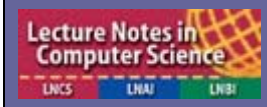

CARDIS 2008, Royal Holloway University of London
Monday, 8th September 2008

	Welcome Reception
18:00-19:30	**Registration and Drinks (Arts Building, Lecture Theatre 1)**

Tuesday, 9th September 2008

08:00	**Registration (Arts Building)**	
08:45-09:00	**Opening Session**	
	Organising and Program Committee Chairs	
09:00	**Session - I: Java and Smart Card (Chair: Keith Mayes)**	
09:00-09:30	**Malicious Code on Java Card Smartcards: Attacks and Countermeasures**	*Wojciech Mostowski and Erik Poll*
09:30-10:00	**Static program analysis for Java Card applets**	*Vasilios Almaliotis, Alexandros Loizidis, Panagiotis Katsaros, Panagiotis Louridas, Diomidis Spinellis*
10:00-10:30	**On Practical Information Flow Policies for Java-Enabled Multiapplication Smart Cards**	*Dorina Ghindici and Isabelle Simplot-Ryl*
10:30	*Coffee*	
11:00	**Session - II: Fault attacks (Chair: Kostas Markantonakis)**	
11:00-11:30	**New Differential Fault Analysis on AES Key Schedule: Two Faults are enough**	*Chong Hee Kim and Jean-Jacques Quisquater*
11:30-12:00	**DSA Signature Scheme Immune to the Fault Cryptanalysis**	*Maciej Nikodem*
12:00-14:00	*Lunch (Founder's Building Dining Hall)*	
14:00	**Session - III: Efficient Implementations (Chair: Jean-Jacques Quisquater)**	
14:00-14:30	**A Black Hen Lays White Eggs: Bipartite Multiplier out of Montgomery One for On-Line RSA Verification**	*Masayuki Yoshino, Katsuyuki Okeya, Camille Vuillaume*
14:30-15:00	**Ultra-Lightweight Implementations for Smart Devices - Security for 1000 Gate Equivalents;**	*Carsten Rolfes, Axel Poschmann, Gregor Leander, Christof Paar*
15:00-15:30	**Fast Hash-Based Signatures on Constrained Devices**	*Sebastian Rohde, Erik Dahmen, Thomas Eisenbarth, Johannes Buchmann, Christof Paar*
15:30	*Coffee*	
16:00-17:00	**Session - IV: Invited talk I (Chair: Gilles Grimaud)**	
	"Getting Started with Java Card 3.0 Platform" by Ram Banerjee and Anki Nelaturu, Sun Microsystems.	
19:30	*Gala Dinner (Founder's Building Dining Hall)*	

Wednesday, 10th September 2008

08:30-09:00	**Registration (Arts Building)**	
09:00	**Session - V: Embedded Infrastructure (Chair: Isabelle Simplot-Ryl)**	
09:00-09:30	**Fraud Detection and Prevention in Smart-Card Based Environments Using Artificial Intelligence**	*Wael William Malek, Keith Mayes, Kostas Markantonakis*
09:30-10:00	**TEM: A new secure device model**	*Luis F. G. Sarmenta, Victor Costan, Marten van Dijk, Srinivas Devadas*
10:00-10:30	**Management of Multiple Secure Elements in NFC-Devices**	*Gerald Madlmayr, Josef Langer, Josef Scharinger*
10:30	*Coffee*	
11:00	**Session - VI: RFIDs (Chair: Gerhard Hancke)**	
11:00-11:30	**Coupon Recalculation for the GPS Authentication Scheme**	*Georg Hofferek and Johannes Wolkerstorfer*
11:30-12:00	**Provably secure grouping-proofs for RFID tags**	*Mike Burmester, Breno de Medeiros, Rossana Motta*
12:00	*Lunch (Founder's Building Dining Hall)*	
14:00	**Session - VII: Side-Channel Attacks (Chair: Chong Hee Kim)**	
14:00-14:30	**Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices**	*Pierre-Louis Cayrel, Philippe Gaborit, Emmanuel Prouff*
14:30-15:00	**A Practical DPA Countermeasure with BDD Architecture**	*Toru Akishita, Masanobu Katagi, Yoshikazu Miyato, Asami Mizuno, Kyoji Shibutani*
15:00-15:30	**SCARE of an Unknown Hardware Feistel Implementation**	*Denis Real, Mhamed Drissi, Vivien Dubois, Anne Marie Guillou, Frederic Valette*
15:30	*Coffee*	
16:00-17:00	**Session - VII: Invited talk II (Chair: François-Xavier Standaert)**	
	"Recent Advances in Electronic Cash Design" by Aline Gouget, Security Labs, Gemalto	
19:00	*BBQ (Founder's Building – Crosslands)*	

Thursday, 11th September 2008

09:00	**Session - IX: Applications (Chair: Eduard de Jong)**	
09:00-09:30	**Evaluation of Java Card Performance**	*Samia Bouzefrane, Julien Cordry, Hervé Meunier, Pierre Paradinas*
09:30-10:00	**Application of Network Smart Cards to Citizens Identification Systems**	*Joaquin Torres, Mildrey Carbonell, Jesus Tellez, Jose M. Sierra*
10:00-10:30	**SmartPRO: A Digital Content Protection With Personal Smart Cards**	*Alain Durand, Marc Eluard, Sylvain Lelievre, Christophe Vincent*
10:30	*Coffee*	
11:00	**Session - X: Physical Security (Chair: Mike Burmester)**	
11:00-11:30	**A Practical Attack on the MIFARE Classic**	*Gerhard de Koning Gans, Jaap-Henk Hoepman, Flavio D. Garcia*
11:30-12:00	**A Chemical Memory Snapshot**	*Jörn-Marc Schmidt*
12:00	*Closing Remarks* *Lunch (Founder's Building Dining Hall)*	