Announcement and Call for Papers

SPACE 2023: Thirteenth International Conference on Security, Privacy and Applied Cryptographic Engineering

December 14-17, 2023, IIT Roorkee, India

Program Chairs

Francesco Regazzoni, University of Amsterdam and Università della Svizzera Italiana
Sri Parameswaran, University of New South Wales
Bodhisatwa Mazumdar, IIT Indore

General Chair

Debdeep Mukhopadhyay, IIT Kharagpur
Sugata Gangopadhyay, IIT Roorkee

Contact Information

Technical Information

Bodhisatwa Mazumdar
Indian Institute of Technology Indore, Indore
Email: bodhisatwa@iiti.ac.in

General Information

•**Debdeep Mukhopadhyay**
Indian Institute of Technology Kharagpur, Kharagpur
Email: debdeep@cse.iitkgp.ac.in
•**Sugata Gangopadhyay**
Indian Institute of Technology Roorkee, Roorkee
Email: sugata.gangopadhyay@cs.iitr.ac.in

Important Dates

Paper submission deadline: **Sep. 01, 2023**
Notification of Acceptance: **Oct. 15, 2023**
Camera-ready version: **Nov. 1, 2023**
Conference: **Dec. 14-17, 2023**

Overview

International Conference on Security, Privacy and Applied Cryptographic Engineering 2023 (SPACE 2023) is thirteenth in the series of conferences which started in 2011. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. SPACE 2023 will be held at IIT Roorkee, from 14th to 17th December, 2023. The program co-chairs for SPACE 2023 are Francesco Regazzoni (University of Amsterdam), Sri Parameswaran (University of New South Wales) and Bodhisatwa Mazumdar (Indian Institute of Technology Indore, Indore).

Topics

We invite authors to submit previously unpublished original research. Topics include but are not limited to:

Cryptographic Engineering

- Design of cryptographic primitives
- Random Number generators and PUFs
- Cryptographic protocols and implementations
- Security architectures
- Formal methods in Cryptographic Engineering
- Attacks and countermeasures
- Post-quantum Cryptography Implementations
- Cryptographic Software/ Hardware Design
- IP Protection

Security and Privacy

- Security of Cyber-Physical Systems
- AI in Security and Privacy
- Security of AI
- Secure Networking Protocols
- Securing Human-in-the-loop Systems
- Data privacy and Authentication
- Botnets and Malware
- Anonymization Techniques and attacks
- Network Security and Intrusion detection
- Operating Systems Security
- Trustworthy Computing
- Verification and Testing for Security

Side-Channel Analysis and Countermeasures

- Fault Analysis and countermeasures
- Reverse Engineering and Tampering
- Hardware Trojan and counterfeit Detection
- Micro-architectural Attacks
- AI-assisted side-channel attacks
- Cryptanalysis

Paper Submission

All SPACE 2023 submissions must be original and not simultaneously submitted to or published in another journal or conference. SPACE 2023 follows a strict double-blind policy: all submissions must be anonymous, with no author names, affiliations, acknowledgements, or obvious references. Full paper submissions must be written in English, should strictly follow the LNCS format, and should be at most 20 pages (including the bibliography but excluding clearly marked appendices). Submission to SPACE will imply the willingness of at least one of the authors to register and present the paper in the conference. Authors should mention in abstract if a submission should be considered as short paper/work-in-progress. Authors should consult Springer's Instructions for Authors of Proceedings and use either the LaTeX or the Word templates provided on the authors' page for the preparation of their papers. Springer encourages authors to include their ORCIDs in their papers. Springer's proceedings LaTeX templates are also available in Overleaf. In addition, the corresponding author of each paper, acting on behalf of all of the authors of that paper, must complete and sign a Consent-to-Publish form. The corresponding author signing the copyright form should match the corresponding author marked on the paper. Once the files have been sent to Springer, changes relating to the authorship of the papers cannot be made." The appropriate links should be made available to the authors.