

4th PQC Standardization Conference
November 29 – December 1, 2022 [Virtual]

All times are Eastern Time (New York)

Tuesday, November 29, 2022	
Session I – Welcome and Algorithm Updates	
<i>Session Chair: Dustin Moody</i>	
10:00 – 10:30	Opening – NIST Welcome – Matt Scholl, NIST, Computer Security Division Chief NIST PQC: Looking into the Future – Dustin Moody, NIST
10:30 – 10:45	CRYSTALS-Kyber <i>Presented by: Peter Schwabe, MPI-SP & Radboud University</i>
10:45 – 11:00	CRYSTALS-Dilithium <i>Presented by: Vadim Lyubashevsky, IBM Research Europe, Zurich</i>
11:00 – 11:15	FALCON <i>Presented by: Thomas Prest, PQShield SAS</i>
11:15 – 11:30	SPHINCS+ <i>Presented by: Andreas Hülsing, TU Eindhoven</i>
11:30 – 11:50	SPHINCS+C: Compressing SPHINCS+ With (Almost) No Cost <i>Presented by: Eyal Ronen, Tel Aviv University</i>
11:50 – 12:10	Twelve-round Keccak for secure hashing <i>Presented by: Gilles Van Assche, STMicroelectronics</i>
12:10 – 12:13	1st Annual RWPQC 2023 announcement <i>Daniel Apon, MITRE</i>
12:15 – 13:00	BREAK
Session II – Side Channels	
<i>Session Chair: Yi-Kai Liu</i>	
13:00 – 13:20	A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext <i>Presented by: Guillaume Goy, Université Grenoble Alpes, CEA</i>
13:20 – 13:40	FALCON Down: Breaking FALCON Post-Quantum Signature Scheme through Side-Channel Attacks <i>Presented by: Aydin Aysu, North Carolina State University</i>
13:40– 14:00	Leveling Dilithium against Leakage, Revisited Sensitivity Analysis and Improved Implementations <i>Presented by: Melissa Azouaoui, NXP Semiconductors</i>
14:00– 14:20	The Challenge of Side-Channel Countermeasures on Post-Quantum Crypto <i>Presented by: Rina Zeitoun, IDEMIA</i>
14:20– 14:40	Towards Leakage-Resistant Post-Quantum CCA-Secure Public Key Encryption <i>Presented by: François-Xavier Standaert & Thomas Peters, UCLouvain</i>
14:40– 15:00	Optimization for SPHINCS+ using Intel® Secure Hash Algorithm Extensions <i>Presented by: Qian Wang, Intel</i>
15:00	ADJOURN

Last Updated: November 29, 2022
Speakers/times are subject to change.

Wednesday, November 30, 2022

Session III – NSA Talk / Security

Session Chair: Angela Robinson

10:00 – 10:40	Transitioning National Security Systems to a Post Quantum Future <i>Morgan Stern, NSA</i>
10:40 – 11:00	Practical Improvements on BKZ Algorithm <i>Presented by: Ziyu Zhao, Tsinghua University</i>
11:00 – 11:20	Probabilistic Hash-and-Sign with Retry in the Quantum Random Oracle Model <i>Presented by: Haruhisa Kosuge, Japan Ministry of Defense</i>
11:20 – 11:40	A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem <i>Presented by: Christopher Battarbee, University of York, UK</i>
11:40 – 12:00	Quantum Augmented Dual Attack [this talk will not be recorded] <i>Presented by: Yixin Shen, Royal Holloway, University of London</i>
12:00 – 13:00	BREAK
Session IV – Candidate Updates / Hardware I	
<i>Session Chair: Quynh Dang</i>	
13:00– 13:15	BIKE <i>Presented by: Rafael Misoczki, Google</i>
13:15– 13:30	Classic McEliece <i>Presented by: Tung Chou, Academia Sinica</i>
13:30– 13:45	HQC <i>Presented by: Philippe Gaborit, University of Limoges, France</i>
13:45– 14:00	SIKE <i>Presented by: David Jao, University of Waterloo</i>
14:00– 14:20	Benchmarking and Analysing NIST PQC Lattice-Based Signature Scheme Standards on the ARM Cortex M7 <i>Presented by: James Howe, SandboxAQ</i>
14:20– 14:40	A Flexible Shared Hardware Accelerator for NIST-Recommended Algorithms CRYSTALS-Kyber and CRYSTALS-Dilithium with SCA Protection <i>Presented by: Abubakr Abdulgadir, PQSecure Technologies</i>
14:40– 15:00	High-Performance Hardware Implementation of Lattice-Based Digital Signatures <i>Presented by: Luke Beckwith, George Mason University</i>
15:00– 15:40	PANEL: Impact of PQC Signatures in Protocols and Applications <i>Moderated by: David Cooper, NIST</i> <i>Panelists: Scott Fluhrer, Cisco</i> <i>Russ Housley, Vigil Security, LLC</i> <i>Bas Westerbaan, Cloudflare</i> <i>Eric Rescorla, Mozilla</i>
15:40	ADJOURN

Thursday, December 1, 2022

Session V – Migration

Session Chair: Daniel Smith-Tone

10:00 – 10:15	The National Cybersecurity Center of Excellences (NCCoE) Migration to Post-Quantum Cryptography Project <i>Bill Newhouse, NIST/NCCoE</i>
10:15 – 10:50	PANEL - Approaches to PQC Migration <i>Moderated by: Curt Barker, MITRE/NIST-NCCoE</i> <i>Panelists: Anne Dames, IBM</i> <i>Bruno Couillard, Crypto4A</i> <i>Avesta Hajjati, DigiCert</i>
10:50 – 11:10	Algebraic Relation of Three MinRank Algebraic Modelings <i>Presented by: Hao Guo, Tsinghua University</i>
11:10 – 11:30	Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice <i>Presented by: Burt Kaliski, Verisign</i>
11:30 – 11:50	An Efficient and Generic Construction for Signal’s Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable <i>Presented by: Thomas Prest, PQShield SAS</i>
11:50 – 13:00	BREAK
Session VI – Hardware II	
<i>Session Chair: Ray Perlner</i>	
13:00 – 13:20	A Masked Pure-Hardware Implementation of Kyber Cryptographic Algorithm <i>Presented by: Tendayi Kamucheka, University of Arkansas</i>
13:20 – 13:40	Mckeycutter: A High-throughput Key Generator of Classic McEliece on Hardware <i>Presented by: Yihong Zhu, Tsinghua University</i>
13:40 – 14:00	Fast and Efficient Hardware Implementation of HQC <i>Presented by: Sanjay Deshpande, Yale University & Kashif Nawaz, Technology Innovation Institute</i>
14:00 – 14:20	Complete and Improved FPGA Implementation of Classic McEliece <i>Presented by: Sanjay Deshpande, Yale University</i>
14:20 – 14:40	Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions <i>Presented by: Duc Tri Nguyen, George Mason University</i>
14:40 – 14:50	Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange <i>Presented by: John Preuß Mattsson, Ericsson</i>
14:50 – 15:10	Post-Quantum Protocols for Banking Applications [this talk will not be recorded] <i>Presented by: Emmanuelle Dottax, IDEMIA</i>
15:10 – 15:30	Wrap-Up <i>NIST PQC Team</i>
15:30	ADJOURN