PROCEEDINGS OF THE

CECC 2021

21st Central European Conference on Cryptology

23–25 June, 2021

Editors

Andrea Huszti and Attila Pethő

Department of Computer Science
Faculty of Informatics
University of Debrecen

Central European Conference on Cryptology (CECC) is an annual conference, focusing on all aspects of cryptology, including cryptanalysis, cryptographic applications in information security, design of cryptographic systems, general cryptographic protocols, post-quantum cryptography, pseudorandomness, cryptocurrencies, blockchain.

The CECC conference series started in 2001, TATRACRYPT '01 was held in Liptovský Ján, Slovakia. Since then, the event has been organized every year in different countries in Central Europe. Hungary hosted it four times. In 2021, due to the pandemic situation, it was held online at the Faculty of Informatics of the University of Debrecen in Debrecen, Hungary.

Three plenary speakers have been invited: Maria Eichlseder Assistant Professor, Graz University of Technology, Graz, Austria; Riccardo Focardi Full Professor, Ca' Foscari University, Venice, Italy and Klaus Schmeh, who works for a German cryptology company.

There have been 29 regular talks delivered and publications related to 8 talks are included in this Supplementum. The papers were carefully peer-reviewed according to the rules of Publicationes Mathematicae Debrecen. We are grateful to the members of organizing committee and the sponsor of the conference.

The conference was financially supported by EFOP 3.6.3, a project co-financed by the Hungarian Government and European Union through the European Regional Development Fund.

Andrea Huszti and Attila Pethő

SZÉCHENYI 2020
Magyarország Kormánya
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE

Conference Chair

Andrea Huszti – University of Debrecen

Program Committee

- **Nicolas Courtois**	University College London
- **László Csirmaz**	Central European University
- **Andrej Dujella**	University of Zagreb
- **Peter Gaži**	IOHK Research
- **Otokar Grosek**	Slovak University of Technology in Bratislava
- **Jan Hajny**	Brno University of Technology
- **Clemens Heuberger**	Alpen-Adria-Universität Klagenfurt
- **Miroslaw Kutylowski**	Wroclaw University of Science and Technology
- **Vashek Matyáš**	Masaryk University
- **Florian Mendel**	Infineon Technologies
- **Ferenc Molnár**	CCLab Ltd.
- **Karol Nemoga**	Slovak Academy of Sciences
- **Attila Pethő**	University of Debrecen
- **Stefan Porubsky**	Czech Academy of Sciences
- **Havard Raddum**	Simula UiB, Norway
- **Vincent Rijmen**	KU Leuven and University of Bergen
- **Martin Stanek**	Comenius University
- **Rainer Steinwandt**	The University of Alabama in Huntsville
- **Pavol Zajac**	Slovak University of Technology in Bratislava
- **Damian Vizár**	CSEM, Switzerland

Local Organizing Committee

- **Andrea Huszti (chair)**
- **Tamás Herendi**
- **Zoltán Szabolcs Kovács**
- **Norbert Oláh**
- **Viktória Padányi**
- **Ádám Vécsi**