Program PQC 2010

last update: 19.05.2010

Time	Wednesday 26th		Thursday 27th	
0830		Registration	Design of Encryption Schemes	Key Exchange and Encryption Schemes Based on Non-commutative Skew Polynomials *Delphine Boucher, Philippe Gaborit, Willi Geiselmann, Olivier Ruatta, and Felix Ulmer*
0900				Designing a Rank Metric Based McEliece Cryptosystem *Pierre Loidreau*
0930	Cryptanalysis of Multivariate Systems	Properties of the Discrete Differential with Cryptographic Applications *Daniel Smith-Tone*		Secure Variants of the Square Encryption Scheme *Crystal Lee Clough and Jintai Ding*
1000		Growth of the Ideal Generated by a Quadratic Boolean Function *Jintai Ding, Timothy J. Hodges, and Victoria Kruglov*		Low-Reiter: Niederreiter Encryption Scheme for Embedded Microcontrollers *Stefan Heyse*
1030		Coffee Break		Coffee Break
1100		Mutant Zhuang-Zi Algorithm *Jintai Ding and Dieter S. Schmidt*		**Invited Talk** The Learning with Errors Problem *Oded Regev*
1130		Cryptanalysis of Two Quartic Encryption Schemes and One Improved MFE Scheme *Weiwei Cao, Xiuyun Nie, Lei Hu, Xiling Tang, and Jintai Ding*		
1200		Lunch		Lunch
1230				
1300				
1330		**Invited Talk** Provable post-quantum security *Renato Renner*	Design of Signature Schemes	Strongly Unforgeable Signatures and Hierarchical Identity-Based Signatures from Lattices without Random Oracles *Markus Rückert*
1400				Proposal of a Signature Scheme Based on STS Trapdoor *Shigeo Tsujii, Masahito Gotaishi, Kohtaro Tadaki, and Ryo Fujita*
1430	Cryptanalysis of Code-based Systems	Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes *Christian Wieschebrink*		Selecting Parameters for the Rainbow Signature Scheme *Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann*
1500		Grover vs. McEliece *Daniel J. Bernstein*		Coffee Break
1530		Information-Set Decoding for Linear Codes over Fq *Christiane Peters*		Free
1600		Coffee Break		
1630		A Timing Attack against the Secret Permutation in the McEliece PKC *Falko Strenzke*		
1700		Practical Power Analysis Attacks on Software Implementations of McEliece *Stefan Heyse, Amir Moradi, and Christof Paar*		Excursion
1730		Free		
1800				
1830				
1900				Dinner

Time	Friday 28th	
0830	Recent Results	Practical Key Recovery Attacks On Two McEliece Variants *Gregor Leander, Valérie Gauthier Umana*
0855		Ball-collision Decoding *Christiane Peters*
0920		Noisy Diffie-Hellman Procotols *Philippe Gaborit*
0945		A Distinguisher for High Rate McEliece Cryptosystem *Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich*
1010		Selecting Secure Parameters for Lattice-based Cryptography *Markus Rückert, Michael Schneider*
1035		Coffee Break
1100		**Invited Talk** The Road to Post-Quantum Privacy *Gregory Neven*
1130		
1200		Lunch
1300		
1330		
1400	Recent Results	Sieving for Shortest Vectors in Ideal Lattices *Michael Schneider*
1425		Security analysis of rSTS type multivariate public key cryptosystems against algebraic attack using Gröbner bases *Ryo Fujita*
1450		Conjugate Searching Problem over Braid Groups vs. Hidden Subgroup *Licheng Wang*
1515		McBits & Post-quantum RSA *Daniel J. Bernstein*
1540		Adjourn
1630		Free
1700		
1730		
1800		
1830		
1900		