Special Issue on Cryptology – Guest Editorial

Václav (Vashek) Matyáš, Pavol Zajac, Jan Hajný and Marek Sýs

Abstract—**This special issue brings selected papers from the 2019 Central European Conference on Cryptology, held in Telč, June 12-14, 2019.**

This special issue focuses on the area of applied cryptography, bringing up selected papers from the 2019 Central European Conference on Cryptology, covering various aspects of cryptology. All accepted papers went through two rounds of reviews and the authors duly incorporated the feedback in their revised papers.

The first paper of Michal Andrzejczak and Wladyslaw Dudzic "SAT Attacks on ARX Ciphers with Automated Equations Generation" investigates a new approach to algebraic attacks on block ciphers with SAT solvers. Authors try to find encryption keys for ciphers SIMON and SPECK by solving a specific system of equations. The equations are converted to satisfiability problem, and solved with standard SAT solvers. The novel approach of the authors is not to model so-called key expansion algorithm, producing a smaller system, but with a possibility of finding invalid keys. Probability of invalid keys is reduced by using multiple input-output pairs, which however increases the system.

The second paper of Mithilesh Kumar et al. "Reducing Lattice Enumeration Search Trees" deals with the security of post-quantum lattice-based schemes. In particular, the paper focuses on algorithms solving the shortest vector problem (SVP). Two optimized methods are proposed in the paper. The first method (hybrid enumeration) is based on finding suitable permutations, the second (sign-based pruning) is based on the estimation of coefficient signs. The paper also presents the experimental results provided for both methods and the comparison with standard techniques.

The third paper "The search of square m-sequences with maximum period via GPU and CPU" of Paweł Augustynowicz and Krzysztof Kanciak is concerned with the efficient parallel search of square m-sequences on modern CPUs and GPUs. The authors come up with the idea to exploit particular vector processor instructions, with the aim to utilize the advantages of the Single Instruction Multiple Data and Single Instruction Multiple Threads execution patterns. The authors also present the early abort sieving strategy based on the application of SAT-solvers. The paper shows that the proposed solution can exhaustively search m-sequences up to the degree 32.

The last paper "A New Type of Signature Scheme Derived from a MRHS Representation of a Symmetric Cipher" of Pavol Zajac and Peter Špaček introduces a fundamentally new idea of a post-quantum signature scheme. The scheme is defined by Multiple-Right-Hand-Side (MRHS) equations representing the entire SPN of the given cipher. The paper describes key procedures of the algorithm (key generation, signature generation, signature verification) and provides simplified examples for some critical steps of the algorithm. The security of the scheme is based on the difficulty of solving MRHS equations, or equivalently on the difficulty of the decoding problem (both are NP-hard).

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. Hajný include research into modern cryptography and privacy protection. Prof. Hajný 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.