NIST Lightweight Cryptography Workshop Agenda

November 4-6, 2019, *Gaithersburg, Maryland*

Monday, November 4, 2019	
8:00 – 9:00	Badge pick-up
Session I – NIST Lightweight Cryptography Standardization *Session Chair:* Andrew Regenscheid	
9:00 – 9:10	Opening Remarks – **Matthew Scholl**
9:10 – 9:55	*NIST Lightweight Cryptography Standardization*, **Meltem Sönmez Turan**
9:55 – 10:40	Invited talk: *Lightweight Trusted Computing,* **Tom Broström**
10:40-11:00	☕ Break
Session II – Updates on Candidates I *Session Chair:* Kerry McKay	
11:00 – 11:25	*Ascon v1.2 – Analysis of Security and Efficiency*, Christoph Dobraunig, Maria Eichlseder, **Florian Mendel** and Martin Schläffer
11:25 – 11:50	*What the Fork: Implementation Aspects of a Forkcipher*, **Antoon Purnal, Elena Andreeva**, Arnab Roy, and Damian Vizar
11:50 – 12:15	*ESTATE Authenticated Encryption Mode: Hardware Benchmarking and Security Analysis*, **Avik Chakraborti**, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas Lopez, Mridul Nandi, Yu Sasaki
12:15 – 12:40	*On the Security of COMET Authenticated Encryption Scheme*, **Shay Gueron**, Ashwin Jha, and Mridul Nandi
12:40 – 2:00	🍽 Lunch
Session III – Software Benchmarking *Session Chair:* Çağdaş Çalık	
2:00 – 2:25	*FELICS-AEAD: Benchmarking of Lightweight Authenticated Encryption Algorithms*, **Luan Cardoso dos Santos**, Johann Grobschadl, and Alex Biryukov
2:25 – 2:50	*FELICS-AE: a framework to benchmark lightweight authenticated block ciphers,* Kévin Le Gouguec **Presented by: Paul Huynh**
2:50 – 3:15	*Benchmarking Software Implementations of 1st Round Candidates of the NIST LWC Project on Microcontrollers,* **Sebastian Renner**, Enrico Pozzobon, Jurgen Mottok
3:15 – 3:45	☕ Break
Session IV – Hardware Benchmarking *Session Chair:* Larry Bassham	
3:45 – 4:10	*A Comprehensive Framework for Fair and Efficient Benchmarking of Hardware Implementations of Lightweight Cryptography* **Jens-Peter Kaps**, William Diehl, Michael Tempelmeier, Farnoud Farahmand, Ekawat Homsirikamol and Kris Gaj
4:10 – 4:35	*Will the Future Lightweight Standard be RISC-V Friendly?* Gorkem Nisanci, Remzi Atay, Meltem Kurt Pehlivanoglu, Elif Bilge Kavun and **Tolga Yalcin**
~~4:35 – 5:00~~	~~*Benchmarking and Optimizing AES for Lightweight Cryptography on ASICs*, Jenny W. Yu and **Mark D. Aagaard**~~ Unable to attend.

Agenda is subject to change

NIST Lightweight Cryptography Workshop Agenda

November 4-6, 2019, *Gaithersburg, Maryland*

Tuesday, November 5, 2019	
Session V – Cryptanalysis *Session Chair:* Meltem Sönmez Turan	
9:00 - 9:20	*Forgery on Qameleon and SIV-TEM-PHOTON and SIV-Rijndael256*, Nilanjan Datta, Ashwin Jha and **Mridul Nandi**
9:20 – 9:40	*Breaking REMUS and TGIF in the light of NIST Lightweight Cryptography Standardization Project*, Nilanjan Datta, Ashwin Jha, Alexandre Mège and **Mridul Nandi**
9:40 – 10:00	*Cryptanalysis of Internal Keyed Permutation of FlexAEAD*, Mostafizar Rahman, Dhiman Saha, Goutam Paul **Presented by: Avik Chakraborti**
10:00 – 10:20	*Practical Forgery Attacks on Limdolen and HERN*, **Raghvendra Rohit** and Guang Gong
10:20 – 10:40	*Distinguishers for Reduced Round Ascon, DryGASCON, and Shamash Permutations*, **Cihangir Tezcan**
10:40 – 11:00	☕ Break
Session VI – Implementations *Session Chair:* Larry Bassham	
11:00 – 11:25	*Does gate count matter? Hardware efficiency of logic-minimization techniques for cryptographic primitives*, Shashank Raghuraman and **Leyla Nazhandali**
11:25 – 11:50	*Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look*, **Behnaz Rezvani** and William Diehl
11:50 – 12:15	~~*Hardware Design and Analysis of the ACE and WAGE Ciphers*, **Mark D. Aagaard**, Marat Sattarov, and Nusa Zidaric~~ Unable to attend.
12:15 – 12:40	*Implementation of three LWC Schemes in the WiFi 4-Way Handshake with Software Defined Radio*, Yunjie Yi, Guang Gong and **Kalikinkar Mandal**
12:40 – 2:00	🍽 Lunch
Session VII – Lightweight Cryptography Standardization *Session Chair:* John Kelsey	
2:00-2:25	*Cryptography in Industrial Embedded Systems: our experience of needs and constraints*, Jean-Philippe Aumasson, **Antony Vennard**
2:25-3:15	Open Discussion – Lightweight Cryptography Standardization – **Moderated by John Kelsey**
3:15 – 3:45	☕ Break
Session VIII – Side Channel Resistance *Session Chair:* Angela Robinson	
3:45 – 4:10	*Analyzing the Leakage-Resistance of some Round 1 Candidates of the NIST's Lightweight Crypto Standardization Process*, **François-Xavier Standaert**
4:10 – 4:35	*An Open-Source Platform for Evaluating Side-Channel Countermeasures in Hardware Implementations of Lightweight Authenticated Ciphers*, **Abubakr Abdulgadir**, William Diehl and Jens-Peter Kaps

Agenda is subject to change

NIST Lightweight Cryptography Workshop Agenda

November 4-6, 2019, *Gaithersburg, Maryland*

Wednesday, November 6, 2019	
Session IX – Updates on the Candidates II *Session Chair:* Andrew Regenscheid	
9:00 – 9:25	*Security Proofs for Oribatida*, Arghya Bhattacharjee, Eik List, Cuauhtemoc Mancillas López and **Mridul Nandi**
9:25 – 9:50	*Dumbo, Jumbo, and Delirium: Parallel Authenticated Encryption for the Lightweight Circus,* Tim Beyne, Yu Long Chen, Christoph Dobraunig, and **Bart Mennink**
9:50 – 10:15	*LOTUS and LOCUS AEAD: Hardware Benchmarking and Security Analysis*, **Avik Chakraborti**, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas Lopez, Mridul Nandi, Yu Sasaki
10:15 – 10:40	*Updates on Romulus, Remus and TGIF*, Tetsu Iwata, Mustafa Khairallah, **Kazuhiko Minematsu**, and Thomas Peyrin
10:40 – 11:00	☕ Break
Session X – Updates on the Candidates III *Session Chair:* Donghoon Chang	
11:00 – 11:25	*Security Proof of mixFeed*, Bishwajit Chakraborty and **Mridul Nandi**
11:25 – 11:50	*Security Analysis of HyENA Authenticated Encryption Mode,* **Avik Chakraborti**, Nilanjan Datta, Ashwin Jha, Snehal Mitragotri, Mridul Nandi
11:50 – 12:15	*Security Proof of Beetle and SpoC,* Bishwajit Chakraborty and Ashwin Jha and **Mridul Nandi**
12:15 – 12:40	*Security Proof of ORANGE-Zest*, Bishwajit Chakraborty and **Mridul Nandi**
12:40 – 2:00	🍽 Lunch
Session XI – Updates on the Candidates, Cryptanalysis, and Testing *Session Chair:* Çağdaş Çalık	
2:00 – 2:25	*Leakage Resilience of the ISAP Mode: A Vulgarized Summary*, Christoph Dobraunig and **Bart Mennink**
2:25 – 2:45	*A Practical Forgery Attack on Lilliput-AE*, Orr Dunkelman, Nathan Keller, **Eran Lambooij**, and Yu Sasaki
2:45 – 3:10	*Systematic Testing of Lightweight Cryptographic Implementations*, Sydney Pugh, **M S Raunak**, D. Richard Kuhn, and Raghu Kacker
3:10 – 3:30	☕ Break
Session XII – Next Steps *Session Chair:* Kerry McKay	
3:30 – 3:45	Next Steps **- Kerry McKay**
3:45– 4:30	Open discussion and closing remarks

Agenda is subject to change