PQC'11 Programme

Tuesday 29 November 2011

18:30–21:00	**Registration and Reception** in the Howard International House

Wednesday 30 November 2011

8:30	**Registration**
8:45	**Opening remarks**
	Session I: Multivariate Cryptography, chair: Bo-Yin Yang
8:50	*On the Differential Security of Multivariate Public Key Cryptosystems* **Daniel Smith-Tone**
9:25	*On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack* **Koichi Sakumoto**, Taizo Shirai, Harunaga Hiwatari
10:00	*A security analysis of uniformly-layered Rainbow – Revisiting Sato-Araki's non-commutative approach to Ong-Schnorr-Shamir signature towards Post Quantum Paradigm* **Takanori Yasuda**, Kouichi Sakurai
10:35	**Coffee Break**
	Invited Talk I, chair: Johannes Buchmann
11:15	*Predicting Lattice Reduction: Progress and Pitfalls* **Phong Nguyen**
12:15	**Lunch in the Garden Cafeteria of Howard International House**
	Session II: Cryptanalysis I, chair: Tanja Lange
13:45	*Decoding One Out of Many* **Nicolas Sendrier**
14:20	*An Efficient Attack on All Concrete KKS Proposals* Ayoub Otmani, **Jean-Pierre Tillich**
14:55	*Full cryptanalysis of the Chen identification protocol* **Philippe Gaborit**, Julien Schrek, Gilles Zémor
15:30	**Coffee Break**
	Session III: Others, chair: Helger Lipmaa
16:00	*Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies* **David Jao**, Luca De Feo
16:35	*A New Spin on Quantum Cryptography: Avoiding Trapdoors and Embracing Public Keys* Lawrence M. Ioannou, **Michele Mosca**
17:10	**Meeting of the Steering Committee** in the conference room
18:30	**Dinner in the Dining Room B1 of Howard International House**

Thursday 1 December 2011

Session IV: Code-based Cryptography, chair: Nicolas Sendrier	
8:45	*Statistical decoding of codes over $\mathbb{F}_q$* **Robert Niebuhr**
9:20	*Monoidic Codes in Cryptography* Paulo S. L. M. Barreto, Richard Lindner, **Rafael Misoczki**
9:55	*Simplified high-speed high-distance list decoding for alternant codes* **Daniel J. Bernstein**
10:30	**Coffee Break**
Invited Talks II & III, chair: Chen-Mou Cheng	
11:00	*How was Cryptology with Systems of Multivariate Polynomials as Public Keys Conceived* **Tsutomu Matsumoto**
11:45	*Upper and lower bounds of degree of regularity of HFE and its variants* **Jintai Ding**
12:15	**Lunch in the Garden Cafeteria of Howard International House**
14:00	**Excursion**
18:30	**Banquet in the Palace Museum**

Friday 2 December 2011

Session V: New Schemes, chair: Daniel J. Bernstein	
8:45	*XMSS - A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions* Johannes Buchmann, Erik Dahmen, **Andreas Hülsing**
9:20	*Wild McEliece Incognito* Daniel J. Bernstein, Tanja Lange, **Christiane Peters**
9:55	*Efficient Threshold Encryption from Lossy Trapdoor Functions* Xiang Xie, Rui Xue, **Rui Zhang**
10:35	**Coffee Break**
Session VI: Cryptanalyis II, chair: Jintai Ding	
11:00	*Roots of Square: Cryptanalysis of Double-Layer Square and Square+* Enrico Thomae and **Christopher Wolf**
11:35	*General Fault Attacks on Multivariate Public Key Cryptosystems* **Yasufumi Hashimoto**, Tsuyoshi Takagi, Kouichi Sakurai
12:10	**Lunch in the Garden Cafeteria of Howard International House**
Session VII: Implementations, chair: Lim Seongan	
13:40	*Implementation of McEliece based on Quasi-Dyadic Goppa Codes for Embedded Devices* **Stefan Heyse**
14:15	*High-speed Hardware Implementation of Rainbow Signature on FPGAs* **Shaohua Tang**, Haibo Yi, Jintai Ding, Huan Chen, Guomin Chen
Session VIII: Recent Results, chair: TBA	
14:55	*Atom arrays in semiconductors: from quantum computers to quantum encryption* **Enrico Prati**
15:15	*Hidden Pair of Bijection Signature (Part II)* **Masahito Gotaishi**
16:25	**Closing remarks**
16:30	**End & Coffee break**
18:30	**Snack attack at the night market**