CHES 2012 Program

[Sunday, 9/9] [Monday, 10/9] [Tuesday, 11/9] [Wednesday, 12/9]

Sunday, September 9

Time	Event		
	Session	Authors	Title
08:45 - 09:00	Registration De Nieuwe Valk, Tiensestraat 41		
09:00 - 10:45	Tutorial 1 De Nieuwe Valk, Tiensestraat 41	Junfeng Fan, KU Leuven	Cryptographic hardware: how to make it cool, fast and unbreakable
10:45 - 11:10	Morning Break		
11:10 - 12:25	Tutorial 1 De Nieuwe Valk, Tiensestraat 41	Junfeng Fan, KU Leuven	Cryptographic hardware: how to make it cool, fast and unbreakable
12:25 - 13:40	Lunch		
13:40 - 15:10	Tutorial 2 De Nieuwe Valk, Tiensestraat 41	Diego Aranha, Univ. of Brasília	Efficient binary field arithmetic and applications to curve-based cryptography
15:10 - 15:35	Afternoon Break		
15:35 - 17:00	Tutorial 2 De Nieuwe Valk, Tiensestraat 41	Diego Aranha, Univ. of Brasília	Efficient binary field arithmetic and applications to curve-based cryptography
17:00 - 18:00			
18:00 - 18:30	Registration Auditorium Pieter De Somer, Deberiotstraat 24		
18:30 - 21:00	Reception and Registration Pauscollege, Hogeschoolplein 3 (if raining: Auditorium Pieter De Somer, Deberiotstraat 24)		

Monday, September 10
Auditorium Pieter De Somer, Deberiotstraat 24

Time	Event		
	Session	Authors	Title
08:00 - 08:45	Registration		
08:45 - 09:00	Welcome		
9:00 - 10:15	Intrusive Attacks and Countermeasures Chair: Matthias Wagner	Sebastien Briais (Secure-IC), Stéphane Caron (ENS), Jean-Michel Cioranesco (Univ. Paris 2), Jean-Luc Danger, Sylvain Guilley (TELECOM ParisTech), Jacques-Henri Jourdan, Arthur Milchior, David Naccache (ENS), Thibault PorteBoeuf (Secure-IC)	3D hardware canaries
		Sergei Skorobogatov (Univ. of Cambridge), Christopher Woods (Quo Vadis Labs)	Breakthrough silicon scanning discovers backdoor in military chip
		Alexander Schloesser, Dmitry Nedospasov, Juliane Kraemer, Susanna Orlic, Jean-Pierre Seifert (TU Berlin)	Simple photonic emission analysis of AES

10:15 - 10:45	Morning Break + Posters		
10:45 - 12:25	Masking Chair: Stefan Mangard	Andrew Moss (Blekinge Institute of Technology), Elisabeth Oswald, Dan Page, Michael Tunstall (Univ. of Bristol)	Compiler assisted masking
		Begul Bilgin, Svetla Nikova (KU Leuven), Ventzislav Nikov (NXP Semiconductors), Vincent Rijmen(KU Leuven and TU Gratz), G. Stütz (TU Graz)	Threshold implementations of all 3x3 and 4x4 S-boxes
		Amir Moradi, Oliver Mischke (RU Bochum)	How far should theory be from practice? Evaluation of a countermeasure
		Blandine Debraize (Gemalto)	Efficient and provably secure methods for switching from arithmetic to boolean masking
12:25 - 14:00	Lunch Salons Georges, Hogeschoolplein 15		
14:00 - 14:50	Improved Fault Attacks and Side Channel Analysis (Part 1) Chair: Marc Joye	Subhadeep Banik, Subhamoy Maitra, Santanu Sarkar (IST)	A differential fault attack on the grain family of stream ciphers
		Yossef Oren (Tel Aviv Univ.), Mathieu Renauld, François-Xavier Standaert (UCL Crypto Group), Avishai Wool (Tel Aviv Univ.)	Algebraic side-channel analysis beyond the Hamming weight leakage model
14:50 - 15:10	Afternoon Break + Posters		
15:10 - 16:00	Improved Fault Attacks and Side Channel Analysis (Part 2) Chair: Marc Joye	Oscar Reparaz, Benedikt Gierlichs, Ingrid Verbauwhede (KU Leuven)	Selecting time samples for multivariate DPA attacks
		Benoît Gérard, François-Xavier Standaert (UCL Crypto Group)	Unified and optimized linear collision attacks and their application in a non-profiled setting
16:00 - 16:30	Posters		
16:30 - 17:30	Brewery Visit (Group 1) Buses depart at 16:30 from Deberiotstraat 24		Walking Tour Departs from Deberiotstraat 24
17:30 - 18:30	Brewery Visit (Group 2) Buses depart at 17:30 from Deberiotstraat 24		
18:00 - 19:30	Walking Dinner		
19:30 - 21:30	Rump Session		
21:30 - 22:15	Big Band Concert		

Tuesday, September 11
Auditorium Pieter De Somer, Deberiotstraat 24

Time	Event		
	Session	Authors	Title
08:45 - 09:00	Registration		
09:00 - 10:15	Leakage Resiliency and Security Analysis Chair: Olivier Pereira	Marcel Medwed, François-Xavier Standaert (UCL Crypto Group), Antoine Joux (Univ. de Versailles)	Towards super-exponential side-channel security with efficient leakage-resilient PRFs
		Sebastian Faust (Aarhus Univ.), Krzysztof Pietrzak, Joachim Schipper (IST Austria)	Practical leakage-resilient symmetric cryptography
		Yunsi Fei (Northeastern Univ., Boston), Qiasi Luo (Marvell Technology), A. Adam Ding (Northeastern	A statistical model for DPA with novel algorithmic confusion analysis

		Univ., Boston)	
10:15 - 10:45	Morning Break + Posters		
10:45 - 12:25	Physically Unclonable Functions Chair: Nele Mentens	Urich Rührmair (TU München), Marten van Dijk (RSA Laboratories)	Practical security analysis of PUF-based two-player protocols
		Vincent van der Leest (Intrinsic-ID), Bart Preneel (KU Leuven and IBBT), Erik van der Sluis (Intrinsic-ID)	Soft decision error correction for compact memory-based PUFs
		Stefan Katzenbeisser, Ünal Kocabas (TU Darmstadt), Vladimir Rozic (KU Leuven), Ahmad-Reza Sadeghi (TU Darmstadt), Ingrid Verbauwhede (KU Leuven), Christian Wachsmann (TU Darmstadt)	PUFs: myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) poured in silicon
		Roel Maes, Anthony Van Herrewege, Ingrid Verbauwhede (KU Leuven and IBBT)	PUFKY: a fully functional PUF-based cryptographic key generator
12:25 - 14:00	Lunch Salons Georges, Hogeschoolplein 15		
14:00 - 15:00	Invited Talk I Chair: Patrick Schaumont	Steven Murdoch, Univ. of Cambridge	Banking security: attacks and defences
15:00 - 15:20	Afternoon Break + Posters		
15:20 - 16:10	Efficient Implementations (Part 1) Chair: Kazuo Sakiyama	Daniel J. Bernstein, Peter Schwabe (Univ. of Illinois at Chicago and Academia Sinica)	NEON crypto
		Stefan Heyse, Tim Güneysu (RU Bochum)	Towards one cycle per bit asymmetric encryption: code-based cryptography on reconfigurable hardware
16:10 - 16:20	Intermezzo		
16:20 - 17:10	Efficient Implementations (Part 2) Chair: Kazuo Sakiyama	Tung Chou (Academia Sinica), Chen-Mou Cheng (National Taiwan Univ. and Intel Connected Context Computing Center), Ruben Niederhagen (Eindhoven Univ. of Technology and Academia Sinica), Bo-Yin Yang (Academia Sinica)	Solving quadratic equations with XL on parallel architectures
		Peter Czypek, Stefan Heyse, Enrico Thomae (RU Bochum)	Efficient implementations of MQPKS on constrained devices
17:10 - 19:30			
19:30 - 22:15	Banquet Faculty Club, Groot Begijnhof 14		

Wednesday, September 12
Auditorium Pieter De Somer, Deberiotstraat 24

Time	Event		
	Session	Authors	Title
08:45 - 09:00	Registration		
		Stéphanie Kerckhof, François Durvaux, Cédric Hocquet,	Towards green cryptography: a comparison of

09:00 - 10:15	Lightweight Cryptograhy Chair: Jens-Peter Kaps	David Bol, François-Xavier Standaert (UCL Crypto Group)	lightweight ciphers from the energy viewpoint
		Seiichi Matsuda (Sony Corporation), Shiho Moriai (NICT)	Lightweight cryptography for the cloud: exploit the power of bitslice implementation
		Miroslav Knezevic, Ventzislav Nikov, Peter Rombouts (NXP Semiconductors)	Low-latency encryption - is "lightweight = light + wait"?
10:15 - 10:45	Morning Break + Posters		
10:45 - 12:25	We still love RSA Chair: Cetin Koc	Pierre-Alain Fouque (ENS / INRIA Rennes), Nicolas Guillermin, Delphine Leresteux (DGA IS), Mehdi Tibouchi (NTT Secure Platform Laboratories), Jean-Christophe Zapalowicz (INRIA Rennes)	Attacking RSA-CRT signatures with faults on Montgomery multiplication
		Michael Vielhaber (Hochschule Bremerhaven)	Reduce-by-feedback: timing resistant and DPA-aware modular multiplication, plus: how to break RSA by DPA
		Santanu Sarkar, Subhamoy Maitra (ISI)	Side channel attack to actual cryptanalysis: breaking CRT-RSA with low weight decryption exponents
12:25 - 14:00	Lunch Salons Georges, Hogeschoolplein 15		
14:00 - 15:00	Invited Talk II Chair: Emmanuel Prouff	Christof Tarnovsky, Flylogic Engineering	(In)security of commonly found smart cards
15:00 - 15:20	Afternoon Break + Posters		
15:20 - 16:10	Hardware Implementations (Part 1) Chair: Viktor Fischer	Chester Rebeiro, Sujoy Sinha Roy, Debdeep Mukhopadhyay (IIT)	Pushing the limits of high-speed GF(2^m) elliptic curve scalar multiplication on FPGAs
		Norman Göttert, Thomas Feller, Michael Schneider, Sorin A. Huss, Johannes Buchmann (TU Darmstadt)	On the design of hardware building blocks for modern lattice-based encryption schemes
16:10 - 16:20	Intermezzo		
16:20 - 17:10	Hardware Implementations (Part 2) Chair: Viktor Fischer	Tim Güneysu (RU Bochum), Vadim Lyubashevsky (INRIA / ENS), Thomas Pöppelmann (RU Bochum)	Practical lattice-based cryptography: a signature scheme for embedded systems
		Jen-Wei Lee, Szu-Chi Chung, Hsie-Chia Chang, Chen-Yi Lee (National Chiao Tung Univ.)	An efficient countermeasure against correlation power-analysis attacks with randomized Montgomery operations for DF-ECC processor
17:10 - 17:30	Closing		