Mikulášská kryptobesídka / SantaCrypt 2020/21

http://mkb.tns.cz/

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

Programme

2. září 2021 (čtvrtek) / September 2, 2021 (Thursday)

9:00 –	*Registrace / Registration*
9:44 – 9:55	*Zahájení workshopu / Workshop opening*
9:55 – 10:55	*Keynote* Vasily Mikhalev: CrypTool. Learning cryptography can be fun!
10:55 – 12:15	*KEYMAKER I* Antonín Dufka: Smartcard Cosigning of Bitcoin Transactions Jakub Klemsa: Multivalue TFHE for Neural Networks Jan Kvapil: Security analysis of JavaCard Virtual Machine Vladimír Sedláček: Fooling primality tests on smartcards
12:15 – 13:45	*Oběd / Lunch*
13:45 – 14:45	*Keynote* Miloslav Dušek: Quantum cryptography
14:45 – 15:15	*KEYMAKER II* Ján Jančár: PYECSCA: Reverse-engineering Black-box Elliptic Curve Cryptography Implementations
15:15 – 15:45	*Přestávka na kávu a čaj / Coffee & tea break*
15:45 – 16:25	*KEYMAKER III* Martin Podhora: Smart card power trace database Tomáš Gono: Identification and separation of parts of nomenclator keys
16:25 – 17:15	*Rump session*
17:17 –	*Večeře / Dinner*

Mikulášská kryptobesídka / SantaCrypt 2020/21

http://mkb.tns.cz/

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

3. září 2021 (pátek) / September 3, 2021 (Friday)

9:09 – 9:15	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:15 – 10:15	*Keynote* Otokar Grošek: Existuje dokonalá náhodnosť?
10:15 – 10:45	*Přestávka na kávu a čaj / Coffee & tea break*
10:45 – 11:45	*KEYMAKER III* Jiří Horák: Distribution Portal For Applications For Cryptographic Smartcards Tomáš Novotný: On pairing-friendly 2-cycles of elliptic curves containing a curve from a family Martin Pastyřík: On the Security and Privacy of Pietrzak's Decentralised Contact Tracing Scheme
11:45 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...