Krypto-Tag@genua, 07/08 June 2018

Donnerstag, 07.06.2018			Art	Speaker	Affiliation	Title
12:00	13:00	1:00	**Reception and Lunch**			
13:00	13:05	0:05	Welcome	Daniel Loebenberger	genua	Introduction
13:05	13:10	0:05	Welcome	Michael Nüsken	b-it, Bonn	Hello from GI Leitungsgremium
13:10	13:15	0:05	Welcome	Kai Dörnemann	genua	Welcome to genua
13:15	13:30	0:15	Welcome	Alexander von Gernler	GI Vizepräsident / genua	Address of Welcome of the Vice President of the GI
13:30	14:00	0:30	Talk	Stefan-Lukas Gazdag	genua	Post-Quantum Software Updates
14:00	14:30	0:30	**Coffee Break**			
14:30	15:30	1:00	*Discussion*	All		Cryptography in Theory and Practice: An Area of Conflict?
15:30	16:00	0:30	**Coffee Break**			
16:00	16:25	0:25	Talk	Tim Fritzmann	TU München	Error-Correcting Codes for Lattice-Based Key Exchange
16:25	16:50	0:25	Talk	Thomas Schamberger	TU München	Post-quantum security: Power Analysis of NTRUEncrypt
16:50	17:15	0:25	Talk	Andreas Zankl	Fraunhofer AISEC	DATA – Differential Address Trace Analysis
17:15	17:30	0:15				
17:30	18:00	0:30	GI FG Krypto			GI Fachgruppentreffen "Angewandte Kryptologie'
18:00	19:00	1:00	„Kofferpause“			
19:00			**Social Event**			
Freitag, 08.06.2018			**Art**	**Speaker**	**Affiliation**	**Title**
8:30	9:00	0:30	**Coffee & „Brezen“**			
9:00	9:30	0:30	Tour		genua	genua Showroom
9:30	10:15	0:45	Talk	Kai Mindermann	Uni Stuttgart	CryptoExamples: Secure, minimal, complete, copyable and tested code examples for Crypto APIs
10:15	10:45	0:30	**Coffee Break**			
10:45	11:15	0:30	Talk	Manish Kumar	TU Darmstadt	Advanced Reconfigurable Physical Unclonable Functions (AR-PUFs) and Their Security Applications
11:15	11:40	0:25	Talk	Yufan Fan	TU Darmstadt	Addressing the Effects of Temperature Variations on Intrinsic Memory-Based Physical Unclonable Functions
11:40	12:00	0:20	**Coffee Break**			
12:00	12:20	0:20	Talk	Christoph Frisch	TU München	Wiretap Coding in the Context of PUFs
12:20	12:45	0:25	Talk	Paul Walther	Universität Dresden	Chains and Whips - An approach to lighweight MACs
12:45	13:45	1:00	**Lunch**			Greek Food