Winter School PQCrypto 2016

Monday, February 22	
9:00 – 10:15	Registration
10:15 – 10:30	Opening Remark
10:30 – 12:00	***State of Art of MPKC*** **Jintai Ding (University of Cincinnati)**
12:00 – 13:30	Lunch
13:30 – 15:00	***Lattice-Based Cryptography*** **Phong Nguyen (Inria and CNRS/JFLI and the University of Tokyo)**
15:00 – 15:30	Coffee Break
15:30 – 17:00	***Gröbner Bases Techniques in Post-Quantum Cryptography*** **Ludovic Perret (UPMC/INRIA/CNRS)**
17:00 – 17:10	Group Picture
18:00 –	Reception (Fukuoka SRP Center Building)

Tuesday, February 23	
9:30 – 10:30	Registration
10:30 – 12:00	***Code-Based Cryptography*** **Tanja Lange (Technische Universiteit Eindhoven)**
12:00 – 13:30	Lunch
13:30 – 15:00	***Quantum Algorithms*** **Michele Mosca (University of Waterloo)**
15:00 – 15:30	Coffee Break
15:30 – 17:00	***Hash-Based Signatures*** **Andreas Hülsing (Technische Universiteit Eindhoven)**

Post-Quantum Cryptography 2016

Wednesday, February 24	
8:30 – 9:15	Registration (Venue opens at 8:30)
9:15 – 9:30	Opening Remark
9:30 – 10:00	**NIST Announcement**
	Preliminary Plan for the Potential Standardization of Quantum-Resistant Algorithms Presentation: Dustin Moody
10:00 – 10:30	**Code-Based Cryptography I (Chair: Nicolas Sendrier)**
	IND-CCA Secure Hybrid Encryption from QC-MDPC Niederreiter Ingo von Maurich, Lukas Heberle, and Tim Güneysu
10:30 – 11:00	*RankSynd a PRNG Based on Rank Metric* Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich
11:00 – 11:30	Coffee Break
11:30 – 12:30	**Invited Talk I (Chair: Daniel Smith-Tone)**
	The Post-Quantum Internet Daniel Bernstein (University of Illinois at Chicago)
12:30 – 12:40	Group Picture
12:40 – 14:00	Lunch
14:00 – 14:30	**Quantum Security (Chair: Michele Mosca)**
	Applying Grover's Algorithm to AES: Quantum Resource Estimates Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt
14:30 – 15:00	*Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation* Dominique Unruh, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Mayuresh Vivekanand Anand
15:00 – 15:30	*Post-Quantum Security Models for Authenticated Encryption* Vladimir Soukharev, David Jao, and Srinath Seshadri
15:30 – 16:00	*Quantum Collision-Resistance of Non-Uniformly Distributed Functions* Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh
16:00 – 16:30	Coffee Break
16:30 – 17:30	**Invited Talk II (Chair: Rainer Steinwandt)**
	Quantum Key Distribution Platform and Its Applications Masahide Sasaki (Quantum ICT Laboratory, NICT)
18:20 –	Reception (Fukuoka SRP Center Building)

Post-Quantum Cryptography 2016

Thursday, February 25	
8:30 – 9:00	Registration (Venue opens at 8:30)
	Code-Based Cryptography II (Chair: Tanja Lange)
9:00 – 9:30	*An Efficient Attack on a Code-based Signature Scheme* Aurélie Phesso and Jean-Pierre Tillich
9:30 – 10:00	*Vulnerabilities of "McEliece in the World of Escher"* Dustin Moody and Ray Perlner
10:00 – 10:30	*Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes* Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich
10:30 – 11:00	*Analysis of Information Set Decoding for a Sub-Linear Error Weight* Rodolfo Canto Torres and Nicolas Sendrier
11:00 – 11:30	Coffee Break
	Invited Talk III (Chair: Johannes Buchmann)
11:30 – 12:30	*The Intel Strategy for Post Quantum Cryptography* Ernie Brickell (Intel)
12:30 – 14:00	Lunch
	Multivariate Polynomial Cryptography (Chair: Bo-Yin Yang)
14:00 – 14:30	*On the Differential Security of the HFEv- Signature Primitive* Ryann Cartor, Ryan Gipson, Daniel Smith-Tone, and Jeremy Vates
14:30 – 15:00	*Extension Field Cancellation: a New Central Trapdoor for Multivariate Quadratic Systems* Alan Szepieniec, Jintai Ding, and Bart Preneel
15:00 – 15:30	*Security Analysis and Key Modification for ZHFE* Ray Perlner and Daniel Smith-Tone
15:30 – 16:00	*Efficient ZHFE Key Generation* John B. Baena, Daniel Cabarcas, Daniel E. Escudero, Jaiberth Porras-Barrera, and Javier A. Verbel
16:00 – 16:30	Coffee Break
	Invited Talk IV (Chair: Jintai Ding)
16:30 – 17:30	*Challenges for Lattice Cryptography* Steven Galbraith (University of Auckland)
18:30 –	Banquet (Restaurant Sanshirou: reserved bus from the venue, 10 minutes drive)

Post-Quantum Cryptography 2016

Friday, February 26	
8:30 – 9:00	Registration (Venue opens at 8:30)
9:00 – 9:30 9:30 – 10:00	**Lattice-Based Cryptography (Chair: Keita Xagawa)** *Additively Homomorphic Ring-LWE Masking* Oscar Reparaz, Sujoy Sinha Roy, Frederik Vercauteren, Ingrid Verbauwhede, and Ruan de Clercq *An Homomorphic LWE based E-voting Scheme* Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène
10:00 – 10:30	Coffee Break
10:30 – 11:30	**Hot Topic Session (Chair: Chen-Mou Cheng)**
11:30 – 12:30	**NIST Announcement Q&A** Moderators: Dustin Moody, Ray Perlner, and Daniel Smith-Tone
12:30 – 12:35	Closing
Afternoon	Excursion (Optional)

Hot Topic Session

Multi-Prime Numbers MPKC for Post-Quantum Cryptosystem
Shigeo Tsujii, Masahito Gotaishi, Ryo Fujita

May-Ozerov Algorithm for Nearest Neighbor Problem over F_q and its Application to Information Set Decoding
Shoichi Hirose

Breaking the Fukuoka MQ Challenges
Tung Chou, Ruben Niederhagen, Bo-Yin Yang

QcBits: constant-time small-key code-based cryptography
Tung Chou

The HIMMO Scheme and its Contest
Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen

NTRU Prime: Security and Performance Analysis
Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal

A new lattice-based, efficient, quantum secure signature scheme
Jeffrey Hoffstein

A Framework for Evaluating Software/Hardware Implementations of Post-Quantum Public-Key Algorithms using Zynq SoC
Brian Loop, Ahmed Ferozpuri, Kris Gaj

Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3
Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, John Schanck

An overview of PQC workshops/projects and standardization concerns in China
Hong Xiang, Tao Xiang, Zhen-Feng Zhang, Zheng-Fu Han