

Date	Time	Session	Speaker	Title
Intro				
10/17/2019	13:00		<i>Daniel Loebenberger</i>	Begrüßungsrunde + Crypto Day Matters
10/17/2019	13:15		<i>Marcel Selhorst</i>	Introduction to QPSI - Who we are and what we do
Hardware				
10/17/2019	13:30		<i>Victor van der Veen</i>	When Memory Serves Not So Well - Memory Errors 30 Years Later
10/17/2019	14:00		<i>Marcin Aftowicz</i>	Evaluation of the ECDSA IHP Hardware Accelerator
10/17/2019	14:30		<i>Nils Wisiol</i>	Towards Secure Strong PUFs
10/17/2019	15:00	Coffee Break		
Crypto				
10/17/2019	15:30		<i>Alejandro Sosa</i>	On the Impact of the Sampling Rate on the Success of Horizontal DEMA Attack
10/17/2019	16:00		<i>Kris Shrishak</i>	Securing DNSSEC Keys via Threshold ECDSA From Generic MPC
10/17/2019	16:30		<i>Patrick Struck</i>	Sponges Resist Leakage: The Case of Authenticated Encryption
10/17/2019	17:00		<i>Roman Natarov</i>	Edge computing devices assessment for cryptography and biomedical signal analysis
10/17/2019	17:30		<i>Yauhen Varabei</i>	Intelligent Clustering as a Means to Improve K-means Based Horizontal Attacks
10/17/2019	18:00	Brewery Tour & Tasting		
10/17/2019	19:00	Dinner		
Networks				
10/18/2019	9:00		<i>Markus Brandt</i>	Distributed Domain Validation (DDV)
10/18/2019	9:30		<i>Daniel Loebenberger</i>	Towards Quantum-resistant Virtual Private Networks
10/18/2019	10:00		<i>Shinjo Park</i>	Anatomy of Commercial IMSI Catchers and Detectors
10/18/2019	10:30	Coffee Break & Breakfast		
Protocols & ML				
10/18/2019	11:00		<i>Tim Ohlendorf</i>	SLIDEDroid: A Secure Lightweight Identity for the Android Platform
10/18/2019	11:30		<i>Robert Buhren</i>	Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation
10/18/2019	12:00		<i>Franziska Boenisch</i>	Applying Differential Privacy to Machine Learning: Challenges and Potentials
10/18/2019	12:30		<i>Kai Lehniger</i>	Using machine learning techniques for hardware performance counter classification and ROP attack detection
10/18/2019	13:00	End of Crypto Day		