PERMUTATION-BASED CRYPTO

PBC 2025 – Call for contributions

In the last decade it has become clear that permutation-based cryptography is highly competitive in terms of performance and resource usage when compared to classical block ciphers and their modes. The goal of PBC workshop is to bring together academics and industry experts to discuss recent advances in this research area, as well as provide an introduction to anyone interested in discovering more about this field.

As an affiliated event of Eurocrypt, the PBC workshop will feature invited talks and contributed talks. The latter will be selected by the organizing committee through peer-review.

Talks can be about recent unpublished results, works in progress as well as results recently published in other venues. Submissions are welcome on all technical aspects of permutation-based cryptography including, but not limited to:

- cryptanalysis
- modes
- applications and protocols
- implementations
- side-channel and fault attacks

Submissions must include the name of the speaker, a title and an abstract of at most two pages. Contributors can submit their proposal to `submission@permutationbasedcrypto.org`.

Practical details

Submission deadline: February 28, 2025
Notification of acceptance: March 15, 2025
Workshop: May 4, 2025 (the Sunday before Eurocrypt)

Venue: Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid (UCM), located at Plaza de Ciencias 3, Ciudad Universitaria. 28040 - Madrid (España)

Organizing committee

Stelvio Cimato, University of Milan, Italy
Joan Daemen, Radboud University, Netherlands
Silvia Mella, Radboud University, Netherlands
Gilles Van Assche, STMicroelectronics, Belgium