Call for Papers

LATINCRYPT 2014

September 17-19, 2014, Florianópolis, Brazil

`latincrypt2014.labsec.ufsc.br`

Latincrypt 2014 (`http://latincrypt2014.labsec.ufsc.br/`) is the Third International Conference on Cryptology and Information Security in Latin America, and is organized by Federal University of Santa Catarina and Carleton University, in cooperation with the International Association for Cryptologic Research (IACR).

Original papers on all technical aspects of Cryptology are solicited for submission to Latincrypt 2014. 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.

1 Important dates:

- **Submission deadline:** July ~~05~~ **11**, 2014, 23:59 UTC
- **Notification:** August 23, 2014
- **Preproceedings version:** September 6, 2014
- **Final version:** October 4, 2014

2 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 `https://secure.iacr.org/websubrev/latcrypt/submit/`. Late submissions and non-electronic submissions will not be considered. No new submissions will be accepted after the submission deadline (**July 11, 2014**). 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 2_ε according to the instructions listed on `http://www.springer.de/comp/lncs/authors.html`. These instructions are mandatory for the final papers.

3 Invited speakers

- Appelbaum, Jacob (The Tor Project, Germany)
- Diaz, Claudia (KU/Leuven, Belgium)
- Halderman, J. Alex (University of Michigan, USA)
- Lauter, Kristin (Microsoft Research, USA)

4 Program committee

- Abdalla, Michel (École Normale Supérieure, France)
- Aumasson, Jean-Philippe (Kudelski Security, Switzerland)
- Barreto, Paulo (University of São Paulo, Brazil)
- Batina, Lejla (Radboud University Nijmegen, Netherlands)
- Daemen, Joan (STMicroeletronics, Belgium)
- Dahab, Ricardo (University of Campinas, Brazil)
- Detrey, Jérémie (INRIA, France)
- Dunkelman, Orr (University of Haifa, Israel)
- Gathen, Joachim von zur (Universität Bonn, Germany)
- Gonzalez Vasco, Maribel (Universidad Rey Juan Carlos de Madrid, Spain)
- Graaf, Jeroen van de (Universidade Federal de Minas Gerais, Brazil)
- Handschuh, Helena (Cryptography Research/KULeuven, Belgium)
- Heninger, Nadia (University of Pennsylvania, USA)
- Hevia, Alejandro (University of Chile, Chile)
- Ionica, Sorina (Microsoft Research, USA)
- Lange, Tanja (Technische Universiteit Eindhoven, Netherlands)
- Longa, Patrick (Microsoft Research, USA)
- López, Julio (University of Campinas, Brazil)
- Nascimento, Anderson (University of Brasília, Brazil)
- Neven, Gregory (IBM Zurich Research Laboratory, Switzerland)
- Paterson, Kenny (Royal Holloway, University of London, UK)
- Peyrin, Thomas (Nanyang Technological University, Singapore)
- Rodríguez-Henríquez, Francisco (CINVESTAV-IPN, Mexico)
- Schwabe, Peter (Radboud University Nijmegen, Netherlands)
- Sendrier, Nicolas (INRIA, France)
- Stebila, Douglas (Queensland University of Technology, Australia)
- Stehle, Damien (École Normale Supérieure de Lyon, France)
- Thomé, Emmanuel (INRIA, France)
- Thériault, Nicolas (Universidad del Bío-Bío, Chile)
- Viola, Alfredo (Universidade de la República, Uruguay)
- Yilek, Scott (University of St. Thomas, USA)

5 Conference organizers

- **Program chairs:** Diego F. Aranha (University of Campinas), Alfred Menezes (University of Waterloo).
- **General chairs:** Ricardo Custódio (Federal University of Santa Catarina), Daniel Panario (Carleton University).