ASIACRYPT 2022
Call for Papers

December 5–9, 2022, Taiwan
`http://asiacrypt.iacr.org/2022/`

Submission deadline	May 27, 2022, 11:59 am UTC (noon)
First round notification	July 20, 2022
Rebuttals due	July 26, 2022
Final notification	August 25, 2022
Camera-ready version	September 20, 2022
Conference	December 5–9, 2022

ASIACRYPT 2022, the 28th Annual International Conference on the Theory and Applications of Cryptology and Information Security, will take place in Taiwan on December 5–9, 2022. The conference is organized by the International Association for Cryptologic Research (IACR). Original research papers on all aspects of cryptology are solicited for submission.

Instructions for Authors

Submissions must be at most 30 pages excluding any auxiliary supporting material, and using the Springer LNCS format (in particular, do not modify the LNCS default font sizes or margins). Details on the Springer LNCS format can be obtained via `http://www.springer.de/comp/lncs/authors.html`. It is strongly encouraged that submissions are processed in LaTeX. All submissions must have page numbers, e.g., using Latex command `\pagestyle{plain}`.

All submissions will be blind-refereed and thus must be anonymous, with no author names, affiliations, acknowledgments, or obvious references (however, submissions may already be uploaded to preprint servers such as the IACR eprint or arXiv.org). Submissions should begin with a title, a short abstract, and a list of keywords, followed by an introduction, a main body, an appendix (if any), and references, within 30 pages. The introduction should summarize the contributions of the paper at a level understandable for a non-expert reader. 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.

Optionally, if an author desires, a clearly-marked Supplementary Material can be appended to the submission. The Supplementary Material has no prescribed form or page limit and might be used, for instance, to provide background definitions, program code, additional experimental data, etc. The IACR encourages authors to include in their Supplementary Material responses to reviews from previous IACR events. Alternatively, the auxiliary supporting material can be submitted as a separate file from the submission. The reviewers are not required to read the auxiliary supporting material and submissions should be intelligible without it. The final published version of an accepted paper is expected to closely match the submitted 30 pages.

Submissions must be submitted electronically in PDF format. A detailed description of the electronic submission procedure and a submission link will be available on the ASIACRYPT 2022 website.

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

For papers that are accepted, the length of the proceedings version will be at most 30 pages using Springer's standard fonts, font sizes, and margins. The proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science series and will be available at the conference. Authors of accepted papers must complete the IACR copyright assignment form available at http://www.iacr.org/docs/copyright_form.pdf for their work to be published in the proceedings. Moreover, authors of accepted papers must guarantee that their paper will be presented at the conference and agree that the presentations will be video recorded during the event. The camera-ready version of the accepted articles will be automatically uploaded to the IACR ePrint server (https://eprint.iacr.org/).

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 with published proceedings. Accepted submissions may not appear in any other conference or workshop with published 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/irregular.pdf.

Program committee members are permitted to submit either one single-author paper or at most two co-authored papers.

The Program Committee may choose to bestow a best paper award.

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/). In particular, the authors of each submission are asked during the submission process 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 of 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.

Schedule

ASIACRYPT 2022 will operate a two-round review system with rebuttal phase. In the first round, the program committee selects a subset of submissions for further consideration in the second round, and the authors receive the first round notification with review comments. The authors of the selected submissions are invited to submit a text-based rebuttal letter to the review comments. In the second round, the program committee further reviews the selected submissions by taking into account their rebuttal letter, and makes the final decision of acceptance or rejection. The submissions that have not been selected during the first round of reviews may be submitted in other conferences after the first round notification date. The schedule is as follows:

Submission deadline	May 27, 2022, 11:59 am UTC (noon)
First round notification	July 20, 2022
Rebuttals due	July 26, 2022
Final notification	August 25, 2022
Camera-ready version	September 20, 2022
Conference	December 5–9, 2022

Conference Information and Stipends

The primary source of information is the conference website. Students whose papers have been accepted and who present their talks at the conference will have their registration waived. A limited number of stipends are available to those unable to obtain funding to attend the conference. Students, whose papers are accepted and who will present the paper themselves, are encouraged to apply if such assistance is needed. Requests for stipends should be sent to the general chair.

Program Committee

Divesh Aggarwal	*NUS, Singapore*
Shweta Agrawal(Co-Chair)	*Indian Institute of Technology Madras, India*
Adi Akavia	*University of Haifa, Israel*
Martin Albrecht	*Royal Holloway, University of London, UK*
Ghada Almashaqbeh	*University of Connecticut, USA*
Benny Applebaum	*Tel Aviv University, Israel*
Lejla Batina	*Radboud University, The Netherlands, Netherlands*
Carsten Baum	*Aarhus Univ, Denmark*
Sonia Belaïd	*CryptoExperts, France*
Mihir Bellare	*University of California, San Diego, USA*
Andrej Bogdanov	*Chinese University of Hong Kong, Hong Kong*
Christina Boura	*Université de Versailles, France*
Ran Canetti	*Boston University, USA*
Yilei Chen	*Tsinghua University, China*
Jie Chen	*East China Normal University, China*
Jung Hee Cheon	*Seoul National University, Korea*
Ilaria Chillotti	*Zama, France*
Michele Ciampi	*The University of Edinburgh, UK*
Craig Costello	*Microsoft Research, USA*
Itai Dinur	*Ben-Gurion University, Israel*
Nico Döttling	*Helmholtz Center for Information Security (CISPA), Germany*
Maria Eichlseder	*Graz University of Technology, Austria*
Saba Eskandarian	*University of North Carolina at Chapel Hill, USA*
Marc Fischlin	*TU Darmstadt, Germany*
Pierre-Alain Fouque	*Rennes University and Institut Universitaire de France, France*
Steven Galbraith	*University of Auckland, New Zealand*
Chaya Ganesh	*Indian Institute of Science, India*
Juan Garay	*Texas A&M University, USA*
Sanjam Garg	*University of California, Berkeley and NTT Research, USA*
Daniel Genkin	*Georgia Tech, USA*
Siyao Guo	*New York University Shanghai, China*
Jian Guo	*Nanyang Technological University, Singapore*
Mohammad Hajiabadi	*University of Waterloo, Canada*
Mike Hamburg	*Rambus Inc, USA*
David Heath	*Georgia Institute of Technology, USA*
Viet Tung Hoang	*Florida State University, USA*
Xinyi Huang	*Fujian Normal University, China*
Takanori Isobe	*University of Hyogo, Japan*
Tetsu Iwata	*Nagoya University, Japan*
Khoongming Khoo	*DSO National Laboratories, Singapore*
Elena Kirshanova	*I.Kant Baltic Federal University, Russia*
Ilan Komargodski	*Hebrew University of Jerusalem and NTT Research, Israel*
Gregor Leander	*Ruhr-Universität Bochum, Germany*
Dongdai Lin(Co-Chair)	*Institute of Information Engineering, Chinese Academy of Sciences, China*
Qipeng Liu	*Simons Institute for the Theory of Computing, USA*
Tianren Liu	*Peking University, China*
Shengli Liu	*Shanghai Jiao Tong University, China*

Zhe Liu	*Nanjing University of Aeronautics and Astronautics, China*
Hemanta Maji	*Purdue University, USA*
Giulio Malavolta	*Max Planck Institute, Germany*
Bart Mennink	*Radboud University Nijmegen, the Netherlands*
Tal Moran	*Reichman University , Israel*
Pratyay Mukherjee	*Swirlds/Hedera, USA*
Omkant Pandey	*Stony Brook University, USA*
Anat Paskin-Cherniavsky	*Ariel university, Israel*
Alain Passelègue	*INRIA and ENS de Lyon, France*
Svetla Petkova-Nikova	*KU Leuven, Belgium*
Duong Hieu Phan	*Télécom Paris, France*
Cécile Pierrot	*French National Institute for Computer Science Research INRIA, France*
Silas Richelson	*UC Riverside, USA*
Yu Sasaki	*NTT Corporation, Japan*
Tobias Schneider	*NXP Semiconductors, Austria, Austria*
Dominique Schröder	*Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany*
abhi shelat	*Northeastern, USA*
Mark Simkin	*Ethereum Foundation, USA*
Ling Song	*Jinan University, Guangzhou, China*
Fang Song	*Portland State University, USA*
Pratik Soni	*Carnegie Mellon University, USA*
Akshayaram Srinivasan	*Tata Institute of Fundamental Research, India*
Damien Stehlé	*ENS de Lyon, France*
Ron Steinfeld	*Monash University, Australia*
Qiang Tang	*University of Sydney, Australia*
Yiannis Tselekounis	*Carnegie Mellon University, USA*
Meiqin Wang	*Shandong University, China*
Xiaoyun Wang	*Institute for Advanced Study, Tsinghua University, China*
David Wu	*UT Austin, USA*
Wenling Wu	*Chinese Academy of Sciences, China*
Shota Yamada	*AIST, Japan*
Takashi Yamakawa	*NTT Corporation, Japan*
Jiang Zhang	*State Key Laboratory of Cryptology, China*

Contact Information

Kai-Min Chung
General Co-Chair
Academia Sinica, Taiwan
`asiacrypt2022@iacr.org`

Bo-Yin Yang
General Co-Chair
Academia Sinica, Taiwan
`asiacrypt2022@iacr.org`

Shweta Agrawal
Program Co-Chair
Indian Institute of Technology Madras, India
`asiacrypt2022programchairs@iacr.org`

Dongdai Lin
Program Co-Chair
Institute of Information Engineering, Chinese Academy of Sciences, China
`asiacrypt2022programchairs@iacr.org`

Recommended Submission Style

Electronic submissions to ASIACRYPT 2022 must be in Portable Document Format (PDF) and follow the standard LNCS guidelines. The submission should preferably use Type 1 fonts (rather than Type 3 fonts which usually look fuzzy and ugly when viewed on screen).

The following procedure is recommended for generating submissions.

Preparing the LaTeX file. To follow the standard LNCS guidelines, you obtain the `llncs` package and use the following line at the beginning of your LaTeX file:

```
\documentclass{llncs}
```

You should not use any other command to set the margin and/or change the font. This LaTeX style will be used for the preproceedings.

Generating PDF file with `pdflatex`. After using the above declaration, assuming that your paper is stored in the file `paper.tex`, it suffices to type the command:

```
$ pdflatex paper
```

This generates a file `paper.pdf` ready for submission. There are other, more complex, procedures to generate such PDF files. These alternative procedures are not recommended. If, for some reason, an alternative procedure is used, the resulting PDF file should be verified using the following commands:

```
$ pdfinfo paper.pdf
$ pdffonts paper.pdf
```

These two commands respectively print general information (including paper size) and font information.

Including graphics. To insert graphics into your PDF file, there are two different options:

➢ Generate the graphics using a text description within LaTeX.
➢ Include an externally generated graphics file.

➢ For the first option, authors should consider the PGF package. It can be used by including the following line in the LaTeX file:

```
\usepackage{pgf}
```

➢ To use externally generated graphics, a convenient method relies on the following package:

```
\usepackage{graphicx,color}
```

With this package, a PDF file `drawing.pdf` can be included using:

```
\includegraphics{drawing}
```

Authors should make sure that their externally generated graphics PDF files have a correct bounding box specification.

A set of various cryptography related graphics source codes can be found on the IACR website: `https://www.iacr.org/authors/tikz/`