# Call for Papers
# Special Issue on Applied Cryptography

This special issue will focus on the area of applied cryptography, bringing up selected papers from SantaCrypt 2012. Santa's Crypto Get-Together (SantaCrypt) started in 2001 as the first annual Czech and Slovak workshop aiming to facilitate closer cooperation of professionals working in the field of applied cryptography and related areas of security. This get-together of experts is organised in order to foster exchange of information and ideas on past, ongoing, and also future projects. The special issue of the Infocommunications Journal will focus on the following areas:

- Applied Cryptography
- Practical Cryptanalysis
- Cryptographic Protocols
- Security Mechanisms Deploying Cryptography

Submissions to Santacrypt 2012 should be mailed to matyas AT fi.muni.cz, and clearly marked with Subject “SantaCrypt 2012”. The manuscripts should follow the MKB format (http://mkb.buslab.org/cfp.htm.en) with the maximum length of 10 pages (corresponds to 8 pages in the IEEE format). The final deadline for the submissions is 1st October 2012. Submissions will be evaluated by the program committee and authors will be informed about the evaluation results by 29th October. Camera-ready versions for the workshop proceedings have to be delivered by 12th November. The workshop takes place in Prague, Czechia, on November 29-30, 2012.

No more than 4 papers from the workshop shall be then 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 workshop – final versions for the special issue will be due December 9.

## Guest Editors:

**VÁCLAV (VASHEK) MATYÁS** is a Professor at the Masaryk University, Brno, Czech Republic, 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, 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. Zdenek has been working with the WG 5 (Identity management and privacy technologies) of ISO/IEC JTC 1/SC 27. His research interests include smartcard security, PKI, security of biometric systems and machine readable travel documents. Zdenek can be contacted at *zriha@fi.muni.cz*.

**PETR SVENDA** is an Assistant Professor at the Masaryk University, Faculty of Informatics, in Brno, Czech Republic. He received his PhD degree from Masaryk University, working in the area of the cryptographic protocols for restricted environments such as wireless sensor networks, with focus on automatic generation of cryptographic protocols with the help of evolutionary algorithms. In 2008, he worked at TU Dresden on secure logging for the AN.ON anonymity service. He is also interested in practical aspects of security in cryptographic smartcards and their resistance against side-channel attacks and properties of random number generators available on smartcards and mobile devices. Petr can be contacted at *svenda@fi.muni.cz*.