Kryptotag Bosch, 6./7. September 2018

Donnerstag, 06.09.2018			Art	Speaker	Affiliation	Title
13:00	13:30	0:30	**Get Together**			
13:30	13:35	0:05	Welcome	Michael Nüsken	b-it, Bonn	Hello
13:35	13:50	0:15	*Keynote Talk*	Christopher Huth	Bosch, CR/AEX4	Welcome at Bosch
13:50	14:05	0:15	Talk	Daniel Günther	TU Darmstadt	Private Function Evalutation with Universal Circuits
14:05	14:20	0:15	Talk	Andreas Schaffhauser	University of Applied Sciences in Saarbrücken, FernUniversität in Hagen	Algebraic Analysis of the Initialization Phase Grain Version 1 using a Degree-Oriented Interpolation Technique
14:20	14:35	0:15	Talk	Patrick Struck	TU Darmstadt	Challenges in Post-Quantum Security Reductions
14:35	14:55	0:20	**Coffee Break**			
14:55	15:10	0:15	Talk	Markus Klingenstein	Bosch, BEG/ESB2	Hardware Accelerated Sender Identi cation for the Controller Area Network
15:10	15:25	0:15	Talk	Oleg Schell	KIT; Bosch, BEG/ESB2	Machine Learning Based Sender Identification for Controller Area Network
15:25	15:40	0:15	Talk	Friedrich Wiemer	HGI - Ruhr-University Bochum	BISON - Instantiating the Whitened Swap-Or-Not Construction
15:40	15:55	0:15	Talk	Dan Kreiser	IHP, Frankfurt/Oder	HCCA against Montgomery kP Design
15:55	16:15	0:20	**Coffee Break**			
16:15	16:30	0:15	Talk	Christian Wittke	IHP, Frankfurt/Oder	Placement of Gates in ECC Designs
16:30	16:45	0:15	Talk	Petryk Dmytro	IHP, Frankfurt/Oder	Optical Fault Injections: Most Often Used Setups
16:45	17:00	0:15	Talk	Ievgen Kabin	IHP, Frankfurt/Oder	Low-Cost Countermeasure against Horizontal Bus and Address-Bit SCA
17:00	17:15	0:15	Talk	Ievgen Kabin	IHP, Frankfurt/Oder	Comments On: Constant Time Modular Inversion
17:15	18:15	1:00	"Kofferpause"			
18:15			**Excursion**			
Freitag, 07.09.2018			**Art**	**Speaker**	**Affiliation**	**Title**
9:00	10:00	1:00	Guided tour			
10:00	10:20	0:20	**Coffee Break**			
10:20	10:35	0:15	Talk	Eike Stadtländer	Universität Bonn	Automatic Security Analysis in the Symbolic Model using Tamarin-Prover
10:35	10:50	0:15	Talk	Jakob Nussbaumer	Universität Bonn	Cryptographic Game-style language in EasyCrypt
10:50	11:05	0:15	Talk	Daniel Rausch	SEC - University of Stuttgart	Universal Composability: A Comparison of Different Models
11:05	11:25	0:20	**Coffee Break**			
11:25	11:40	0:15	Talk	Amos Treiber	TU Darmstadt	Examining Leakage from Access Counts in ORAM Constructions
11:40	11:55	0:15	Talk	Oleksandr Tkachenko	TU Darmstadt	Privacy-Preserving Genomics on a Large Scale
11:55	12:10	0:15	Talk	Marcel Fourné	Universität Duisburg-Essen	Can Verification of Cryptographic Libraries be liberated from the von Neumann Style?
12:10	12:25	0:15	GI FG Krypto			GI Fachgruppentreffen “Angewandte Kryptographie”
12:25	13:25	1:00	**Lunch**			