Special Issue on Cryptology

Call for Papers

This special issue will focus on the area of cryptology and will include selected papers from the 2019 Central European Conference on Cryptology. It will cover various aspects of cryptology, including but not limited to

- cryptanalysis,
- cryptographic applications in information security,
- design of cryptographic systems,
- encryption schemes,
- general cryptographic protocols,
- post-quantum cryptography,
- pseudorandomness,
- signature schemes,
- cryptocurrencies, blockchain,
- steganography.

Detailed information on submissions to CECC 2019 and other information is provided at https://www.fi.muni.cz/cecc/ , with April 1, 2019 being the deadline for the submission of abstracts that will be reviewed by the program committee and authors will be informed about acceptance or rejection by April 22, 2019. The conference registration deadline will be May 15, 2019, and the conference dates are June 12-14.

Submissions and presentations at the conference will be evaluated by the program committee and authors will be informed about the evaluation results no later than June 21.

No more than 5 papers from the workshop shall be selected for the special issue of the Infocommunications Journal, and authors of these papers will have the opportunity to revise their papers (including typesetting in the IEEE format) after the conference – final versions for the special issue will be due July 22, 2019.

Guest Editors:

Václav (Vashek) Matyáš is a Professor at Masaryk University, Brno, CZ, acting as the Vice-Dean for Industrial and Alumni Relations at the Faculty of Informatics. His research interests are related to applied cryptography and security; he has published well over 150 peer-reviewed papers and articles and has co-authored several books. He worked in the past with Red Hat Czech, CyLab at Carnegie Mellon University, as a Fulbright-Masaryk Visiting Scholar at the Center for Research on Computation and Society of Harvard University, Microsoft Research Cambridge, University College Dublin, Ubilab at UBS AG, and as a Royal Society Postdoctoral Fellow with the Cambridge University Computer Lab. Vashek also worked on the Common Criteria and in ISO/IEC JTC1 SC27. Vashek is a member of the Editorial Board of the Infocommunications Journal and can be contacted at matyas AT fi.muni.cz.

Pavol Zajac is a Professor of Applied Computer Science at Slovak University of Technology in Bratislava, Slovakia. His research interests are related to mathematical cryptography and information security. Nowadays he works mostly with post-quantum cryptography and related algebraic problems. Pavol can be contacted pavol.zajac AT stuba.sk.

Jan Hajný works as an Associate Professor at the Faculty of Electrical Engineering and Communication at Brno University of Technology. He is the head of the Advanced Cybersecurity group, member of the faculty's Scientific Committee and the person responsible for the Information Security study programs. The scientific activities of prof. Hajny include research into modern cryptography and privacy protection. Prof. Hajny is the principal investigator of many projects, including Czech grants (GAČR, TAČR) and international projects (Horizon 2020). He is also active in the contractual research for major Czech companies and in international collaboration with institutions visited as a visiting researcher, i.e., KU Leuven, BE; IBM Research Zurich, CH; and University of Minnesota, USA.

Marek Sýs is an Assistant Professor at Masaryk University, Brno, CZ. His research interests are related to applied cryptography where he published 12 peer-review papers. His collaborative work received Real-World Award at ACM CCS 2017 for discovering ROCA vulnerability. He worked in the past as Postdoctoral Research Associate at Masaryk University and Assistant Professor at Technical University, Bratislava. He received his PhD degree from the Technical University, Bratislava, and can be contacted at syso AT mail.muni.cz.