Call for Papers, CT-RSA 2022 Cryptographers Track at RSAC

February 7–10, 2022, San Francisco
Programme Chair Steven Galbraith, University of Auckland, NZ
https://ct-rsa-2022.blogs.auckland.ac.nz/

Submission deadline	Thursday September 23, 2021 (23:59 UTC)
Final notification	Thursday November 11, 2021
Camera-ready version	Sunday December 5, 2021

CT-RSA 2022, the Cryptographers' Track at the RSA Conference, is the venue for scientific papers on cryptography within the RSA Conference. The RSA Conference is the main trade show for the security industry; pre-COVID over 40,000 people would attend the exhibition floor, keynote addresses, events, seminars, training events and various technical tracks. CT-RSA is a great venue to ensure that scientific results not only get published to the wider cryptologic community, but also get exposed to technical attendees from industry, government and wider afield. The conference is organised by the RSA Conference organisation, and the CT-RSA Program Chair for 2022 is Steven Galbraith from the University of Auckland, who was appointed by the CT-RSA steering committee. For questions about the CT-RSA conference please contact s.galbraith@auckland.ac.nz

The conference organisers of the RSA Conference intend to hold a physical event, but the CT-RSA track will not require authors to present their paper in person. So virtual/remote participation will be allowed. The exact details of the presentations are not yet decided, but are likely to include a pre-recorded video and participation in a live event. The RSA Conference will coordinate with pre-recording talks. Authors of accepted papers will be required to comply with all the deadlines and processes of the RSA Conference, such as providing a first draft of their presentation by December 6, 2021 and the final version of their presentation by January 10, 2022.

Instructions for Authors

Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Submissions must be written in English. Submissions should begin with a title, and a short abstract. The length of the main body of submissions should be at most 24 pages, including bibliography.

It is strongly encouraged that submissions are processed in LaTeX using Springer's LNCS package (see Springer Lecture Notes in Computer Science instructions for authors https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines) with no changes to the style. Springer encourages authors to include their ORCIDs in the final published versions of their papers. All submissions must have page numbers, e.g., using Latex command \pagestyle{plain}.

Any number of clearly marked appendices may be supplied following the main body of the paper. However, the committee members are not required to read appendices; the paper should be intelligible without them. Authors are advised to write their papers clearly and carefully, to provide good motivation for their work, and to give a high-level overview of the arguments and techniques used to obtain the main results. Papers are likely to be rejected if the results are unable to be verified by the PC within the short review timeframe.

Submitted papers must be in PDF format and should be submitted electronically via the conference website.

Submissions not meeting these guidelines risk rejection without consideration of their merits.

Systematization of Knowledge papers

As in past years, we will solicit Systematization of Knowledge (SoK) papers that evaluate, systematize, and contextualize existing knowledge, since such papers can provide a high value to our community.

During reviewing, they will be held to the same standards as traditional research papers, but they will be accepted based on their treatment of existing work and value to the community, and not based on any new research results they may contain. Suitable SoK papers are those that provide an important new viewpoint on an established, major research area, support or challenge long-held beliefs in such an area with compelling evidence, or present a convincing, comprehensive new taxonomy of such an area. Survey papers without such insights are not appropriate for acceptance. Accepted SoK papers will be presented at the conference and included in the proceedings.

Authors submitting a Systematization of Knowledge paper should have a title consisting of "SoK: Title". This is to ensure the committee is aware that the paper is an SoK paper. To accommodate the greater number of references that would be expected in SoK papers, such submissions should be at most 30 pages, including bibliography (with format as above).

Publication and reviewing

The proceedings will be published in the Springer LNCS series, and will be available electronically at the conference. Each publication will be limited to 24 pages (30 pages for SoK papers) including the bibliography, and the submitted paper should represent what the authors expect to finally publish. In addition, the corresponding author of each accepted paper, acting on behalf of all of the authors of that paper, must complete and sign a Consent-to-Publish form. The corresponding author signing the copyright form should match the corresponding author marked on the paper. Once the files have been sent to Springer, changes relating to the authorship of the papers cannot be made.

Hard copies of the proceedings will not be provided to authors.

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to a journal or any other conference/workshop that has proceedings. Authors may also not submit the work to any other venue with published proceedings until after the date of notification of acceptance/rejection. Accepted submissions may not appear in any other conference or workshop that has proceedings. The CT-RSA 2022 chair 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/irregular.pdf`.

All submissions will be blind-refereed and thus must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Note that anonymous submission does not prevent authors from submitting to eprint (see discussion at `https://eprint.iacr.org/about.html`). We will run a one-round review process with no author rebuttals. Each submission will be assigned to at least three reviewers (four if the paper includes a Program Committee member as an author, or if it is a "Systemization of Knowledge" paper).

Conflicts of Interest

Authors, program committee members, and reviewers must follow the IACR Policy on Conflicts of Interest (available from `https://www.iacr.org/docs/`). Authors should send an email to the PC chair to identify all members of the Program Committee who have an automatic conflict of interest (COI) with the submission.

A reviewer and an author have an automatic COI if one was the thesis advisor/supervisor to the other, or if they've shared an institutional affiliation within the last two years, or if they've published two or more joint authored works within the last three years, or if they are in the same family. Any further COIs of importance should be separately disclosed. It is the responsibility of all authors to ensure correct reporting of COI information. Submissions with incorrect or incomplete COI information may be rejected without consideration of their merits.

Program Committee

Masayuki Abe	*NTT Laboratories, Japan*
Gorjan Alagic	*University of Maryland, USA*
Man Ho Au	*University of Hong Kong, Hong Kong*
Shi Bai	*Florida Atlantic University, USA*
Paulo Barreto	*University of Washington, USA*
Lejla Batina	*Radboud University, The Netherlands*
Josh Benaloh	*Microsoft Research, USA*
Nina Bindel	*University of Waterloo and Institute for Quantum Computing, Canada*
Olivier Blazy	*Ecole Polytechnique, France*
Ran Cohen	*Northeastern University, USA and IDC Herzliya, Israel*
Gareth T. Davies	*Bergische Universität Wuppertal, Germany*
Jean Paul Degabriele	*TU Darmstadt, Germany*
Prastudy Fauzi	*Simula UiB, Bergen, Norway*
Luca De Feo	*IBM Research Europe – Zurich, Switzerland*
Steven Galbraith (Chair)	*University of Auckland, New Zealand*
Pierrick Gaudry	*CNRS, Nancy, France*
Qian Guo	*Lund University, Sweden*
Helena Handschuh	*Rambus Cryptography Research, USA*
Stanislaw Jarecki	*University of California, Irvine, USA*
Shuichi Katsumata	*AIST, Japan*
Marcel Keller	*CSIRO Data61, Australia*
Veronika Kuchta	*University of Queensland, Australia*
Joseph Liu	*Monash University, Australia*
Anna Lysyanskaya	*Brown, USA*
Giorgia Azzurra Marson	*NEC Labs Europe, Germany*
Willi Meier	*University of Applied Sciences and Arts Northwestern Switzerland (FHNW) Windisch, Switzerland*
Brice Minaud	*Inria and ENS, France*
Tarik Moataz	*MongoDB, USA*
Khoa Nguyen	*Nanyang Technological University, Singapore and University of Wollongong, Australia*
Bertram Poettering	*IBM Research Europe – Zurich, Switzerland*
David Pointcheval	*ENS, France*
Bart Preneel	*KU Leuven, Belgium*
Mike Rosulek	*Oregon State University, USA*
Adeline Roux-Langlois	*Univ Rennes, CNRS, IRISA, France*
Arnab Roy	*University of Klagenfurt, Austria*
Reihaneh Safavi-Naini	*University Calgary, Canada*
Yu Sasaki	*NTT Laboratories, Japan*
abhi shelat	*Northeastern University, USA*
Luisa Siniscalchi	*Aarhus University, Denmark*
Nigel Smart	*KU Leuven, Belgium*
Willy Susilo	*University of Wollongong, Australia*
Qiang Tang	*University of Sydney, Australia*
Jacques Traoré	*Orange Labs, France*
Fernando Virdia	*ETH Zürich, Switzerland*