Red dates are tentative!

Asiacrypt 2025

Call for Papers (draft)

December ~~7–11~~ 8 - 12, 2025, Melbourne, Australia

`https://asiacrypt.iacr.org/2025/`

Submission Deadline	May 16, 12:00 GMT
First Round Notification	July 13
Rebuttals Due	July 18
End of Interactive Rebuttals	July 25
Final Notification	August 10
Camera-Ready Version	September 10

Asiacrypt 2025 is organized by the International Association for Cryptologic Research (IACR) in Melbourne from Dec. ~~7–11~~ 8-12, run by General Chair Prof. **Joseph Liu**. The proceedings will be published by Springer in the Lecture Notes in Computer Science (LNCS) series. We solicit all original research papers on all aspects of cryptology for submission.

As a general IACR conference, we would like to be as inclusive as possible; in particular, a topic for any IACR (area) conference is a topic for Asiacrypt, and PC members are no longer allowed to issue reviews such as "This topic is more suitable for [area conference]".

Instructions for Authors

Submissions must be at most 28 pages excluding 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 `https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines`. It is strongly encouraged that submissions are processed in LaTeX. All submissions must have page numbers, e.g., using LaTeXcommand \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, **appendices (if any), then 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. Except in exceptional cases, papers are likely to be rejected if the results cannot 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, program code, computer proofs, experimental data, etc.; to be considered the Best Practical Paper (see below)

one should include runnable programs in the Supplementary Material.

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 only asked to read the auxiliary supporting material insofar as past reviews are addressed, 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 2025 website.

For papers that are accepted, the limit of the proceedings version is by default 30 pages excluding 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 paper, or at most two co-authored papers one of which must include a student co-author, or at most three co-authored papers each including at least one **supervised** student(s).

Submissions not meeting these guidelines risk rejection without consideration on 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, acting on all answers of questions issued as pertinent to the decision. The PC chairs make the final decision of acceptance or rejection in consultation with the Area Chairs and the reviewers. Submissions that have not been selected during the first round of reviews may be resubmitted in other conferences after the first round notification date.

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). The Best Practical Paper must have an accepted artifact.
- With comparable merit, priority will be given to papers with machine-verified proofs.

Stipends and Conference Information

Students whose papers have been accepted, who will present their talks at the conference, and contact the General Chair in a timely fashion will have their registration waived. The primary source of information is the conference website, however, 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, or **from groups who are underrepresented at Asiacrypt at least in the last decade** are especially encouraged to apply. Requests for stipends should go to the General Chair.

The Program Chairs may in consultation with the PC choose to bestow two best (theory and practical) paper awards, and a best early-career paper award.

Program Co-Chairs

- **Goichiro Hanaoka**, AIST, JP
- **Bo-Yin Yang**, Academia Sinica, TW

Area Chairs

ADV Advanced Functionalities not FHE related: **Feng-Hao Liu**, WA State U., US

ESI Efficient and Secure Implementations (CHES): **Naofumi Homma**, Tohoku U., JP

FHE Fully Homomorphic Encryption: **Damien Stehlé**, CryptoLab, FR

FUN Fundamental (Complexity theory incl quantum): **Chris Brzuska**, Aalto U., FI

ITC Information Theoretic Crypto: **Manoj M. Prabhakaran**, IIT Bombay, IN

MATH Higher mathematics in cryptography: **Steven Galbraith**, U. of Auckland, NZ

MPC Multi-Party Computation: **Takahiro Matsuda**, AIST, JP

PQC Post-Quantum Crypto (not FHE/higher maths): **Keita Xagawa**, TII, AE

RWC Real World Crypto: **Sherman S. M. Chow**, Chinese U. of HK, HK

SYM Symmetric Crypto (FSE): **Meiqin Wang**, Shandong U,, CN

Conflicts of Interest

Authors (as well as 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 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 on merits.**

Recommended Submission Style

Electronic submissions to Asiacrypt 2025 must be in Portable Document Format (PDF) and follow the standard LNCS guidelines, preferably using Type 1 and not Type 3 fonts. Before preparing your LaTeX file, obtain the `llncs` from `https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines`, and use `\documentclass{llncs}` at the beginning of your LaTeX file. **You should not use any other command to set the margin and/or change the font.** This LaTeXstyle will be used for the proceedings. Assuming that your paper is stored in the file paper.tex, it should suffice to type the command: `$ pdflatex paper` or `$ latexmk -pdf paper` to generate a file `paper.pdf` ready for submission. If, for some reason, an alternative procedure to generate such PDF files is used, prepare a clearly-marked compilation script and the resulting PDF file should be verified using the following commands:

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

These commands print general information (including paper size) and font information. To insert graphics into your PDF file, there are two different options: Generate the graphics using a text description within LaTeX, or include an externally generated graphics file. For the first option, authors should consider the PGF package. It can be used by including the following LaTeXcommand `\usepackage{pgf}`. To use externally generated graphics, a convenient method relies on the following packages: `\usepackage{graphicx,color}` where 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/`