PQCrypto 2025

16th International Conference on Post-Quantum Cryptography

April 8–10, 2025 — Academia Sinica, Taipei, Taiwan

https://pqcrypto2025.iis.sinica.edu.tw/

ANNOUNCEMENT AND CALL FOR PAPERS

The aim of PQCrypto is to serve as a forum for researchers to present results and exchange ideas on cryptography in an era with large-scale quantum computers. Original research papers on all technical aspects of cryptographic research related to post-quantum cryptography are solicited. Topics of interest include (but are not restricted to):

- Cryptanalysis of post-quantum systems, and quantum cryptanalysis.
- Cryptosystems that have the potential to be safe against quantum computers such as: code-based, hash-based, isogeny-based, lattice-based, and multivariate constructions.
- Implementations of, and side-channel attacks on, post-quantum cryptosystems.
- Integration of and migration to post-quantum cryptography.
- Security models for the post-quantum era.

Instructions to authors

Accepted papers are planned to be published in Springer's LNCS series. Submissions must not exceed 30 pages, **excluding** appendices and references, and must be in a single column format in 10pt fonts using the default llncs class without adjustments. Additional material (datasets, code, long machine proofs, etc.) can be submitted as separate file. Reviewers are not required to read appendices and additional material, and submissions are expected to be intelligible and complete without them.

If the submission is accepted, the length of the final version is at most 35 pages **including** references and appendices, in the llncs class format. The additional material will not be part of the conference proceedings. Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings.

The review process is single-blinded. The submission should begin with a title, the **authors' names and affiliations**, a short abstract, and a list of key words. Its introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Submissions ignoring these guidelines may be rejected without further consideration.

All papers must be submitted with a meaningful abstract by the initial submission deadline. This is a firm deadline. Papers not registered by this deadline will not be considered. Authors may update or withdraw their submission at any time between the initial and final submission deadline.

Important dates (AoE):

- Initial submission deadline: October 25, 2024
- Final submission deadline: November 1, 2024
- Notification of acceptance: January 6, 2025
- Final version due: January 20, 2025

General chairs:

- Kai-Min Chung (Academia Sinica, Taiwan)
- Matthias Kannwischer (Chelpis Quantum Corp., Taiwan)
- Bo-Yin Yang (Academia Sinica, Taiwan)

Program chairs:

- Ruben Niederhagen (Academia Sinica, Taiwan, and University of Southern Denmark)
- Markku-Juhani O. Saarinen (Tampere University, Finland)

Paper submission page: https://easychair.org/conferences/?conf=pqcrypto2025

Program Committee

Aaram Yun
(Ewha Womans University)

Alain Couvreur
(École Polytechnique)

Alexander Wallet
(PQShield)

Andreas Hülsing
(Eindhoven University of Technology and Sandbox AQ)

Andre Esser
(Technology Innovation Institute)

Angela Robinson
(National Institute of Standards and Technology)

Atsushi Takayasu
(University of Tokyo)

Benjamin Smith
(Inria)

Bow-Yaw Wang
(Academia Sinica)

Bo-Yin Yang
(Academia Sinica)

Daniel Cabarcas
(Universidad Nacional de Colombia sede Medellín)

Daniel J. Bernstein
(University of Illinois at Chicago)

David Jao
(University of Waterloo)

Dustin Moody
(National Institute of Standards and Technology)

Edoardo Persichetti
(Florida Atlantic University and Sapienza University)

Elena Kirshanova
(Technology Innovation Institute)

Elisabeth Oswald
(University of Klagenfurt and University of Birmingham)

Fabio Campos
(Radboud University and RheinMain University of Applied Sciences)

Gelo Noel Tabia
(National Cheng Kung University)

Gustavo Banegas
(Inria and École Polytechnique)

Jean-Pierre Tillich
(Projet Secret and Inria)

Juliane Krämer
(University of Regensburg)

Julius Hermelink
(Max Planck Institute for Security and Privacy)

Kostas Papagiannopoulos
(Radboud University)

Magali Bardet
(University of Rouen Normandy)

Martin Ekerå
(KTH Royal Institute of Technology)

Matthias J. Kannwischer
(Chelpis Quantum Corp.)

Mélissa Rossi
(Thales, École Normale Supérieure, and French National Cybersecurity Agency)

Mike Hamburg
(Rambus)

Momonari Kudo
(Fukuoka Institute of Technology)

Monika Trimoska
(Eindhoven University of Technology)

Nicolas Sendrier
(Inria)

Olivier Blazy
(École Polytechnique)

Palash Sarkar
(Indian Statistical Institute)

Peter Pessl
(Infineon Technologies)

Philippe Gaborit
(University of Limoges)

Phong Nguyen
(Inria and École Normale Supérieure)

Qian Guo
(Lund University)

Rainer Steinwandt
(University of Alabama in Huntsville)

Ray Perlner
(National Institute of Standards and Technology)

Rina Zeitoun
(IDEMIA)

Sanjit Chatterjee
(Indian Institute of Science)

Sarah Arpin
(Virginia Polytechnic Institute and State University)

Scott Fluhrer
(Cisco Systems)

Shi Bai
(Florida Atlantic University)

Simona Samardjiska
(Radboud University)

Somindu C. Ramanna
(Indian Institute of Technology)

Takashi Yamakawa
(NTT Social Informatics Laboratories and Kyoto University)

Tako Boris Fouotsa
(Ecole Polytecnique Federale de Lausanne)

Thibauld Feneuil
(CryptoExperts)

Thomas Decru
(Katholieke Universiteit Leuven)

Thom Wiggers
(PQShield)

Tommaso Gagliardoni
(Kudelski Security)

Tsuyoshi Takagi
(University of Tokyo)

Yang Yu
(Tsinghua University)

Yu Yu
(Shanghai Jiao Tong University)