CALL FOR PAPERS
Special Issue on Cryptology

This special issue will focus on the area of cryptology and will include selected papers from the 2013 Central European Conference on Cryptology. CECC 2013 covers various aspects of cryptology, including but not limited to:

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

Detailed information on submissions to CECC 2013 and other information is provided at *http:// ww.fi.muni.cz/cecc/*, with April 15, 2013 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 29, 2013. The conference registration deadline will be May 22, 2013, and the conference dates are June 26-28.

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 30.

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, 2013.

Papers from the general public are also welcome. The deadline for submission of such papers is May 15. Papers will be peer-reviewed as usual.

Guest Editors:

VÁCLAV (VASHEK) MATYÁS 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. He received his PhD degree from Masaryk University, Brno and can be contacted at *matyas@fi.muni.cz*.

ZDENEK RÍHA is an Assistant Professor at the Masaryk University, Faculty of Informatics, in Brno (CZ). 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. Zdenek has been working with the WG 5 (Identity management and privacy technologies) of ISO/IEC JTC 1/SC 27. Zdenek's research interests include smartcard security, PKI, security of biometric systems and machine readable travel documents. Zdenek can be contacted at *zriha@fi.muni.cz*.

MAREK KUMPOST is a Research Assistant at the Masaryk University, Faculty of Informatics, in Brno (CZ). 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 project 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 spent 3 months with the LIACC (Laboratory of Artificial Intelligence and Computer Science) group working on user profiling based on information from NetFlow. He is also interested in network security, web application security and cloud security. Marek can be contacted at *kumpost@fi.muni.cz*.