Latincrypt 2025 – Call for Papers

Latincrypt 2025 is the Ninth International Conference on Cryptology and Information Security in Latin America, and is organized by Universidad Nacional de Colombia and Universidad EAFIT, in Medellín, Colombia, in cooperation with IACR, the International Association for Cryptologic Research. Latincrypt 2025 seeks original contributions on all technical aspects of cryptology, including, but not limited to: symmetric and public-key primitives, symmetric and public-key cryptanalysis, cryptographic protocols, security notions and models, formal methods, software and hardware implementations and their security, applied cryptography and privacy, as well as cryptologic aspects of network security, complexity theory, information theory, coding theory, number theory, and quantum computing.

Important dates

Abstract submission:	April 11th 2025, 23:59 AoE
Paper submission:	April 18th 2025, 23:59 AoE
Notification:	July 4th 2025
Camera-ready:	July 25th 2025

Note that no new submissions will be accepted after the abstract submission deadline.

Submission server

https://easychair.org/conferences/?conf=latincrypt2025

Instructions for authors

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop with formally published proceedings. Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Each submission must be written in English, and should begin with a title, a short abstract, a list of keywords, and an introduction that summarizes the contributions of the paper at a level appropriate for a non-specialist reader. Submissions must be typeset using LaTeX using the **unmodified Springer LNCS style file**. The final versions of accepted papers will be published as a volume of Springer's Lecture Notes in Computer Science series.

The page limit for submissions is **30 pages including references and all appendices**. The same page limit will apply to the final versions of papers. Authors are permitted to additionally submit auxiliary material (like source code, long proofs, etc.), which reviewers may—but do not have to—take into account when judging the merits of papers. This

material must be submitted using the "Supplementary Material" form in Easychair. Submissions not meeting these guidelines risk rejection without consideration of their merits.

All papers must be submitted electronically through the submission system of **Latincrypt 2025**. Late submissions and non-electronic submissions will not be considered. **No new submissions will be accepted after the abstract submission deadline**. Authors of accepted papers must guarantee that their paper will be presented at the conference. Submissions by program committee members will be held to higher standards than other submissions.

As in previous editions, accepted papers will be published in Springer's Lecture Notes in Computer Science, and proceedings will be made available at the conference (Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers).

Conflicts of interest

During submission, authors will have to indicate conflicts of interest with members of the program committee. Latincrypt 2025 follows the **IACR policy on conflicts of interest**. In short, authors have a conflict of interest with PC members:

- if one is or was the thesis advisor to the other, no matter how long ago;
- if they shared an institutional affiliation within the prior two years;
- if they published two or more jointly authored works in the last three years; or
- if they are immediate family members

Program committee

Abdelrahaman Aly	Technology Innovation Institute	UAE
Miguel Ambrona	IOHK	Hong Kong
Sebastian Angel	University of Pennsylvania	USA
Marshall Ball	New York University	USA
Gustavo Banegas	INRIA and École polytechnique	France
Magali Bardet	University of Rouen Normandie	France
Thaís Bardini Idalino	Universidade Federal de Santa Catarina	Brazil
Paulo Barreto	University of Washington | Tacoma	USA
Lejla Batina	Radboud University	Netherlands
Alexander Bienstock	JP Morgan AI Research & JP Morgan AlgoCRYPT CoE	USA
Allison Bishop	Proof Trading	USA

Katharina Boudgoust	CNRS, Univ Montpellier, LIRMM	France
Dung Bui	IRIF, CNRS, Université Paris Cité, France	France
Benedikt Bunz	New York University	USA
Fabio Campos	Bonn-Rhein-Sieg University of Applied Sciences	Germany
Nishanth Chandran	Microsoft	India
Aisling Connolly	TACEO	Switzerland
Anamaria Costache	NTNU	Norway
Anders Dalskov	Partisia	Denmark
Bernardo David	IT University of Copenhagen	Denmark
Luca De Feo	IBM Research Zürich	Switzerland
Jintai Ding	Xi'san Jiaotong-Liverpool University, China and Basques center for applied mathematics (BCAM), Spain	China and Spain
Andre Esser	Technology Innovation Institute	UAE
Diego F. Aranha	Aarhus University	Denmark
Antonio Florez-Gutierrez	NTT Social Informatics Laboratories	Japan
Chaya Ganesh	Indian Institute of Science, Bangalore	India
Juan A. Garay	Texas A&M University	USA
Adria Gascon	Google	USA
Valérie Gauthier-Umaña	Universidad de los Andes	Colombia
Maria Isabel Gonzalez Vasco	Universidad Carlos III de Madrid	Spain
Elisa Gorla	University of Neuchatel	Switzerland
Lucjan Hanzlik	CISPA Helmholtz Center for Information Security	Germany
Alejandro Hevia	Department of Computer Science, University of Chile	Chile
Andreas Hülsing	Eindhoven University of Technology, Eindhoven & Sandbox AQ, Palo Alto	Netherlands and USA
Elena Kirshanova	Technology Innovation Institute	UAE
Lisa Kohl	CWI Amsterdam	Netherlands
Markulf Kohlweiss	University of Edinburgh and IOG	UK
Yashvanth Kondi	Silence Laboratories	USA
Hilder Vitor Lima Pereira	Universidade Estadual de Campinas (UNICAMP)	Brazil
Chen-Da Liu Zhang	Lucerne University of Applied Sciences and Arts & Web3 Foundation	Switzerland
Patrick Longa	Microsoft	USA
Cuauhtemoc Mancillas Lopez	Cinvestav	México
Elisaweta Masserova	Carnegie Mellon University	USA

Kelsey Melissaris	Aarhus University	Denmark
Nicky Mouha	FedWriters	USA
Leah Namisa Rosenbloom	Northeastern University	USA
Ngoc Khanh Nguyen	King's College London	UK
Anca Nitulescu	ENS Paris	France
Ariel Nof	Technion	Israel
Miyako Ohkubo	NICT	Japan
Claudio Orlandi	Aarhus University	Denmark
Elena Pagnin	Chalmers University of Technology	Sweden
Daniel Panario	Carleton University	Canada
Alberto Pedrouzo-Ulloa	atlanTTic, Universidade de Vigo	Spain
Octavio Perez Kempner	NTT Social Informatics Laboratories	Japan
Ray Perlner	NIST	USA
Ludovic Perret	EPITA and Sorbonne University	France
Bart Preneel	COSIC, University of Leuven	Belgium
Carla Ràfols	Universitat Pompeu Fabra	France
Divya Ravi	University of Amsterdam	Netherlands
Francisco Rodríguez	Technology Innovation Institute	UAE
Thomas Schneider	TU Darmstadt	Germany
Peter Scholl	Aarhus University	Denmark
Phillipp Schoppmann	Google	USA
Sruthi Sekar	Indian Institute of Technology, Bombay	India
Luisa Siniscalchi	Technical University of Denmark	Denmark
Daniel Slamanig	Universität der Bundeswehr München	Germany
Daniel Smith-Tone	NIST	USA
Yifan Song	Tsinghua University and Shanghai Qi Zhi Institute	China
Eduardo Soria-Vazquez	Technology Innovation Institute	UAE
Katerina Sotiraki	Yale University	USA
Nick Spooner	Cornell University	USA
Ajith Suresh	Technology Innovation Institute (TII), Abu Dhabi	UAE
Akira Takahashi	JP Morgan AI Research & JP Morgan AlgoCRYPT CoE	USA
Mehdi Tibouchi	NTT Social Informatics Laboratories	Japan
Muthuramakrishnan Venkitasubramaniam	Georgetown University	USA
Javier Verbel	Technology Innovation Institute	UAE
Frederik Vercauteren	K.U.Leuven - COSIC	Belgium
Alfredo Viola	Universidad de la República de Uruguay	Uruguay
Fernando Virdia	King's College London	UK

Chenkai Weng	Arizona State University	USA
Sophia Yakoubov	Aarhus University	Denmark
Arantxa Zapico	Ethereum Foundation	Argentina

Contact information

Conference email:
latincrypt2025_med@unal.edu.co

General co-chairs

Daniel Cabarcas
Universidad Nacional de Colombia, Medellín, Colombia
dcabarc@unal.edu.co

Juan Guillermo Lalinde
Universidad EAFIT, Medellín, Colombia
jlalinde@eafit.edu.co

Program co-chairs

Daniel Escudero
JP Morgan AI Research & JP Morgan AlgoCRYPT CoE, USA
daniel.escudero@protonmail.com

Ivan Damgård
Aarhus University, Denmark
ivan@cs.au.dk