ASIACRYPT 2017
Call for Papers

December 3–7, 2017, Hong-Kong, China
`http://asiacrypt.iacr.org/2017/`

Submission deadline	May 19, 2017 (02:00 a.m. UTC)
First round notification	July 9, 2017
Rebuttals due	July 14, 2017
Final notification	August 13, 2017
Camera-ready version	September 7, 2017
Conference	December 3–7, 2017

ASIACRYPT 2017, the 23rd Annual International Conference on the Theory and Applications of Cryptology and Information Security, will take place in The University of Hong Kong, China, on December 3-7, 2017. 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. 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 the level understandable for a non-expert reader.

Optionally, if an author desires, a clearly-marked auxiliary supporting material can be appended to the submission. The auxiliary supporting material has no prescribed form or page limit and might be used, for instance, to provide program code, additional experimental data. 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 2017 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`.

Articles will not be reviewed by reviewers who have a conflict of interest with at least one author of the submission. As the IACR does not impose a detailed policy on conflicts of interest, the Program co-Chairs will decide on what constitutes a conflict according to high standards in terms of scientific integrity (at least colleagues from the same research group, people in a current or very recent student-advisor relationship, close friends, and family members have a conflict).

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

Schedule

ASIACRYPT 2017 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 19, 2017 (02:00 a.m. UTC)
First round notification	July 9, 2017
Rebuttals due	July 14, 2017
Final notification	August 13, 2017
Camera-ready version	September 7, 2017
Conference	December 3–7, 2017

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*
Céline Blondeau	*Aalto University, Finland*
Joppe W. Bos	*NXP Semiconductors, Belgium*
Chris Brzuska	*TU Hamburg, Germany*

Jie Chen	*East China Normal University, China*
Sherman S.M. Chow	*Chinese University of Hong Kong, Hong Kong SAR, China*
Kai-Min Chung	*Academia Sinica, Taiwan*
Nico Döttling	*University of California, Berkeley, USA*
Thomas Eisenbarth	*Worcester Polytechnic Institute, USA*
Dario Fiore	*IMDEA Software Institute, Madrid, Spain*
Georg Fuchsbauer	*ENS Paris, France*
Steven Galbraith	*Auckland University, New-Zealand*
Jian Guo	*Nanyang Technological University, Singapore*
Viet Tung Hoang	*Florida State University, USA*
Jérémy Jean	*ANSSI, France*
Jooyoung Lee	*KAIST, Korea*
Dongdai Lin	*Chinese Academy of Sciences, China*
Feng-Hao Liu	*Florida Atlantic University, USA*
Stefan Mangard	*Graz University of Technology, Austria*
Takahiro Matsuda	*AIST, Japan*
Alexander May	*Ruhr University Bochum, Germany*
Bart Mennink	*Radboud University, The Netherlands*
Amir Moradi	*Ruhr University Bochum, Germany*
Pratyay Mukherjee	*Visa Research, USA*
Mridul Nandi	*Indian Statistical Institute, India*
Khoa Nguyen	*Nanyang Technological University, Singapore*
Miyako Ohkubo	*NICT, Japan*
Tatsuaki Okamoto	*NTT laboratories, Japan*
Arpita Patra	*Indian Institute of Science, India*
Bart Preneel	*KU Leuven, Belgium*
Matthieu Rivain	*CryptoExperts, France*
Rei Safavi-Naini	*University of Calgary, Canada*
Yu Sasaki	*NTT Secure Platform Laboratories, Japan*
Peter Schwabe	*Radboud University, The Netherlands*
Fang Song	*Portland State University, USA*
Francois-Xavier Standaert	*UCL, Belgium*
Damien Stehlé	*ENS Lyon, France*
Ron Steinfeld	*Monash University, Australia*
Rainer Steinwandt	*Florida Atlantic University, USA*
Mehdi Tibouchi	*NTT laboratories, Japan*
Dominique Unruh	*University of Tartu, Estonia*
Gilles Van Assche	*STMicroelectronics, Belgium*
Serge Vaudenay	*EPFL, Switzerland*
Ingrid Verbauwhede	*KU Leuven, Belgium*
Ivan Visconti	*University of Salerno, Italy*
Lei Wang	*Shanghai Jiaotong University, China*
Meiqin Wang	*Shandong University, China*
Jiang Zhang	*State Key Laboratory of Cryptology, China*

Contact Information

Duncan Wong
General Co-chair
City University of Hong Kong, China
ac2017@iacr.org

Siu Ming Yiu
General Co-chair
The University of Hong Kong, China
ac2017@iacr.org

Tsuyoshi Takagi
Program Co-chair
University of Tokyo, Japan
ac2017programchairs@iacr.org

Thomas Peyrin
Program Co-chair
Nanyang Technological University, Singapore
ac2017programchairs@iacr.org

Recommended Submission Style

Electronic submissions to ASIACRYPT 2017 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/`