Mikulášská kryptobesídka / SantaCrypt 2015

http://mkb.tns.cz/

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

Programme

3. prosince 2015 (čtvrtek) / December 3, 2015 (Thursday)

8:45 –	*Registrace / Registration*
9:30 – 9:40	*Zahájení workshopu / Workshop opening*
9:40 – 10:40	*Keynote* Peter Schwabe: Post-quantum cryptography
10:40 – 11:40	*Keynote* Joan Daemen: Sponge-based authenticated encryption
11:40 – 12:10	Marek Sýs: NIST Statistical Test Suite – result interpretation and optimization
12:10 – 13:30	*Oběd / Lunch*
13:40 – 14:40	*Keynote* Stefan Dziembowski: Research challenges in cryptocurrencies
14:40 – 15:30	*KEYMAKER I* Romana Linkeová: Diffie & Hellman exchanging matrices over a group ring Lukáš Pohanka: Memory-constrained EdDSA on MSP430
15:30 – 16:00	*Přestávka na kávu a čaj / Coffee & tea break*
16:00 – 16:50	*KEYMAKER II* Karel Kubíček: New results on reduced-round Tiny Encryption Algorithm using genetic programming František Uhrecký: BitPunch The McEliece Crypto Library
16:50 – 17:22	*Rump session*
17:30 –	*Večeře / Dinner*

Mikulášská kryptobesídka / SantaCrypt 2015

http://mkb.tns.cz/

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

4. prosince 2015 (pátek) / December 4, 2015 (Friday)

9:00 – 9:10	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:10 – 10:10	*Keynote* Pavel Vondruška: Tajné symboly uzavřených komunit
10:10 – 10:40	*Přestávka na kávu a čaj / Coffee & tea break*
10:40 – 11:55	*KEYMAKER III* Dominik Breitenbacher: Paralelizované Self-Initializing Quadratic Sieve užitím OpenMP Marek Klein: Postranní kanály v softwarové implementaci McEliece PKC Tomáš Smetka: Kryptoanalýza symetrických šifrovacích algoritmů s využitím symbolické regrese a genetického programování
11:55 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...