PQCRYPTO 2024 DAY 1

Wednesday June 12, 2024 – Mathematical Institute, University of Oxford

Wed 08:00 Registration

Wed 09:00 Opening remarks

Wed 09:15 **TRANSFORMS AND PROOFS**
Chair:

Kathrin Hövelmanns and Christian Majenz: *"Explicitly rejecting Fujisaki-Okamoto transforms and worst-case correctness - completing the picture"*

Kamil Doruk Gür, Jonathan Katz and Tjerand Silde: *"Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption"*

Thomas Aulbach, Samed Düzlü, Michael Meyer, Patrick Struck and Maximiliane Weishäupl: *"Hash your Keys before Signing: BUFF Security of the Additional NIST PQC Signatures"*

Yao Cheng, Xianhui Lu, Ziyi Li and Bao Li: *"Revisiting Anonymity in Post-Quantum Public Key Encryption"*

Wed 10:35 Coffee Break

Wed 11:00 **INVITED SPEAKER 1**

Nadia Heninger: *Title TBD.*

Wed 12:25 Lunch

Wed 14:00 **MULTIVARIATE CRYPTOGRAPHY 1**
Chair: Ludovic Perret

Pierre Pébereau: *"One vector to rule them all: Key recovery from one vector in UOV schemes"*

Peigen Li and Jintai Ding: *"Cryptanalysis of the SNOVA signature scheme"*

Hiroki Furue and Momonari Kudo: *"Polynomial XL: A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings"*

Wed 15:00 Coffee Break

Wed 15:30 **LATTICES 1**
Chair: Thomas Prest

Henry Bambury and Phong Nguyen: *"Improved Provable Reduction of NTRU and Hypercubic Lattices"*

Shi Bai, Hansraj Jangir, Hao Lin, Tran Ngo, Weiqiang Wen and Jinwei Zheng: *"Compact Encryption based on Module-NTRU problems"*

Leizhang Wang: *"Analyzing Pump and jump BKZ algorithm using dynamical systems"*

Wed 16:30 Evening program

PQCRYPTO 2024 DAY 2

Thursday June 13, 2024 – Mathematical Institute, University of Oxford

Thu 09:15 **GROUP ACTIONS**
Chair:

Jonas Meers and Doreen Riepel: *"CCA Secure Updatable Encryption from Non-Mappable Group Actions"*

Benjamin Benčina, Alessandro Budroni, Jesús-Javier Chi-Domínguez and Mukul Kulkarni: *"Properties of Lattice Isomorphism as a Cryptographic Group Action"*

Markus Bläser, Zhili Chen, Dung Duong, Antoine Joux, Tuong Nguyen, Thomas Plantard, Youming Qiao, Willy Susilo and Gang Tang: *"On digital signatures based on group actions: QROM security and ring signatures"*

Antonin Leroux and Maxime Roméas: *"Updatable Encryption from Group Actions"*

Thu 10:35 Coffee Break

Thu 11:00 **INVITED SPEAKER 2**

Sabrina Kunzweiler: *"The higher dimensional picture: And its role in isogeny-based cryptography"*

Thu 12:25 Lunch

Thu 14:00 **LATTICES 2**
Chair: Jintai Ding

Corentin Jeudy, Adeline Roux-Langlois and Olivier Sanders: *"Phoenix: Hash-and-Sign with Aborts from Lattice Gadgets"*

Toi Tomita and Junji Shikata: *"Efficient Identity-Based Encryption with Tight Adaptive Anonymity from RLWE"*

Zhen Liu, Vishakha, Jintai Ding, Chi Cheng and Yanbin Pan: *"An Improved Practical Key Mismatch Attack Against NTRU"*

Thu 15:00 Coffee Break

Thu 15:30 **MULTIVARIATE CRYPTOGRAPHY 2**
Chair: Tung Chou

Thomas Aulbach, Simona Samardjiska and Monika Trimoska: *"Practical key-recovery attack on MQ-Sign and more"*

Hao Guo, Yi Jin, Yuansheng Pan, Xiaoou He, Boru Gong and Jintai Ding: *"Practical and Theoretical Cryptanalysis of VOX"*

Pierre Varjabedian, Benoit-Michel Cogliati, Gilles Macario-Rat and Jacques Patarin: *"State of the art of HFE variants Is it possible to repair HFE with appropriate perturbations?"*

Thu 16:30 Evening program

PQCRYPTO 2024 DAY 3

Friday June 14, 2024 – Mathematical Institute, University of Oxford

Fri 09:15 **ATTACKS**

Chair: Liqun Chen

Martin Ekerå and Joel Gärtner: *"Extending Regev's factoring algorithm to compute discrete logarithms"*

Christopher Battarbee, Delaram Kahrobaei, Ludovic Perret and Siamak F. Shahandashti: *"A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem"*

Tomoki Moriya, Hiroshi Onuki, Maozhi Xu and Guoqing Zhou: *"Adaptive attacks against FESTA without input validation or constant-time implementation"*

Jeonghwan Lee, Donghoe Heo, Hyeonhak Kim, Gyusang Kim, Suhri Kim, Heeseok Kim and Seokhie Hong: *"Fault attack on SQISign"*

Fri 10:35 Coffee Break

Fri 11:00 **INVITED SPEAKER 3**

N.N. (NCSC Technical Director for Cryptography): *"Post-Quantum Cryptography in UK Government"*

Fri 12:25 Lunch

Fri 14:00 **APPLICATIONS AND PROTOCOLS**

Chair: Tjerand Silde

Loïc Ferreira and Johan Pascal: *"Post-Quantum Secure ZRTP"*

Liqun Chen, Changyu Dong, Nada El Kassem, Christopher J.P. Newton and Yalan Wang: *"A New Hash-based Enhanced Privacy ID Signature Scheme"*

(No break between these short sessions.)

Fri 14:40 **CODE-BASED CRYPTOGRAPHY**

Chair: Tjerand Silde

Nicolas Aragon, Pierre Briaud, Victor Dyseryn, Philippe Gaborit and Adrien Vinçotte: *"The Blockwise Rank Syndrome Learning problem and its applications to cryptography"*

Tung Chou, Ruben Niederhagen, Lars Ran and Simona Samardjiska: *"Reducing Signature Size of Matrix-code-based Signature Schemes"*

Fri 15:20 Closing remarks

Fri 15:30 Adjourn

(Version 20240610183300)