Kryptotag IHP, 7./8. Dezember 2017

Donnerstag, 7. Dezember 2017			Art	Speaker	Affiliation	Title
13:00	13:30	0:30	**Get Together**			Zusammentreffen (mit kleinem Imbiss) mit Teilnehmer 5. Technologie- und Anwendungs-Dialoges „No safety without security“
13:30	13:35	0:05	Welcome	Michael Nüsken	b-it, Bonn	Hello
13:35	14:05	0:30	*Keynote Talk*	Peter Langendörfer	IHP	Welcome
14:05	14:35	0:30	Talk	Zoya Dyka	IHP	Low-cost and high effcient horizontal attacks against ECDSA
14:35	15:05	0:30	Talk	Zoya Dyka	IHP	Improving DEMA attack results using different compression methods
15:05	15:30	0:25	**Coffee Break**			
15:30	16:00	0:30	Talk	Jäschke Angela	Uni Mannheim	(Finite) Field Work: Choosing the Best Encoding of Numbers for FHE Computation
16:00	16:30	0:30	Talk	Nikolaos Athanasios Anagnostopoulos	TU Darmstadt	An extensive classi cation and analysis of attacks against Physical Unclonable Functions (PUFs)
16:30	16:55	0:25	**Coffee Break**			
16:55	17:25	0:30	Talk	Ravi Sarangdhar	TU Darmstadt	An investigation of the effects of radiation on current key storage solutions and on Physical Unclonable Functions (PUFs) being used as key storage
17:25	17:55	0:30	Talk	Frank Vater	IHP	Secure Programming and Debug Interface
17:55	19:00	1:05	"Kofferpause"			
19:00			**Excursion**			
Freitag, 8. Dezember 2017			**Art**	**Speaker**	**Affiliation**	**Title**
9:00	9:55	0:55	Guided tour			
9:55	10:20	0:25	**Coffee Break**			
10:20	10:30	0:10	Talk	Ernst-Günter Giessmann	HU Berlin	Is This RSA Key Weak?
10:30	11:00	0:30	Talk	Elisabeth Vogel	IHP	Localized EMA as a mean to nd spatial and time SCA leakage sources
11:00	11:30	0:30	Talk	Zoya Dyka	IHP	Implementation of a Latency Optimized ECC-Design
11:30	12:00	0:30	Talk	Wael Adi	TU Braunschweig	Secret Unknown Cipher Concept as Physical Security Anchor
12:00	13:00	1:00	**Lunch**			