AGENDA
Third NIST Workshop on Block Cipher Modes of Operation 2023

National Cybersecurity Center of Excellence
Rockville, Maryland

Tuesday, October 3, 2023	
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 – 10:00	Keynote Address: Radical CS *Phillip Rogaway*
10:00 – 10:30	Report on the Block Cipher Modes of Operation in the NIST SP 800-38 Series *Nicky Mouha*
10:30 – 11:00	Break
Session II – Security Notions *Session Chair: Nicky Mouha*	
11:00 – 11:20	Overloading the Nonce: Rugged PRPs, Nonce-Set AEAD, and Order-Resilient Channels *Jean Paul Degabriele and Vukašin Karadžic*
11:20 – 11:40	Upgrading AEAD Privacy: The AE2 goal *Mihir Bellare*
11:40 – 12:00	The Landscape of Committing Authenticated Encryption *Mihir Bellare, Viet Tung Hoang, and Cong Wu*
12:00 – 1:20	Lunch
Session III – Tweakable Wide Encryption *Session Chair: Meltem Sönmez Turan*	
1:20 – 1:40	SHAKE Modes of Operation *Joan Daemen, Seth Hoffert, Silvia Mella, and Gilles Van Assche*
1:40 – 2:00	Deck-Based Wide Block Cipher Modes *Aldo Gunsing, Joan Daemen, and Bart Mennink*
2:00 – 2:20	Length-Preserving Encryption with HCTR2 *Paul Crowley, Nathan Huckleberry, and Eric Biggers*
2:20 – 2:50	Break
Session IV – Perspectives on Standardization *Session Chair: John Kelsey*	
2:50 – 3:10	Practical Challenges with AES-GCM and the Need for a New Cipher *Panos Kampanakis, Matt Campagna, Eric Crocket, and Adam Petcher*
3:10 – 3:30	Proposals for Standardization of Encryption Schemes *John Preuß Mattsson, Ben Smeets, and Erik Thormarker*
3:30 – 5:00	Panel Discussion: Lessons Learned *Lily Chen, Joan Daemen, Phillip Rogaway, and Miles Smid* Moderator: *John Kelsey*
5:15	Shuttle Departs NCCoE to Return to Hotel

Updated 10/2/2023

Wednesday, October 4, 2023	
8:15	Shuttle Departs Courtyard Gaithersburg Washingtonian Center
8:30 – 9:00	Arrival/Badging/Continental breakfast.
Session V – Authenticated Encryption *Session Chair: Yu Long Chen*	
9:00 – 9:20	Short Tweak TBC and Its Applications in Symmetric Ciphers *Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi, and Yu Sasaki*
9:20 – 9:40	Galois Counter Mode with Secure Short Tags (GCM-SST) *Matthew Campagna, Alexander Maximov, and John Preuß Mattsson*
9:40 – 10:00	Constructions based on the AES Round and Polynomial Multiplication that are Efficient on Modern Processor Architectures *Shay Gueron*
10:00 – 10:30	Break
Session VI – Government Interests *Session Chair: Yu Sasaki*	
10:30 – 11:00	Validation Testing for Block Cipher Modes *Christopher Celi*
11:00 – 11:30	Update on Standardization of Ascon family *Meltem Sönmez Turan*
11:30 – 12:00	Authenticated Encryption Modes for use in National Security Systems *Matthew Simpson*
12:00 – 1:20	Lunch
Session VII – Key/Context Commitment *Session Chair: Donghoon Chang*	
1:20 – 1:40	Key Committing Security of AEZ *Yu Long Chen, Antonio Flórez-Gutiérrez, Akiko Inoue, Ryoma Ito, Tetsu Iwata, Kazuhiko Minematsu, Nicky Mouha, Yusuke Naito, Ferdinand Sibleyras, and Yosuke Todo*
1:40 – 2:00	Flexible Authenticated Encryption *Sanketh Menda, Julia Len, Viet Tung Hoang, Mihir Bellare, and Thomas Ristenpart*
2:00 – 2:20	KIVR: Context-Committing Authenticated Encryption Using Plaintext Redundancy and Application to GCM and Variants *Yusuke Naito, Yu Sasaki, and Takeshi Sugawara*
2:20 – 2:50	Break
Session VIII – Closing *Session Chair: Morris Dworkin*	
2:50 – 3:20	Lightning Talks *Talks will be recorded. By presenting, you acknowledge and consent to being recorded.*
3:20 – 3:30	Next Steps *Morris Dworkin*
3:30 – 4:45	Open Discussion
5:00	Shuttle Departs NCCoE to Return to Hotel