Call for papers – Eurocrypt 2018

Original papers on practical and theoretical aspects of cryptology are solicited for submission to Eurocrypt 2018, the 37th Annual Eurocrypt Conference. Eurocrypt 2018 is organized by the International Association for Cryptologic Research (IACR). The conference is held in Tel Aviv Apr 29 - May 3, 2018.

Dates

- Submission deadline: Sep 19, 11:59 AM CET
- Reviews sent out for rebuttals: Nov 15
- Rebuttals due: Nov 22, 23:59 CET
- Notification: Jan 15
- Conference version due: Feb 1, 23:59 CET
- Conference: Apr 29 - May 3

Instructions for Authors

Submissions must be at most 30 pages in the Springer's LNCS format including title page, abstract, references and appendices. Any amount of clearly marked supplementary material may be supplied, following after the main body of the paper or in separate files (for example, program code or experimental data). The submission should be intelligible without the supplementary material, as reviewers are not required to access the supplementary material.

It is mandatory that the submission be processed in LaTeX2e according to the instructions given by Springer [http://www.springer.de/comp/lncs/authors.html]. Submissions must be typeset in plain Springer LNCS format, in particular without changing the font size, margins or linespacing.

Submitted papers must be in PDF format and submitted electronically via the submission server. The submission server asks for a list of authors. The list is not visible to reviewers. The list of authors should include all those, and only those, who have contributed to the submission.

The submission must be anonymous with no author names, affiliations or obvious references. It should begin with a title, a short abstract, and an introduction. The introduction should summarise the contributions of the paper at the level understandable for a non-expert reader. The introduction should also explain the relation to related work.

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings. IACR reserves the right to share information about submissions with other program committees to detect parallel submissions and the IACR policy on irregular submissions will be strictly enforced. For further details, see http://www.iacr.org/docs/.

Submissions not meeting the above guidelines may be rejected without consideration of their merits.

For accepted papers the formatting instruction will be the same as for submissions and the length of the final version will be at most 30 pages, including title page, abstract, references and appendices.

Program committee members are allowed to submit one paper, and a second one if both submissions are co-authored. Any PC member submission will be held to higher standards than other submissions. Program chairs are not allowed to submit.

Conference Proceedings

Proceedings will be published in Springer's Lecture Notes in Computer Science and will be available at the conference. Authors of accepted papers must complete the IACR copyright assignment form for their work to be published in the proceedings, and guarantee that their paper will be presented at the conference. At the conference presentations will be recorded and published for the sake of people that cannot attend the conference or the track in which the presentation was scheduled.

Program Committee

Martin R. Albrecht (Royal Holloway, UK)
Joël Alwen (IST Austria and Wickr, Austria)
Paulo Barreto (University of Washington, USA)
Nir Bitansky (Tel Aviv University, Israel)
Andrey Bogdanov (DTU, Denmark)
Chris Brzuska (TU Hamburg, Germany)
Jan Camenisch (IBM Zurich, Switzerland)
Ignacio Cascudo (Aalborg University, Denmark)
Melissa Chase (Microsoft Research, USA)
Joan Daemen (Radboud University, the Netherlands, and STMicroelectronics, Belgium)
Yevgeniy Dodis (New York University, USA)
Nico Döttling (UC Berkeley, USA)
Sebastian Faust (Ruhr-Universität Bochum, Germany)
Serge Fehr (CWI Amsterdam, The Netherlands)
Georg Fuchsbauer (ENS/INRIA, France)
Jens Groth (University College London, UK)
Jian Guo (Nanyang Technological University, Singapore)
Martin Hirt (ETH Zurich, Switzerland)
Dennis Hofheinz (KIT, Germany)
Yuval Ishai (Technion, Israel, and UCLA, USA)
Thomas Johansson (Lund University, Sweden)
Nathan Keller (Bar Ilan University, Israel)
Eike Kiltz (Ruhr-Universität Bochum, Germany)
Gregor Leander (Ruhr-Universität Bochum, Germany)
Yehuda Lindell (Bar Ilan University, Israel)
Mohammad Mahmoody (University of Virginia, USA)
Willi Meier (FHNW, Windisch, Switzerland)

Florian Mendel (Infineon, Germany)
Bart Mennink (Radboud University, The Netherlands)
María Naya-Plasencia (INRIA, France)
Svetla Nikova (KU Leuven, Belgium)
Jesper Buus Nielsen (Aarhus University, Denmark) [co-chair]
Arpita Patra (Indian Institute of Science, India)
David Pointcheval (CNRS and DI/ENS, PSL Research University, France)
Bart Preneel (KU Leuven, Belgium)
Vincent Rijmen (KU Leuven, Belgium) [co-chair]
Thomas Ristenpart (University of Wisconsin - Madison, USA)
Alon Rosen (IDC Herzliya, Israel)
Mike Rosulek (Oregon State University, USA)
Louis Salvail (University of Montreal, Canada)
Yu Sasaki (NTT Secure Platform Laboratories, Japan)
Thomas Schneider (Ruhr-Universität Bochum, Germany)
Jacob Schuldt (AIST, Japan)
Nigel Smart (Bristol University, UK)
Adam Smith (Pennsylvania State University, USA)
Damien Stehlé (ENS de Lyon, France)
Björn Tackmann (IBM Research - Zurich, Switzerland)
Dominique Unruh (University of Tartu, Estonia)
Vinod Vaikuntanathan (MIT, USA)
Gilles Van Assche (STMicroelectronics, Belgium)
Muthuramakrishnan Venkitasubramaniam (University of Rochester, USA)
Frederik Vercauteren (KU Leuven, Belgium)
Damien Vergnaud (ENS de Paris, France)
Ivan Visconti (University of Salerno, Italy)
Moti Yung (Columbia University and Snap Inc., USA)