



Qualcomm



crypto day matters

Beiträge vom 31. Kryptotag

17.– 18.10.2019

Qualcomm CDMA GmbH, Kurfürstendamm 21, 10719 Berlin, Germany

Edited by Marcel Selhorst, Daniel Loebenberg and Michael Nüsken
for the interest group „Angewandte Kryptographie“

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