Fifth NIST Lightweight Cryptography Workshop 2022 – Draft Agenda

DAY 1 – May 9, 2022 – Monday

Welcome (10 min)

Lily Chen

Session 1 Standardization process and applications

Chair: Kerry McKay

10:10am – 11:50pm EDT (14:00 – 15:50 UTC) each talk 25 min including questions

Update on the NIST Lightweight Cryptography Standardization Process
Meltem Sönmez Turan

Low-Latency Crypto: An Emerging Paradigm of Lightweight Cryptography
Santosh Ghosh

Need for Low-latency Ciphers – A Comparative Study of NIST LWC Finalists
Tolga Yalcin and Samaneh Ghandali

A Real-World Analysis of Lightweight Cryptographic Algorithm ASCON
Jeffrey Avery, Bryson Fraelich, William Duran, Andrew Lee, Agustin Sullivan, Zane Mechalke, Maj. Bobby Birrer, Sameul Dick, and Jordon Cochran

BREAK (70 min)

Session 2 Benchmarking and side channel resistance

Chair: Larry Bassham

1:00pm – 3:00pm EDT (17:00 – 19:00 UTC), each talk 24 min including questions

3rd Round Ciphers Evaluation on Microcontrollers
Sebastian Renner

RISC-V Instruction Set Extensions for Lightweight Symmetric Cryptography
Hao Cheng, Johann Großschädl, Ben Marshall, Dan Page, and Thinh Pham

General Framework for Evaluating LWC Finalists in Terms of Resistance to Side-Channel Attacks
Jens-Peter Kaps, Kris Gaj, Abubakr Abdulgadir, and Kamyar Mohajerani

Analyzing the Leakage Resistance of the NIST's Lightweight Crypto Standardization Process Finalists
Corentin Verhamme, Gaëtan Cassiers, and François-Xavier Standaert

Review of the White-Box Encodability of NIST Lightweight Finalists
Alex Charlès and Chloé Gravouil

DAY 2 – May 10, 2022 - Tuesday

Session 3 Cryptanalysis
Chair: Kerry McKay
10:00am – 12:00pm EDT (14:00 – 16:00 UTC) each talk 20 min including questions

Birthday-Bound Slide Attacks on TinyJAMBU's Keyed-Permutations for All Key Sizes
Ferdinand Sibleyras, Yu Sasaki, Yosuke Todo, Akinori Hosoyamada, and Kan Yasuda

Revisiting Higher-Order Differential(-Linear) Attacks from an Algebraic Perspective –Applications to Ascon, Grain v1, Xoodoo, and ChaCha
Kai Hu and Thomas Peyrin

Differential-Linear Cryptanalysis on Xoodyak
Orr Dunkelman and Ariel Weizman

Practical Cube-attack against Nonce-misused Ascon
Jules Baudrin, Anne Canteaut, and Léo Perrin

Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon
Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun

A New Conditional Cube Attack on Reduced-Round Ascon-128a in a Nonce-misuse Setting,
Donghoon Chang, Jinkeon Kang, and Meltem Sönmez Turan

BREAK (60 min)

Session 4 Side channel resistance
Chair: Noah Waller
1:00pm – 3:00pm EDT (17:00 – 19:00 UTC) each talk 24 min including questions

Fast Side-Channel Key-Recovery Attack against Elephant Dumbo
Louis Vialar

Root-cause Analysis of Power-based Side-channel Leakage in Lightweight Cryptography Candidates
Zhenyuan Liu and Patrick Schaumont

Side-Channel Resistant Implementations of Three Finalists of the NIST Lightweight Cryptography Standardization Process: Elephant, TinyJAMBU, and Xoodyak
Abubakr Abdulgadir, Richard Haeussler, Sammy Lin, Jens-Peter Kaps, and Kris Gaj

Survey on the Effectiveness of DAPA-Related Attacks against Shift Register Based AEAD Schemes
Shivam Bhasin, Dirmanto Jap, Wei Cheng (Derrick) Ng, and Siang Meng Sim

TVLA, Correlation Power Analysis and Side-Channel Leakage Assessment Metrics
William Unger, Liljana Babinkostova, Mike Borowczak, Robert Erbes, and Aparna Srinath

DAY 3 – May 11, 2022 - Wednesday

Session 5 Updates on the finalists

Chair: Donghoon Chang

10:00am – 12:00pm EDT (14:00 – 16:00 UTC) each talk 24 min including questions

Romulus as NIST LWC Finalist
Chun Guo, Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin

Update on the Security Analysis of Ascon
Christoph Dobraunig, Maria Eichlseder, Johannes Erlacher, Florian Mendel, and Martin Schläffer

Update on the Performance and Mode-level Properties of ISAP
Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas, and Thomas Unterluggauer

Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle
Akiko Inoue, Tetsu Iwata, and Kazuhiko Minematsu

Tight Preimage Resistance of the Sponge Construction
Charlotte Lefevre and Bart Mennink

BREAK (60 min)

Session 6 Algorithm-specific implementations and Open discussions

Chair: Meltem Sönmez Turan

1:00pm – 3:00pm EDT (17:00 – 19:00 UTC) each talk 24 min including questions

Fast Skinny-128 SIMD Implementations for Sequential Modes of Operation
Alexandre Adomnicai, Kazuhiko Minematsu, and Maki Shigeri

Hardware Implementations of Romulus: Exploring Nonce Misuse Resistance and Boolean Masking
Mustafa Khairallah and Shivam Bhasin

New Ascon Implementations
Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Robert Primas, and Martin Schläffer

Randomness Testing of the NIST Light Weight Cipher Finalist Candidates
Emanuele Bellini and Yun Ju Huang

Open discussion and closing remarks
Kerry McKay and Meltem Sönmez Turan