# Agenda

## NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

National Cybersecurity Center of Excellence

Rockville, Maryland

| Thursday, June 20, 2024 | |
|---|---|
| 8:15 | Shuttle Departs Courtyard Gaithersburg Washingtonian Center<br>*The shuttle is provided as a courtesy for guests staying at the Courtyard Gaithersburg Washingtonian Center.* |
| 8:30 – 9:00 | Arrival/Badging/Continental breakfast. |
| **Session I – Opening** *Session Chair: Morris Dworkin* | |
| 9:00 – 9:10 | Welcome<br>*Matthew Scholl* |
| 9:10 – 9:35 | Overview of the NIST Block Cipher Modes Project<br>*Meltem Sönmez Turan* |
| 9:35 – 10:00 | Introduction to the Accordion Mode and Derived Functions<br>*Alyssa Thompson* |
| 10:00 – 10:30 | Break |
| **Session II – Accordion Mode Requirements/Features (I)** *Session Chair: Yu Long Chen* | |
| 10:30 – 11:20 | Toward a New Block Cipher Mode Standard: Reasoning about Requirements Featuring the NECST Framework<br>*Nicky Mouha* |
| 11:20 – 11:40 | Comments on NIST Requirements for an Accordion Cipher Mode<br>*John Preuß Mattsson* |
| 11:40 – 12:00 | Security Goals for an Accordion Mode: Release of Unverified Plaintext and Multi-user Security<br>*Guy B.* |
| 12:00 – 1:20 | Lunch |

*Last Update: 6/21/2024*
*Speakers/times are subject to change.*

| Thursday, June 20, 2024 (con't) | |
|---|---|
| **Session III – Use Cases** *Session Chair: Andrew Regenscheid* | |
| 1:20 – 1:30 | NIST Options for Encryption Algorithms and Modes of Operation<br>*Andrew Regenscheid* |
| 1:30 – 2:30 | Panel Discussion: Adoption Perspectives<br>*Paul Crowley, Shai Halevi, Matthew Simpson, Krystian Matusiewicz*<br>Moderator: *Andrew Regenscheid* |
| 2:30 – 3:00 | Break |
| **Session IV – Accordion Mode Requirements/ Features (II)** *Session Chair: Nicky Mouha* | |
| 3:00-3:20 | Accordion Cipher-mode Preferable Features<br>*Tushar Patel* |
| 3:20-3:40 | Requirements for an Accordion Mode<br>*Guy B.* |
| 3:40-4:40 | Open Discussion |
| 4:45 | Shuttle Departs NCCoE to Return to Hotel<br>*The shuttle is provided as a courtesy for guests staying at the Courtyard Gaithersburg Washingtonian Center.* |

*Last Update: 6/21/2024*
*Speakers/times are subject to change.*

| Friday, June 21, 2024 | |
|---|---|
| 8:15 | Shuttle Departs Courtyard Gaithersburg Washingtonian Center<br>*The shuttle is provided as a courtesy for guests staying at the Courtyard Gaithersburg Washingtonian Center.* |
| 8:30 – 9:00 | Arrival/Badging/Continental breakfast. |
| **Session V – Lightning Talks** *Session Chair: Alyssa Thompson* | |
| 9:00 – 9:20 | *There were no lightning talks presented.* |
| **Session VI – Authenticated Encryption** *Session Chair: Alyssa Thompson* | |
| 9:20 – 9:40 | Galois Extended Mode<br>*Scott Arciszewski* |
| 9:40 – 10:00 | Double-Nonce-Derive-Key-GCM (DNDK-GCM) General Design Paradigms and Application<br>*Shay Gueron* |
| 10:00 – 10:30 | Break |
| **Session VII – Design Approaches** *Session Chair: Yu Sasaki* | |
| 10:30 – 10:50 | Efficient Instances of Docked Double Decker With AES, and Application to Authenticated Encryption<br>*Christoph Dobraunig* |
| 10:50 – 11:10 | Universal Hash Designs for an Accordion Mode<br>*Jean Paul Degabriele* |
| 11:10 – 11:30 | Accordion mode based on Hash-Encrypt-Hash<br>*Pablo Garcia Fernandez* |
| 11:30 – 11:50 | Open Discussion |
| 11:50 – 1:20 | Lunch |

*Last Update: 6/21/2024*
*Speakers/times are subject to change.*

| Friday, June 21, 2024 (con't) | |
|---|---|
| **Session VIII – Potential Security Properties** *Session Chair: Donghoon Chang* | |
| 1:20 – 1:40 | Committing Wide Encryption Mode with Minimum Ciphertext Expansion<br>*Yusuke Naito* |
| 1:40 – 2:00 | A BBB Secure Accordion Mode from HCTR<br>*Byeonghak Lee* |
| 2:00 – 2:20 | Information-theoretic Security with Asymmetries<br>*Yu Long Chen* |
| 2:20 – 2:40 | Open Discussion |
| 2:40 – 3:10 | Break |
| **Session IX – Next Steps** *Session Chair: Meltem Sönmez Turan* | |
| 3:10 – 3:30 | Preliminary NIST Proposal for a Development Process<br>*Morris Dworkin* |
| 3:30 – 4:30 | Open Discussion |
| 4:45 | Shuttle Departs NCCoE to Return to Hotel<br>*The shuttle is provided as a courtesy for guests staying at the Courtyard Gaithersburg Washingtonian Center.* |

*Last Update: 6/21/2024*
*Speakers/times are subject to change.*