NIST Lightweight Cryptography Standardization: Next Steps

Kerry McKay
NIST Lightweight Cryptography Workshop
November 6, 2019
Goal of the project

• New standard(s) optimized for constrained environments
  • Not a ’drop-in-replacement’ for the current standards, rather an addition to the portfolio of NIST standards.

Portfolio of algorithms?

• Ideally, single winner with several variants with different optimization.
• It is possible to approve more than one algorithm.
• If there is no algorithm better than current standards both in terms of security or performance, no standardization is an option too.
• Arguments both for and against portfolio
  • Cost: implementation, validation/certification, maintenance
  • Coverage and agility: meeting the needs for a wide variety of devices and applications
  • Optimize the design or optimize the implementations
How will NIST evaluate Round 2 Candidates?

• Categories to narrow scope for benchmarking and evaluation

• Performance will play a bigger role this round
  • NIST will not require submitters to use an API or framework that was not in call
  • NIST encourages analysis of algorithms and implementations using widely-available tools to facilitate fair comparisons
Design Tweaks

- A **minor** modification to the primitive to improve efficiency, or to avoid a cryptographic attack
  - E.g., updating tunable parameters (number of rounds), changing constants
  - Adding a new functionality, changing the underlying block cipher or primitive may not be accepted as a tweak

- No tweaks are allowed in Round 2. The Round 3 candidates will be given an opportunity to tweak
  - It is acceptable for designers publishing proposed updates on their webpage. These tweaks will **not** be considered as official submissions.
Merging Candidates?

• Merging candidates is not a part of the standardization process
• PQC allowed merging candidates

• It could be considered by NIST, the discussion will be followed through the lwc-forum
Tentative Timeline

• Round 3 selection around September 2020
• Hold 4th LWC workshop
• Final selection in 2021
Standardization

• Will be selecting variant(s) for standardization, not necessarily all variants in a submission

• Specify/standardize final parameters, as appropriate
  • Coordinate with submission team
  • Public and transparent process
THANK YOU!

• Submission teams
• Speakers and attendees
• Everyone who has provided feedback
• Everyone who made this workshop possible