AFRICACRYPT 2025

16th International Conference on Cryptology

July 21–23, 2025 • Rabat, Morocco

Important dates

Submission deadline: **March 10, 2025**
Notification: May 1, 2025
Camera-ready version: May 10, 2025
Conference dates: July 21-23, 2025

Program chairs

Svetla Petkova-Nikova, *KU Leuven, Belgium*
Vincent Rijmen, *KU Leuven, U. Bergen*
Abderrahmane Nitaj, *U. Caen, France*

General chairs

Mostafa Belkasmi, *ENSIAS, Rabat, Morocco*
Said Eddahmani, *U. Paris VIII, France*

Program committee

Gora Adj, *TII, UAE*
Riham Altawy, *U. Victoria, Canada*
Elena Andreeva, *TU Wien, Austria*
Ahmed Azouaoui, *I. Tofail U. Kenitra, Morocco*
Hatem M. Bahig, *Ain Shams U., Egypt*
Hussain Ben-Azza, *Moulay Ismail U., Morocco*
Olivier Blazy, *Ecole Polytechnique, France*
Sébastien Canard, *Télécom Paris, France*
Céline Chevalier, *Paris-Panthéon-Assas, France*
Joan Daemen, *Radboud U., The Netherlands*
Luca De Feo, *IBM Research Zürich, Switzerland*
Christoph Dobraunig, *Intel Corporation*
Sylvain Duquesne, *U. Rennes 1, France*
Betül Durak, *Microsoft*
Laila El Aimani, *U. Cadi Ayyad, Morocco*
Nadia El Mrabet, *Mines Saint-Etienne, France*
Muhammad Elsheikh, *Nat. Inst. Std, Egypt*
Tony Ezome, *ENS Libreville, Gabon*
Georgios Fotiadis, *=nil; foundation*
Emmanuel Fouotsa, *U. Bamenda, Cameroon*
Tako Boris Fouotsa, *EPFL, Switzerland*
Essam Ghadafi, *Newcastle U., UK*
Loubna Ghammam, *ITK Engineering GmbH*
Javier Herranz, *U. Politècnica Catalunya, Spain*
Sorina Ionica, *U. Picardie Jules Verne, France*
Tetsu Iwata, *Nagoya U., Japon*
Samuel Jaques, *University of Waterloo, Canada*
Hervé Tale Kalachi, *NASE, Yaoundé, Cameroon*
Juliane Krämer, *U. Regensburg, Germany*
Péter Kutas, *U. Birmingham, E. Loránd U., UK*
Pascal Lafourcade, *U. Clermont, France*
Xiangyu Liu, *Purdue U., Georgia IT, USA*
Marine Minier, *LORIA, Nancy, France*
Mainack Mondal, *IIT, Kharagpur, India*
Abderrahmane Nitaj, *U. Caen, France*
Yanbin Pan, *Ch. Acad. of Sciences, China*
Christophe Petit, *Birmingham, ULB, Belgium*
Svetla Petkova-Nikova, *KU Leuven, Belgium*
Vincent Rijmen, *KU Leuven, U. Bergen*
Yann Rotella, *Paris-Saclay U., France*
Simona Samardjiska, *Radboud U., NL*
Palash Sarkar, *Indian Stat. Inst., India*
Ali Aydin Selçuk, *TOBB University, Turkey*
El Mamoun Souidi, *MV U., Rabat, Morocco*
Pantelimon Stanica, *NPS, Monterey, USA*
Yash Vasani, *FIPS, USA*
Fernando Virdia, *NOVA Lisboa, Portugal*

Africacrypt is an annual international conference on cryptology. Africacrypt 2025 is organized by the ENSIAS College of Mohammed V University in Rabat wih partnership of the General Directorate of Information Systems Security (DGSSI), Morocco, in cooperation with the International Association for Cryptologic Research (IACR). The aim of Africacrypt 2025 is to provide a forum for practitioners and researchers from industry, academia and government from all over the world for open discussion on all aspects of cryptology and its applications.

The program committee is seeking original research papers, systematization of knowledge (SOK) papers as well as tutorials, on topics, including but not limited to the following list:

- Foundations and underlying theory : (vector) Boolean function, coding theory, information theory, probability theory, complexity theory, game theory, formal methods.
- Public-key cryptography: key establishment, entity authentication protocols, digital signatures, factoring based crypto, discrete-log based crypto including ECC, post-quantum cryptography.
- Symmetric cryptography: authenticated encryption, hashing, message authentication, design and cryptanalysis of primitives: block ciphers, permutations, stream ciphers, extendable output functions (XOF), deck functions, security proofs of modes and constructions.
- Cryptographic engineering: dedicated hardware implementations, software implementations and benchmarking, implementation attacks and countermeasures: side channel and fault injection attacks formal verification of implementations, artificial intelligence for cryptanalysis.
- Advanced cryptographic protocols: fully homomorphic encryption, multi-party computation, attribute-based encryption and authentication, pairing-based crypto.
- Applications of cryptography: electronic voting, privacy and anonymity.

Instructions for authors

Authors are invited to submit papers electronically in PDF format. 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 25 pages in total including bibliography and appendices. Submissions will be blind-refereed. Authors of accepted papers must guarantee that their paper will be presented physically at the conference, and can publish a full version of their paper online.

Authors shall consult Springer's authors' guidelines and use their proceedings templates, for LaTeX, for the preparation of their papers. Springer encourages authors to include their ORCIDs in their papers. In addition, the corresponding author of each paper, acting on behalf of all the authors of that paper, must complete and sign a Consent-to-Publish form.

For submission, please use Springer's Nature **EquinOCS** at

https://equinocs.springernature.com/service/africacrypt2025

Further information and instructions can be found at:

https://africacrypt2025.sciencesconf.org

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 http://bit.ly/2HaWmko

Contact

Svetla Petkova-Nikova: svetla.nikova@esat.kuleuven.be
Vincent Rijmen: vincent.rijmen@kuleuven.be
Abderrahmane Nitaj: abderrahmane.nitaj@unicaen.fr