

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

Session III – Hardware

Session Chair: Angela Robinson

[*On Demand Video*](#)

14:40– 14:50	Compact Coprocessor for KEM Saber: Novel Scalable Matrix Originated Processing <i>Presented by: Jiafeng Xie, Villanova University</i>
14:50– 15:10	High-Speed Hardware Architectures and Fair FPGA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber <i>Presented by: Kris Gaj, George Mason University</i>
15:10– 15:30	pqm4: NISTPQC Round 3 Results on the Cortex-M4 <i>Presented by: Matthias J. Kannwischer, Max Planck Institute for Security and Privacy</i>
15:30– 15:40	Rainbow on Cortex-M4 <i>Presented by: Matthias J. Kannwischer, Max Planck Institute for Security and Privacy</i>
15:40– 15:50	Hardware Deployment of Hybrid PQC <i>Presented by: Reza Azarderakhsh, PQSecure Technologies</i>
15:50	ADJOURN

Tuesday, June 8, 2021

Session IV – NIST-DHS Talk / Side Channels

Session Chair: Rene Peralta

[On Demand Video](#)

10:00 – 10:20	Getting Ready for Post-Quantum Cryptography <i>Bill Newhouse, NIST/NCCoE and Nick Reese, Department of Homeland Security</i>
10:20– 10:35	A Side-Channel Assisted Attack on NTRU <i>Presented by: Amund Askeland, University of Bergen</i>
10:35– 10:45	Power-based Side Channel Attack Analysis on PQC Algorithms <i>Presented by: Tendayi Kamucheka, University of Arkansas</i>
10:45– 11:00	First-Order Masked Kyber on ARM Cortex-M4 <i>Presented by: Daniel Heinz, Universität der Bundeswehr</i>
11:00– 11:15	Techniques for Masking Saber and Kyber <i>Presented by: Michiel Van Beirendonck, imec-COSIC KU Leuven</i>
11:15– 11:35	Side-Channel Protections for Picnic Signatures <i>Presented by: Akira Takahashi, Aarhus University and Okan Seker, University of Lübeck</i>
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 <i>Presented by: Prasanna Ravi, Nanyang Technological University</i>
11:50 – 12:30	BREAK

Session V – Applications

Session Chair: David Cooper

[On Demand Video](#)

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 <i>Presented by: Leonardo Augusto D. S. Ribeiro, Universidade Federal de Pernambuco</i>
12:45– 13:00	Smartcard and Post-Quantum Crypto <i>Presented by: Aurélien Greuet, IDEMIA - Crypto & Security Labs</i>
13:00– 13:15	Requirements for Post-Quantum Cryptography on Embedded Devices in the IoT <i>Presented by: Derek Atkins, Veridify Security [Pre-Recorded]</i>
13:15– 13:30	Suitability of 3rd Round Signature Candidates for Vehicle-to-Vehicle Communication <i>Presented by: Nina Bindel, University of Waterloo</i>
13:30– 13:40	PQ-WireGuard: we did it again <i>Presented by: Mathilde Raynal, Kudelski Security/EPFL</i>
13:40– 14:20	PANEL: PQC Considerations for DNSSEC Moderator: Haya Shulman, Hebrew University of Jerusalem <ul style="list-style-type: none"> • <i>Jim Goodman, Crypto4a Technologies Inc.</i> • <i>Russ Housley, Vigil Security LLC</i> • <i>Burt Kaliski, Verisign</i> • <i>Victoria Risk, Internet Systems Consortium</i> • <i>Douglas Stebila, University of Waterloo</i> • <i>Roland van Rijswijk-Deij, University of Twente and NLnet Labs</i>
14:20 – 14:40	BREAK

Session VI – Candidate Updates

Session Chair: Quynh Dang

[*On Demand Video*](#)

14:40 – 14:55	BIKE <i>Presented by: Rafael Misoczki, Google</i>
14:55 – 15:10	HQC <i>Presented by: Philippe Gaborit, University of Limoges</i>
15:10 – 15:25	FrodoKEM <i>Presented by: Patrick Longa, Microsoft</i>
15:25 – 15:40	NTRUprime <i>Presented by: Daniel J. Bernstein, University of Illinois at Chicago; Ruhr University Bochum</i>
15:40 – 15:55	SIKE <i>Presented by: Luca De Feo, IBM Research Europe</i>
15:55	ADJOURN

Wednesday, June 9, 2021

Session VII – Performance / Candidate Updates

Session Chair: Daniel Smith-Tone

[*On Demand Video*](#)

10:00 – 10:10	Classic McEliece on the ARM Cortex-M4 <i>Presented by: Tung Chou, Academia Sinica</i>
10:10 – 10:30	Optimized Software Implementations of CRYSTALS-Kyber, NTRU, and Saber Using NEON-Based Special Instructions of ARMv8 <i>Presented by: Duc Tri Nguyen, George Mason University</i>
10:30– 10:50	Verifying Post-Quantum Signatures in 8 kB of RAM <i>Presented by: Ruben Anthony Gonzalez, Hochschule Bonn-Rhein-Sieg</i>
10:50– 11:05	Fast verified post-quantum software, part 1: RAM subroutines <i>Presented by: Daniel J. Bernstein, University of Illinois at Chicago; Ruhr University Bochum [Pre-Recorded]</i>
11:05– 11:20	Classic McEliece <i>Presented by: Tanja Lange, Eindhoven University of Technology [Pre-Recorded]</i>
11:20– 11:35	CRYSTALS-Kyber <i>Presented by: Peter Schwabe, Max Planck Institute for Security and Privacy and Radboud University</i>
11:35– 11:50	Saber <i>Presented by: Frederik Vercauteren, KU Leuven, COSIC/ESAT</i>
11:50– 12:05	NTRU <i>Presented by: John Schanck, University of Waterloo</i>
12:05 – 12:45	BREAK
Session VIII – Security II / Implementations I	
<i>Session Chair: Carl Miller</i>	
<i>On Demand Video</i>	
12:45– 12:50	The Case for SIKE: A Decade of the Supersingular Isogeny Problem <i>Presented by: Craig Costello, Microsoft Research</i>
12:50– 13:10	BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures <i>Presented by: Rune Fiedler, TU Darmstadt</i>
13:10– 13:20	Faster Lattice-based KEMs via Fujisaki-Okamoto Transform in the Multi-User Setting via Prex-Hashing <i>Presented by: Julien Duman, Ruhr-Universität Bochum</i>
13:20– 13:40	Boosting the Hybrid Attack on NTRU: Torus LSH, Permuted HNF and Boxed Sphere <i>Presented by: Phong Nguyen, Inria Paris [Pre-Recorded]</i>
13:40– 14:00	Resistance of Isogeny-Based Cryptographic Implementations to a Fault Attack <i>Presented by: Élise Tasso, CEA-Leti, Université Grenoble Alpes</i>
14:00– 14:20	Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon <i>Presented by: Thomas Espitau, NTT Corporation</i>
14:20 – 14:40	BREAK

Session IX –Implementations II / NIST Q&A

Session Chair: Yi-Kai Liu

[*On Demand Video*](#)

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