Zoltán Móczár received his M.Sc. degree in computer science from the Budapest University of Technology and Economics (BME), Hungary in 2011. Currently he is a Ph.D. student at the High Speed Networks Laboratory, Department of Telecommunications and Media Informatics, BME. His research interests include traffic engineering, performance evaluation of high-speed transport protocols and Future Internet design. He has participated in several academic and applied research projects.

Sándor Molnár is an Associate Professor at the Department of Telecommunications and Media Informatics, Budapest University of Technology and Economics (BME). In electrical engineering he received his M.Sc. in 1991 and Ph.D. in 1996 from BME. Dr. Molnár is serving in the editorial board of international journals and is working in the TPC of IEEE conferences. He has been participating in various EU projects and was the BME project leader of the Gold Award winner 2009 CELTIC project titled "Traffic Measurements and Models in Multi-Service Networks (TRAMMS)". His main interests include teletraffic analysis and performance evaluation of modern communication networks.

CALL FOR PAPERS
Special Issue on Applied Cryptography and Security

This special issue will focus on the area of applied cryptography, bringing up selected papers from *Santa Crypt 2014*. 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 2014 should be mailed to matyas@fi.muni.cz, and clearly marked with Subject "SantaCrypt 2014". The manuscripts should follow the MKB format (http://mkb.tns.cz/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 30th September 2014. Submissions will be evaluated by the program committee and authors will be informed about the evaluation results by 30th October. Camera-ready versions for the workshop proceedings have to be delivered by 11th November. The workshop takes place in Prague, Czechia, on November 27-28, 2014.

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 January 11, 2015.

Guest Editors:

VÁCLAV (VASHEK) MATYÁS is a Professor at the Masaryk University, Brno, CZ, and Vice-Dean for Foreign Affairs and External Relations, Faculty of Informatics. His research interests relate to applied cryptography and security, where he published over 150 peer-reviewed papers and articles, and co-authored several books. He was a Fulbright-Masaryk Visiting Scholar with Harvard University, Center for Research on Computation and Society in 2011-12, and previously he worked also 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 edited the Computer and Communications Security Reviews, and worked on the development of Common Criteria and with ISO/IEC JTC1 SC27. 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. 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 Android security, smartcard security, PKI, security of biometric systems and machine readable travel documents. Zdeněk can be contacted at *zriha@fi.muni.cz*.

PAVOL ZAJAC is an Assistant Professor at the Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Slovakia (FEI STU). He received his PhD degree in Applied Mathematics from FEI STU. His main research focus is in the area of mathematical cryptology, including mathematical principles of cipher design, and algebraic cryptanalysis. He also works on various application projects, including efficient implementation of post-quantum cryptosystems, and improving privacy of user data on mobile devices. Pavol can be contacted at *pavol.zajac@stuba.sk*.