Mikulášská kryptobesídka / SantaCrypt 2014

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS MU / Organized by TNS, a.s. and CROCS MU

Program

27. listopadu 2014 (čtvrtek) / November 27, 2014 (Thursday)

8:45 –	*Registrace / Registration*
9:30 – 9:40	*Zahájení workshopu / Workshop opening*
9:40 – 10:40	*Keynote* Joachim Posegga: Alice in the Sky – On Security of Air Traffic Control Communication
10:40 – 11:40	*Keynote* Gregor Leander: A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro
11:40 – 12:10	Martin Stanek: Experimenting with Shuffle Block Cipher and SMT Solvers
12:10 – 13:30	*Oběd / Lunch*
13:30 – 14:30	*Keynote* Peter Gaži: Key-Length Extension for Block Ciphers: Plain and Randomized Cascades
14:30 – 15:00	*Přestávka na kávu a čaj / Coffee & tea break*
15:00 – 16:00	*KEYMAKER I* Martin Ukrop: Formal verification in practice – secure storage in insecure environment Matúš Kyseľ: Cloning contactless payment cards Josef Bárta: TC-linearisation of tweakable polynomials
16:00 – 16:30	Marek Sýs: Optimizing the NIST Statistical Test Suite
16:30 – 17:xx	*Rump session*
17:17 –	*Večeře / Dinner*

Následují neformální diskuze v prostorách vyhrazených pouze pro účastníky kryptobesídky. / Followed by informal discussions in the hall reserved for the workshop participants.

Mikulášská kryptobesídka / SantaCrypt 2014

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS MU / Organized by TNS, a.s. and CROCS MU

28. listopadu 2014 (pátek) / November 28, 2014 (Friday)

9:00 – 9:05	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:05 – 10:05	Bohuslav Rudolf: Iontové pasti, kvantová hradla a DiVincenzova kritéria
10:05 – 10:25	*KEYMAKER II* Ladislav Öllős: Algebraická kryptoanalýza na GRIDe
10:25 – 10:55	*Přestávka na kávu a čaj / Coffee & tea break*
10:55 – 11:55	*Keynote* Karthik Bhargavan: Breaking and Fixing Transport Layer Security
11:55 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...