ASIACRYPT 2020
Call for Papers

December 6–10, 2020, Daejeon, Korea
`http://asiacrypt.iacr.org/2020/`

Submission deadline	May 22, 2020 (05:00 a.m. UTC)
First round notification	July 12, 2020
Rebuttals due	July 18, 2020
Final notification	August 16, 2020
Camera-ready version	September 13, 2020
Conference	December 6–10, 2020

ASIACRYPT 2020, the 26th Annual International Conference on the Theory and Applications of Cryptology and Information Security, will take place at the Daejeon Convention Center, Daejeon, Korea on December 6–10, 2020. The conference is organized by the International Association for Cryptologic Research (IACR).

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 eprint or arxiv). 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 2020 website at a later date.

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 that has proceedings. Accepted submissions may not appear in any other conference or workshop that has 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`.

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.

Program committee members are permitted to submit either one single-author paper or at most two co-authored papers. Papers submitted by PC members are reviewed by at least 5 reviewers.

The Program Committee may select a paper for the best paper award.

Schedule

ASIACRYPT 2020 will operate a two-round review system with rebuttal phase. In the first round, the program committee selects the submissions which are considered of value for proceeding to 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 22, 2020 (05:00 a.m. UTC)
First round notification	July 12, 2020
Rebuttals due	July 18, 2020
Final notification	August 16, 2020
Camera-ready version	September 13, 2020
Conference	December 6–10, 2020

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

Shweta Agrawal	*IIT Madras, India*
Gorjan Alagic	*University of Maryland, USA*
Shi Bai	*Florida Atlantic University, USA*
Zhenzhen Bao	*Nanyang Technological University, Singapore*
Paulo Barreto	*UW Tacoma, USA*
Lejla Batina	*Radboud University, Netherlands*
Amos Beimel	*Ben-Gurion University, Israel*
Sonia Belaïd	*CryptoExperts, France*
Olivier Blazy	*University of Limoges, France*
Jie Chen	*East China Normal University, China*
Yilei Chen	*Visa Research, USA*
Chen-Mou Cheng	*Osaka University, Japan*
Jun Furukawa	*NEC Israel Research Center, Israel*
David Galindo	*University of Birmingham and Fetch AI, UK*
Jian Guo	*Nanyang Technological University, Singapore*
Swee-Huay Heng	*Multimedia University, Malaysia*
Xinyi Huang	*Fujian Normal University, China*
Andreas Hülsing	*TU Eindhoven, Netherlands*
Takanori Isobe	*University of Hyogo, Japan*
David Jao	*University of Waterloo and evolutionQ, Inc. Canada*
Jérémy Jean	*ANSSI, France*
Zhengfeng Ji	*University of Technology Sydney, Australia*
Hyung Tae Lee	*Jeonbuk National University, Korea*
Jooyoung Lee	*KAIST, Korea*
Benoit Libert	*CNRS and ENS de Lyon, France*
Dongdai Lin	*Chinese Academy of Sciences, China*
Helger Lipmaa	*University of Tartu, Estonia ; Simula UiB, Norway*
Feng-Hao Liu	*Florida Atlantic University, USA*
Giorgia Azzurra Marson	*University of Bern, Switzerland/NEC Laboratories Europe, Germany*
Daniel Masny	*Visa Research, USA*
Takahiro Matsuda	*AIST, Japan*
Brice Minaud	*Inria and ENS, France*
Shiho Moriai	*NICT, Japan*
Kartik Nayak	*Duke University/VMware Research, USA*
Khoa Nguyen	*Nanyang Technological University, Singapore*
Svetla Nikova	*KU Leuven, Belgium*
Carles Padró	*UPC, Spain*
Jiaxin Pan	*NTNU, Norway*
Arpita Patra	*Indian Institute of Science, India*
Thomas Peters	*UCL, Belgium*
Duong Hieu Phan	*University of Limoges, France*
Raphael C.-W. Phan	*Monash University, Malaysia*
Josef Pieprzyk	*CSIRO, Australia*
Carla Ràfols	*Universitat Pompeu Fabra, Spain*
Ling Ren	*VMware Research/University of Illinois, Urbana-Champaign, USA*
Rei Safavi-Naini	*University of Calgary, Canada*
Yu Sasaki	*NTT laboratories, Japan*
Jae Hong Seo	*Hanyang University, Korea*
Ron Steinfeld	*Monash University, Australia*
Willy Susilo	*University of Wollongong, Australia*
Qiang Tang	*New Jersey Institute of Technology, USA*
Mehdi Tibouchi	*NTT laboratories, Japan*

Huaxiong Wang	*Nanyang Technological University, Singapore*
Xiaoyun Wang	*Tsinghua University, China*
Yongge Wang	*University of North Carolina at Charlotte, USA*
Chaoping Xing	*Shanghai Jiaotong University, China and NTU, Singapore*
Yu Yu	*Shanghai Jiaotong University, China*
Mark Zhandry	*Princeton University & NTT Research, USA*

Contact Information

Kwangjo Kim
General Chair
KAIST, Korea
`asiacrypt2020@iacr.org`

Shiho Moriai
Program Co-chair
NICT, Japan
`asiacrypt2020programchairs@iacr.org`

Huaxiong Wang
Program Co-chair
Nanyang Technological University, Singapore
`asiacrypt2020programchairs@iacr.org`

Recommended Submission Style

Electronic submissions to ASIACRYPT 2020 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/`