

5th PQC Standardization Conference
 April 10-12, 2024
 Draft Agenda

Hilton Washington DC/Rockville Hotel
 Plaza Ballroom (Lobby Level)

All times are Eastern Daylight Time (New York)

| Wednesday, April 10, 2024 | |
|--|---|
| 7:30 – 5:00 | Badge Pick Up and Coffee/Beverage Service |
| Session I – Welcome and Algorithm Updates <i>Session Chair: Dustin Moody, NIST</i> | |
| 9:00 – 9:10 | Welcome and Opening Remarks <i>Matt Scholl, NIST</i> |
| 9:10 – 9:20 | The U.S. Government's Transition to PQC <i>Dylan Presman, Office of the National Cyber Director</i> |
| 9:20 – 9:40 | Are we there yet? An Update on the NIST PQC Standardization Project <i>Dustin Moody, NIST</i> |
| 9:40 – 10:00 | FALCON <i>Presented by: Thomas Prest, PQShield</i> |
| 10:00 – 10:20 | BIKE <i>Presented by: Rafael Misoczki, Meta</i> |
| 10:20 – 10:40 | HQC <i>Presented by: Phillipe Gaborit, University of Limoges</i> |
| 10:40 – 11:00 | Classic McEliece <i>Presented by: Edoardo Persichetti, Florida Atlantic University</i> |
| 11:00 – 11:30 | BREAK |
| Session II – Side Channels <i>Session Chair: Carl Miller, NIST</i> | |
| 11:30 – 11:50 | Side Channel Resistant Sphincs⁺ <i>Presented by: Scott Fluhrer, Cisco</i> |
| 11:50 – 12:10 | Single trace HQC shared key recovery with SASCA <i>Presented by: Guillaume Goy, XLIM, University of Limoges</i> |
| 12:10 – 12:30 | Single-Trace Side-Channel Attacks on CRYSTALS-Dilithium: Myth or Reality? <i>Presented by: Kalle Ngo, KTH Royal Institute of Technology</i> |
| 12:30 – 2:00 | LUNCH – On Your Own Onsite Restaurant – Olives: Lunch 11:00AM – 1:00PM List of Local Restaurants |

Last Update: 4/12/2024
 Send corrections/updates to: pqc2024@nist.gov
 Speakers/times are subject to change.

| Wednesday, April 10, 2024 (con't) | |
|---|--|
| Session III – 4th Round Panel / Poster Session 1 <i>Session Chair: Angela Robinson, NIST</i> | |
| 2:00 – 3:00 | PANEL: BIKE / HQC / Classic McEliece <i>Moderator: Angela Robinson, NIST</i> <i>Panelists: Nicolas Sendrier, INRIA</i> <i>Carlos Aguilar Melchor, SandboxAQ</i> <i>Edoardo Persichetti, Florida Atlantic University</i> |
| 3:00 – 3:30 | POSTER SESSION 1: Onramp Signature Candidates – Regency Room |
| 3:30 – 4:00 | BREAK |
| Session IV – Transitions <i>Session Chair: Quynh Dang, NIST</i> | |
| 4:00 – 4:20 | Migrating Some Legacy e-Governance Applications to Post-Quantum Cryptography <i>Presented by: Petr Muzikant, Cybernetica AS</i> |
| 4:20 – 4:40 | PQC Standardization A Vendor's Perspective <i>Presented by: Michael Hamburg, Rambus</i> |
| 4:40 – 5:00 | The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections <i>Presented by: Panos Kampanakis, AWS</i> |
| 5:00 | ADJOURN |

| Thursday, April 11, 2024 | |
|--|---|
| 8:00 – 5:00 | Badge Pick Up and Coffee/Beverage Service |
| Session V – Signatures <i>Session Chair: Ray Perlner, NIST</i> | |
| 9:00 – 9:20 | Post-Quantum Signatures from Threshold Computation in the Head <i>Presented by: Matthieu Rivain, CryptoExperts</i> |
| 9:20 – 9:40 | One Tree to Rule Them All: Optimizing GGM Trees and OWFs for Post-Quantum Signatures -- Preliminary Report <i>Presented by: Lawrence Roy, Aarhus University</i> |
| 9:40 – 10:00 | ANTRAG: Simplifying and Improving Falcon Without Compromising Security <i>Presented by: Thi Thu Quyen Nguyen, IDEMIA, Université de Rennes - Irisa</i> |
| 10:00 – 10:20 | A note on SPHINCS+ parameter sets <i>Presented by: Stefan Kölbl, Google</i> |
| 10:20 – 10:40 | Accelerating SLH-DSA by Two Orders of Magnitude with a Single Hash Unit <i>Presented by: Markku-Juhani O. Saarinen, SoC Hub Research Centre, Tampere University, Finland</i> |
| 10:40 – 11:00 | Threshold Raccoon <i>Presented by: Thomas Prest, PQShield</i> |
| 11:00 – 11:20 | BREAK |
| Session VI – NIST Standards Talks <i>Session Chair: Jacob Lichtinger, NIST</i> | |
| 11:20– 11:40 | FIPS 203 <i>Presented by: Quynh Dang, NIST</i> |
| 11:40– 12:00 | FIPS 204 <i>Presented by: Ray Perlner, NIST</i> |
| 12:00– 12:20 | FIPS 205 <i>Presented by: John Kelsey, NIST</i> |
| 12:20 – 1:45 | LUNCH – On Your Own Onsite Restaurant – Olives: Lunch 11:00AM – 1:00PM List of Local Restaurants |
| Session VII – NCCoE Panel - Discovery / Poster Session 2 <i>Session Chair: Bill Newhouse, NIST/NCCoE</i> | |
| 1:45 – 2:30 | PANEL: <i>Managing Cryptography: Cryptographic Discovery & PQC Migration</i> Moderator: Evgeny Gervis, SafeLogic, Inc. Panelists: Philip Lafrance, ISARA Corporation Tommy Charles, HP Vladimir Soukharev, InfoSec Global Carlos Aguilar Melchor, SandboxAQ |
| 2:30 – 3:00 | POSTER SESSION 2: Onramp Signature Candidates – Regency Room |
| 3:00 – 3:20 | BREAK |

Last Update: 4/12/2024
Send corrections/updates to: pqc2024@nist.gov
Speakers/times are subject to change.

f

| Thursday, April 11, 2024 (con't) | |
|--|--|
| Session VIII – Cryptanalysis <i>Session Chair: Maxime Bros, NIST</i> | |
| 3:20 – 3:40 | Preliminary Cryptanalysis of the Biscuit Signature Scheme <i>Presented by: Julia Sauvage, Sorbonne Université</i> |
| 3:40 – 4:00 | Efficacy and Mitigation of the Cryptanalysis on AIM <i>Presented by: Seongkwang Kim, Samsung SDS</i> |
| 4:00 – 4:20 | Finding isomorphisms between trilinear forms, slightly faster <i>Presented by: Anand Narayanan, SandboxAQ</i> |
| 4:20 – 4:40 | Cryptanalysis of the SNOVA signature scheme merged w/ Practical and Theoretical Cryptanalysis of VOX <i>Presented by: Jintai Ding, Beijing Institute of Mathematical Sciences and Applications and Tsinghua University</i> |
| 4:40 – 5:00 | New security analysis for UOV-based signature candidates with small public key size <i>Presented by: Yasuhiko Ikematsu, Kyushu University</i> |
| 5:00 | ADJOURN |

*Last Update: 4/12/2024
Send corrections/updates to: pqc2024@nist.gov
Speakers/times are subject to change.*

| Friday, April 12, 2024 | |
|--|---|
| 8:00 – 4:00 | Badge Pick Up and Coffee/Beverage Service |
| Session IX – Hardware <i>Session Chair: Hamilton Silberg, NIST</i> | |
| 9:00 – 9:20 | Nibbling MAYO: Optimized Implementations for AVX2 and Cortex-M4 <i>Presented by: Ward Beullens, IBM Research Europe</i> |
| 9:20 – 9:40 | SDitH in Hardware <i>Presented by: Sanjay Deshpande, Yale University</i> |
| 9:40 – 10:00 | pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers <i>Presented by: Matthias J. Kannwischer, Quantum Safe Migration Center</i> |
| 10:00 – 10:20 | Novel Schoolbook-Originated Polynomial Multiplication Accelerators for NTRU-based PQC <i>Presented by: Jiafeng (Harvest) Xie, Villanova University</i> |
| 10:20 – 10:50 | BREAK |
| Session X – Theory <i>Session Chair: Yi-Kai Liu, NIST</i> | |
| 10:50– 11:00 | A lean BIKE KEM design for ephemeral key agreement <i>Presented by: Shay Gueron, University of Haifa and Meta</i> |
| 11:00– 11:20 | How Multi-Recipient KEMs can help the Deployment of Post-Quantum Cryptography <i>Presented by: Thomas Prest, PQShield</i> |
| 11:20– 11:40 | Bit-flipping Decoder Failure Rate Estimation for (v,w)-regular Codes <i>Presented by: Alessandro Barenghi, Politecnico di Milano</i> |
| 11:40– 12:00 | On the Practical cost of Grover for AES Key Recovery <i>Presented by: Sarah D., NCSC</i> |
| 12:00 – 1:30 | LUNCH – On Your Own Onsite Restaurant – Olives: Lunch 11:00AM – 1:00PM List of Local Restaurants |
| Session XI – NCCoE Panel - Interoperability <i>Session Chair: Andy Regenscheid, NIST</i> | |
| 1:30 – 2:30 | PANEL: NIST SP 1800-38C, Quantum Readiness: Testing Draft Standards for Interoperability and Performance Moderator: Christian Paquin, Microsoft Panelists: Jim Goodman, Crypto4A Technologies, Inc. John Gray, Entrust Volker Krummel, Utimaco |

*Last Update: 4/12/2024
Send corrections/updates to: pqc2024@nist.gov
Speakers/times are subject to change.*

Friday, April 12, 2024 (con't)

Session XII – Pre-Hash Panel

Session Chair: John Kelsey, NIST

2:30 – 3:00

PANEL: Rehashing Pre-Hashing

Moderated by: John Kelsey, NIST

Panelists: Scott Fluhrer, Cisco

Joseph Harvey, Verisign

Markku-Juhani O. Saarinen, SoC Hub Research Centre, Tampere

University, Finland

3:00 –

Wrap-Up and Adjourn

Last Update: 4/12/2024

Send corrections/updates to: pqc2024@nist.gov

Speakers/times are subject to change.