# 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

**Session Chair:** Dustin Moody

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 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**  
Presented by: Peter Schwabe, MPI-SP & Radboud University |
| 10:45 – 11:00 | **CRYSTALS-Dilithium**  
Presented by: Vadim Lyubashevsky, IBM Research Europe, Zurich |
| 11:00 – 11:15 | **FALCON**  
Presented by: Thomas Prest, PQShield SAS |
| 11:15 – 11:30 | **SPHINCS+**  
Presented by: Andreas Hülsing, TU Eindhoven |
| 11:30 – 11:50 | **SPHINCS+C: Compressing SPHINCS+ With (Almost) No Cost**  
Presented by: Eyal Ronen, Tel Aviv University |
| 11:50 – 12:10 | **Twelve-round Keccak for secure hashing**  
Presented by: Gilles Van Assche, STMicroelectronics |
| 12:10 – 12:15 | **1st Annual RWPQC 2023 announcement**  
Daniel Apon, MITRE |
| 12:15 – 13:00 | **BREAK** |

### Session II – Side Channels

**Session Chair:** Yi-Kai Liu

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 13:00 – 13:20 | **A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext**  
Presented by: Guillaume Goy, Université Grenoble Alpes, CEA |
| 13:20 – 13:40 | **FALCON Down: Breaking FALCON Post-Quantum Signature Scheme through Side-Channel Attacks**  
Presented by: Aydin Aysu, North Carolina State University |
| 13:40 – 14:00 | **Leveling Dilithium against Leakage, Revisited Sensitivity Analysis and Improved Implementations**  
Presented by: Melissa Azouaoui, NXP Semiconductors |
| 14:00 – 14:20 | **The Challenge of Side-Channel Countermeasures on Post-Quantum Crypto**  
Presented by: Rina Zeitoun, IDEMIA |
| 14:20 – 14:40 | **Towards Leakage-Resistant Post-Quantum CCA-Secure Public Key Encryption**  
Presented by: François-Xavier Standaert & Thomas Peters, UCLouvain |
| 14:40 – 15:00 | **Optimization for SPHINCS+ using Intel® Secure Hash Algorithm Extensions**  
Presented by: Qian Wang, Intel |
| 15:00       | **ADJOURN** |

Last Updated: November 10, 2022  
Speakers/times are subject to change.
## Wednesday, November 30, 2022

### Session III – NSA Talk / Security
*Session Chair: Angela Robinson*

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00 – 10:40</td>
<td>Transitioning National Security Systems to a Post Quantum Future</td>
<td>Morgan Stern, NSA</td>
</tr>
<tr>
<td>10:40 – 11:00</td>
<td>Practical Improvements on BKZ Algorithm</td>
<td>Ziyu Zhao, Tsinghua University</td>
</tr>
<tr>
<td>11:00 – 11:20</td>
<td>Probabilistic Hash-and-Sign with Retry in the Quantum Random Oracle Model</td>
<td>Haruhisa Kosuge, Japan Ministry of Defense</td>
</tr>
<tr>
<td>11:20 – 11:40</td>
<td>A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem</td>
<td>Christopher Battarbee, University of York, UK</td>
</tr>
<tr>
<td>11:40 – 12:00</td>
<td>Quantum Augmented Dual Attack [this talk will not be recorded]</td>
<td>Yixin Shen, Royal Holloway, University of London</td>
</tr>
</tbody>
</table>

12:00 – 13:00 **BREAK**

### Session IV – Candidate Updates / Hardware I
*Session Chair: Quynh Dang*

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:00 – 13:15</td>
<td>BIKE</td>
<td>Rafael Misoczki, Google</td>
</tr>
<tr>
<td>13:30 – 13:45</td>
<td>HQC</td>
<td>Philippe Gaborit, University of Limoges, France</td>
</tr>
<tr>
<td>13:45 – 14:00</td>
<td>SIKE</td>
<td>David Jao, University of Waterloo</td>
</tr>
<tr>
<td>14:00 – 14:20</td>
<td>Benchmarking and Analysing NIST PQC Lattice-Based Signature Scheme Standards on the ARM Cortex M7</td>
<td>James Howe, SandboxAQ</td>
</tr>
<tr>
<td>14:20 – 14:40</td>
<td>A Flexible Shared Hardware Accelerator for NIST-Recommended Algorithms</td>
<td>Abubakr Abdulgadir, PQSecure Technologies</td>
</tr>
<tr>
<td>14:40 – 15:00</td>
<td>High-Performance Hardware Implementation of Lattice-Based Digital Signatures</td>
<td>Luke Beckwith, George Mason University</td>
</tr>
<tr>
<td>15:00 – 15:40</td>
<td>PANEL: Impact of PQC Signatures in Protocols and Applications</td>
<td>David Cooper, NIST</td>
</tr>
</tbody>
</table>

*Panelists: Scott Fluhrer, Cisco  Russ Housley, Vigil Security, LLC  Bas Westerbaan, Cloudflare  Eric Rescorla, Mozilla*

15:40 **ADJOURN**
# Thursday, December 1, 2022

## Session V – Migration

**Session Chair: Ray Perlner**

10:00 – 10:15  **The National Cybersecurity Center of Excellences (NCCoE) Migration to Post-Quantum Cryptography Project**  
*Bill Newhouse, NIST/NCCoE*

10:15 – 10:50  **PANEL - Approaches to PQC Migration**  
*Moderated by: Curt Barker, MITRE/NIST-NCCoE  
Panelists: Anne Dames, IBM  
Bruno Couillard, Crypto4A  
Avesta Hajjati, DigiCert*

10:50 – 11:10  **Algebraic Relation of Three MinRank Algebraic Modelings**  
*Presented by: Hao Guo, Tsinghua University*

11:10 – 11:30  **Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice**  
*Presented by: Burt Kaliski, Verisign*

11:30 – 11:50  **An Efficient and Generic Construction for Signal’s Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable**  
*Presented by: Thomas Prest, PQShield SAS*

11:50 – 12:00  **Cloudflare PQC experiment**  
*Presented by: Bas Westerbaan, Cloudflare*

12:00 – 13:00  **BREAK**

## Session VI – Hardware II

**Session Chair: Daniel Smith-Tone**

13:00 – 13:20  **A Masked Pure-Hardware Implementation of Kyber Cryptographic Algorithm**  
*Presented by: Tendayi Kamucheka, University of Arkansas*

13:20 – 13:40  **Mckeycutter: A High-throughput Key Generator of Classic McEliece on Hardware**  
*Presented by: Yihong Zhu, Tsinghua University*

13:40 – 14:00  **Fast and Efficient Hardware Implementation of HQC**  
*Presented by: Sanjay Deshpande, Yale University & Kashif Nawaz, Technology Innovation Institute*

14:00 – 14:20  **Complete and Improved FPGA Implementation of Classic McEliece**  
*Presented by: Sanjay Deshpande, Yale University*

14:20 – 14:40  **Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions**  
*Presented by: Duc Tri Nguyen, George Mason University*

14:40 – 14:50  **Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange**  
*Presented by: John Preuß Mattsson, Ericsson*

14:50 – 15:10  **Post-Quantum Protocols for Banking Applications** [this talk will not be recorded]  
*Presented by: Emmanuelle Dottax, IDEMIA*

15:10 – 15:30  **Wrap-Up**  
*NIST PQC Team*

15:30  **ADJOURN**