NIST Interagency Report
NIST IR 8537

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

Workshop Report

Alyssa Thompson
Meltem Sönmez Turan

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8537

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8537

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

Workshop Report

Alyssa Thompson

National Security Agency

Guest Researcher, Computer Security Division
Information Technology Laboratory

Meltem Sönmez Turan

Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8537

November 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Publication History
Approved by the NIST Editorial Review Board on 2024-11-08

How to cite this NIST Technical Series Publication
Thompson A, Sönmez Turan M (2024) NIST Workshop on the Requirements for an Accordion Cipher Mode 2024: Workshop Report. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8537. https://doi.org/10.6028/NIST.IR.8537

Author ORCID iDs
Alyssa Thompson: 0009-0009-8137-2589
Meltem Sönmez Turan: 0000-0002-1950-7130

Contact Information
ciphermodes@nist.gov

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8537/final, including related content, potential updates, and document history.

Abstract

NIST hosted the *NIST Workshop on the Requirements for an Accordion Cipher Mode 2024* on June 20–21, 2024, at the National Cybersecurity Center of Excellence in Rockville, Maryland. This report summarizes the participant feedback, key takeaways, and future directions discussed during the event.

Keywords

accordion mode; block ciphers; cryptography; performance; standardization.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Table of Contents

1. Introduction 1

1.1. Background 1

2. Workshop Topics and Discussion 2

2.1. Opening Talks 2

2.2. Accordion Mode Features and Requirements 3

2.3. Panel Discussion on Adoption Perspectives 4

2.4. Authenticated Encryption 5

2.5. Design Approaches 6

2.6. Potential Security Properties 6

2.7. Next Steps 7

3. Summary of Feedback on Key Topics 9

Appendix A. Agenda 11

Appendix B. List of Accepted Presentations 13

Acknowledgments

The authors thank Drew Bowerman (NSA), Donghoon Chang, Yu Long Chen, Morris Dworkin, Jim Foti, Sara Kerman, Yu Sasaki, and Isabel Van Wyk for the valuable feedback they provided during the development of this document.

1. Introduction

On June 20–21, 2024, the National Institute of Standards and Technology (NIST) held an in-person Workshop on the Requirements for an Accordion Cipher Mode [1] at the National Cybersecurity Center of Excellence (NCCoE) in Rockville, Maryland. The event brought together 43 participants representing diverse perspectives from government, industry, and academia.

The purpose of the workshop was to discuss the development of a new *accordion* mode of the Advanced Encryption Standard (AES) that is a tweakable variable-input-length-strong pseudorandom permutation (VIL-SPRP) with a reduction proof to the security of the underlying block cipher. NIST also collected feedback on requirements from industry and government and initiated a discussion on the development of an accordion mode. Prior to the workshop, NIST published a discussion draft [2] with a preliminary set of proposed requirements for an accordion mode.

Topics of interest included the parameter sizes of the accordion mode, requirements and features for the main use cases, security notions under consideration, performance requirements, and the development and standardization process. Specific topics for which NIST requested feedback included multi-user security, key/context commitment, nonce hiding, and key-dependent input (KDI) security.[1] A summary of key takeaways is included in Sec. 3.

The workshop consisted of nine sessions scheduled over two days. The first day included introductory material from NIST researchers, presentations and an open discussion about the requirements and features of the accordion mode, and a panel discussion on adoption perspectives. The second day included presentations and open discussions on authenticated encryption designs, accordion design approaches, and potential security properties. The schedule on day two reserved time for lightning talks, but this was dropped since no requests for lightning talks were received. The workshop concluded with a session on the development process and next steps, including a preliminary NIST proposal for the process and open discussion. The full workshop agenda is available in Appendix A, and videos of the talks are available on the workshop website [1].

1.1. Background

Two topics of particular interest were the number of variants of the accordion mode that would be needed and the related projects that would be required as a result. This was largely influenced by the need for higher data limits and for crypto agility. Variants of the accordion mode might emerge from providing options for birthday bound security and beyond-birthday bound (BBB) security or from operating on different underlying primitives. Related projects that could result from these decisions include specifying a new underlying

[1] For more information, refer to the workshop announcement and the call for abstracts [1].

primitive or considering a stopgap solution that could be standardized quickly while in-depth techniques for the accordion are developed.

While BBB techniques would increase the data limits of the accordion mode, they would result in various trade-offs, including reduced performance and a more complicated security proof. An alternative approach that would also increase the data limits of the accordion mode is to specify a block cipher with a larger block size. An example with a 256-bit block size and a 256-bit key that could be considered is Rijndael-256-256, which was part of the original AES submission to NIST [3]. This approach would also provide an increased measure of crypto-agility, as would a Keccak-based encryption scheme as an underlying primitive. However, both options may result in a delay while the new primitive is standardized and deployed. In this scenario, standardizing a stopgap measure (e.g., AES-GCM-SIV [4]) could provide a mode of operation with improved security as quickly as possible.

These decisions depend on one another, and the answers will determine a base direction for the project. NIST collected feedback on these topics throughout the workshop, and the panel discussion explored many of these ideas (see Sec. 2.3).

2. Workshop Topics and Discussion

2.1. Opening Talks

NIST initiated the workshop with a set of introductory talks. During the opening session, Matthew Scholl, the Chief of the Computer Security Division (CSD) in NIST's Information Technology Laboratory (ITL), welcomed the workshop participants. The workshop featured three talks by NIST-affiliated speakers:

- In "Overview of the NIST Block Cipher Modes Project," Meltem Sönmez Turan briefly explained the development of NIST-approved block cipher modes, provided a timeline of the project starting from the 1980s, and gave a status update on reviews of the NIST Special Publication (SP) 800-38 series [5–11].
- In "Introduction to the Accordion Mode and Derived Functions," Alyssa Thompson explained the parameters of the accordion mode (including the block size, tweak size, granularity, message size, etc.) and provided a formal definition for it. The presentation introduced the derived functions, including authenticated encryption with associated data (AEAD), tweakable encryption, and deterministic authenticated encryption. It also explained the layered structure of the accordion (see Fig. 1).
- In "Toward a New Block Cipher Mode Standard: Reasoning About Requirements Featuring the NECST Framework," Nicky Mouha discussed the proposed requirements for an accordion mode that NIST published in [2] and provided a framework called *New features*, *Efficiency*, *Compatibility*, *Security and Technical reason* (NECST) for evaluating and making decisions on the requirements.

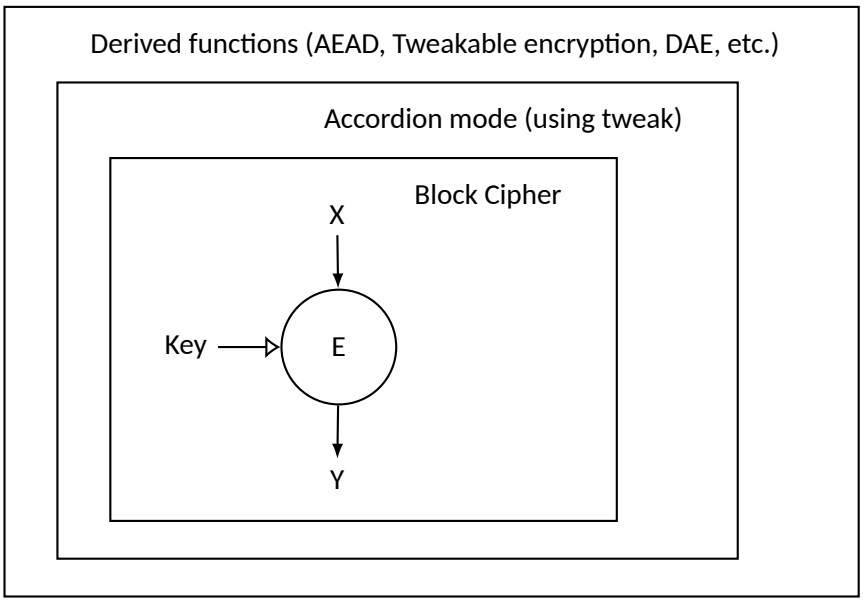

Figure 1. Layered structure of the accordion mode and derived functions

2.2. Accordion Mode Features and Requirements

The workshop included four talks on the features and requirements of the accordion mode:

- John Preuß Mattsson presented "Comments on NIST Requirements for an Accordion Cipher Mode," which was joint work with Ben Smeets and Erik Thormarker. The presentation included support for NIST's proposal to standardize an accordion mode and derived functions and then responded to the feedback requested by NIST. The feedback emphasized a need for several accordions built on different primitives to support crypto-agility, in addition to an accordion built on Rijndael-256-256. Comments on parameter sizes included a strong preference for a granularity of ≤ 8, 256-bit keys, variable-length tweaks of ≥ 256 bits, a minimum plaintext size of 16 or 32 bytes, and a maximum plaintext size of 2^{48} or 2^{64} bytes. The preferred security goals included nonce hiding, replay protection, nonce misuse resistance, and robust authenticated encryption (RAE) or release of unverified plaintext (RUP) security. There was also a recommendation to drop the deterministic authenticated encryption derived function and instead use an AEAD as a "hedged" authenticated encryption.
- Guy B. from the U.K. National Cyber Security Centre (NCSC) gave two talks titled "Security Goals for an Accordion Mode: Release of Unverified Plaintext and Multi-user Security" and "Requirements for an Accordion Mode," which were joint work with John H. and Charlotte S. Both talks highlighted how the NCSC prioritizes high-security requirements. The first talk stated the need for strong RUP security and beyond-birthday bounds that are practical and secure for multi-user environments. In the second talk, Guy B. emphasized the need for a solution in the near-term while also

looking ahead for a long-term solution. Some of NCSC's highest priorities included simple security analysis, compatibility with AES, misuse-resistant authenticated encryption and RUP security, and BBB data limits.

- Tushar Patel presented "Accordion Cipher-mode Preferable Features," which included recommendations to support a 256-bit block cipher, variable-length tweaks that are a multiple of 128 bits, as much parallelism as possible, and key commitment. Some additional implementation features to consider were proposed, including fast drop tags, padding attack prevention, and ciphertext segmentation.

Open discussion. The "Accordion Mode Requirements/Features" topic concluded with a one-hour open discussion. Rijndael-256-256 under a birthday bound accordion mode and AES under a BBB accordion mode were discussed first. While standardizing a 256-bit block cipher was generally supported by workshop participants, most also accepted that this might not be a straightforward transition and could take additional time. The solution of a BBB accordion mode using AES-256 had mixed support. There was some concern that this would lead to a more complex mode, although others maintained that a nonce-based key derivation for AEAD is achievable.

The next topic discussed was granularity (denoted as g), or coarseness of the allowed plaintext sizes [2]. The discussion centered on the value of supporting $g < 8$, including which use cases require it and how complicated it would be to support. Although several participants and speakers proposed a granularity of $g = 1$ or $g = 8$, there was agreement during the open discussion that $g = 1$ would be more difficult to support, and no one provided a concrete requirement for it. However, Chris Celi from the Security Testing, Validation and Measurement Group at NIST pointed out that while it is more complicated, bit-level testing is used by some and is typically available for hashes and some AES testing. It was unclear why bit-level testing was supported in the past and whether those using it today have a requirement for it.

The open discussion concluded with some brief comments on the minimum plaintext size and variable-length tweaks. It was noted that the AEAD derived function will need variable-length tweaks. The group also generally agreed that a minimum plaintext size smaller than the block size adds complexity and, if needed, a padding scheme could be specified in an additional derived function.

2.3. Panel Discussion on Adoption Perspectives

Andrew Regenscheid, Group Leader of the Cryptographic Technology Group at NIST, moderated a panel called "Adoption Perspectives." The panelists were Shai Halevi (AWS), Paul Crowley (Google), Matthew Simpson (NSA), and Krystian Matusiewicz (Intel). The discussion was related to the requirements and features topic and also included approaches to increasing the usage bounds.

Shai Halevi asserted that it is urgent to get a wider block cipher for "the mountains of data that need to be moved" and that a BBB accordion mode would be too slow for practical use and not worth the extra effort. The development of a wider block cipher should consider the trade-offs between new techniques and Rijndael-256-256. Shai Halevi prioritized key commitment and performance of the accordion mode, expected that a small number of accordion modes will be needed, and preferred availability as soon as possible, suggesting that around four years might be realistic.

Paul Crowley emphasized that Google is moving petabytes of data with a single key, and a quick solution to increased usage bounds should be prioritized. Rijndael-256-256 without modification would be the quickest way to achieve this. Having three primitives for the accordion mode to operate on — AES-256, Rijndael-256-256, and TurboSHAKE — may be worthwhile. Paul Crowley also prioritized nonce misuse resistance and suggested a small granularity ($g = 1$) but is not convinced that key commitment or KDI security are needed. There are several applications, including storage encryption on Android, that will be unable to use an accordion because they require a streaming mode.

Matthew Simpson stated that the highest priority for national security systems is an authenticated encryption with nonce misuse resistance that operates over AES, preferably available in the near term. In addition, the derived functions are essential to using the accordion mode and will be needed at the same time as the accordion. Some additional features that would be nice to have are larger maximum plaintext sizes, RUP security, multi-user security and BBB security. Matthew Simpson also pointed out that performance goals should be practical and that a small granularity would cover the most use cases. In addition, having too many variants of the accordion may create interoperability issues. A wider block cipher could slow down deployment, but having this as a second option or version seems reasonable.

Krystian Matusiewicz spoke on the importance of robustness and graceful degradation, and on the difficulty of balancing performance versus high-assurance security. There is significant value in producing a standard soon, but there are also benefits in taking the time to produce a new wide block cipher. Krystian Matusiewicz also suggested a granularity equal to the block size to optimize performance and a small number of accordion variants tailored to different use cases.

2.4. Authenticated Encryption

The session on "Authenticated Encryption" included two talks with proposals for achieving authenticated encryption over Galois/Counter Mode (GCM). The proposals related to some stopgap measures that could be considered while the accordion mode is developed and standardized.

- Scott Arcizewski presented "Galois Extended Mode," which modifies GCM to support increased usage bounds, longer messages, key commitment, and short tags.

- Shay Gueron presented "Double-Nonce-Derive-Key-GCM (DNDK-GCM) General Design Paradigms and Application," which uses a nonce-based key derivation wrapped around GCM to achieve increased usage bounds, good performance, and optional key commitment. This method is designed to use the existing GCM standard.

2.5. Design Approaches

The session on "Design Approaches" included three talks. followed by 20 minutes of open discussion.

- Christoph Dobraunig presented "Efficient Instances of Docked Double Decker with AES, and Application to Authenticated Encryption," which was joint work with Krystian Matusiewicz, Bart Mennink, and Alexander Tereschenko. This work included three variants of a docked-double-decker accordion mode over AES, each with different features (i.e., birthday bound, BBB, and variable-length tweaks).
- Jean Paul Degabriele presented "Universal Hash Designs for an Accordion Mode," which was a joint work with Jan Gilcher, Jérôme Govinden, and Kenneth G. Paterson. This presentation reasoned that a good universal hash function is essential in the design of an accordion mode, particularly when using a hash-encrypt-hash approach, and included five new candidates for universal hash functions that offer good performance and higher security compared to Poly1305.
- Pablo Garcia Fernandez presented "Accordion mode based on Hash-Encrypt-Hash," which was a joint work with Hieu Nguyen Duy, Aleksei Udovenko, and Alex Biryukov. In this proposal, three keys are derived and then used in an HCTR-like construction to achieve variable-length tweaks, multi-key security, context commitment, and larger maximum plaintext size.

Open Discussion. During the short open discussion, workshop participants expressed support for a hash-encrypt-hash approach over an encrypt-mix-encrypt approach, although KDI security may be infeasible using this technique. Support for a wider block cipher was reiterated, and it was noted that a BBB accordion mode over a *tweakable* block cipher would be simpler to design than one over AES.

2.6. Potential Security Properties

The session on "Potential Security Properties" included three presentations followed by 20 minutes of open discussion.

- Yusuke Naito presented "Committing Wide Encryption Mode with Minimum Ciphertext Expansion," which was a joint work with Yu Sasaki and Takeshi Sugawara. This presentation introduced a technique to achieve authenticated encryption on a wide encryption cipher by using a Feistel structure with a keyed hash function. The re-

sulting properties are context commitment, RAE security, and minimal ciphertext expansion.

- Byeonghak Lee presented "A BBB Secure Accordion Mode from HCTR," which proposed a modified HCTR that uses a hash and underlying encryption function with a $2n$-bit state size to achieve BBB security.
- Yu Long Chen presented "Information-theoretic Security with Asymmetries," which was a joint work with Tim Beyne. This work introduced power bounds as an alternative security measurement to the traditional advantage bound and included methods to convert single-user power bounds to multi-user power bounds.

Open Discussion. The session concluded with a short open discussion that focused on key commitment. It was noted that application- and protocol-level designers often assume that an algorithm has security properties that are not there or have not been considered, and this is how the idea of key commitment came about. Some suggested making a list of properties of an algorithm for protocol designers. Others suggested that protocol designers should provide a list of the properties that they require (or assume). However, it was also recognized that neither approach truly bridges the communication gap between cryptographic and protocol-level designers.

2.7. Next Steps

The last session of the workshop, "Next Steps," focused on creating a high-level plan for the project and the process to standardization.

Morris Dworkin presented "Preliminary NIST Proposal for a Development Process," which highlighted three potential paths to standardization: a competition, a NIST design, or a NIST-led collaboration. Morris indicated a preference for the last option, which would begin with a request for information on design approaches. After collecting public input, NIST would propose a few design options around mid-2025. Time for public comments and a workshop would follow, after which NIST would finalize the design.

In general, this option was well-received by the workshop participants. A few comments were voiced to reiterate that the derived functions should be developed concurrently. It was pointed out that it is difficult to verify the correctness of security proofs and there is little incentive to do the verification. A suggestion was made to form a committee of experts to analyze the security proof and write a report. A request was also made for the NIST modes team to interact more with the public community.

After the presentation, Meltem Sönmez Turan opened a discussion period and presented some possible paths for the project. These paths included an accordion over AES, an accordion over a new block cipher (e.g., Rijndael-256-256), a Keccak-based AEAD, and a stopgap measure (e.g., AES-GCM-SIV). Following this, the workshop participants offered some suggestions for how NIST might interact with the community more, including informal

discussions on the mailing list and virtual meetings. The question of how many accordion variants will be needed was also discussed, and opinions on this were mixed. One participant pointed out that a Rijndael-256-256-based accordion and a BBB accordion over AES are competing options. Another pointed out that an AES-based mode is needed, so both of these options should be pursued. Finally, there was a comment that applications that would use AES-GCM-SIV have some overlap with those of the accordion and it could be considered as an alternative to a BBB accordion. There was also a question raised on whether the existing modes in the SP 800-38 series would be extended to support a 256-bit block cipher, should it be standardized. Overall, the comments in the open discussion were supportive of the accordion mode project and the collaborative process that NIST proposed.

3. Summary of Feedback on Key Topics

The following is a summary of the key points discussed during the workshop presentations, open discussions, and panel discussion. They represent a summary of feedback and an aggregation of recurrent comments received throughout the workshop rather than formal statements or individual positions of workshop participants. Furthermore, these are not statements of NIST's intentions but are in the form of requests or recommendations made to NIST.

Takeaway 1. *Development Process:* A NIST-led collaborative development process is appropriate for the accordion mode, with the derived functions developed concurrently. NIST should interact frequently with the community and form a committee of experts to verify the security proof.

Takeaway 2. *Parameters:* Of the accordion parameters discussed, there was significant support for variable-length tweaks, a large maximum plaintext size, and a granularity of $g = 8$. A value of $g < 8$ should also be considered, but there are trade-offs.

Takeaway 3. *Security Features:* In NIST's example AEAD derived function, nonce misuse resistance and RUP security are automatically achieved. These are important security properties that should be explicitly listed in the requirements.

Takeaway 4. *Additional Features:* KDI security is considered unnecessary and may even be infeasible. Key and context commitment are not needed by all, although there is some support for key commitment, possibly as an optional feature. The limited discussion of nonce hiding may indicate low interest, but the comments received were in favor.

Takeaway 5. *Performance:* Performance and parallelization should be prioritized without sacrificing security. Concrete performance requirements were not received, and regardless of priorities, the accordion may be impractical in some cases.

Takeaway 6. *Larger Block Size:* The accordion should support AES-256 and a 256-bit block cipher. Rijndael-256-256 without modification is a promising candidate for the larger block cipher, but trade-offs to pursuing a modified Rijndael-256-256 or an all-new cipher should be considered.

Takeaway 7. *Stopgap Solution:* A BBB solution over AES is a priority for some and will be needed in the short term. There is no clear direction on whether a BBB accordion, a stopgap measure (e.g., AES-GCM-SIV), or both are preferred.

Takeaway 8. *Crypto-Agility:* A small number of accordions that operate over different underlying primitives should be supported for crypto-agility. In addition to AES-256 and a 256-bit block cipher, a Keccak-based primitive could be considered.

References

[1] NIST Workshop on the Requirements for an Accordion Cipher Mode 2024 (2024). Available at https://csrc.nist.gov/Events/2024/accordion-cipher-mode-workshop-2024.

[2] Chen YL, Davidson M, Dworkin M, Kang J, Kelsey J, Sasaki Y, Sönmez Turan M, Chang D, Mouha N, Thompson A (2024) Proposal of Requirements for an Accordion Mode, National Institute of Standards and Technology, Workshop Discussion Draft. Available at https://csrc.nist.gov/files/pubs/other/2024/04/10/proposal-of-requirements-for-an-accordion-mode-dis/iprd/docs/proposal-of-requirements-for-an-accordion-mode-discussion-draft.pdf.

[3] Daemen J, Rijmen V (1999) AES Proposal: Rijndael, AES Algorithm Submission. Available at https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/aes-development/Rijndael-ammended.pdf.

[4] Gueron S, Langley A, Lindell Y (2019) AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption, RFC 8452. DOI:10.17487/RFC8452. Available at https://www.rfc-editor.org/info/rfc8452

[5] Dworkin M (2001) Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST SP 800-38A. https://doi.org/10.6028/NIST.SP.800-38A.

[6] Dworkin M (2005) Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST SP 800-38B. https://doi.org/10.6028/NIST.SP.800-38B.

[7] Dworkin M (2004) Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, NIST SP 800-38C. https://doi.org/10.6028/NIST.SP.800-38C.

[8] Dworkin M (2007) Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST SP 800-38D. https://doi.org/10.6028/NIST.SP.800-38D.

[9] Dworkin M (2010) Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, NIST SP 800-38E. https://doi.org/10.6028/NIST.SP.800-38E.

[10] Dworkin M (2012) Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST SP 800-38F. https://doi.org/10.6028/NIST.SP.800-38F.

[11] Dworkin M (2016) Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption, NIST SP 800-38G. https://doi.org/10.6028/NIST.SP.800-38G.

Appendix A. Agenda

Thursday, June 20, 2024	
8:15	Shuttle Departs Courtyard Gaithersburg Washingtonian Center
8:30 – 9:00	Arrival/Badging/Continental breakfast.
Session I – Opening *Session Chair: Morris Dworkin*	
9:00 – 9:10	Welcome *Matthew Scholl*
9:10 – 9:35	Overview of the NIST Block Cipher Modes Project *Meltem Sönmez Turan*
9:35 – 10:00	Introduction to the Accordion Mode and Derived Functions *Alyssa Thompson*
10:00 – 10:30	Break
Session II – Accordion Mode Requirements/Features (I) *Session Chair: Yu Long Chen*	
10:30 – 11:20	Preliminary NIST Proposals and the NECST Evaluation Framework *Nicky Mouha*
11:20 – 11:40	Comments on NIST Requirements for an Accordion Cipher Mode *John Preuß Mattsson*
11:40 – 12:00	Security Goals for an Accordion Mode: Release of Unverified Plaintext and Multi-user Security *Guy B.*
12:00 – 1:20	Lunch
Session III – Use Cases *Session Chair: Andrew Regenscheid*	
1:20 – 1:30	NIST Options for Supporting Larger Usage Bounds *Andrew Regenscheid*
1:30 – 2:30	Panel Discussion: Adoption Perspectives *Paul Crowley, Shai Halevi, Krystian Matusiewicz, Matthew Simpson* 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 *Tushar Patel*
3:20-3:40	Requirements for an Accordion Mode *Guy B.*
3:40-4:40	Open Discussion
4:45	Shuttle Departs NCCoE to Return to Hotel

Friday, June 21, 2024	
8:15	Shuttle Departs Courtyard Gaithersburg Washingtonian Center
8:30 – 9:00	Arrival/Badging/Continental breakfast.
Session V – Lightning Talks *Session Chair: Alyssa Thompson*	
9:00 – 9:20	*Talks will be recorded. By presenting, you acknowledge and consent to being recorded.*
Session VI – Authenticated Encryption *Session Chair: Alyssa Thompson*	
9:20 – 9:40	Galois Extended Mode *Scott Arciszewski*
9:40 – 10:00	Double-Nonce-Derive-Key-GCM (DNDK-GCM) General Design Paradigms and Application *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 *Christoph Dobraunig*
10:50 – 11:10	Universal Hash Designs for an Accordion Mode *Jean Paul Degabriele*
11:10 – 11:30	Accordion mode based on Hash-Encrypt-Hash *Pablo Garcia Fernandez*
11:30 – 11:50	Open Discussion
11:50 – 1:20	Lunch
Session VIII – Potential Security Properties *Session Chair: Donghoon Chang*	
1:20 – 1:40	Committing Wide Encryption Mode with Minimum Ciphertext Expansion *Yusuke Naito*
1:40 – 2:00	A BBB Secure Accordion Mode from HCTR *Byeonghak Lee*
2:00 – 2:20	Information-theoretic Security with Asymmetries *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 *Morris Dworkin*
3:30 – 4:30	Open Discussion

Appendix B. List of Accepted Presentations

1. *Accordion Cipher-mode Preferable Features*, Tushar Patel (Atna-cipher LLC)
2. *Efficient Instances of Docked Double Decker With AES, and Application to Authenticated Encryption*, Christoph Dobraunig (Intel Labs), Krystian Matusiewicz (Intel Corporation), Bart Mennink (Radboud University), and Alexander Tereschenko (Intel Corporation)
3. *Universal Hash Designs for an Accordion Mode*, Jean Paul Degabriele (Technology Innovation Institute), Jan Gilcher (ETH Zurich), Jérôme Govinden (TU Darmstadt), and Kenneth G. Paterson (ETH Zurich)
4. *Committing Wide Encryption Mode with Minimum Ciphertext Expansion*, Yusuke Naito (Mitsubishi Electric Corporation), Yu Sasaki (NTT Social Informatics Laboratories, NIST), and Takeshi Sugawara (University of Electro-Communications)
5. *Security Goals for an Accordion Mode: Release of Unverified Plaintext and Multi-user Security*, John H. (UK National Cyber Security Centre), Charlotte S. (UK National Cyber Security Centre), and Guy B. (UK National Cyber Security Centre)
6. *Requirements for an Accordion Mode*, John H. (UK National Cyber Security Centre), Charlotte S. (UK National Cyber Security Centre), and Guy B. (UK National Cyber Security Centre)
7. *Accordion Mode Based on Hash-Encrypt-Hash*, Hieu Nguyen Duy (University of Luxembourg), Pablo García Fernández (University of Luxembourg), Aleksei Udovenko (University of Luxembourg), and Alex Biryukov (University of Luxembourg)
8. *A BBB Secure Accordion Mode from HCTR*, Byeonghak Lee (Samsung SDS)
9. *Galois Extended Mode*, Scott Arciszewski (Trail of Bits)
10. *Comments on NIST Requirements for an Accordion Cipher Mode*, John Preuß Mattsson (Ericsson), Ben Smeets (Ericsson), and Erik Thormarker (Ericsson)
11. *Double-Nonce-Derive-Key-GCM (DNDK-GCM): General Design Paradigms and Application*, Shay Gueron (University of Haifa, Meta)
12. *Information-theoretic Security with Asymmetries*, Tim Beyne (imec-COSIC) and Yu Long Chen (imec-COSIC, NIST)