Special Issue on Applied Cryptography – Guest Editorial

Václav (Vashek) Matyáš, Zdeněk Říha and Pavol Zajac

***Abstract*—This special issue brings selected papers from the SantaCrypt 2015 workshop, held in Prague, December 3-4, 2015.**

THIS special issue focuses on the area of applied cryptography, bringing up selected papers from Santa's Crypto Get-Together (SantaCrypt), a workshop that runs since 2001 as an annual Czech and Slovak workshop aiming to facilitate closer cooperation of professionals working in the field of applied cryptography and related areas of security. All three papers deal with cryptanalysis, although each of them approaches this area from a completely different perspective.

The first paper "New results on reduced-round Tiny Encryption Algorithm using genetic programming" of Karel Kubíček et al. explores use of evolutionary computing for cryptanalysis of the Tiny Encryption Algorithm (TEA). The authors deploy EACirc, a genetically inspired randomness testing framework based on finding a dynamically constructed test of statistical properties of TEA outputs. This test works as a probabilistic distinguisher separating cipher outputs from truly random data. TEA was chosen as a "benchmark"' algorithm and the paper provides results of EACirc applied to the TEA ciphertext created from differently structured plaintext. A different construction of EACirc tests also allows the authors to determine which part of the cipher's output is relevant to the decision of a well-performing randomness distinguisher.

The second paper "Side Channels in SW Implementation of the McEliece PKC" of Marek Klein deals with the McEliece cryptosystem – that is considered secure in the presence of quantum computers because there is no known quantum algorithm to solve the problem this cryptosystem is built on. The author examines a naïve implementation of the cryptosystem from the point of side channels, which can be used to gather information about the message or the secret key. The paper presents results of chosen timing attacks on straightforward implementation of this cryptosystem, as well as practical countermeasures and evaluation of their effectiveness.

The third paper "Cryptanalysis based on the theory of symmetric group representations" of Romana Linkeová and Pavel Příhoda focuses on an alternative of the famous key exchange protocol of Diffie and Hellman, working over a structure of small matrices over a group ring, as proposed by D. Kahrobaei et al. 2013. Their modification aimed to address an issue of the original proposal of Diffie and Hellman, the issue of performance faced by devices with a limited computational power. Research of alternative algebraic structures lead, among others, to the proposal of D. Kahrobaei et al. Linkeová and Příhoda attack this modification and prove that it is not secure with the help of the theory of symmetric group representations.

Václav (Vashek) Matyáš is a Professor at the Masaryk University, Brno, CZ, and serves as a Vice-Dean for Foreign Affairs and External Relations, Faculty of Informatics. His research interests relate to applied cryptography and security, publishing over a hundred peer-reviewed papers and articles, and co-authoring six books. He was a Fulbright Visiting Scholar with Harvard University, Center for Research on Computation and Society, and also worked with Microsoft Research Cambridge, University College Dublin, Ubilab at UBS AG, and was a Royal Society Postdoctoral Fellow with the Cambridge University Computer Lab. Vashek was one of the Editors-in-Chief of the Identity in the Information Society journal, and he also edited the Computer and Communications Security Reviews, and worked on the development of Common Criteria and with ISO/IEC JTC1 SC27. Vashek is a member of the Editorial Board of the Infocommunications Journal and a Senior Member of the ACM. He received his PhD degree from Masaryk University, Brno and can be contacted at matyas AT fi.muni.cz.

Zdeněk Říha is an Assistant Professor at the Masaryk University, Faculty of Informatics, in Brno, Czech Republic. He received his PhD degree from the Faculty of Informatics, Masaryk University. In 1999 he spent 6 months on an internship at Ubilab, the research lab of the bank UBS, focusing on security and usability aspects of biometric authentication systems. Between 2005 and 2008 he was seconded as a Detached National Expert to the European Commission's Joint Research Centre in Italy, where he worked on various projects related to privacy protection and electronic passports. He was involved in the ePassport interoperability group known as the Brussels Interoperability Group. Zdeněk has been working with the WG 5 (Identity management and privacy technologies) of ISO/IEC JTC 1/SC 27. Zdeněk's research interests include smartcard security, PKI, security of biometric systems and machine readable travel documents. Zdeněk can be contacted at zriha AT fi.muni.cz.

Pavol Zajac is an Associate Professor at the Slovak University of Technology in Bratislava. His main research interests lie in the area of mathematical cryptography. Nowadays he works mostly with post- quantum cryptography and related algebraic problems. Pavol can be contacted at pavol.zajac AT stuba.sk.