceedings with revised selected papers will be published in Springer-Verlag's Lecture Notes in Computer Science. Authors of accepted papers must guarantee that their paper will be presented at the conference.
In addition to the 25-minute presentations of the accepted papers that will be published in the proceedings, a poster session will be organized. When submitting a paper, please indicate if you want it to be considered for this poster session if not accepted for publication.
Authors of selected outstanding papers will be invited to submit extended versions of their papers for consideration of publication in International Journal of Applied Cryptography (IJACT) http://www.inderscience.com/jhome.php?jcode=ijact

Important Dates

Abstract Submission deadline:	**December 14th, 2015** at 16:00 UTC
Paper Submission deadline:	**December 17th, 2015** at 16:00 UTC
Paper Acceptance notification:	January 23rd, 2016
Proceedings version:	February 3rd, 2016
Poster Submission deadline:	**March 14th, 2016**
Poster Acceptance notification:	March 30th, 2016
Conference:	**April 13–15, 2016**

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://africacrypt2016.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 20 pages in the llncs style, and clear instructions will be sent to the authors of accepted papers. Thus, the document submitted (excluding clear marked 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.

Poster Session

On the front page of your paper submission, please indicate if your submission is also a candidate for the poster session in case it is not selected as a published paper. For additional poster submissions, please send a 2-page description of the work to the program chairs: africacrypt2016@di.ens.fr.
Posters can present ongoing work or already published results.

Conference Organizers

General chair :	Dr. Tajje-eddine Rachidi (Alakhawayn University in Ifrane)
Program chair :	David Pointcheval (ENS Paris, France)
Co-program chair :	Abderrahmane Nitaj (Caen Univ., France)

Program Committee

Muhammad Rezal Kamel Ariffin
Abdelhak Azhari
Hussain Benazza
Colin Boyd
Dario Catalano
Jie Chen
Sherman S.M. Chow
Jean-Sébastien Coron
Itai Dinur
Léo Ducas
Orr Dunkelman
Dario Fiore
Pierre-Alain Fouque
Georg Fuchsbauer
Essam Ghadafi
Tetsu Iwata
Seny Kamara
Benoit Libert
David M'Raihi
Mark Manulis
Jesper Buus Nielsen
Ayoub Otmani
Duong Hieu Phan
Tajje-eddine Rachidi
Magdy Saeb
Palash Sarkar
Peter Schwabe
Francesco Sica
Djiby Sow
Ron Steinfeld
François-Xavier Standaert
Christine Swart
Isamu Teranishi
Mehdi Tibouchi
Susan Thomson
Xiaoyun Wang
Amr M. Youssef