PQCrypto 2024 Accepted Papers (final)

07: Peigen Li and Jintai Ding: "Cryptanalysis of the SNOVA signature scheme"
08: Corentin Jeudy, Adeline Roux-Langlois and Olivier Sanders: "Phoenix: Hash-and-Sign with Aborts from Lattice Gadgets"
09: Pierre Pébereau: "One vector to rule them all: Key recovery from one vector in UOV schemes"
12: Jonas Meers and Doreen Riepel: "CCA Secure Updatable Encryption from Non-Mappable Group Actions"
15: Kathrin Hövelmanns and Christian Majenz: "Explicitly rejecting Fujisaki-Okamoto transforms and worst-case correctness - completing the picture"
16: Toi Tomita and Junji Shikata: "Efficient Identity-Based Encryption with Tight Adaptive Anonymity from RLWE"
21: Nicolas Aragon, Pierre Briaud, Victor Dyseryn, Philippe Gaborit and Adrien Vinçotte: "The Blockwise Rank Syndrome Learning problem and its applications to cryptography"
26: Tung Chou, Ruben Niederhagen, Lars Ran and Simona Samardjiska: "Reducing Signature Size of Matrix-code-based Signature Schemes"
27: Benjamin Benčina, Alessandro Budroni, Jesús-Javier Chi-Domínguez and Mukul Kulkarni: "Properties of Lattice Isomorphism as a Cryptographic Group Action"
28: Hiroki Furue and Momonari Kudo: "Polynomial XL: A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings"
29: Tomoki Moriya, Hiroshi Onuki, Guoqing Zhou and Maozhi Xu: "Adaptive attacks against FESTA without input validation or constant-time implementation"
30: Antonin Leroux and Maxime Roméas: "Updatable Encryption from Group Actions"
35: Zhen Liu, Vishakha, Jintai Ding, Chi Cheng and Yanbin Pan: "An Improved Practical Key Mismatch Attack Against NTRU"
37: Loïc Ferreira and Johan Pascal: "Post-Quantum Secure ZRTP"
42: 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?"
45: Christopher Battarbee, Delaram Kahrobaei, Ludovic

Perret and Siamak F. Shahandashti: "A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem"
47: Liqun Chen, Changyu Dong, Nada El Kassem, Christopher J.P. Newton and Yalan Wang: "A New Hash-based Enhanced Privacy ID Signature Scheme"
49: Kamil Doruk Gur, Jonathan Katz and Tjerand Silde: "Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption"
58: Thomas Aulbach, Simona Samardjiska and Monika Trimoska: "Practical key-recovery attack on MQ-Sign and more"
59: Jeonghwan Lee, Donghoe Heo, Hyeonhak Kim, Gyusang Kim, Suhri Kim, Heeseok Kim and Seokhie Hong: "Fault attack on SQISign"
60: Henry Bambury and Phong Nguyen: "Improved Provable Reduction of NTRU and Hypercubic Lattices"
63: 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"
70: Shi Bai, Hansraj Jangir, Hao Lin, Tran Ngo, Weiqiang Wen and Jinwei Zheng: "Compact Encryption based on Module-NTRU problems"
72: Thomas Aulbach, Samed Düzlü, Michael Meyer, Patrick Struck and Maximiliane Weishäupl: "Hash your Keys before Signing: BUFF Security of the Additional NIST PQC Signatures"
75: Martin Ekerå and Joel Gärtner: "Extending Regev’s factoring algorithm to compute discrete logarithms"
81: Yao Cheng, Xianhui Lu, Ziyi Li and Bao Li: "Revisiting Anonymity in Post-Quantum Public Key Encryption"
84: Leizhang Wang: "Analyzing Pump and jump BKZ algorithm using dynamical systems"
88: Hao Guo, Yi Jin, Yuansheng Pan, Xiaoou He, Boru Gong and Jintai Ding: "Practical and Theoretical Cryptanalysis of VOX"