"Best Practices in Cryptology and Information Security"

at the Slovak University of Technology in Bratislava, June 25 - 27, 2014

June 25

1. Boolean functions in Cryptology - Oto Grosek 9:00- 9:50
2. Fault Cryptanalysis of Stream ciphers - Viliam Hromada 10:00-10:50
3. Introduction to Steganography - Milan Vojvoda 11:00-11:50

June 26

4. Methods of Fingerprint Recognition - Pavol Marak 9:00-9:50
5. Nature-inspired Heuristic methods in Classical cipher Cryptanalysis - Eugen Antal 10:00-10:50
6. Side Channel Attacks against ECC and McEliece algorithms – Marek Repka 11:00-11:50
7. PCA and Canonical Correlations in Cryptanalysis - Tomas Fabsic 12:00-12:50

June 27

8. Number theory in Cryptography - Karol Nemoga 9:00- 9:50
9. Simple Power Analysis of RSA - Pavol Zajac 10:00-10:50
10. Introduction to Android security - Juraj Varga 11:00-11:50

Secure implementation of post-quantum cryptography

NPD: Otokar Grosek

SPS Project Number: 984520