Kangacrypt 2018

Australian Workshop on Offensive Cryptography

Adelaide, Australia, 7–8 December, 2018

Call for Papers

Taking place in the National Wine Centre of Australia, amid the fourth largest wine collection in the southern hemisphere, the aim of the Kangacrypt workshop is to bring together practitioners and researchers interested in all aspects of breaking cryptography.

The workshop consists of four invited tutorial talks. In addition, we seek submissions of original research papers within the scope of the workshop. We anticipate that there will be space for 15–20 submissions.

Submissions may present theory, techniques and practical experience on topics including, but not limited to:

- Mathematical and statistical attacks on cryptographic primitives
- Micro-architectural attacks
- Physical attacks, such as power and electromagnetic analysis
- Attacks on cryptographic protocols
- Analysis of implementation of cryptographic functions.

Instructions for Authors

Submissions should be made electronically in PDF format to the Kangacrypt submission web site (https://easychair.org/conferences/?conf=kangacrypt2018). Submissions must be written in English, should begin with a title, a short abstract and an introduction that summarises the contributions of the paper at a level appropriate for a non-specialist reader. Submissions should follow the Springer LNCS paper format, and be at most 16 pages excluding bibliography and clearly marked appendices.

Pre-proceedings and special issue in CCDS

Accepted papers will be distributed electronically to all participants. The authors of accepted papers will be invited to submit a full paper to appear (subject to further review) in a special issue of the Springer Journal of Cryptography and Communications.

Important dates:

- Submission deadline: 15 June 2018
- Notification deadline: 15 August 2018
- Pre-proceeding deadline: 30 September 2018

Australian Government
Department of Defence
Science and Technology

DATA 61

CSIRO

Kangacrypt 2018

Australian Workshop on Offensive Cryptography

Adelaide, Australia, 7–8 December, 2018

Program co-chairs

- Lejla Batina (Radboud University)
- Daniel J. Bernstein (University of Illinois at Chicago)
- Yuval Yarom (University of Adelaide and Data61)

Program committee

- Diego Aranha (University of Campinas)
- Valentina Banciu (Riscure BV)
- Lynn Batten (Deakin University)
- Shivam Bhasin (Nanyang Technological University)
- Chitchanok Chuengsatiansup (INRIA and ENS de Lyon)
- Joan Daemen (Radboud University)
- Jean-Luc Danger (Télécom ParisTech/LTCI)
- Thomas Eisenbarth (University of Lübeck and WPI)
- Yunsi Fei (Northeastern University)
- Daniel Gruss (Graz University of Technology)
- Shay Gueron (University of Haifa and Amazon Web Services)
- Tim Güneysu (Ruhr University Bochum and DFKI)
- Annelie Heuser (CNRS/IRISA)
- Michael Hutter (Cryptography Research Inc.)
- Andreas Hülsing (Eindhoven University of Technology)
- Nele Mentens (Katholieke Universiteit Leuven)
- Veelasha Moonsamy (Utrecht University)
- Debdeep Mukhopadhyay (IIT Kharagpur)
- David Oswald (The University of Birmingham)
- Thomas Peyrin (Nanyang Technological University)
- Stjepan Picek (Delft University of Technology)
- Ilia Polian (University of Stuttgart)
- Francesco Regazzoni (ALaRI - USI)
- Kazuo Sakiyama (The University of Electro-Communications)
- Patrick Schaumont (Virginia Tech)
- Tobias Schneider (Université catholique de Louvain)
- Peter Schwabe (Radboud University)
- Juraj Somorovsky (Ruhr University Bochum)
- Ron Steinfeld (Monash University)
- Vanessa Teague (The University of Melbourne)

Australian Government
Department of Defence
Science and Technology

DATA 61

CSIRO