PROGRAM EUROCRYPT 2015

MONDAY, April 27th		
9:00	Welcome	
9:15	**Invited Talk:** A Privacy Research Roadmap for a National Privacy Research Strategy, *Tal Rabin, IBM T.J.Watson Research Center, USA*	
10:15	Coffee Break	
	R-Track	**I-Track**
10:40	**Random Number Generators** A Provable-Security Analysis of Intel's Secure Key RNG, *Thomas Shrimpton; R. Seth Terashima* A Formal Treatment of Backdoored Pseudorandom Generators, *Yevgeniy Dodis; Chaya Ganesh; Alexander Golovnev; Ari Juels; Thomas Ristenpart*	**Signatures** Universal Signature Aggregators, *Susan Hohenberger; Venkata Koppula; Brent Waters* Fully Structure-Preserving Signatures and Shrinking Commitments, *Masayuki Abe; Markulf Kohlweiss; Miyako Ohkubo; Mehdi Tibouchi*
11:30	Swap	
11:35	**Number Field Sieve** Improving NFS for the discrete logarithm problem in non-prime finite fields, *Razvan Barbulescu; Pierrick Gaudry; Aurore Guillevic; François Morain* The Multiple Number Field Sieve with Conjugation and Generalized, *Joux-Lercier Methods; Cécile Pierrot*	**Zero-Knowledge Proofs** Disjunctions for Hash Proof Systems: New Constructions and Applications, *Michel Abdalla; Fabrice Benhamouda; David Pointcheval* Quasi-Adaptive NIZK for Linear Subspaces Revisited, *Eike Kiltz; Hoeteck Wee*
12:30	Lunch	
14:00	**Algorithmic Cryptanalysis** Better Algorithms for LWE and LWR, *Alexandre Duc; Florian Tramèr; Serge Vaudenay* On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes, *Alexander May; Ilya Ozerov*	**Leakage-Resilient Cryptography** Leakage-Resilient Circuits Revisited - Optimal Number of Computing Components without Leak-free Hardware, *Dana Dachman-Soled; Feng-Hao Liu; Hong-Sheng Zhou* Noisy Leakage Revisited *Stefan Dziembowski; Sebastian Faust; Maciej Skórski*
14:50	Swap	
14:55	**Symmetric Cryptanalysis I** Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE, *Itai Dinur* A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro, *Gregor Leander; Brice Minaud; Sondre Rønjom*	**Garbled Circuits** Privacy-Free Garbled Circuits with Applications To Efficient Zero-Knowledge, *Tore Kasper Frederiksen; Jesper Buus Nielsen; Claudio Orlandi* Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits using Half Gates, *Samee Zahur; Mike Rosulek; David Evans*
15:45	Coffee Break	
16:15	**Symmetric Cryptanalysis II** Structural Evaluation by Generalized Integral Property, *Yosuke Todo* Cryptanalysis of SP Networks with Partial Non-Linear Layers, *Achiya Bar-On; Itai Dinur; Orr Dunkelman; Nathan Keller; Virginie Lallemand; Boaz Tsaban*	**Crypto Currencies** One-out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin, *Jens Groth; Markulf Kohlweiss* The Bitcoin Backbone Protocol: Analysis and Applications, *Juan Garay; Aggelos Kiayias; Nikos Leonardos*

TUESDAY, April 28th		
9:00	**Best paper and honourable mentions** Cryptanalysis of the Multilinear Maps over the Integers, *Jung Hee Cheo; Kyoohyung Han; Changmin Lee; Hansol Ryu; Damien Stehlé* Robust Authenticated-Encryption: AEZ and the Problem that it Solves, *Viet Tung Hoang; Ted Krovetz; Phillip Rogaway* On the behaviors of affine equivalent Sboxes regarding differential and linear attacks, *Anne Canteaut; Joëlle Roué*	
10:15	Coffee Break	
	R-Track	**I-Track**
10:40	**Hash Functions** The Sum Can Be Weaker Than Each Part, *Gaëtan Leurent; Lei Wang* SPHINCS: practical stateless hash-based signatures, *Daniel J. Bernstein; Daira Hopwood; Andreas Hülsing; Tanja Lange; Ruben Niederhagen; Louiza Papachristodoulou; Michael Schneider;Peter Schwabe; Zooko Wilcox O'Hearn*	**Secret Sharing** Function Secret Sharing, *Elette Boyle; Niv Gilboa; Yuval Ishai* Linear Secret Sharing Schemes from Error Correcting Codes and Universal Hash Functions, *Ronald Cramer; Ivan Damgaard; Nico Doettling; Serge Fehr; Gabriele Spini*
11:30	Swap	
11:35	**Evaluating Implementations** Making Masking Security Proofs Concrete (Or How to Evaluate the Security of any Leaking Device) *Alexandre Duc; Sebastian Faust; François-Xavier Standaert* Ciphers for MPC and FHE, *Martin Albrecht; Christian Rechberger; Thomas Schneider; Tyge Tiessen; Michael Zohner*	**Outsourcing Computations** Cluster Computing in Zero Knowledge, *Alessandro Chiesa; Eran Tromer; Madars Virza* Hosting Services on an Untrusted Cloud, *Dan Boneh; Divya Gupta; Ilya Mironov; Amit Sahai*
12:30	Lunch	
14:00	**Masking** Verified Proofs of Higher-Order Masking, *Gilles Barthe; Sonia Belaid; Francois Dupressoir; Pierre-Alain Fouque; Benjamin Gregoire; Pierre-Yves Strub* Inner Product Masking Revisited, *Josep Balasch; Sebastian Faust; Benedikt Gierlichs*	**Obfuscation and E-Voting** How to Obfuscate Programs Directly, *Joe Zimmerman* End-to-End Verifiable Elections in the Standard Model, *Aggelos Kiayias; Thomas Zacharias; Bingsheng Zhang*
18:30	Walking Diner and Rump Session	

WEDNESDAY, April 29th		
9:15	**Invited talk:** Practical Applications of Homomorphic Encryption**,** *Kristin Lauter, Microsoft Research, USA*	
10:15	Coffee Break	
	R-Track	**I-Track**
10:40	**Fully Homomorphic Encryption I** Fully Homomophic Encryption over the Integers Revisited, *Jung Hee Cheo; Damien Stehle* (Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces, *Koji Nuida; Kaoru Kurosawa*	**Multi-Party Computations** Cryptographic Agents: Towards a Unified Theory of Computing on Encrypted Data, *Shashank Agrawal; Shweta Agrawal; Manoj Prabhakaran* Executable Proofs, Input-Size Hiding Secure Computation and a New Ideal World, *Melissa Chase; Rafail Ostrovsky; Ivan Visconti*
11:30	Swap	
11:35	**Related-Key Attacks** KDM-CCA Security from RKA Secure Authenticated Encryption, *Xianhui Lu; Bao Li; Dingding Jia* On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks, *Benoit Cogliati; Yannick Seurin*	**Encryption** Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation, *Dan Boneh; Kevin Lewi; Mariana Raykova; Amit Sahai; Mark Zhandry; Joe Zimmerman* Improved Dual System ABE in Prime-Order Groups via Encodings, *Jie Chen; Romain Gay; Hoeteck Wee*
12:30	Lunch	
14:00	**Fully Homomorphic Encryption II** FHEW: Bootstrapping in less than a second, *Léo Ducas; Daniele Micciancio* Bootstrapping for HElib, *Shai Halevi; Victor Shoup*	**Resistant Protocols** Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model*, Mihir Bellare; Viet Tung Hoang* Cryptographic Reverse Firewalls, *Ilya Mironov; Noah Stephens-Davidowitz*
14:50	Swap	
14:55	**Efficient Two-Party Protocols** More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries, *Gilad Asharov; Yehuda Lindell; Thomas Schneider; Michael Zohner* How to Efficiently Evaluate RAM Programs with Malicious Security, *Arash Afshar; Zhangxiang Hu; Payman Mohassel; Mike Rosulek*	**Key Exchange** Mind the Gap: Modular Machine-checked Proofs of One-Round Key *Exchange Protocols, Gilles Barthe; Juan Manuel Crespo; Yassine Lakhnech; Benedikt Schmidt* Authenticated Key Exchange from Ideal Lattices, *Jiang Zhang; Zhenfeng Zhang; Jintai Ding; Michael Snook; Özgür Dagdelen*
15:45	Coffee Break	
16:00	**IACR membership meeting**	
20:00	Banquet	

THURSDAY, April 30th		
9:15	**Invited talk:** Threshold Implementations**,** *Vincent Rijmen, KU Leuven, Belgium*	
10:15	Coffee Break	
	R-Track	**I-Track**
10:40	**Symmetric Cryptanalysis III** Cube Attacks and Cube-attack-like Cryptanalysis on the Round-reduced Keccak Sponge Function, *Itai Dinur; Pawel Morawiecki; Josef Pieprzyk; Marian Srebrny; Michal Straus* Twisted Polynomials and Forgery Attacks on GCM, *Mohamed Ahmed Abdelraheem; Peter Beelen; Andrey Bogdanov; Elmar Tischhauser*	**Quantum Cryptography** Non-interactive zero-knowledge proofs in the quantum random oracle model, *Dominique Unruh* Privacy Amplification in the Isolated Qubits Model, *Yi-Kai Liu*
11:30	Swap	
11:35	**Lattices** Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices, *Vadim Lyubashevsky; Thomas Prest*	**Discrete Logarithms** Generic Hardness of the Multiple Discrete Logarithm Problem *Aaram Yun*
12:00	Lunch	