PERMUTATION-BASED CRYPTO

PBC 2020 – 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 the 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 2020 in Zagreb, Croatia, the PBC workshop will feature invited talks and contributed talks. The latter will be selected by the steering committee from the received contributions.

Talks can be about recent unpublished results, work in progress as well as results recently published in other venues.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 extended abstract (up to 3 pages) or the full paper (up to 15 pages). Contributors can send their proposal to `submission@permutationbasedcrypto.org`.

`https://permutationbasedcrypto.org/2020/`

Important dates

Submission deadline:	March 20, 2020
Notification of acceptance:	April 10, 2020
Workshop:	May 9, 2020 (Saturday before Eurocrypt)

Steering committee

Christof Beierle	Ruhr University Bochum, Germany
Stelvio Cimato*	University of Milan, Italy
Joan Daemen*	Radboud University, Netherlands
Christoph Dobraunig	Radboud Univeristy, Netherlands
Silvia Mella*	STMicroelectronics, Italy
Ling Song	IIE, Chinese Academy of Sciences, China
Gilles Van Assche*	STMicroelectronics, Belgium
Benoît Viguier	Radboud University, Netherlands
Damian Vizár	Centre suisse d'électronique et de microtechnique (CSEM), Switzerland
David Wong	Blockchain Facebook, USA

* organizers

SILC workshop

The Security and Implementation of Lightweight Cryptography (SILC) workshop takes place the day after PBC 2020. As there is an intersection between permutation-based and lightweight cryptography, *we allow double submissions between SILC and PBC*. If it is the case, please specify it when submitting.