Latincrypt 2015

August 23-26, 2015, Guadalajara, Mexico

Call for Papers

Latincrypt 2015 is the Fourth International Conference on Cryptology and Information Security in Latin America, and is organized by CINVESTAV-IPN, in cooperation with IACR, the International Association for Cryptologic Research. Original papers on all technical aspects of Cryptology are solicited for submission to Latincrypt 2015. The conference seeks original contributions on new cryptographic primitive proposals, cryptanalysis, security models, 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**: Sun, March 15th, 2015, 6:00 a.m. UTC.
- **Full submission**: Sun, March 22nd, 2015, 6:00 a.m. UTC.
- **Acceptance notification**: Fri, May 15th, 2015.
- **Final version due**: Mon, June 1st, 2015.
- **Workshop presentations**: Sun, August 23rd-Wed, August 26th 2015.

Instructions to 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. The page limit for submissions is 12 pages excluding references and clearly marked appendices, using at least 11-point font and reasonable margins. The final versions of accepted papers will be limited to 20 pages including references and appendices. Reviewers are not required to read the appendices, so the paper should be intelligible and self-contained without them. Submissions not meeting these guidelines risk rejection without consideration of their merits.

All papers must be submitted electronically at the Latincrypt web site (`www.latincrypt.org`). Late submissions and non-electronic submissions will not be considered. No new submissions will be accepted after the abstract submission deadline (March 15th, 2015). Authors of accepted papers must guarantee that their paper will be presented at the conference. Program Committee member submissions will be held to higher standards than other submissions.

Accepted papers will be published in Springer's Lecture Notes in Computer Science and will be available after the conference (final approval pending). Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers. It is encouraged that the submission be processed in latex according to the instructions listed on Springer_LNCS. These instructions are mandatory for the final papers.

Committees

Program Chairs:
◦ Kristin Lauter, *Microsoft Research, USA*
◦ Francisco Rodríguez-Henríquez, *CINVESTAV-IPN, Mexico*

Program Committee
So far the following people have accepted to serve on the Program Committee of Latincrypt 2015:
◦ Michel Abdalla (*École Normale Supérieure, France*)
◦ Diego Aranha (*University of Campinas, Brazil*)
◦ Jean-Philippe Aumasson (*Kudelski Security, Switzerland*)
◦ Paulo Barreto (*University of São Paulo, Brazil*)
◦ Lejla Batina (*Radboud University Nijmegen, Netherlands*)
◦ Guido Bertoni (*STMicroelectronics, Italy*)
◦ Debrup Chakraborty (*CINVESTAV-IPN, Mexico*)
◦ Ray C. C. Cheung (*City University of Hong Kong, Hong Kong*)
◦ Nishanth Chandran (*Microsoft Research, India*)
◦ Ricardo Dahab (*University of Campinas, Brazil*)
◦ Jérémie Detrey (*INRIA, France*)
◦ Thomas Eisenbarth (*Worcester Polytechnic Institute, USA*)
◦ Tim Güneysu (*Ruhr-Universität Bochum, Germany*)
◦ Alejandro Hevia (*University of Chile, Chile*)
◦ Sorina Ionica (*University of Bordeaux and INRIA, France*)
◦ Tanja Lange (*Technische Universiteit Eindhoven, Netherlands*)
◦ Julio López (*University of Campinas, Brazil*)
◦ Florian Luca (*UNAM, Mexico and University of Witwatersrand, South Africa*)
◦ Alfred Menezes (*University of Waterloo, Canada*)
◦ Payman Mohassel (*Yahoo Labs, USA*)
◦ Guillermo Morales-Luna (*CINVESTAV-IPN, Mexico*)
◦ Michael Naehrig (*Microsoft Research, USA*)
◦ Gregory Neven (*IBM Zurich Research Laboratory, Switzerland*)
◦ Daniel Panario (*Carleton University, Canada*)

◦ Cécile Pierrot (*UPMC/Sorbonne University, Paris, France*)
◦ Bart Preneel (*KU Leuven and iMinds, Belgium*)
◦ Erkay Savas (*Sabanci University, Turkey*)
◦ Peter Schwabe (*Radboud University Nijmegen, Netherlands*)
◦ Jae Hong Seo (*Myongji University, Korea*)
◦ Damien Stehlé (*École Normale Supérieure de Lyon, France*)
◦ Rainer Steinwandt (*Florida Atlantic University, USA*)
◦ Nicolas Thériault (*Universidad del Bío-Bío, Chile*)
◦ Frederik Vercauteren (*KU Leuven, Belgium*)
◦ Alfredo Viola (*Universidad de la República, Uruguay*)
◦ Bogdan Warinschi (*University of Bristol, United Kingdom*)

Steering Committee
◦ Michel Abdalla (*École Normale Supérieure, France*)
◦ Paulo Barreto (*University of São Paulo, Brazil*)
◦ Ricardo Dahab (*University of Campinas, Brazil*)
◦ Alejandro Hevia (*University of Chile, Chile*)
◦ Julio López (*University of Campinas, Brazil*)
◦ Daniel Panario (*Carleton University, Canada*)
◦ Francisco Rodríguez-Henríquez (*CINVESTAV-IPN, Mexico*)
◦ Alfredo Viola (*Universidad de la República, Uruguay*)

Local Organization Committee:
◦ Nareli Cruz-Cortés, *CIC-IPN, Mexico*
◦ Luis J. Domínguez-Pérez, *CIMAT, Mexico*
◦ Jorge E. González Díaz, *Intel, Mexico*