# NIST Threshold Workshop 2019 — Program schedule

All talks take place in the Green Auditorium in the Main Building (101) at the NIST campus in Gaithersburg, MD, USA.

## Attendees

Attendees need to pre-register to attend the conference. Badge pick-up (for on time and late arrivals) is done in front of the Green auditorium.

## Shuttle Information

For guests at the Courtyard by Marriott Hotel, Gaithersburg, a shuttle will be available (both days) at 7:30am for Hotel → NIST, and at 5:45pm (Monday) or 5:30pm (Tuesday) for NIST → Hotel.

- A NIST shuttle to Shady Grove Metro Station departs from the NIST Building 101 at 5 and 35 minutes past the hour. The last NIST shuttle leaves NIST at 6:00 p.m.

- See https://www.nist.gov/about-nist/getting-nist-gaithersburg for further details

---

### 1st day of workshop (Monday, March 11, 2019)

<table>
<thead>
<tr>
<th>Session</th>
<th>Hour</th>
<th>Time</th>
<th>1st day of workshop (Monday, March 11, 2019)</th>
<th>Source</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opening</td>
<td>08:00-08:45</td>
<td>45</td>
<td>Badge pick-up; light refreshments available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.1. Threshold Schemes</td>
<td>09:00-09:10</td>
<td>10</td>
<td>NIST Computer Security Division welcoming. Matthew Scholl (NIST, USA)</td>
<td>Invited Keynote</td>
<td></td>
</tr>
<tr>
<td></td>
<td>09:10-09:25</td>
<td>15</td>
<td>Enter the Threshold (The NIST Threshold Cryptography Project). Luis Brandão (NIST, USA)</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>09:25-10:15</td>
<td>50</td>
<td>Threshold Cryptography: Ready for Prime Time? Hugo Krawczyk (IBM Research, USA)</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>10:15-10:40</td>
<td>25</td>
<td>Platform for Robust Threshold Cryptography. Christian Cachin (University of Bern, Switzerland), Hugo Kravczyk (IBM Research, USA), Tal Rabin (IBM Research, USA), Jason Resch (IBM, USA), Chryssoula Statathopoulos (IBM research, Zurich, Switzerland)</td>
<td>Submitted</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>10:40-10:10</td>
<td>30</td>
<td>Coffee break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.2. NIST Standards (Chair: Andrew Regenscheidt, NIST)</td>
<td>11:10-11:40</td>
<td>30</td>
<td>The NIST Standardization Approach on Cryptography — Past, Present, and Future. Lily Chen (NIST, USA)</td>
<td>NIST</td>
<td>5</td>
</tr>
<tr>
<td>I.3. Threshold Post-Quantum (Chair: Daniel Apon, NIST)</td>
<td>12:00-12:15</td>
<td>25</td>
<td>Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme. Michael Kraisberg (Unbound Technology, Israel), Yehuda Lindell (Bar-Ilan University, Unbound Technology, Israel), Valery Osheter (Unbound Technology, Israel), Nigel P. Smart (KU Leuven, Belgium; University of Bristol, UK), Younes Talibi Alaaoui (KU Leuven, Belgium)</td>
<td>Submitted</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>12:25-13:45</td>
<td>80</td>
<td>Lunch (at the heritage room)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.4. Threshold Signatures (Chair: Daniel Apon, NIST)</td>
<td>13:45-14:10</td>
<td>25</td>
<td>Fully Distributed Non-Interactive Adaptively-Secure Threshold Signature Scheme with Short Shares: Efficiency Considerations and Implementation. Benoît Libert (CNRS and ENS de Lyon, France), Marc Joye (OneSpan, Belgium), Moti Yung (Google Inc. and Columbia University, USA), Fabrice Mouhartem (ENS de Lyon, France)</td>
<td>Submitted</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>14:10-14:35</td>
<td>25</td>
<td>A Multiparty Computation Approach to Threshold ECDSA. Jack Doerner (Northeastern University, USA), Yashavantar Kondi (Northeastern University, USA), Eysa Lee (Northeastern University, USA), abhi shelat (Northeastern University, USA), Samuel Ranellucci (Unbound Tech, Israel)</td>
<td>Submitted</td>
<td>9</td>
</tr>
<tr>
<td>I.5. Panel on Threshold for DSS (Chair: Hugo Kravczyk, IBM Research)</td>
<td>14:35-15:35</td>
<td>60</td>
<td>Threshold Protocols for the Digital Signature Standard. Moderator: Hugo Krawczyk (IBM Research, USA); Panelists: Rosario Gennaro (CUNY, USA), abhi shelat (Northeastern University, USA), Samuel Ranellucci (Unbound Tech, Israel)</td>
<td>Submitted</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>15:35-16:05</td>
<td>30</td>
<td>Coffee break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.6. Validation (Chair: Michael Cooper, NIST)</td>
<td>16:05-16:45</td>
<td>40</td>
<td>Quo Vadis, Crypto Validation? Apostol Vassilev (NIST, USA)</td>
<td>NIST</td>
<td>11</td>
</tr>
<tr>
<td>I.7. Discussion (Chair: Michael Cooper, NIST)</td>
<td>16:45-17:30</td>
<td>45</td>
<td>Open guided discussion. Moderator: Nicky Mouha (NIST, USA)</td>
<td>NIST</td>
<td>12</td>
</tr>
</tbody>
</table>

---

### 2nd day of workshop (Tuesday, March 12, 2019)

<table>
<thead>
<tr>
<th>Session</th>
<th>Hour</th>
<th>Time</th>
<th>2nd day of workshop (Tuesday, March 12, 2019)</th>
<th>Source</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>II. Threshold Primitives (Chair: John Kelsey, NIST)</td>
<td>08:00-08:45</td>
<td>45</td>
<td>Badge pick-up; light refreshments available</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>08:45-09:05</td>
<td>25</td>
<td>Optimized Threshold Implementations: Number of Shares and Area/Latency Trade-off. Dušan Božilov (NXP Semiconductors, Belgium; COSIC KU Leuven and imec, Belgium), Miroslav Knežević (NXP Semiconductors, Belgium), Ventzislav Nikov (NXP Semiconductors, Belgium)</td>
<td>Submitted</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>09:09-09:35</td>
<td>25</td>
<td>The pitfalls of threshold cryptography in hardware. Marco Macchetti (Kudelski Group, Switzerland), Karine Villegas (Kudelski Group, Switzerland), Claudio Favi (Kudelski Group, Switzerland)</td>
<td>Submitted</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>09:35-10:00</td>
<td>25</td>
<td>Threshold Cryptography against Combined Physical Attacks. Lauren De Meyer (KU Leuven, Belgium)</td>
<td>Submitted</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>10:25-10:55</td>
<td>30</td>
<td>Coffee break</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12:10-12:30</td>
<td>80</td>
<td>Lunch (at the heritage room)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13:55-14:20</td>
<td>25</td>
<td>DISF: Distributed Symmetric-key Encryption. Shashank Agrawal (Visa Research, USA), Payman Mohassel (Visa Research, USA), Pratyay Mukherjee (Visa Research, USA), Peter Rindal (Visa Research, USA)</td>
<td>Submitted</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>14:20-14:50</td>
<td>50</td>
<td>Challenges for Multisignature and Threshold Signature Implementation in a Bitcoin Context. Andrew Poelstra (Blockstream, USA)</td>
<td>Invited Keynote</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>15:10-15:40</td>
<td>30</td>
<td>Coffee break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.4. Threshold Cryptography Applications and Experience (Chair: Daniel Apon, NIST)</td>
<td>15:40-16:05</td>
<td>25</td>
<td>SplitKey Case Study. Maximilian van de Poll (Cybernetica AS, Estonia), Aivo Kalu (Cybernetica AS, Estonia)</td>
<td>Submitted</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>16:05-16:30</td>
<td>25</td>
<td>Practical Threshold Cryptography for Cloud and Cryptocurrencies. Jakob Pagter (Sepior, Denmark)</td>
<td>Submitted</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>16:30-16:55</td>
<td>25</td>
<td>Practice Based Recommendations for Standardization of Threshold Cryptography. Daniel Shumow (Microsoft Research, USA)</td>
<td>Submitted</td>
<td>23</td>
</tr>
<tr>
<td>Closing</td>
<td>16:55-17:15</td>
<td>20</td>
<td>Final remarks. Moderator: Luis Brandão (NIST, USA)</td>
<td>NIST</td>
<td>24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Time durations are in minutes</th>
</tr>
</thead>
</table>

---

Available shuttle times:

- For guests at the Courtyard by Marriott Hotel, Gaithersburg, a shuttle will be available (both days) at 7:30am for Hotel → NIST, and at 5:45pm (Monday) or 5:30pm (Tuesday) for NIST → Hotel.

- A NIST shuttle to Shady Grove Metro Station departs from the NIST Building 101 at 5 and 35 minutes past the hour. The last NIST shuttle leaves NIST at 6:00 p.m.

- See https://www.nist.gov/about-nist/getting-nist-gaithersburg for further details

See online updates at the conference webpage: https://csrc.nist.gov/Events/2019/NTCW19