AGENDA
NIST Lightweight Cryptography Workshop 2023
June 21-22, 2023 (virtual)

All times are Eastern Daylight Time (New York, UTC-04:00)

Wednesday, June 21, 2023	
Session I – Lightweight Cryptography Selection Process *Session Chair: Kerry McKay*	
10:00 – 10:10	Opening remarks *Jim St. Pierre, Acting Director, Information Technology Laboratory, NIST*
10:10 – 10:50	Evaluation of the Finalists and the Selection of Ascon *Meltem Sönmez Turan*
10:50 – 11:20	SCA Evaluation and Benchmarking of Finalists in the NIST Lightweight Cryptography Standardization Process *Kamyar Mohajerani, Luke Beckwith, Abubakr Abdulgadir, Eduardo Ferrufino, Jens-Peter Kaps, and Kris Gaj*
11:20 – 12:00	*Invited talk:* The Ascon Family: Lightweight Authenticated Encryption, Hashing, and More *Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer*
12:00 – 13:00	Break
Session II - Implementations and Side-channel Resistance *Session Chair: Larry Bassham*	
13:00 – 13:20	Hardware Implementation of ASCON *Aneesh Kandi, Anubhab Baksi, Tomáš Gerlich, Sylvain Guilley, Peizhou Gan, Jakub Breier, Anupam Chattopadhyay, Ritu Ranjan Shrivastwa, Zdeněk Martinásek, and Shivam Bhasin*
13:20 – 13:40	FPGA Implementations of Message Authentication Codes based on Ascon-p *Mustafa Khairallah and Srinivasan Yadhunathan*
13:40 – 14:00	A New Leakage Exploitation Framework and Its Application to Authenticated Encryption *Vahid Jahandideh, Léo Weissbart, Bart Mennink, and Lejla Batina*
14:00 – 14:20	Efficient Second-Order Masked Software Implementations of Ascon in Theory and Practice *Barbara Gigerl, Florian Mendel, Martin Schläffer, and Robert Primas*
14:20 – 14:40	Root-cause Analysis of the Side Channel Leakage from ASCON implementations *Zhenyuan Liu and Patrick Schaumont*
14:40 – 15:00	Quantum Implementation of ASCON Linear Layer *Soham Roy, Anubhab Baksi, and Anupam Chattopadhyay* Will not be presented live

Thursday, June 22, 2023	
Session III – Cryptographic Security *Session Chair: Donghoon Chang*	
10:00 – 10:40	*Invited talk:* Security of Permutation-Based Modes and its Application to Ascon *Bart Mennink*
10:40 – 11:00	Exact Security Analysis of ASCON *Bishwajit Chakraborty, Chandranan Dhar, and Mridul Nandi*
11:00 – 11:20	Differential-Linear Cryptanalysis of ASCON: Theory vs. Practice *Cihangir Tezcan*
11:20 – 11:40	A Closer Look at the S-box: Deeper Analysis of Round-Reduced ASCON-HASH *Xiaorui Yu, Gaoli Wang, Fukang Liu, Siwei Sun, and Willi Meier*
11:40 – 12:00	Cryptanalysis of Ascon – An Information Theoretic Perspective – A Position Paper *Nicolas T. Courtois, Florian Caullery, Fred Amiel, and William Whyte*
12:00 – 13:00	Break
Session IV – Implementation and Standardization *Session Chair: Meltem Sönmez Turan*	
13:00 – 13:20	Lightweight Usable Cryptography - A usability evaluation of the Ascon 1.2 family *Arne Padmos*
13:20 – 13:40	Efficient Implementation of Permutation-Based Hash Functions for the RISC-V Architecture *Issam Jomaa, Hao Cheng, and Johann Großschädl, Peter Ryan*
13:40 – 14:00	Proposals for Standardization of the Ascon Family *John Preuß Mattsson, Göran Selander, Santeri Paavolainen, Ferhat Karakoç, Marco Tiloca, and Robert Moskowitz*
14:00 – 14:20	Additional modes for Ascon *Rhys Weatherley*
14:20 – 15:00	Open Discussion and Closing Remarks *Kerry McKay and Meltem Sönmez Turan*