ITG Fachgruppe „Angewandte Informationstheorie”

Program of the 42. Meeting, 29.05.2024

— Security and Privacy —

TU München, Professur für Codierung und Kryptographie
Gebäude N4, 2. Obergeschoss, Raum N2408
Theresienstr. 90, 80333 München

9:00 – 9:00	Dirk Wübben, *Department of Communications Engineering, University of Bremen* **Welcome**
9:05 – 9:30	Antonia Wachter-Zeh, *Chair of Coding and Cryptography, TU Munich* *Hannes Bartz, Institute of Communications and Navigation, DLR Oberpfaffenhofen* **Welcome by the host**

Session I

9:30 – 9:50	Sebastian Bitzer, *Chair of Coding and Cryptography, TU Munich* **HQC Beyond the BSC - Towards Error Structure-Aware Decoding**
9:50 – 10:10	Werner Henkel, *Constructor University, Bremen* **Physical Layer Secret Key Generation for FDD Systems**
10:10 – 10:30	Frederik Walter, *Chair of Coding and Cryptography, TU Munich* **DNA-based in-product authentication schemes**
10:30 – 11:00	**Coffee break**

Session II

11:00 – 11:20	*Klaus Schilling, Institute of Computer Science, Julius-Maximilians-Universität Würzburg* ***The QUBE nano-satellite for quantum key distribution to support secure communication (since August 2024 in orbit)***
11:20 – 11:40	Luis Torres-Figueroa, *Chair of Theoretical Information Technology, TU Munich* **Embedding Security by Design into Post-Quantum 6G Systems**
11:40 – 12:00	Amelie Sophia Ettinger, *Institute of Computer Science, Julius-Maximilians-Universität Würzburg* **Secret Key Rates of Entanglement-Based Quantum Key Distribution**
12:00 – 13:10	**Lunch break**

Session III

13:10 – 13:30	Chen Yiqi, *Chair of Theoretical Information Technology, TU Munich* **Distribution-Preserving Integrated Sensing and Communication with Secure Reconstruction**
13:30 – 13:50	Hugo Sauerbier Couvée, *Chair of Coding and Cryptography, TU Munich* **Generic Decoders for the Rank Metric and their Relations to the Hamming Metric**
13:50 – 14:10	Cornelia Ott, *Institute of Communications and Navigation, DLR* **Crystals Dilithium: A New NIST Standard for Post-Quantum Cryptography**

ITG Fachgruppe
„Angewandte Informationstheorie”

14:10 – 14:40	**Coffee break**

Session IV

14:40 – 15:00	Johannes Voichtleitner, *Chair of Theoretical Information Technology, TU Munich*
	Statistical verification of Physical Layer Security
15:00 – 15:20	Hannes Bartz, *Institute of Communications and Navigation, DLR*
	Some? What? Fully? Homomorphic Encryption
15:20 –	**Closing**