ASIACRYPT 2023
Call for Papers

December 4–8, 2023, Guangzhou, China
`https://asiacrypt.iacr.org/2023/`

Submission deadline	May 26, 2023, 11:59 am UTC (noon)
First round notification	July 20, 2023
Rebuttals due	August 1, 2023
Final notification	August 25, 2023
Camera-ready version	September 20, 2023
Conference	December 4–8, 2023

ASIACRYPT 2023, the 29th Annual International Conference on the Theory and Applications of Cryptology and Information Security, will take place in Guangzhou, China on December 4-8, 2023. 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 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 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 2023 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 31 pages excluding 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 2023 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, 2023, 11:59 am UTC (noon)
First round notification	July 20, 2023
Rebuttals due	August 1, 2023
Final notification	August 25, 2023
Camera-ready version	September 20, 2023

Conference	December 4–8, 2023

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

Behzad Abdolmaleki	University of Sheffield, UK
Masayuki Abe	NTT Social Informatics Laboratories, Japan
Miguel Ambrona	Nomadic Labs, France
Daniel Apon	MITRE Labs, USA
Shi Bai	Florida Atlantic University, USA
Gustavo Banegas	Qualcomm, France
Zhenzhen Bao	Tsinghua University, China
Andrea Basso	University of Bristol, UK
Ward Beullens	IBM Research Europe, Switzerland
Katharina Boudgoust	Aarhus University, Denmark
Matteo Campanelli	Protocol Labs, USA
Ignacio Cascudo	IMDEA Software Institute, Spain
Wouter Castryck	imec-COSIC, KU Leuven, Belgium
Jie Chen	East China Normal University, China
Yilei Chen	Tsinghua University, China
Jung Hee Cheon	Seoul National University and Cryptolab, Korea
Sherman S. M. Chow	Chinese University of Hong Kong, Hong Kong, China
Kai-Min Chung	Academia Sinica, Taiwan
Michele Ciampi	The University of Edinburgh, UK
Bernardo David	IT University of Copenhagen, Denmark
Yi Deng	Institute of Information Engineering, Chinese Academy of Sciences, China
Patrick Derbez	University of Rennes, France
Xiaoyang Dong	Tsinghua University, China
Nico Döttling	Helmholtz Center for Information Security, Germany
Rafael Dowsley	Monash University, Australia
Maria Eichlseder	Graz University of Technology, Austria
Muhammed F. Esgin	Monash University, Australia
Thomas Espitau	PQShield, France
Jun Furukawa	NEC Corporation, Japan
Aron Gohr	Independent Researcher, New Zealand
Junqing Gong	ECNU, China
Lorenzo Grassi	Ruhr University Bochum, Germany
Tim Güneysu	Ruhr University Bochum, Germany
Chun Guo	Shandong University, China
Siyao Guo	NYU Shanghai, China

Fuchun Guo	University of Wollongong, Australia
Mohammad Hajiabadi	University of Waterloo, Canada
Lucjan Hanzlik	CISPA Helmholtz Center for Information Security, Germany
Xiaolu Hou	Slovak University of Technology, Slovakia
Yuncong Hu	Shanghai Jiao Tong University, China
Xinyi Huang	Hong Kong University of Science and Technology (Guangzhou), China
Tibor Jager	University of Wuppertal, Germany
Elena Kirshanova	Technology Innovation Institute, Abu Dhabi, UAE
Eyal Kushilevitz	Technion, Israel
Russell W. F. Lai	Aalto University, Finland
Tanja Lange	Eindhoven University of Technology, Netherlands
Hyung Tae Lee	Chung-Ang University, Korea
Eik List	Nanyang Technological University, Singapore
Meicheng Liu	Institute of Information Engineering, Chinese Academy of Sciences, China
Guozhen Liu	Nanyang Technological University, Singapore
Fukang Liu	Tokyo Institute of Technology, Japan
Shengli Liu	Shanghai Jiao Tong University, China
Feng-Hao Liu	Florida Atlantic University, USA
Hemanta K. Maji	Purdue University, USA
Takahiro Matsuda	AIST, Japan
Christian Matt	Concordium, Switzerland
Pierrick Méaux	University of Luxembourg , Luxembourg
Tomoyuki Morimae	Kyoto University, Japan
Mridul Nandi	Indian Statistical Institute, Kolkata, India
María Naya-Plasencia	Inria, France
Khoa Nguyen	University of Wollongong, Australia
Ryo Nishimaki	NTT Social Informatics Laboratories, Japan
Anca Nitulescu	Protocol Labs, France
Ariel Nof	Bar Ilan University, Israel
Adam O’Neill	UMass Amherst, USA
Emmanuela Orsini	Bocconi University, Italy
Morten Øygarden	Simula UiB, Norway
Sikhar Patranabis	IBM Research India, India
Alice Pellet-Mary	CNRS and University of Bordeaux, France
Edoardo Persichetti	Florida Atlantic University and Sapienza University, USA
Duong Hieu Phan	Telecom Paris, Institut Polytechnique de Paris, France
Josef Pieprzyk	CSIRO, Data61, Australia and IPI PAS, Poland
Axel Y. Poschmann	PQShield, UK
Thomas Prest	PQShield, France
Adeline Roux-Langlois	CNRS, GREYC, France
Amin Sakzad	Monash University, Australia
Yu Sasaki	NTT Social Informatics Laboratories, Japan
Jae Hong Seo	Hanyang University, Korea
Yaobin Shen	UCLouvain, Belgium
Danping Shi	Institute of Information Engineering, Chinese Academy of Sciences, China
Damien Stehlé	CryptoLab, France
Bing Sun	National University of Defense Technology, China
Shi-Feng Sun	Shanghai Jiao Tong University, China
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Qiang Tang	The University of Sydney, Australia
Vanessa Teague	Thinking Cybersecurity Pty Ltd and the Australian National University, Australia
Jean-Pierre Tillich	Inria de Paris, France

Yosuke Todo	NTT Social Informatics Laboratories, Japan
Alexandre Wallet	Université de Rennes, Inria, IRISA, France
Meiqin Wang	Shandong University, China
Qingju Wang	Télécom Paris, France
Yongge Wang	UNC Charlotte , USA
Yuyu Wang	University of Electronic Science and Technology of China, China
Benjamin Wesolowski	CNRS and ENS de Lyon, France
Shuang Wu	Huawei International, Singapore
Keita Xagawa	Technology Innovation Institute, UAE
Chaoping Xing	Shanghai Jiao Tong University, China
Jun Xu	Institute of Information Engineering, Chinese Academy of Sciences, China
Takashi Yamakawa	NTT Social Informatics Laboratories, Japan
Kang Yang	State Key Laboratory of Cryptology, China
Yu Yu	Shanghai Jiao Tong University, China
Yang Yu	Tsinghua University, China
Yupeng Zhang	University of Illinois Urbana-Champaign and Texas A&M University, USA
Liangfeng Zhang	ShanghaiTech University, China
Raymond K. Zhao	CSIRO's Data61, Australia
Hong-Sheng Zhou	Virginia Commonwealth University, USA

Area Chairs

Kai-Min Chung	Information-Theoretic and Complexity-Theoretic Cryptography
Tanja Lange	Efficient and Secure Implementations
Shengli Liu	Public-Key Cryptography Algorithms and Protocols
Khoa Nguyen	Multi-Party Computation and Zero-Knowledge
Duong Hieu Phan	Public Key Primitives with Advanced Functionalities
Yu Sasaki	Symmetric-Key Cryptology

Program Co-Chairs

Jian Guo	Ron Steinfeld
Nanyang Technological University, Singapore	Monash University, Australia

asiacrypt2023programchairs@iacr.org

General Co-Chairs

Jian Weng	Fangguo Zhang
Jinan University, China	Sun Yat-sen University, China

asiacrypt2023@iacr.org

Recommended Submission Style

Electronic submissions to ASIACRYPT 2023 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/