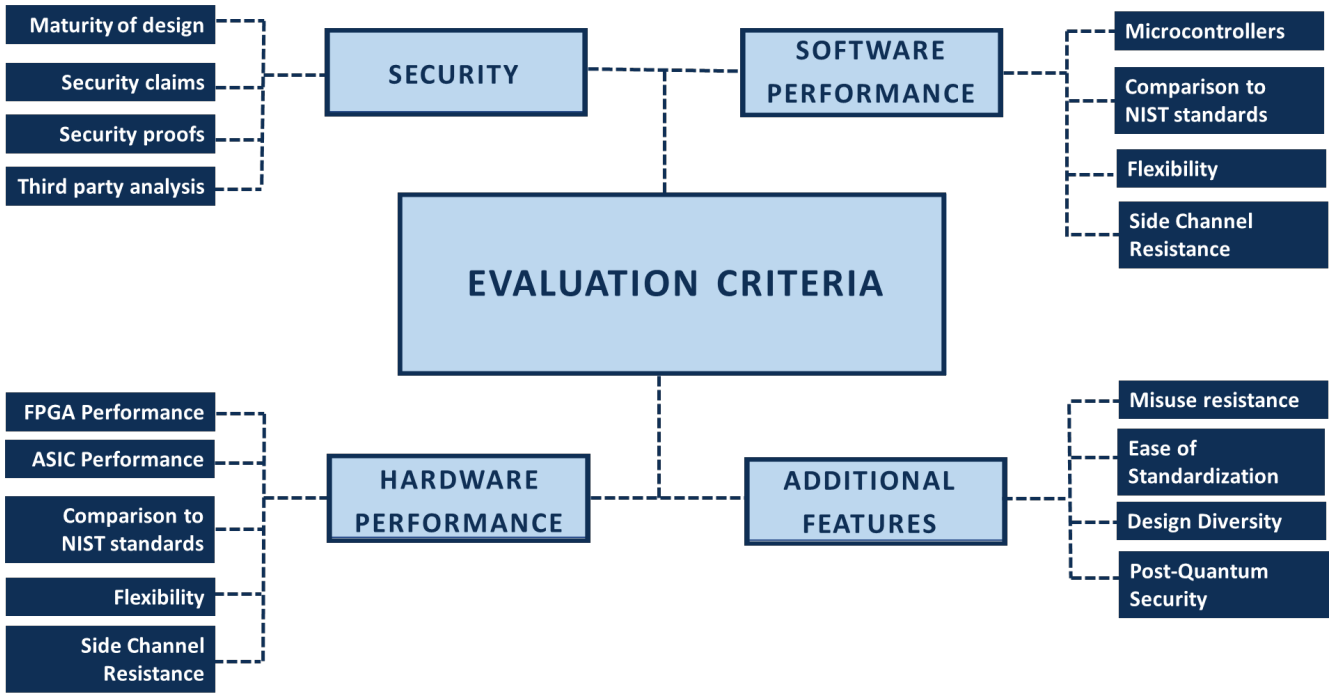
Open Discussion

NIST Lightweight Cryptography Workshop, May 9-11, 2022

National Institute of Standards and Technology
U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

Selecting the Winners



- More challenging than previous rounds
- Evaluation criteria have multiple dimensions
- Joint work with cryptographic community

Security

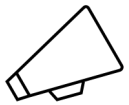
- Do we have enough confidence in the security of the finalists for standardization?
- How much weight should additional features (e.g., misuse resistance) have on the selection of the winners?

Share your observations/published results via lwc-forum

Performance Benchmarking

- Do the implementations reflect the true performance of the finalists in the field?
- Do the benchmarking platforms match with target applications?
- When do groups benchmarking implementations anticipate they will share results?
- Will new finalist implementations be benchmarked in hardware?

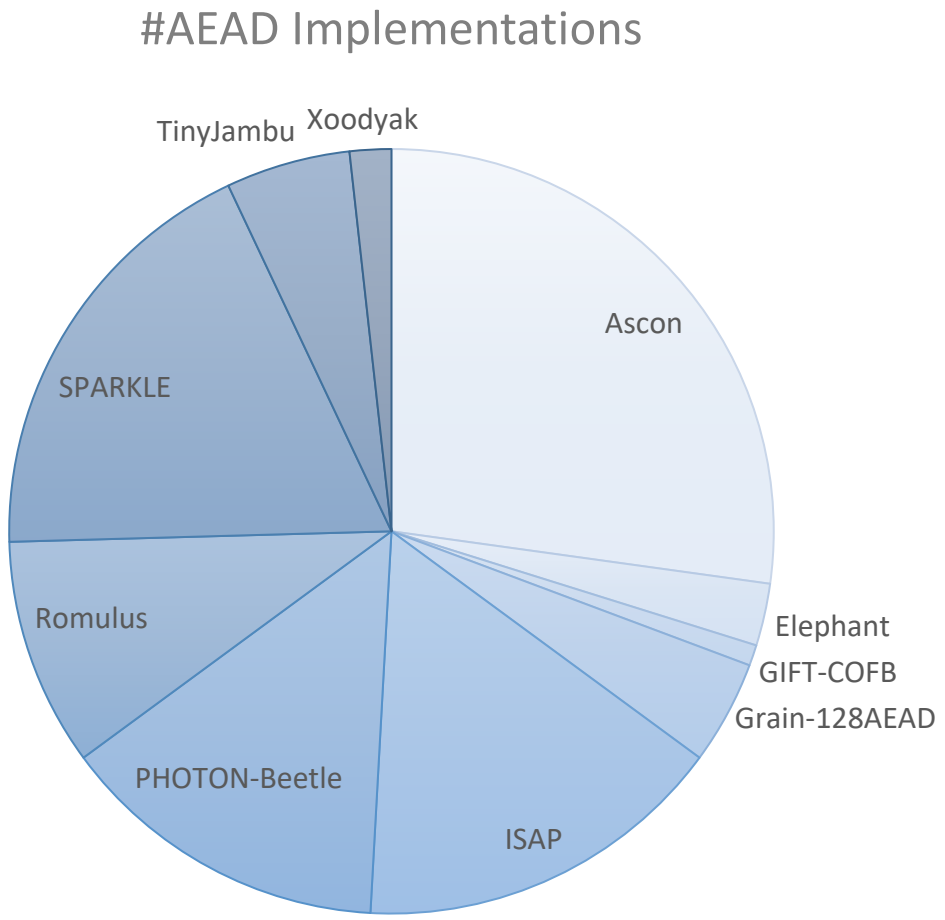
- We encourage the LWC community to support benchmarking efforts



Please notify the NIST LWC team if you plan to benchmark the finalists. Use the lwc-forum to let the community know about your effort and share your results.

Software Benchmarking

- NIST microcontroller benchmarking results will be available on GitHub
- Some candidates have a relatively few number of implementations
  - We encourage submitters and interested third-parties to provide more optimized and additional implementations for these candidates
- Suggestions for additional platforms?



Protected Implementations

In Session 2, GMU CERG presented their effort for evaluating the side-channel resistance of implementations and benchmarking protected implementations

- GMU benchmarking on FPGA platforms
- Request volunteers to support ASIC and software implementation benchmarking
- Details: https://cryptography.gmu.edu/athena/index.php?id=LWC

We encourage the LWC community to support this effort

Next Steps

- Continue evaluating the finalists. Status updates (optional) from the finalists expected deadline early Fall 2022
- Selection of the winner(s) and the publication of the status report
- Standardization (in 2023)

General Questions

- *How has optimization of SW implementations been handled? (Has this effort been organized in anyway, or have optimizations been more ad-hoc by the community?)*

- *Does NIST plan to standardize an algorithm for a specific application?*
  - For KECCAK modes or other requests, please inform NIST cryptographic technology group about the industry need
    - Written feedback explaining the need for a new standard is helpful as we prioritize our efforts

- *Does NIST have any plan to extend its CAVP and/or CMVP programs for validation testing of the winner?*
  - Yes; we will work with the validation team after standardization

Thank You

- Thanks to all those who submitted designs for consideration
- Thanks to the presenters and session chairs
- Thanks to Sara Kerman, Karen Startsman, Christina Robinson, Akeem Henry, Kevin Hill, and the rest of the A/V team for making this event possible

- Thank you all for participating in this process

CONTACT NIST TEAM

lightweight-crypto@nist.gov

PUBLIC FORUM

lwc-forum@list.nist.gov

GITHUB

https://github.com/usnistgov/Lightweight-Cryptography-Benchmarking

WEBSITE

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