NIST Lightweight Cryptography Workshop Agenda

October 19-21, 2020 *[Virtual]*

All times are Eastern Time (New York)

Monday, October 19, 2020	
Session I – Welcome and Opening *Session Chair: Meltem Sönmez Turan* *On-Demand Webcast*	
11:00 – 11:10	***Opening Remarks*** ***Matt Scholl**, Chief, Computer Security Division (NIST/ITL)*
11:10 – 11:30	***NIST Lightweight Cryptography Standardization*** ***Kerry McKay**, NIST*
11:30 – 11:50	***Benchmarking Round 2 Candidates on Microcontrollers*** ***Çağdaş Çalık**, Munawar Hasan and Jinkeon Kang NIST*
11:50 – 12:10	***Classification of AEAD*** ***Avik Chakraborti**, Nilanjan Datta, Ashwin Jha, and Mridul Nandi*
12:10 – 13:00	**BREAK**
Session II – Candidate Updates *Session Chair: Kerry McKay* *On-Demand Webcast*	
13:00 – 13:20	***Revisiting the Security of COMET Authenticated Encryption Scheme*** *Shay Gueron, Ashwin Jha, and **Mridul Nandi***
13:20 – 13:40	***New Results and Insights on ForkAE*** *Elena Andreeva, Arne Deprez, Jowan Pittevils, Arnab Roy, Amit Singh Bhati, and **Damian Vizár***
13:40 – 14:00	***Security Analysis of KNOT-AEAD and KNOT-Hash*** ***Wentao Zhang**, Tianyou Ding, Chunning Zhou and Fulei Ji*
14:00 – 14:20	***Updates on Elephant*** ***Tim Beyne**, Yu Long Chen, Christoph Dobraunig, and Bart Mennink*
14:20 – 14:40	***New Results on Romulus*** *Testsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu and **Thomas Peyrin***
14:40 – 15:00	***AET-LR: Rate-1 Leakage-Resilient AEAD based on the Romulus Family*** *Chun Guo, **Mustafa Khairallah** and Thomas Peyrin*

Tuesday, October 20, 2020	
Session III - Cryptanalysis and Use Cases *Session Chair: Donghoon Chang* *On-Demand Webcast*	
11:00 – 11:20	***LWC Use Cases - External Memory Encryption*** ***Sebastien Riou***
11:20 – 11:40	***Can LWC and PEC be Friends?: Evaluating Lightweight Ciphers in Privacy-enhancing Cryptography*** ***Kalikinkar Mandal*** *and Guang Gong*
11:40 – 12:00	***On the Security Margin of TinyJAMBU with Refined Differential and Linear Cryptanalysis*** ***Dhiman Saha****, Yu Sasaki, Danping Shi, Ferdinand Sibleyras, Siwei Sun and Yingjie Zhang*
12:00 – 12:20	***Cryptanalysis of the Permutation Based Algorithm SpoC*** ***Liliya Kraleva****, Raluca Posteuca and Vincent Rijmen*
12:20 – 13:00	**BREAK**
Session IV - Benchmarking I *Session Chair: Larry Bassham* *On-Demand Webcast*	
13:00 – 13:20	***Current and Future Efforts in Benchmarking NIST LWC Ciphers*** ***Sebastian Renner****, Enrico Pozzobon, and Jürgen Mottok*
13:20 – 13:40	***Fixslicing - Application to Some NIST LWC Round 2 Candidates*** ***Alexandre Adomnicai*** *and Thomas Peyrin*
13:40 – 14:00	***A Detailed Report on the Overhead of Hardware APIs for Lightweight Cryptography*** ***Patrick Karl*** *and Michael Tempelmeier*
14:00 – 14:20	***FPGA Benchmarking of Round 2 Candidates in the NIST Lightweight Cryptography Standardization Process: Methodology, Metrics, Tools, and Results*** *Kamyar Mohajerani, Richard Haeussler, Rishub Nagpal, Farnoud Farahmand, Abubakr Abdulgadir,* ***Jens-Peter Kaps and Kris Gaj***
14:20 – 14:40	***Parallel Synchronous Code Generation for Second Round Light Weight Candidates*** ***Pantea Kiaei****, Archanaa S. Krishnan, and Patrick Schaumont*

Wednesday, October 21, 2020	
Session V – Benchmarking II *Session Chair: Çağdaş Çalık* *On-Demand Webcast*	
11:00 – 11:20	***Update on Ascon Implementations*** *Christoph Dobraunig, Maria Eichlseder, Florian Mendel,* ***Martin Schläffer***
11:20 – 11:40	***Updates on the Implementation Security of ISAP*** *Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink,* ***Robert Primas*** *and Thomas Unterluggauer*
11:40 – 12:00	***Active and Passive Side-Channel Key Recovery Attacks on Ascon*** ***Keyvan Ramezanpour****, Abubakr Abdulgadir, William Diehl, Jens-Peter Kaps, and Paul Ampadu*
12:00 – 12:20	***An Evaluation of the Multi-Platform Efficiency of Lightweight Cryptographic Permutations*** *Luan Cardoso dos Santos and* ***Johann Großschädl***
12:20 – 13:00	**BREAK**
Session VI – Protected Implementations *Session Chair: John Kelsey* *On-Demand Webcast*	
13:00 – 13:20	***Secure and Efficient Masking of Lightweight Ciphers in Software and Hardware (with Application to the Spook AEAD)*** *Olivier Brochain,* ***Gaëtan Cassiers*** *and François-Xavier Standaert*
13:20 – 13:40	***Protected Hardware Implementations of WAGE*** *Yunsi Fei, Guang Gong, Cheng Gongye, Kalikinkar Mandal, Raghvendra Rohit, Tianhong Xu, Yunjie Yi and* ***Nusa Zidaric***
13:40 – 14:00	***Toolchain for Timing Leakage Analysis of NIST Lightweight Crypto Candidates*** ***Adam Blatchley Hansen****, Eske Hoy Nielsen and Morten Eskildsen*
14:00 – 14:20	***Open Discussion/Closing*** ***Kerry McKay and Meltem Sonmez Turan***