The 23rd International Conference on Applied Cryptography and Network Security (ACNS 2025) will be held in Munich, Germany, on 23–26 June 2025. ACNS is an annual conference focusing on current developments that advance the areas of applied cryptography, cyber security (including network and computer security) and privacy. The goal is to present both academic research works and advances on industrial and technical frontiers.

Submissions may focus on the modeling, design, analysis, development, deployment, integration, maintenance performance, and usability of algorithms, protocols, standards, implementations, devices, as well as systems, standing in relation with applied cryptography, cyber security and privacy and advancing or bringing new insights to the state of the art.

Areas of interest for ACNS 2025 (in alphabetical order) include but are not limited to:

- Applied cryptography
- Artificial intelligence for security
- Automated security analysis
- Authentication and biometric security and privacy
- Blockchain security and privacy
- Cloud security and privacy
- Critical infrastructure security and privacy
- Cryptanalysis
- Cryptographic primitives and protocols
- Data protection
- Distributed security and consensus protocols
- Email, app and web security and privacy
- Future Internet security and privacy
- Lightweight cryptography
- Identity management

- Internet fraud and cybercrime
- Internet-of-Things security and privacy
- Malicious code and unsolicited software
- Mobile and wireless security
- Network security protocols
- Post-quantum cryptography
- Privacy and anonymity, privacy-enhancing technologies
- Secure electronic voting
- Security and privacy metrics
- Security and privacy of systems based on ML and AI
- Side-channel analysis and physical attacks
- Systems security and privacy
- Trust management and trustworthy computing in networks or systems
- Usable security and privacy

Besides the main conference, ACNS also seeks workshop proposals. Each satellite workshop will provide a forum to address a specific topic at the forefront of cybersecurity research. Papers accepted at the workshops will have post-proceedings published by Springer in the LNCS series as well.

Important Dates

All deadlines are on the given day, 23:59 AoE (Anywhere on Earth).

First submission deadline:

- Submission: September 9, 2024, 23:59 AoE (Anywhere on Earth)
- Notification: November 11, 2024
- Camera-ready: December 2, 2024

Second submission deadline:

- Submission: January 13, 2025, 23:59 AoE (Anywhere on Earth)
- Notification: March 17, 2025
- Camera-ready: April 7, 2025 (firm deadline)

Instructions for Authors

Submissions must be done via the HotCRP website. The link will be announced shortly before the paper deadline.

ACNS 2025 will be an **in-person** conference. Since remote presentations or videos will not be accepted, authors submitting a paper must ensure that one of the authors can present the paper at the conference in person.

Submitted papers must not substantially overlap with papers that have been published (other than preprint) or accepted for publication or that are simultaneously in submission to a journal, conference, or workshop with published proceedings. Information about submissions may be shared with program chairs of other conferences for that purpose.

ACNS encourages promising students to submit and present their results at the conference. ACNS gives a best student paper award, with a 1500 EUR prize sponsored by Springer, to encourage promising students to publish their best results at this venue. To be eligible, the paper must be co-authored by at least one full-time student who will present the paper at the conference.

Systematization of Knowledge

ACNS 2025 solicits the submission of Systematization of Knowledge (SoK) papers, which have been very valuable to help our community to clarify and put into context complex research problems.

It is important to stress that SoK papers go beyond simply summarizing previous research (like in a survey) but also include a thorough examination and analysis of existing approaches, identify gaps and limitations, and offer insights or new perspectives on a given, major research area.

We encourage the authors to distinguish SoK submissions by adding the “SoK:” prefix to the title. SoK submissions will be reviewed by the full PC and held to the same standards as traditional research papers, but they will be accepted based on their treatment of existing work and value to the community, and not based on any new research results they may contain. Accepted papers will be presented at the conference and included in the proceedings.

Submission Guidelines

Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Each submission must begin with a title, short abstract, and a list of keywords. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader.

All submissions must be submitted in PDF format, following the unmodified LNCS format (accessible on the **Springer LCNS author guidelines** webpage) and typeset using the corresponding LaTeX class file. They must fit within a page limit of 20 pages, including title and abstract, figures, etc., but excluding references. Optionally, any amount of clearly marked supplementary material may be supplied, following the main body of the paper; however, reviewers are not required to read or review any supplementary material, and submissions are expected to be intelligible without it. Submissions not meeting these guidelines risk rejection without consideration of their merits. To accommodate for changes requested in reviews, the page limit for the camera-ready proceedings versions is 30 pages, including references and appendices.

For papers that might raise ethical concerns, authors are expected to convince reviewers that proper procedures (such as Institutional Review Board approval) have been followed and due diligence has been made to minimize potential harm.

ACNS 2025 has two submission deadlines (in September and January) that authors may choose to submit their papers to. Papers rejected after the September round cannot be resubmitted at the January round.

We will publish our proceedings with Springer as a volume of the Lecture Notes in Computer Science (LNCS) series.

Conflicts of Interest

The program co-chairs require cooperation from both authors and program committee members to prevent submissions from being evaluated by reviewers who have a conflict of interest. During the submission process, we will ask authors to identify members of the program committee with whom they share a conflict of interest.

We regard the following relationships as conflicts of interest:

1. Anyone who shares an institutional affiliation with an author at the time of submission (including secondary affiliations and consulting work),

2. Anyone who was the advisor or advisee of an author at any time in the past,
3. Anyone the author has collaborated or published within the prior two years,
4. Anyone who is serving as the sponsor or administrator of a grant that funds your research, or
5. Close personal or family ties.

If authors want to specify a conflict of another type than those listed above, they must contact the chairs and explain the perceived conflict. Program committee members who are in a conflict of interest with a paper, including program co-chairs, will be excluded from the evaluation and discussion of the paper by default.

Ethical Considerations for Vulnerability Disclosure (adapted from IEEE S&P)

Where research identifies a vulnerability (e.g., software vulnerabilities in a given program, design weaknesses in a hardware system, or any other kind of vulnerability in deployed systems), we expect that researchers act in a way that avoids gratuitous harm to affected users and, where possible, affirmatively protects those users. In nearly every case, disclosing the vulnerability to vendors of affected systems, and other stakeholders, will help protect users. It is the committee's sense that a disclosure window of 45 days to 90 days ahead of publication is consistent with authors' ethical obligations.

Longer disclosure windows (which may keep vulnerabilities from the public for extended periods of time) should only be considered in exceptional situations, e.g., if the affected parties have provided convincing evidence the vulnerabilities were previously unknown and the full rollout of mitigations requires additional time. The authors are encouraged to consult with the PC chairs in case of questions or concerns.

The version of the paper submitted for review must discuss in detail the steps the authors have taken or plan to take to address these vulnerabilities; but, consistent with the timelines above, the authors do not have to disclose vulnerabilities ahead of submission. The PC chairs will be happy to consult with authors about how this policy applies to their submissions.

Diversity and Inclusion

ACNS is committed to promoting diversity and inclusion in our community. If you have suggestions, concerns, or complaints related to biases or sexual harassment, we encourage you to reach out to the Conference Co-Chairs. We are committed to protecting the anonymity of such reports and helping to address your concerns. We value your feedback and ideas to help us all build a healthier and more welcoming community.

We encourage authors to be mindful of not using language or examples that further the marginalization, stereotyping, or erasure of any group of people, especially historically marginalized and/or under-represented groups (URGs) in computing. Of course, exclusionary treatment can arise unintentionally. Be vigilant and actively guard against such issues in your writing. Reviewers will also be empowered to monitor and demand changes if such issues arise in your submissions.