Latincrypt 2021
Call for Papers

General Information

Latincrypt 2021, the Seventh International Conference on Cryptology and Information Security in Latin America, will take place online on October 6-8, 2021. It is organized by Universidad del Rosario, Colombia, in cooperation with the International Association for Cryptologic Research (IACR).

Original papers on all technical aspects of cryptology are solicited for submission to Latincrypt 2021, including new cryptographic primitives, cryptanalysis, security models, formal methods in cryptography, hardware, and software implementation aspects, cryptographic protocols and applications, as well as submissions about cryptographic aspects of network security, complexity theory, information theory, coding theory, number theory, and quantum computing.

Important dates

- Abstract submission: **May 10, 2021, 23:59 AoE**
- Paper submission: May 17, 2021, 23:59 AoE
- Notification: June 30, 2021
- Conference: October 6-8, 2021

Instructions for authors

Submissions must be at most 20 pages including references and appendices. Authors are encouraged 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. All submissions must be typeset in LaTeX using the unmodified Springer LNCS style file. Details on the Springer LNCS format can be obtained via http://www.springer.de/comp/lncs/authors.html. 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 not meeting these guidelines risk rejection without consideration of their merits.

All papers must be submitted electronically through the submission system of Latincrypt 2021.

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. Late submissions and non-electronic submissions will not be considered. No new submissions will be accepted after the abstract submission deadline. Submissions by program-committee members will be held to higher standards than other submissions.

The final versions of accepted papers will be published as a volume of Springer's Lecture Notes in Computer Science series with the same page limit of 20 pages. The proceedings will be available at the conference. 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, which is going to be held remotely.

Conflicts of interest

During submission, authors will have to indicate conflicts of interest with members of the program committee. Latincrypt 2021 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

Lejla Batina, Radboud University, NL
Carsten Baum, Aarhus University, DK
Nina Bindel, University of Waterloo, CA
Debrup Chakraborty, Indian Statistical Institute, IN
Céline Chevalier, Université Paris II Panthéon-Assas, FR
Jesús-Javier Chi-Domínguez, TII, UAE
Joan Daemen, Radboud University, NL
Jan-Pieter D'Anvers, imec-COSIC/KU Leuven, BE
Bernardo David, IT University of Copenhagen, DK
Luca De Feo, IBM Research Zürich, CH
Orr Dunkelman, University of Haifa, IL
Antonio Faonio, EURECOM, FR
Oriol Farràs, Universitat Rovira i Virgili, ES
Pooya Farshim, University of York, UK
Gina Gallegos García, Instituto Politécnico Nacional, MX
Alonso González, Toposware, JP
Aurore Guillevic, Inria Nancy, FR
Tim Güneysu, Ruhr-Universität Bochum and DFKI, DE
Javier Herranz, Universitat Politècnica de Catalunya, ES
Julia Hesse, IBM Research Zürich, CH
Alejandro Hevia, Universidad de Chile, CL
Sorina Ionica, Université de Picardie Jules Verne, FR
Patrick Longa, Microsoft Research, US (**co-chair**)
Marine Minier, Université de Lorraine, FR
Rafael Misoczki, Google, US
Anderson Nascimento, University of Washington – Tacoma, US
Khoa Nguyen, Nanyang Technological University, SG
Geovandro Pereira, University of Waterloo and evolutionQ, CA
Peter Pessl, Infineon Technologies, DE
Christiane Peters, IBM Security, BE
Carla Ràfols, Universitat Pompeu Fabra, ES (**co-chair**)
Joost Renes, NXP Semiconductors, NL
Oscar Repáraz, Square, US, and COSIC/KU Leuven, BE
Matthieu Rivain, CryptoExperts, FR
Francisco Rodríguez-Henríquez, CINVESTAV-IPN, MX
Sven Schäge, Ruhr-Universität Bochum, DE
Peter Schwabe, MPI-SP, DE and Radboud University, NL
Douglas Stebila, University of Waterloo, CA
Nicolas Thériault, Universidad de Santiago de Chile, CL
Alfredo Viola, Universidad de la República de Uruguay, UY
Greg Zaverucha, Microsoft Research, US

Contact Information

General Chair

Valérie Gauthier Umaña
Applied Mathematics and
Computer Science Department
School of Engineering, Science and Technology
Universidad del Rosario
Bogotá, Colombia
Carrera 6 # 12 C - 16, oficina 502
E-mail: valeriee.gauthier@urosario.edu.co

Program Co-Chairs

Patrick Longa
MSR Security and Cryptography
Microsoft Research, USA
One Microsoft Way, Redmond, WA 98052
E.mail: plonga@microsoft.com

Carla Ràfols
Wireless and Secure Communications Group
Departament de Tecnologies de la Informació i les Comunicacions
Universitat Pompeu Fabra
Roc Boronat, 138 08018 España
E-mail: carla.rafols@upf.edu