PERMUTATION-BASED CRYPTO

PBC 2023 – 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.

Co-located with Eurocrypt 2023 in Lyon, France, the PBC workshop will feature invited talks and contributed talks. The latter will be selected by the steering committee from the received proposals.

Talks can be about recent unpublished results, works in progress as well as results recently published in other venues.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`.

Important dates

Submission deadline: February 28, 2023
Notification of acceptance: March 21, 2023

Steering committee

Christof Beierle	Ruhr University Bochum, Germany
Stelvio Cimato*	University of Milan, Italy
Joan Daemen*	Radboud University, Netherlands
Christoph Dobraunig	Intel Labs, USA
Silvia Mella*	Radboud University, Netherlands
Ling Song	Jinan University, China
Gilles Van Assche*	STMicroelectronics, Belgium
Benoît Viguier	ABN AMRO Bank N.V., Netherlands
Damian Vizár	CSEM, Switzerland
David Wong	O(1) Labs, USA

* organizers

`https://permutationbasedcrypto.org/2023/`