NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

https://csrc.nist.gov/Events/2024/accordion-cipher-mode-workshop-2024

NIST will host a workshop on the development of a new block cipher mode of operation on June 20–21, 2024, at the National Cybersecurity Center of Excellence in Rockville, Maryland.

Important Dates

Workshop: June 20–21, 2024

Submission deadline: May 1, 2024

Notification date: May 17, 2024

Registration deadline: June 13, 2024

NIST plans to develop a new mode of the 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.

The term “accordion cipher mode” (or “accordion mode,” for short) is introduced to indicate that the mode would act as a cipher, not only on a single block but on a range of input sizes. A well-designed accordion mode could potentially provide significant advantages over most of the block cipher modes that NIST currently approves. For example, an accordion mode could provide better resistance to cut-and-paste attacks than CBC, or it could be adapted to provide authenticated encryption with associated data (AEAD) with better properties than GCM, such as resistance to nonce misuse, support for short tags, nonce hiding, and key commitment. An accordion mode could also be adapted to provide key wrapping that is more efficient than KW and KWP.

NIST intends to post preliminary ideas and plans by early April 2024. The goal of the workshop is to solicit public input on the specific requirements for the design and use of an accordion mode and the evaluation criteria in the development process. Potential topics for discussion include:

- Parameter lengths for the accordion mode: keys, tweaks, data input
- Whether the accordion mode should support an underlying block cipher with 256-bit blocks
- Formal security goals for the accordion mode
- Requirements and features for the main use cases (e.g., AEAD)
- Potential design strategies
- Performance targets
- Implementation considerations
- The development and standardization process

Attendees may submit extended abstracts or slides for a short presentation (up to 10 minutes) for any number of the sessions. Submissions must be provided electronically in PDF format and sent to ciphermodes@nist.gov by May 1, 2024. NIST will post the accepted abstracts and presentations on the workshop website, though no formal proceedings will be published.

Most of the workshop sessions are expected to include a panel discussion or extensive open discussion. Time will also be allotted for impromptu "lightning talks" — brief presentations of recent research results without slides. All sessions and lightning talks will be recorded.

Waivers of the registration fee are available for a limited number of students, but no waivers are available for speakers.

Updates and additional information will be posted to the workshop website and ciphermodes-forum email distribution list. Instructions for subscribing to the email forum can be found at https://csrc.nist.gov/Projects/block-cipher-techniques/email-list-ciphermodes-forum.

Inquiries: ciphermodes@nist.gov