3rd PQC Standardization Conference

June 7-9, 2021 *[Virtual]*

All times are Eastern Time (New York)

Monday, June 7, 2021	
Session I – Welcome and Candidate Updates *Session Chair: Dustin Moody*	
10:00 – 10:30	***Opening – NIST*** ***Welcome -*** *Matt Scholl, NIST Computer Security Division Chief* ***Status Update on the 3rd Round –*** *Dustin Moody, NIST*
10:30 – 10:45	**CRYSTALS-Dilithium** *Presented by: Vadim Lyubashevsky, IBM Research Europe*
10:45 – 11:00	**Falcon** *Presented by: Thomas Prest, PQShield*
11:00 – 11:15	**Rainbow** *Presented by: Albrecht Petzoldt, FAU Erlangen Nuremberg*
11:15 – 11:30	**GeMSS** *Presented by: Ludovic Perret, CryptoNext*
11:30 – 11:45	**Picnic** *Presented by: Greg Zaverucha, Microsoft*
11:45 – 12:00	**SPHINCS+** *Presented by: Andreas Hülsing, Eindhoven University of Technology*
12:00 – 12:40	**BREAK**
Session II – Security I *Session Chair: Daniel Apon*	
12:40– 13:00	**Efficient Key Recovery for all HFE Signature Variants** *Presented by: Albrecht Petzoldt, FAU Erlangen Nuremberg*
13:00– 13:20	**Formal Verification of Post-Quantum Cryptography** *Presented by: Matthias Meijers, Eindhoven University of Technology*
13:20– 13:40	**Lower bounds on lattice sieving and information set decoding** *Presented by: Elena Kirshanova, Immanuel Kant Baltic Federal University*
13:40– 14:00	**Torsion point attacks on "SIDH-like" cryptosystems** *Presented by: Péter Kutas, University of Birmingham*
14:00– 14:20	**Anonymous, Robust Post-Quantum Public Key Encryption** *Presented by: Varun Maram, ETH Zurich*
14:20 – 14:40	**BREAK**

Session III – Hardware *Session Chair: Angela Robinson*	
14:40– 15:00	**pqm4: NISTPQC Round 3 Results on the Cortex-M4** *Presented by: Matthias J. Kannwischer, Max Planck Institute for Security and Privacy*
15:00– 15:10	**Rainbow on Cortex-M4** *Presented by: Matthias J. Kannwischer, Max Planck Institute for Security and Privacy*
15:10– 15:20	**Compact Copocessor for KEM Saber: Novel Scalable Matrix Originated Processing** *Presented by: Jiafeng Xie, Villanova University*
	PAPER WITHDRAWN: Benchmarking and Analysing the NIST PQC Finalist Lattice-Based Signature Schemes on the ARM Cortex M7 *Presented by: James Howe, PQShield*
15:20– 15:40	**High-Speed Hardware Architectures and Fair FPGA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber** *Presented by: Kris Gaj, George Mason University*
15:40– 15:50	**Hardware Deployment of Hybrid PQC** *Presented by: Reza Azarderakhsh, PQSecure Technologies*
15:50	**ADJOURN**

Tuesday, June 8, 2021	
Session IV – NIST-DHS Talk / Side Channels *Session Chair: Rene Peralta*	
10:00 – 10:20	**Getting Ready for Post-Quantum Cryptography** *Bill Newhouse, NIST/NCCoE and Nick Reese, Department of Homeland Security*
10:20– 10:35	**A Side-Channel Assisted Attack on NTRU** *Presented by: Amund Askeland, University of Bergen*
10:35– 10:45	**Power-based Side Channel Attack Analysis on PQC Algorithms** *Presented by: Tendayi Kamucheka, University of Arkansas*
10:45– 11:00	**First-Order Masked Kyber on ARM Cortex-M4** *Presented by: Daniel Heinz, Universität der Bundeswehr*
11:00– 11:15	**Techniques for Masking Saber and Kyber** *Presented by: Michiel Van Beirendonck, imec-COSIC KU Leuven*
11:15– 11:35	**Side-Channel Protections for Picnic Signatures** *Presented by: Akira Takahashi, Aarhus University and Okan Seker, University of Lübeck*
11:35– 11:50	**On Generic Side-Channel Assisted Chosen Ciphertext Attacks on Lattice-based PKE/KEMs - Towards key recovery attacks on NTRU-based PKE/KEMs** *Presented by: Prasanna Ravi, Nanyang Technological University*
11:50 – 12:30	**BREAK**
Session V – Applications *Session Chair: David Cooper*	
12:30– 12:45	**Saber Post-Quantum Key Encapsulation Mechanism (KEM): Evaluating Performance in Mobile Devices -- and -- Suggesting Some Improvements and Evaluating Kyber post-quantum KEM in a mobile application** *Presented by: Leonardo Augusto D. S. Ribeiro, Universidade Federal de Pernambuco*
12:45– 13:00	**Smartcard and Post-Quantum Crypto** *Presented by: Aurélien Greuet, IDEMIA - Crypto & Security Labs*
13:00– 13:15	**Requirements for Post-Quantum Cryptography on Embedded Devices in the IoT** *Presented by: Derek Atkins, Veridify Security*
13:15– 13:30	**Suitability of 3rd Round Signature Candidates for Vehicle-to-Vehicle Communication** *Presented by: Nina Bindel, University of Waterloo*
13:30– 13:40	**PQ-WireGuard: we did it again** *Presented by: Mathilde Raynal, Kudelski Security/EPFL*
13:40– 14:20	**PANEL: PQC Considerations for DNSSEC** ***Moderator: Haya Shulman, Hebrew University of Jerusalem*** • *Jim Goodman, Crypto4a Technologies Inc.* • *Russ Housley, Vigil Security LLC* • *Burt Kaliski, Verisign* • *Victoria Risk, Internet Systems Consortium* • *Douglas Stebila, University of Waterloo* • *Roland van Rijswijk-Deij, University of Twente and NLnet Labs*
14:20 – 14:40	**BREAK**

Session VI – Candidate Updates *Session Chair: Quynh Dang*	
14:40 – 14:55	**BIKE** *Presented by: Rafael Misoczki, Google*
14:55 – 15:10	**HQC** *Presented by: Philippe Gaborit, University of Limoges*
15:10 – 15:25	**FrodoKEM** *Presented by: Patrick Longa, Microsoft*
15:25 – 15:40	**NTRUprime** *Presented by: Daniel J. Bernstein, University of Illinois at Chicago; Ruhr University Bochum*
15:40 – 15:55	**SIKE** *Presented by: Luca De Feo, IBM Research Europe*
15:55	**ADJOURN**

Wednesday, June 9, 2021	
Session VII – Performance / Candidate Updates *Session Chair: Daniel Smith-Tone*	
10:00 – 10:10	**Classic McEliece on the ARM Cortex-M**4 *Presented by: Tung Chou, Academia Sinica*
10:10 – 10:30	**Optimized Software Implementations of CRYSTALS-Kyber, NTRU, and Saber Using NEON-Based Special Instructions of ARMv**8 *Presented by: Duc Tri Nguyen, George Mason University*
10:30– 10:50	**Verifying Post-Quantum Signatures in 8 kB of RAM** *Presented by: Ruben Anthony Gonzalez, Hochschule Bonn-Rhein-Sieg*
10:50– 11:05	**Fast verified post-quantum software, part 1: RAM subroutines** *Presented by: Daniel J. Bernstein, University of Illinois at Chicago; Ruhr University Bochum*
11:05– 11:20	**Classic McEliece** *Presented by: Tanja Lange, Eindhoven University of Technology*
11:20– 11:35	**CRYSTALS-Kyber** *Presented by: Peter Schwabe, Max Planck Institute for Security and Privacy and Radboud University*
11:35– 11:50	**Saber** *Presented by: Frederik Vercauteren, KU Leuven, COSIC/ESAT*
11:50– 12:05	**NTRU** *Presented by: John Schanck, University of Waterloo*
12:05 – 12:45	**BREAK**
Session VIII – Security II / Implementations I *Session Chair: Carl Miller*	
12:45– 12:50	**The Case for SIKE: A Decade of the Supersingular Isogeny Problem** *Presented by: Craig Costello, Microsoft Research*
12:50– 13:10	**BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures** *Presented by: Rune Fiedler, TU Darmstadt*
13:10– 13:20	**Faster Kyber and Saber via a Generic Fujisaki-Okamoto Transform for Multi-User Security in the QROM** *Presented by: Julien Duman, Ruhr-Universitat Bochum*
13:20– 13:40	B**oosting the Hybrid Attack on NTRU: Torus LSH, Permuted HNF and Boxed Sphere** *Presented by: Phong Nguyen, Inria Paris*
13:40– 14:00	**Resistance of Isogeny-Based Cryptographic Implementations to a Fault Attack** *Presented by: Élise Tasso, CEA-Leti, Université Grenoble Alpes*
14:00– 14:20	**Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon** *Presented by: Thomas Espitau, NTT Corporation*
14:20 – 14:40	**BREAK**

Session IX –Implementations II / NIST Q&A *Session Chair: Yi-Kai Liu*	
14:40– 14:50	**Updates from the Open Quantum Safe Project** *Presented by: John Schanck, University of Waterloo*
14:50– 15:10	**Zalcon: an alternative FPA-free NTRU sampler for Falcon** *Presented by: Yu Yang, Tsinghua University*
15:10– 15:20	**Fast Quantum-Safe Cryptography on IBM Z** *Presented by: Basil Hess, IBM Research Europe*
15:20– 15:35	**A Lightweight Implementation of Saber Resistant Against Side-Channel Attacks** *Presented by: Abubakr Abdulgadir, George Mason University*
15:35– 15:45	**RFC Key Identification and Serialization** *Presented by: Christine van Vredendaal, NXP Semiconductors*
15:45-16:15	**NIST Q&A**
16:15	**Adjourn**