Special Issue on Cryptology – Guest Editorial

Václav (Vashek) Matyáš, Zdeněk Říha and Marek Kumpošt

***Abstract*—This special issue brings selected papers from the 2013 Central European Conference on Cryptology, held in Telč, June 26-28, 2013.**

This special issue focuses on the area of applied cryptography, bringing up selected papers from the 2013 Central European Conference on Cryptology, covering various aspects of cryptology, including cryptanalysis, cryptographic applications in information security, design of cryptographic systems, general cryptographic protocols, post-quantum cryptography, pseudorandomness, signature schemes, and steganography.

The first paper "Protection of Data Groups from Personal Identity Documents" of Przemysław Kubiak et al. proposes a procedure of presenting a signed face image of the document holder. The aim of this procedure is to authenticate the image by document issuer, but at the same time to prevent misuse of this high quality digital data. The solution reflects the technology challenges related to limits of data storage on a personal identity document chip, and the designed protocols can potentially be used for other than just biometric data.

The second paper "Classes of Garbling Schemes" of Tommi Meskanen et al. extends some results of the work of Bellare et al. from 2012 on garbled circuits from a cryptographic technique to a cryptographic goal, defining several new security notions for garbled circuits. Meskanen et al. provide some new results about the classes of garbling schemes defined by Bellare et al., define new classes of garbling schemes, prove their relation of earlier classes, and also investigate some results concerning the new classes.

The third paper "On a key exchange protocol based on Diophantine equations" of Hirata-Kohno et al. analyzes a key exchange protocol proposed by H. Yosh in 2011, based on the hardness to solve Diophantine equations. The authors analyze the protocol and show that the public key is very large, suggesting also an alternative solution through large families of parameters both in the finite field and in the rational integer cases for which the protocol can be secure.

The last paper "Strongly Secure Password Based Blind Signature for Real World Applications" of Sangeetha Jose et al. password based blind signature that are used in scenarios where a user requires the authentication of the signer without revealing the message to the signer. The authors propose a novel design that ensures the properties unforgeability, blindness and unframeability. Yet for small sizes of passwords, an off-line password guessing attack is of high relevance. The authors propose a strongly secure password based blind short signature that solves the off-line password guessing problem, with the formal proof of the scheme reduced to the computational Diffie-Hellman (CDH) assumption.

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.

Marek Kumpošt is a Research Assistant at the Masaryk University, Faculty of Informatics, in Brno, Czech Republic. He received his PhD in 2009 from the Faculty of Informatics, Masaryk University. The primary area of his doctoral research was oriented on privacy protection, anonymity and user profiling. He was involved in two European-wide projects on privacy protection and identity management – FIDIS (Future of Identity in the Information Society) and PICOS (Privacy and Identity in Management for Community Services). He also worked with the LIACC (Laboratory of Artificial Intelligence and Computer Science) group in Porto on user profiling based on information from NetFlow. He is interested in network security, web application security and cloud security. Marek can be contacted at kumpost AT fi.muni.cz.