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 will take place in Kolkata, India on December 9-13, 2024. Asiacrypt 2024 is organized by the International Association for Cryptologic Research (IACR). The proceedings will be published by Springer in the LNCS series. Original research papers on all aspects of cryptology are solicited 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.

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 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, India.

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 Committee

Bar Alon	Ben-Gurion University
Akshima	NYU Shanghai
Elena Andreeva	TU Wien
Nuttapong Attrapadung	AIST
Subhadeep Banik	University of Lugano
Zhenzhen Bao	Tsinghua University
James Bartusek	University of California, Berkeley
Hanno Becker	Amazon Web Services
Sonia Belaïd	CryptoExperts, France
Ward Beullens	IBM Research Europe
Andrej Bogdanov	University of Ottawa
Pedro Branco	Max-Planck Institute for Security and Privacy
Gaëtan Cassiers	UCLouvain
Avik Chakraborti	IAI, TCG CREST, Kolkata
Nishanth Chandran	Microsoft Research India
Jie Chen	East China Normal University, CN
Yu Long Chen	COSIC, KU Leuven and National Institute of Standards and Technology
Mahdi Cheraghchi	University of Michigan, Ann Arbor
Nai-Hui Chia	Rice University
Wonseok Choi	Purdue University
Tung Chou	Academia Sinica, Taiwan
Arka Rai Choudhuri	NTT Research
Sherman S. M. Chow	Chinese University of Hong Kong, Hong Kong
Chitchanok Chuengsatiansup	The University of Melbourne, Australia
Michele Ciampi	University of Edinburgh
Valerio Cini	NTT Research
Elizabeth Crites	Web3 Foundation
Chevalier Céline	CRED, Université Paris-Panthéon-Assas, and DIENS, Paris
Avijit Dutta	Institute for Advancing Intelligence, TCG CREST
Nico Döttling	CISPA Helmholtz Center
Daniel Escudero	JP Morgan AlgoCRYPT CoE and JP Morgan AI Research
Thomas Espitau	PQShield
Jun Furukawa	NEC Corporation
Rosario Gennaro	City College - CUNY
Junqing Gong	East China Normal University
Rishab Goyal	University of Wisconsin-Madison
Julia Hesse	IBM Research
Akinori Hosoyamada	NTT Social Informatics Laboratories
Michael Hutter	PQShield
Takanori Isobe	University of Hyogo, Japan
Joseph Jaeger	Georgia Institute of Technology
Matthias J. Kannwischer	Chelpis Quantum Tech
Bhavana Kanukurthi	Indian Institute of Science, India
Shuichi Katsumata	PQShield and AIST
Jonathan Katz	Google and University of Maryland
Mustafa Khairallah	Lund University
Fuyuki Kitagawa	NTT Social Informatics Laboratories
Karen Klein	ETH Zurich

Mukul Kulkarni	Technology Innovation Institute, United Arab Emirates
Po-Chun Kuo	BTQ Technologies Corp.
Jooyoung Lee	KAIST, Korea
Wei-Kai Lin	University of Virginia
Shengli Liu	Shanghai Jiao Tong University, China
Qipeng Liu	UC San Diego
Jiahui Liu	Massachusetts Institute of Technology
Feng-Hao Liu	Washington State University
Chen-Da Liu-Zhang	Lucerne University of Applied Sciences and Arts & Web3 Foundation
Yun Lu	University of Victoria
Ji Luo	University of Washington
Silvia Mella	Radboud University, Netherlands
Peihan Miao	Brown University
Daniele Micciancio	University of California, San Diego
Yusuke Naito	Mitsubishi Electric Corporation
Khoa Nguyen	University of Wollongong, Australia
Ruben Niederhagen	Academia Sinica, Taiwan, and University of Southern Denmark, Denmark
Maciej Obremski	NUS
Miyako Ohkubo	NICT
Eran Omri	Ariel University
Jiaxin Pan	University of Kassel, Germany
Anat Paskin-Cherniavsky	Ariel university
Goutam Paul	Indian Statistical Institute
Chris Peikert	University of Michigan
Christophe Petit	University of Birmingham and Université libre de Bruxelles
Rachel Player	Royal Holloway, University of London
Thomas Prest	PQShield
Shahram Rasoolzadeh	Ruhr University Bochum
Alexander Russell	University of Connecticut
Santanu Sarkar	Indian Institute of Technology Madras
Sven Schäge	Eindhoven University of Technology
Gregor Seiler	IBM Research Europe
Sruthi Sekar	Indian Institute of Technology, Bombay
Yaobin Shen	Xiamen University
Danping Shi	Institute of Information Engineering, Chinese Academy of Sciences
Yifan Song	Tsinghua University
Katerina Sotiraki	Yale University
Akshayaram Srinivasan	University of Toronto
Marc Stöttinger	RheinMain University of Applied Sciences
Akira Takahashi	J.P.Morgan AI Research and AlgoCRYPT CoE
Qiang Tang	The University of Sydney
Aishwarya Thiruvengadam	Indian Institute of Technology Madras
Emmanuel Thomé	Inria Nancy, France
Junichi Tomida	NTT Social Informatics Laboratories
Monika Trimoska	Eindhoven University of Technology
Meiqin Wang	Shandong University , China
Qingju Wang	Telecom Paris, Institut Polytechnique de Paris
Huaxiong Wang	Nanyang Technological University, Singapore
David Wu	UT Austin
Keita Xagawa	Technology Innovation Institute
Chaoping Xing	Shanghai Jiao Tong University
Shiyuan Xu	The University of Hong Kong

Anshu Yadav	IST Austria
Shota Yamada	AIST
Yu Yu	Shanghai Jiao Tong University
Mark Zhandry	NTT Research
Hong-Sheng Zhou	Virginia Commonwealth University

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/