Call For Papers

Indocrypt 2020 is the 21st International Conference on Cryptology in India. Due to the pandemic, Indocrypt 2020 will be a fully virtual conference and will take place during 13th-16th December, 2020. Indocrypt 2020 is part of the Indocrypt series organised under the aegis of Cryptology Research Society of India (CRSI), and this edition is held in cooperation with IACR.

The conference website is accessible at [indocrypt2020.iiitb.ac.in](http://indocrypt2020.iiitb.ac.in).

Original papers on all technical aspects of cryptology are solicited for submission to Indocrypt 2020. We welcome submissions on all aspects of cryptography including but not limited to:

- Foundations
- New primitives
- Cryptanalysis
- Security models
- Implementation aspects
- Protocols
- Applications

Submissions on cryptographic aspects of network security, complexity theory, information theory, coding theory, number theory, and quantum computing will also be considered. In addition, Indocrypt is expanding its scope to include formal methods for cryptographic systems, as detailed below.

New Theme: Formal Methods for Cryptographic Systems

We seek papers on the use of formal techniques in the design, analysis, and implementations of cryptographic constructions, protocols, and applications. We especially encourage papers on improved analysis techniques and on case studies that apply such techniques on real-world cryptographic systems.

Possible topics of interest include, but are not limited to:

- Formal security definitions
- Mechanized cryptographic proofs
- New cryptographic protocol designs
- Symbolic protocol analysis
- Domain specific languages for cryptographic algorithms and systems
- Software security
- Testing and fuzzing for cryptographic software
- Tools for finding side-channel attacks
- Verified side-channel countermeasures
- Verified privacy
- Verified accountability
- Verified fairness
- Formal analysis of cryptographic APIs
Timeline

All deadlines correspond to 23:59:59 Anywhere on Earth (UTC-12).

<table>
<thead>
<tr>
<th>Deadline</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submission Deadline</td>
<td>September 7, 2020</td>
</tr>
<tr>
<td>Notification</td>
<td>October 19, 2020</td>
</tr>
<tr>
<td>Camera Ready Deadline</td>
<td>October 26, 2020</td>
</tr>
</tbody>
</table>

Instructions for Authors

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any journal or any other conference or workshop with formally published proceedings. Authors may also not submit the work to any other journal or conference/workshop with published proceedings until the date of notification. Accepted submissions may not appear in any other conference or workshop that has proceedings. Information about submissions may be shared with programme chairs of other conferences for the purpose of detecting duplication.

Submissions must be processed in \LaTeX and must use the Springer LNCS format with default margins and font. Submissions must be anonymous, with no author names, affiliations, acknowledgements, or obvious references. Each submission must begin with a title, a short abstract, and a list of key words, followed by a main body, appendices (if any), and references. The main body should begin with an introduction that summarizes the contributions of the paper at a level appropriate for a non-specialist reader. The length of the paper, including appendices (if any) and excluding references should not exceed 20 pages when formatted using the Springer LNCS format. Details on the LNCS format can be obtained via [www.springer.de/comp/lncs/authors.html](http://www.springer.de/comp/lncs/authors.html).

All submissions must have page numbers, e.g., using \LaTeX command \pagestyle{plain}. If the authors include appendices, they should be placed after the main body and before the references. Submissions not meeting these requirements risk rejection without consideration of their merits.

Optionally, additional supporting material can be appended to the submission. The additional supporting material should be placed after the references, it should be well-marked, and it has no prescribed form or page limit. Alternatively, the supporting material can be submitted as a separate file. Authors are encouraged to use this space to include proofs, source code, and other information allowing verification of results; unverifiable papers risk rejection. However, committee members will read the additional supporting material at their discretion, so the submission should be intelligible and self-contained without it.

*Submissions not meeting these guidelines risk rejection without consideration of their merits.*

The proceedings will be published by Springer in the Lecture Notes in Computer Science series. The final versions of the accepted papers will have a page limit of 20 pages (including appendices (if any) and excluding references). Thus the submitted paper should represent what the authors expect to finally publish.

All accepted papers must conform to the Springer publishing requirements, and authors will be required to sign the Springer’s LNCS Copyright form when submitting the proceedings version of their paper. By submitting a paper, the authors agree that if the paper is accepted, one of the authors will present the paper at the conference.

Due to the pandemic, Indocrypt 2020 will be a fully virtual conference.

Papers must be submitted electronically in PDF format.

The paper can be submitted at [easychair.org/conferences/?conf=indocrypt2020](http://easychair.org/conferences/?conf=indocrypt2020)

Conflicts Of Interest

The authors of each submission are asked during the submission process to identify all members of the Programme 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.

Contacts

Programme Committee Chairs

| Karthikeyan Bhargavan | Elisabeth Oswald | Manoj Prabhakaran |
| INRIA Paris           | University of Klagenfurt | IIT Bombay |
| France                | Austria            | India       |

General and Organising Chairs

| S. Sadagopan | Vishal Saraswat | Srinivas Vivek |
| IIIT Bangalore | Robert Bosch, Bangalore | IIIT Bangalore |
| General Co-chair | General Co-chair | Organising Chair |

Programme Committee

Shweta Agrawal  
Indian Institute of Technology Madras, IN

Shashank Agrawal  
Western Digital, US

Saikrishna Badrinarayanan  
Visa Research, US

Manuel Barbosa  
HASLab - INESC TEC, PT

Mihir Bellare  
University of California San Diego, US

Davide Bellizia  
Université Catholique de Louvain, BE

Karthikeyan Bhargavan  
INRIA Paris, FR (PC Co-chair)

Begül Bilgin  
KU Leuven, BE

Bruno Blanchet  
INRIA Paris, FR

Chris Brzuska  
Aalto University, FI

Nishanth Chandran  
Microsoft Research, IN

Ran Cohen  
Northeastern University, US

Cas Cremers  
CISPA Helmholtz Center for Information Security in Saarbruecken, DE

Apoorva Deshpande  
Snap Inc., US

Maria Eichlseder  
IAIK TU Graz, AT

Pooya Farshim  
University of York, UK

Chaya Ganesh  
Indian Institute of Science, IN

Deepak Garg  
Max Planck Institute for Software Systems, DE

Vipul Goyal  
Carnegie Mellon University, US

Clémentine Gritti  
University of Canterbury, NZ

Divya Gupta  
Microsoft Research, IN

Carmit Hazay  
Bar-Ilan University, IL

James Howe  
PQShield, UK
Jointly Organised By

![mt-b logo](image1)

BOSCH

With Support From

![CRSI logo](image2)

![IAR logo](image3)

Springer