



Programme

5. prosince 2024 (čtvrtek) / December 5, 2024 (Thursday)

9:00 –	<i>Registrace / Registration</i>
9:45 – 10:00	<i>Zahájení workshopu / Workshop opening</i>
10:00 – 11:00	<i>Keynote</i> Peter Schwabe: Formosa Crypto: high-assurance, high-security crypto software
11:00 – 12:00	<i>Keynote</i> Jan Willemson: You must have Internet voting, but what about mobile?
12:00 – 13:15	<i>Oběd / Lunch</i>
13:15 – 14:15	<i>Keynote</i> Vasilios Mavroudis: AI for Security: Overpromise and Underdeliver?
14:15 – 15:05	<i>KEYMAKER</i> Kristýna Mašková: Preprocessing Techniques in Algebraic Cryptanalysis Petr Hanák: Analysis of security features of smart lock protocol
15:05 – 15:40	<i>Přestávka na kávu a čaj / Coffee & tea break</i>
15:40 – 16:40	<i>Keynote</i> Veelasha Moonsamy: Wireless Physical-Layer Sensing: The Good, The Bad, and The Ugly
16:40 – 17:15	<i>Rump session</i>
17:17 –	<i>Večeře / Dinner</i>

Mikulášská kryptobesídka / SantaCrypt 2024

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

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



6. prosince 2024 (pátek) / December 6, 2024 (Friday)

9:00 – 9:05	<i>Zahájení druhého dne workshopu / Opening of the second day of the workshop</i>
9:05 – 10:05	<i>Keynote</i> Bohuslav Rudolf: Informace a entropie z fyzikálního pohledu, část II.
10:05 – 10:40	<i>Přestávka na kávu a čaj / Coffee & tea break</i>
10:40 – 11:40	<i>Keynote</i> Tomáš Mráz: Novinky v OpenSSL projektu
11:40 – 12:20	<i>KEYMAKER</i> Jan Fmka: Nový typ kryptografických schémat na copánkových grupách Filip Mikuš: Detekcia symbolov a transkripcia historických šifrovaných rukopisov pomocou umelej inteligencie
12:22 –	<i>Mikuláš / Santa</i>

Závěr workshopu... / Workshop ends...