ASIACRYPT 2024
Call for Papers

December 9–13, 2024, Kolkata, India
`https://asiacrypt.iacr.org/2024/`

Submission deadline	May 26, 2024, 11:59 am UTC (noon)
First round notification	July 23, 2024
Rebuttals due	July 28, 2024
Final notification	August 25, 2024
Camera-ready version	September 20, 2024
Conference	December 9–13, 2024

ASIACRYPT 2024, the 30th Annual International Conference on the Theory and Applications of Cryptology and Information Security, will take place in Kolkata, India on December 9-13, 2024. 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 28 pages excluding the references and 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. 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 version.

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 2024 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 including the references 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, or at most three co-authored papers all with students.

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 2024 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 26, 2024, 11:59 am UTC (noon)
First round notification	July 23, 2024
Rebuttals due	July 28, 2024
Final notification	August 25, 2024
Camera-ready version	September 20, 2024
Conference	December 9–13, 2024

Artifacts

To encourage open and reproducible research, authors of accepted papers will be invited to submit artifacts associated with their papers, such as software or datasets, for review. The artifact review will be a collaborative process between authors and the artifact review committee. The goal of the process is not just to evaluate artifacts, but also to improve them for reproduction and reusability by the scientific community. Artifacts that pass successfully through the artifact review process will be archived on the IACR's artifact archive at artifacts.iacr.org. Please see the detailed call for artifacts (TBA).

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 co-chairs.

Program Committee

TBA

Area Chairs

Siyao Guo	Information-Theoretic and Complexity-Theoretic Cryptography
Bo-Yin Yang	Efficient and Secure Implementations
Goichiro Hanaoka	Public-Key Cryptography Algorithms and Protocols
Arpita Patra	Multi-Party Computation and Zero-Knowledge
Prabhanjan Ananth	Public Key Primitives with Advanced Functionalities
Tetsu Iwata	Symmetric-Key Cryptology

Program Co-Chairs

Kai-Min Chung

Academia Sinica, Taiwan

Yu Sasaki

NTT Social Informatics Laboratories, Japan
National Institute of Standards and Technology,
associate, US

asiacrypt2024programchairs@iacr.org

General Co-Chair

Bimal Roy

Secretary, Cryptology Research Society of India.
Principal Advisor, TCG-CREST, Kolkata.

Recommended Submission Style

Electronic submissions to ASIACRYPT 2024 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/