



## Tentative Programme

### 7. prosince 2023 (čtvrtek) / December 7, 2023 (Thursday)

- 9:00 – *Registrace / Registration*
- 9:33 – 9:45 *Zahájení workshopu / Workshop opening*
- 9:45 – 10:45 *Keynote*  
Lejla Batina: TBD
- 10:45 – 12:00 *KEYMAKER I*  
Jakub Janků: Schnorr Multi-Signatures for Secure Devices with Restricted Interfaces  
Milan Šorf: Testing random number generators of hardware wallets  
Jakub Klemsa: A Practical TFHE-Based Multi-Key Homomorphic Encryption with Linear Complexity and Low Noise Growth
- 12:00 – 13:15 *Oběd / Lunch*
- 13:15 – 14:15 *Keynote*  
Florian Fröwis: Migration to Quantum-Safe with Quantum Key Distribution
- 14:15 – 15:15 Ján Jančár & Adam Janovský: sec-certs: Examining the security certification practice for better vulnerability mitigation
- 15:15 – 15:45 *Přestávka na kávu a čaj / Coffee & tea break*
- 15:45 – 16:45 *Keynote*  
Stephan Krenn: TBD
- 16:45 – 17:15 *Rump session*
- 17:17 – *Večeře / Dinner*

# Mikulášská kryptobesídka / SantaCrypt 2023

<http://mkb.tns.cz/>

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



## 8. prosince 2023 (pátek) / December 8, 2023 (Friday)

- 9:00 – 9:05      *Zahájení druhého dne workshopu / Opening of the second day of the workshop*
- 9:05 – 10:05      *Keynote*  
Bohuslav Rudolf: Několik slov o kvantové informaci a o kvantové entropii
- 10:05 – 10:45      *Přestávka na kávu a čaj / Coffee & tea break*
- 10:45 – 12:05      *KEYMAKER II*  
Štěpán Horáček: Opal drives and their security  
David Rajnoha: Detection of Bitcoin keys generated according to BIP32 with weak seed  
Juraj Budai: Automatizované rozpoznávání šifrovaných symbolov v dobových nomenklátoroch  
Martin Melicher: Improved integral distinguisher for the PRINCE cipher
- 12:12 –              *Mikuláš              /              Santa*

*Závěr workshopu... / Workshop ends...*