6th PQC Standardization Conference

September 24-26, 2025
Draft Agenda

National Institute of Standards and Technology
Building 101
Green Auditorium

All times are Eastern Daylight Time (New York)

Wednesday, September 24, 2025	
8:00 – 5:00	**Badge Pick Up and Coffee/Beverage Service**
Session I – Welcome and Algorithm Updates *Session Chair: Dustin Moody, NIST*	
9:00 – 9:05	**Welcome and Opening Remarks** *Jon Boyens, NIST*
9:05 – 9:25	**NIST PQC Standardization Project** *Dustin Moody, NIST*
9:25– 9:45	**UOV** *Presented by: Jintai Ding, Xi'an Jiaotong-Liverpool University*
9:45– 10:05	**QR-UOV** *Presented by: Hiroki Furue, Nippon Telegraph and Telephone Corporation (NTT)*
10:05 – 10:25	**Mayo** *Presented by: Ward Beullens, IBM Research - Zurich*
10:25 – 10:45	**SNOVA** *Presented by: Po-En Tseng, National Dong Hwa University*
10:45 – 11:15	**BREAK**
Session II – Security/Cryptanalysis I *Session Chair: Maxime Bros, NIST*	
11:15 – 11:35	**Security Analysis on UOV Families with Odd Characteristics: Using Symmetric Algebra** *Presented by: Boru Gong (Jintai Ding as backup), CCB Fintech Ltd.*
11:35– 11:55	**Exploiting SNOVA's Structure in the Wedge Product Attack** *Presented by: Hung Le, LTCI Telecom Paris, PSL University*
11:55 – 12:15	**That's not my Signature! Fail Stop Signatures for a Post-Quantum World** *Presented by: Cecilia Boschini, ETH Zurich (virtual)*
12:15 – 1:40	**LUNCH** **Box lunches will be provided to in-person attendees**

Last Update: 9/16/2025
Send corrections/updates to:
pqc2025@nist.gov
Speakers/times are subject to change.

Wednesday, September 24, 2025 (con't)	
Session III – CNSA 2.0 and Side Channels *Session Chair: Pierre Ciadoux, NIST*	
1:40-2:00	**CNSA 2.0** *Presented by:*
2:00 – 2:0	**Masking FrodoKEM** *Presented by: Elie Eid, IDEMIA (virtual)*
2:20 – 2:40	**Recent Contributions to the Physical Security of ML-DSA** *Presented by: Melissa Azouaoui, NXP (virtual)*
2:40 – 3:00	**Systematic Timing Leakage Analysis of NIST PQDSS Candidates: Tooling and Lessons Learned** *Presented by: Mahmudul Faisal Al Ameen, CEA-List*
3:00 – 3:20	**Single Trace Side-Channel Attack on the MPC-in-the-Head Framework** *Presented by: Julie Godard, University of Limoges, CEA-LIST*
3:20 – 3:0	**mUOV: Masking the Unbalanced Oil and Vinegar Digital Signature Scheme at First- and Higher-Order** *Presented by: Quinten Norga, COSIC, KU Leuven*
3:40 – 4:00	**BREAK**
Session IV – Applications I *Session Chair: Noah Waller, NIST*	
4:00 – 4:20	**Post-Quantum Ratcheting for Signal** *Presented by: Rolfe Schmidt, Signal Messenger*
4:20 – 4:40	**Post-Quantum Diversity for DNSSEC: Routine Performance, Resilient Fallback** *Presented by: Joe Harvey, Verisign Labs*
4:40 – 5:00	**Efficient Hardware Acceleration for Post-Quantum Scheme HQC - From Component Perspective** *Presented by: Jiafeng Xie, Villanova University*
5:00	**ADJOURN**

Last Update: 9/16/2025
Send corrections/updates to:
pqc2025@nist.gov
Speakers/times are subject to change.

Thursday, September 25, 2025	
8:00 – 5:00	**Badge Pick Up and Coffee/Beverage Service**
Session V – NIST PQC Project Updates *Session Chair: Yi-Kai Liu, NIST*	
9:00 – 9:20	**FIPS 206** *Presented by: Ray Perlner, NIST*
9:20 – 9:40	**SPHINCS+ Smaller Parameter Sets** *Presented by: Quynh Dang, NIST*
9:40 – 10:00	**SP 800-227** *Presented by: Gorjan Alagic, NIST*
10:00 – 10:20	**FIPS 207** *Presented by: Angela Robinson, NIST*
10:20 – 10:50	**BREAK**
Session VI – Algorithm Updates *Session Chair: Angela Robinson, NIST*	
10:50– 11:10	**MiRath** *Presented by: Loïc Bidoux, Technology Innovation Institute*
11:10 – 11:30	**SDitH** *Presented by: Thibauld Feneuil, CryptoExperts, Sorbonne Universite*
11:30 – 11:50	**RYDE** *Presented by: Loïc Bidoux, Technology Innovation Institute*
11:50– 12:10	**MQOM** *Presented by: Thibauld Feneuil, CryptoExperts, Sorbonne Universite*
12:10– 12:30	**Perk** *Presented by: Loïc Bidoux, Technology Innovation Institute*
12:30 – 2:00	**LUNCH** **Box lunches will be provided to in-person attendees**
Session VII – NIST PQC Project Updates / NCCoE Panel *Session Chair: Gorjan Alagic, NIST*	
2:00 – 2:20	**NIST PQC Migration Project and Cryptoagility Project** *Presented by: Bill Newhouse, NIST/NCCoE*
2:20 – 3:20	**PANEL:** ***Moderator:*** *Bill Newhouse, NIST/NCCoE* ***Panelists:*** *Tommy Charles, HP Security Lab* *Judy Furlong, Dell* *Evgeny Gervis, Safelogic* *Jim Goodman, Crypto4A* *Suvi Lampila, SSH Communications Security Corp* *Vladimir Soukharev, InfoSec Global*
3:20 – 3:40	**BREAK**

Last Update: 9/16/2025
Send corrections/updates to:
pqc2025@nist.gov
Speakers/times are subject to change.

Thursday, September 25, 2025 (con't)	
Session VIII – Hardware *Session Chair: Jacob Lichtinger, NIST*	
3:40 – 4:00	**SPHINCSLET: An Area-Efficient Accelerator for the Full SPHINCS+ Digital Signature Algorithm** *Presented by: Sanjay Deshpande, Yale University*
4:00 – 4:20	**Optimizing HQC using Frobenius Additive FFT on a RISC-V-based System-on-Chip** *Presented by: Antonio Ras, CEA-LETI*
4:20 – 4:40	**Efficient Threshold ML-DSA up to 6 parties** *Presented by: Guilhem Niot, PQShield & University of Rennes (virtual)*
4:40 – 5:00	**High-Performance FPGA Accelerator for the Post-quantum Signature Scheme CROSS** *Presented by: Patrick Karl, Technical University of Munich*
5:00	**ADJOURN**

Last Update: 9/16/2025
Send corrections/updates to:
pqc2025@nist.gov
Speakers/times are subject to change.

Friday, September 26, 2025	
8:00 – 4:00	**Badge Pick Up and Coffee/Beverage Service**
Session IX – Algorithm Updates *Session Chair: Ray Perlner, NIST*	
9:00 – 9:20	**CROSS** *Presented by: Patrick Karl, Technical University of Munich*
9:20 – 9:40	**LESS** *Presented by: Edoardo Persichetti, Florida Atlantic University*
9:40 – 10:00	**SQIsign** *Presented by: Luca De Feo, IBM Research Europe*
10:00 – 10:20	**HAWK** *Presented by: Ludo Pulles, Centrum Wiskunde & Informatica*
10:20 – 10:40	**FAEST** *Presented by: Ward Beullens, IBM Research - Zurich*
10:40 – 11:10	**BREAK**
Session X – Security/Cryptanalysis II *Session Chair: Carl Miller, NIST*	
11:10 – 11:30	**A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures** *Presented by: Michele Battagliola, Università Politecnica delle Marche (virtual)*
11:30 – 11:50	**Hawk: Having Automorphisms Weakens Key** *Presented by: Ludo Pulles, Centrum Wiskunde & Informatica*
11:50 – 12:10	**Sieving with Streaming Memory Access** *Presented by: Jintai Ding, Xi'an Jiaotong-Liverpool University*
12:10 – 12:30	**On the Security of Round 2 SNOVA** *Presented by: Jan Adriaan Leegwater, Vacuas*
12:30 – 2:00	**LUNCH** **Box lunches will be provided to in-person attendees**
Session XI – Applications II *Session Chair: Hamilton Silberg, NIST*	
2:00 – 2:20	**A Comprehensive Study of the Signal Handshake Protocol: Bundled Authenticated Key Exchange** *Presented by: Ida Tucker, PQShield (virtual)*
2:20 – 2:40	**(Yet another) Analysis of MLWE's performance impact on specific TLS Use-cases** *Presented by: Panos Kampanakis, Amazon*
2:40 – 3:00	**Namirial's explorations regarding recent PQC solutions** *Presented by: Giulio Di Clemente, Namirial S.p.A.*

Last Update: 9/16/2025
Send corrections/updates to:
pqc2025@nist.gov
Speakers/times are subject to change.

Friday, September 26, 2025 (con't)	
Session XII – Modernization Panel *Session Chair: Thinh Dang, NIST*	
3:00 – 4:00	**PANEL: From Migration to Modernization:** Cryptographic Overhaul at Scale ***Moderated by:*** *Safi Amin, Sandbox AQ* ***Panelists:*** *Dr. Britta Hale, U.S. Dept. Of Defense* *Hubert Lê Văn Gồng, JP Morgan Chase* *Matt Campagna, Amazon Web Services* *Tom Patterson, Accenture*
4:00 – 4:05	**Wrap-Up and Adjourn**

Last Update: 9/16/2025
Send corrections/updates to:
pqc2025@nist.gov
Speakers/times are subject to change.