Next Steps – Timeline

- Announce the finalists in December 2020 (tentative)
- Publish the report explaining the selection process in January 2021 (tentative)
- Publish guidelines for the submission package of the final round (on tweak selection etc.)
- Publish the updated packages in January 2021 (tentative)
- Final round to last about a year

Any comments/questions on the tentative deadline and process?
Selection of the Finalists

- More challenging compared to going from Round 1 to Round 2.
- From 32 candidates to (around) 8 finalists.
- Selection will be based on security, software & hardware benchmarks, additional features etc.
- Diversity of the finalists is another consideration.

Any comments on the target number of finalists?
Diversity as an evaluation criteria?
Security

- Are any of the security claims of the submitters invalidated by third-party analysis?
- Are there undesired properties that might later lead to attacks?
- Is the candidate mature enough for standardization?
- Is the candidate based on a well-analyzed design approach, or use well-analyzed components?
- Do the designers plan to tweak the candidate? How big are the planned changes? What is the purpose? (based on status reports)

Any comments?
Benchmarking

- Does the candidate have optimized software and hardware implementations?
- Does the performance of the benchmarked implementations reflect the performance of the candidate in the field?
- Does the candidate perform better than AES-GCM and SHA256 in target platforms?

- Do the benchmarking platforms match with target applications? Do we need additional platforms?
- Are the software/hardware benchmarks mature enough to fairly evaluate candidate?
- Should SHA-3, SHAKE and small Keccak be included in benchmarking?
- How to benchmark AEAD and hashing together?
Masked/Protected Implementations

- Does the candidate have protected implementations?
- What is the performance overhead for side channel protection?
- Does the design lend itself to side-channel resistant implementations (e.g., leakage resilient, threshold implementations)?

At this stage, how much weight should be given to protected implementations on the finalist selection?
Does the candidate have additional features?

- Variants supporting different key/tag sizes
- Nonce-misuse resistance
- RUP-security
- Related-key security
- Multi-user security
- Etc.

How much weight should additional features have on the finalist selection?
Damian Vizár: “The criteria for the selection of 3rd round candidates did not contain a mention of the lightweight use cases and constraints, which motivate the LWC project. I'd like to ask how will these be factored into the decision?”
Thanks!

https://csrc.nist.gov/Projects/lightweight-cryptography

Email list: lwc-forum@list.nist.gov
NIST team: lightweight-crypto@nist.gov