Kryptotag Online, 15. Januar 2021

Freitag, 15.01.2021			Art	Speaker	Affiliation	Title
9:00	9:20	0:20	**Get Together**		Next session chair: Daniel Loebenberger	
9:20	9:30	0:10	Welcome	Stefan-Lukas Gazdag	genua	Welcome at the first online crypto day
				Michael Nüsken	b-it, Bonn	
				Daniel Loebenberger	Fraunhofer AISEC, OTH Amberg-Weiden	
9:30	9:45	0:15	Talk	Winfried Stephan		Das DDR-Chiffriergerät T-310
9:45	10:00	0:15	Talk	Philipp Winkler	Fernuniversität Hagen	Cycle Structure of RSA with Small Moduli
10:00	10:15	0:15	Talk	Kris Shrishak	TU Darmstadt	Phased Deployment of Distributed RPKI
10:15	10:30	0:15	Talk	Ahmed Alqattaa	OTH Amberg-Weiden	An IoT Crypto Gateway for Resource-Constrained IoT Devices
10:30	10:45	0:15	Talk	Samed Düzlü & Rune Fiedler	TU Darmstadt	BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures
10:45	11:00	0:15	Talk	Johannes Ernst	University of St. Gallen	Efficient Private Stream Aggregation with Labels in the Standard Model
11:00	11:30	0:30	**Coffee Break**		Next session chair: Michael Nüsken	
11:30	11:45	0:15	Talk	Kai Lehniger	IHP	Simplified Control Flow Integrity Method for Permutated Programs
11:45	12:00	0:15	Talk	Dmytro Petryk	IHP	Laser Fault Injection Attacks against IHP Chips
12:00	12:15	0:15	Talk	Ievgen Kabin	IHP	Breaking of an Open Source Fully Balanced Elliptic Curve Design Using Automated Simple SCA
12:15	12:30	0:15	Talk	Dan Klann	IHP	Efficient implementation of unified ECC accelerators based on the Karatsuba multiplication method
12:30	13:30	1:00	**Lunch Break**		Next session chair: Stefan-Lukas Gazdag	
13:30	13:45	0:15	Talk	Marcel Stanislav Müller	Technische Universität Darmstadt	An overview of safe-error attacks on isogeny based cryptography
13:45	14:00	0:15	Talk	Shujie Zhao	Fraunhofer SIT	A Novel Approach to IP ID Classification
14:00	14:15	0:15	Talk	Tobias Guggemos	Ludwig-Maximilians-Universität München	group Identity Based Signatures: Efficiently revoking signing keys in communication groups
14:15	14:30	0:15	Talk	Sophia Grundner-Culemann	Ludwig-Maximilians-Universität München	EUF-ID-UPD-CMA: A security notion for key-updatable identity-based signature schemes
14:30	15:00	0:30	**Coffee Break**		Next session chair: Daniel Loebenberger	
15:00	15:15	0:15	Talk	Jonathan Lennartz & Priya Tomar	Universität Bonn	Approximate K-Means on Encrypted Data
15:15	15:30	0:15	Talk	Hannah Keller	Technische Universität Darmstadt	Privacy-Preserving Clustering
15:30	15:45	0:15	Talk	Felix Dörre	Karlsruhe Institute of Technology	Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy
15:45	16:00	0:15	Talk	Marcel Tiepelt	Karlsruhe Institute of Technology	Towards Everlasting Quantum Bit Commitments
16:00	16:30	0:30	**Coffee Break**		Next session chair: Frederik Armknecht	
16:30	17:30	1:00				Fachgruppentreffen & Wahl