Mikulášská kryptobesídka / SantaCrypt 2025

http://mkb.tns.cz/

Pořádá TNS, a.s., a CRoCS FI MU / Organized by TNS, a.s. and CRoCS FI MU

Programme

4. prosince 2025 (čtvrtek) / December 4, 2025 (Thursday)

9:00 –	*Registrace / Registration*
9:45 – 10:00	*Zahájení workshopu / Workshop opening*
10:00 – 11:00	*Keynote* Peeter Laud: An efficient two-party ML-DSA protocol
11:00 – 12:00	*Keynote* Lenka Mareková: Analysis of Telegram: attacks, proofs, and lessons
12:00 – 13:15	*Oběd / Lunch*
13:15 – 14:15	*Keynote* Vadim Lyubashevsky: Lattice cryptography: From quantum-safe standards to zero-knowledge proofs
14:15 – 14:40	*KEYMAKER* Kristína Hanicová: Encryption of userspace-managed block devices in Linux
14:40 – 15:10	*Přestávka na kávu a čaj / Coffee & tea break*
15:10 – 16:10	*Keynote* Tomáš Sušánka: Lessons learned from practical implementation of cryptocurrency hardware wallets
16:10 – 17:00	*KEYMAKER* Veronika Hanulíková: Improving side-channel resistance of Java Card implementations Berenika Richterová: On security of practical adaptor signatures
17:00 – 17:44	*Rump session*
17:44 –	*Večeře / Dinner*

Mikulášská kryptobesídka / SantaCrypt 2025

http://mkb.tns.cz/

Pořádá TNS, a.s., a CRoCS FI MU / Organized by TNS, a.s. and CRoCS FI MU

5. prosince 2025 (pátek) / December 5, 2025 (Friday)

9:00 – 9:05	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:05 – 10:05	*Keynote* Tomáš Rosa: Electronic attacks in PC interfaces terrain – models and exploits
10:05 – 10:40	*Přestávka na kávu a čaj / Coffee & tea break*
10:40 – 11:40	*Keynote* Marek Sýs: Lattice-based attacks and cryptography
11:40 – 12:20	*KEYMAKER* Matej Olexa: Exploiting BLE timing vulnerabilities with neural networks Ján Mikulec: Implementácia šifrovacieho stroja Condenser PBJ Jakub Chrappa: Segmentácia šifrovacích kľúčov
12:22 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...