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

<table>
<thead>
<tr>
<th>Time</th>
<th>Session I – Welcome and Algorithm Updates</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 – 9:10</td>
<td>Welcome and Opening Remarks</td>
<td>Matt Scholl, NIST</td>
</tr>
<tr>
<td>9:10 – 9:20</td>
<td>The U.S. Government’s Transition to PQC</td>
<td>Dylan Presman, Office of the National Cyber Director</td>
</tr>
<tr>
<td>9:20 – 9:40</td>
<td>Are we there yet? An Update on the NIST PQC Standardization Project</td>
<td>Dustin Moody, NIST</td>
</tr>
<tr>
<td>9:40 – 10:00</td>
<td>FALCON</td>
<td>Thomas Prest, PQShield</td>
</tr>
<tr>
<td>10:00 – 10:20</td>
<td>BIKE</td>
<td>Rafael Misoczki, Meta</td>
</tr>
<tr>
<td>10:20 – 10:40</td>
<td>HQC</td>
<td>Phillipe Gaborit, University of Limoges</td>
</tr>
<tr>
<td>10:40 – 11:00</td>
<td>Classic McEliece</td>
<td>Edoardo Persichetti, Florida Atlantic University</td>
</tr>
<tr>
<td>11:00 – 11:30</td>
<td>BREAK</td>
<td></td>
</tr>
</tbody>
</table>

### Session II – Side Channels

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Chair: Carl Miller, NIST</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:30 – 11:50</td>
<td>Side Channel Resistant Sphincs*</td>
<td>Scott Fluhrer, Cisco</td>
</tr>
<tr>
<td>11:50 – 12:10</td>
<td>Single trace HQC shared key recovery with SASCA</td>
<td>Guillaume Goy, XLIM, University of Limoges</td>
</tr>
<tr>
<td>12:10 – 12:30</td>
<td>Single-Trace Side-Channel Attacks on CRYSTALS-Dilithium: Myth or Reality?</td>
<td>Kalle Ngo, KTH Royal Institute of Technology</td>
</tr>
<tr>
<td>12:30 – 2:00</td>
<td>LUNCH</td>
<td></td>
</tr>
</tbody>
</table>
### Wednesday, April 10, 2024 (con’t)

**Session III – 4\(^{th}\) Round Panel / Poster Session 1**  
*Session Chair: Angela Robinson, NIST*

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 2:00 – 3:00 | **PANEL:** BIKE / HQC / Classic McEliece  
**Moderator:** Angela Robinson, NIST  
**Panelists:** Nicolas Sendrier, INRIA  
Carlos Aguilar Melchor, SandboxAQ  
Edoardo Persichetti, Florida Atlantic University |
| 3:00 – 3:30 | **POSTER SESSION 1:** Onramp Signature Candidates – Regency Room |
| 3:30 – 4:00 | **BREAK** |

**Session IV – Transitions**  
*Session Chair: Quynh Dang, NIST*

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 4:00 – 4:20 | **Migrating Some Legacy e-Governance Applications to Post-Quantum Cryptography**  
*Presented by: Petr Muzikant, Cybernetica AS* |
| 4:20 – 4:40 | **PQC Standardization A Vendor’s Perspective**  
*Presented by: Michael Hamburg, Rambus* |
| 4:40 – 5:00 | **The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections**  
*Presented by: Panos Kampanakis, AWS* |
| 5:00     | **ADJOURN** |
### Thursday, April 11, 2024

#### Session V – Signatures
*Session Chair: Ray Perlner, NIST*

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Presenter Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 – 9:20</td>
<td>Post-Quantum Signatures from Threshold Computation in the Head</td>
<td>Presented by: Matthieu Rivain, CryptoExperts</td>
</tr>
<tr>
<td>9:40 – 10:00</td>
<td>ANTRAG: Simplifying and Improving Falcon Without Compromising Security</td>
<td>Presented by: Thi Thu Quyen Nguyen, IDEMIA, Université de Rennes - Irisa</td>
</tr>
<tr>
<td>10:00 – 10:20</td>
<td>A note on SPHINCS+ parameter sets</td>
<td>Presented by: Stefan Kölbl, Google</td>
</tr>
<tr>
<td>10:20 – 10:40</td>
<td>Accelerating SLH-DSA by Two Orders of Magnitude with a Single Hash Unit</td>
<td>Presented by: Markku-Juhani O. Saarinen, SoC Hub Research Centre, Tampere University, Finland</td>
</tr>
<tr>
<td>10:40 – 11:00</td>
<td>Threshold Raccoon</td>
<td>Presented by: Thomas Prest, PQShield</td>
</tr>
<tr>
<td>11:00 – 11:20</td>
<td>BREAK</td>
<td></td>
</tr>
</tbody>
</table>

#### Session VI – NIST Standards Talks
*Session Chair: Jacob Lichtinger, NIST*

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Presenter Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:20–11:40</td>
<td>FIPS 203</td>
<td>Quynh Dang, NIST</td>
</tr>
<tr>
<td>11:40–12:00</td>
<td>FIPS 204</td>
<td>Ray Perlner, NIST</td>
</tr>
<tr>
<td>12:00–12:20</td>
<td>FIPS 205</td>
<td>John Kelsey, NIST</td>
</tr>
<tr>
<td>12:20 – 1:45</td>
<td>LUNCH</td>
<td></td>
</tr>
</tbody>
</table>

#### Session VII – NCCoE Panel - Discovery / Poster Session 2
*Session Chair: Bill Newhouse, NIST/NCCoE*

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Moderator Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:45 – 2:30</td>
<td>PANEL: NIST SP 1800-38B, Quantum Readiness: Cryptographic Discovery</td>
<td>Evgeny Gervis, SafeLogic, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Philip Lafrance, ISARA Corporation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tommy Charles, HP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vladimir Soukharev, InfoSec Global</td>
</tr>
<tr>
<td>2:30 – 3:00</td>
<td>POSTER SESSION 2: Onramp Signature Candidates – Regency Room none</td>
<td></td>
</tr>
<tr>
<td>3:00 – 3:20</td>
<td>BREAK</td>
<td></td>
</tr>
</tbody>
</table>
### Thursday, April 11, 2024 (con’t)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3:20 – 3:40</td>
<td>Preliminary Cryptanalysis of the Biscuit Signature Scheme</td>
<td>Julia Sauvage, Sorbonne Université</td>
</tr>
<tr>
<td>3:40 – 4:00</td>
<td>Efficacy and Mitigation of the Cryptanalysis on AIM</td>
<td>Seongkwang Kim, Samsung SDS</td>
</tr>
<tr>
<td>4:00 – 4:20</td>
<td>Finding isomorphisms between trilinear forms, slightly faster</td>
<td>Anand Narayanan, SandboxAQ</td>
</tr>
<tr>
<td>4:20 – 4:40</td>
<td>Cryptanalysis of the SNOVA signature scheme merged w/ Practical and Theoretical Cryptanalysis of VOX</td>
<td>Jintai Ding, Beijing Institute of Mathematical Sciences and Applications and Tsinghua University</td>
</tr>
<tr>
<td>4:40 – 5:00</td>
<td>New security analysis for UOV-based signature candidates with small public key size</td>
<td>Yasuhiko Ikematsu, Kyushu University</td>
</tr>
</tbody>
</table>

5:00 ADJOURN
## Friday, April 12, 2024

### Session IX – Hardware

**Session Chair:** Hamilton Silberg, NIST  

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Presenter Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00–9:20</td>
<td>Nibbling MAYO: Optimized Implementations for AVX2 and Cortex-M4</td>
<td>Ward Beullens, IBM Research Europe</td>
</tr>
<tr>
<td>9:20–9:40</td>
<td>SDith in Hardware</td>
<td>Sanjay Deshpande, Yale University</td>
</tr>
<tr>
<td>9:40–10:00</td>
<td>pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers</td>
<td>Matthias J. Kannwischser, Quantum Safe Migration Center</td>
</tr>
<tr>
<td>10:00–10:20</td>
<td>Novel Schoolbook-Originated Polynomial Multiplication Accelerators for NTRU-based PQC</td>
<td>Jiafeng (Harvest) Xie, Villanova University</td>
</tr>
<tr>
<td>10:20–10:50</td>
<td><strong>BREAK</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Session X – Theory

**Session Chair:** Yi-Kai Liu, NIST  

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Presenter Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:50–11:10</td>
<td>A lean BIKE KEM design for ephemeral key agreement</td>
<td>Shay Gueron, University of Haifa and Meta</td>
</tr>
<tr>
<td>11:10–11:20</td>
<td>How Multi-Recipient KEMs can help the Deployment of Post-Quantum Cryptography</td>
<td>Thomas Prest, PQShield</td>
</tr>
<tr>
<td>11:20–11:40</td>
<td>Bit-flipping Decoder Failure Rate Estimation for (v,w)-regular Codes</td>
<td>Alessandro Barenghi, Politecnico di Milano</td>
</tr>
<tr>
<td>11:40–12:00</td>
<td>On the Practical cost of Grover for AES Key Recovery</td>
<td>Sarah D., NCSC</td>
</tr>
<tr>
<td>12:00–1:30</td>
<td><strong>LUNCH</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Session XI – NCCoE Panel - Interoperability

**Session Chair:** Andy Regenscheid, NIST  

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Details</th>
</tr>
</thead>
</table>
Panelists:  
Jim Goodman, Crypto4A Technologies, Inc.  
John Gray, Entrust  
Volker Krummel, Utimaco |
| 2:30–3:00  | **BREAK**                                                                                 |                                                                                           |
### Friday, April 12, 2024 (con’t)

| Session XII – Pre-Hash Panel  
| Session Chair: John Kelsey, NIST  |
|---|---|
| 3:00 – 3:30 | **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 |
| 3:30 – | **Wrap-Up and Adjourn** |
# 5th PQC Standardization Conference
## Onramp Signature Candidates Poster Sessions
### April 10 & 11, 2024
#### Regency Room

<table>
<thead>
<tr>
<th>Algorithm Name</th>
<th>Presenter Name</th>
<th>Session to Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biscuit</td>
<td>Verbel, Javier</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>EagleSign</td>
<td>Sow, Djiby and Djimnaibeye, Sidoine</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>EHT</td>
<td>Feussner, Martin OR Semaev, Igor</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>eMLE-Sig 2.0</td>
<td>Liu, Dongxi</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>Enhanced pqsigRM</td>
<td>Lee, Yongwoo</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>FAEST</td>
<td>Roy, Lawrence</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>Hawk</td>
<td>Prest, Thomas</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>LESS</td>
<td>Persichetti, Edoardo</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>MAYO</td>
<td>Kannwischer, Matthias and Beullens, Ward</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>MQOM</td>
<td>Rivain, Matthieu</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>Perk</td>
<td>Bidoux, Loic</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>RYDE</td>
<td>Bidoux, Loic</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>SDitH</td>
<td>Yue, Dongze (Steven)</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>Squirrels</td>
<td>Prest, Thomas</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>TUOV</td>
<td>Ding, Jintai</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>Wave</td>
<td>Debris-Alazard, Thomas</td>
<td>Wednesday (3pm-3:30pm)</td>
</tr>
<tr>
<td>Aimer</td>
<td>Kim, Seongkwang</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>Alteq</td>
<td>Narayanan, Anand Kumar</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>CROSS</td>
<td>Karl, Patrick</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>DME-Sign</td>
<td>Luengo, Ignacio</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>FuLeeca</td>
<td>Ritterhoff, Stefan</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>HAETAE</td>
<td>Devevey, Julien</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>KAZ</td>
<td>Nagaraja, Aishnavi A/P</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>MEDS</td>
<td>Persichetti, Edoardo</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>Mira</td>
<td>Gabo, Philippe</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>MiRitH</td>
<td>Verbel, Javier</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>Preon</td>
<td>Liu, Feng-Hao</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>QR-UOV</td>
<td>Kinjo, Koha</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>Raccoon</td>
<td>Prest, Thomas</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>SNOVA</td>
<td>Tseng, Po-En and Kuan, Yen-Liang</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>UOV</td>
<td>Yang, Bo-Yin</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
<tr>
<td>Vox</td>
<td>Macario-Rat, Gilles</td>
<td>Thursday (2:30pm-3pm)</td>
</tr>
</tbody>
</table>

*Updated 3/29/2024*