Wednesday, 03th February 2010	
18:00 - 20:00	Registration

Thursday, 04th February 2010			
	Session	Authors	Title
09:00	Registration		
10:15	Welcome, Opening Remarks		
10:30	Invited Talk #1	Pankaj Rohatgi, Cryptographic Research, USA	TBA
11:30	Session 1: Side Channel Attacks I	Oliver Schimmel, Paul Duplys, Eberhard Boehl, Jan Hayek and Wolfgang Rosenstiel	Correlation power analysis in frequency domain
12:00		Philipe Hoogvorst.	The Variance Power Attack
12:30	Lunch		
13:30	Session 2: Side Channel Attacks II	Sylvain Guilley, Olivier Meynard, Laurent Sauvage and Jean-Luc Danger	Side-Channel Analysis based on Rainbow Tables
14:00		Florent Flament, Houssem Maghrebi, Moulay Aziz Elabid, Jean-Luc Danger, Sylvain Guilley and Laurent Sauvage	About Probability Density Function Estimation for Side Channel Analysis
14:30		Pierre-Louis Cayrel and Falko Strenzke	Side-channels attacks in code-based cryptography
15:00	Coffee Break		
15:30	Invited Talk #2	Ingrid Verbauwhede, KU Leuven, Belgium	TBA
16:30	Session 3: Tools	Daniel Shumow and Peter Montgomery	Side Channel Leakage Profiling in Software
17:00		Toshihiro Katashita, Akashi Satoh, Katsuya Kikuchi, Hiroshi Nakagawa and Masahiro Aoyagi	DPA Characteristic Evaluation of SASEBO for Board Level Simulation
17:30		Naofumi Homma, Tohoku University, Japan	SASEBO GII
18:00	Hotel CheckIn / Transfer		
19:00 - 22:30	Social Event „Weststadtbar“		

Friday, 05th February 2010			
	Session	Authors	Title
09:15		CASCADE	Constructive Side Channel Analysis and Secure Design
10:00	Coffee Break		
10:30	Session 4: Protection & Design	Colin Walter	Right-to-Left or Left-to-Right Exponentiation?
11:00		Georg T. Becker, Markus Kasper and Christof Paar	Side-Channel based Watermarks for IP Protection
11:30		Johann Groszschaedl	Performance and Security Aspects of Client-Side SSL/TLS Processing on Mobile Devices
12:00	Lunch		
13:00	Session 5: Preprocessing & Preselection	Yongdae Kim, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki and Akashi Satoh,	Biasing power traces to improve correlation in power analysis attacks
13:30		Martin Baer, Hermann Drexler and Jürgen Pulkus	Improved Point of Interest Search for Template Attacks
14:00	Invited Talk #3	Stefan Mangard, Infineon, Germany	Constructive Power Analysis in Practice
15:00	Coffee Break		
15:30	Session 6: Counter-measures	Christoph Herbst and Marcel Medwe	Randomizing the Montgomery Multiplication to Repel Template Attacks on Multiplicative Masking
16:00		Guillaume Fumaroli, Sylvain Lachartre, Ange Martinelli and Louis Goubin	Towards a Third Order Side Channel Analysis Resistant Table Recomputation Method
16:30	Feedback Session		
17:00	Closing Remarks, Goodbye		