Heavyweight Protection for Constrained Devices

Update on the NIST Lightweight Cryptography Project

MELTEM SONMEZ TURAN, SECURITY RESEARCH REVIEW SEMINAR
NOVEMBER 25, 2020

Motivation

CONSTRAINED DEVICES

e.g., RFID tags, sensor networks, IoT devices

NEW APPLICATIONS

e.g., home automation, healthcare, smart city

LACK OF CRYPTOGRAPHY STANDARDS

NIST crypto standards are optimized for general-purpose computers.

NEW RESEARCH RESULTS

e.g., permutation-based designs, simpler key schedules, inherent side channel resistance

Lightweight Cryptography Standardization

GOAL

Develop new guidelines, recommendations and standards optimized for constrained devices

PROCESS

Public competition-like process with multiple rounds similar to AES, SHA3 and PQC standardization

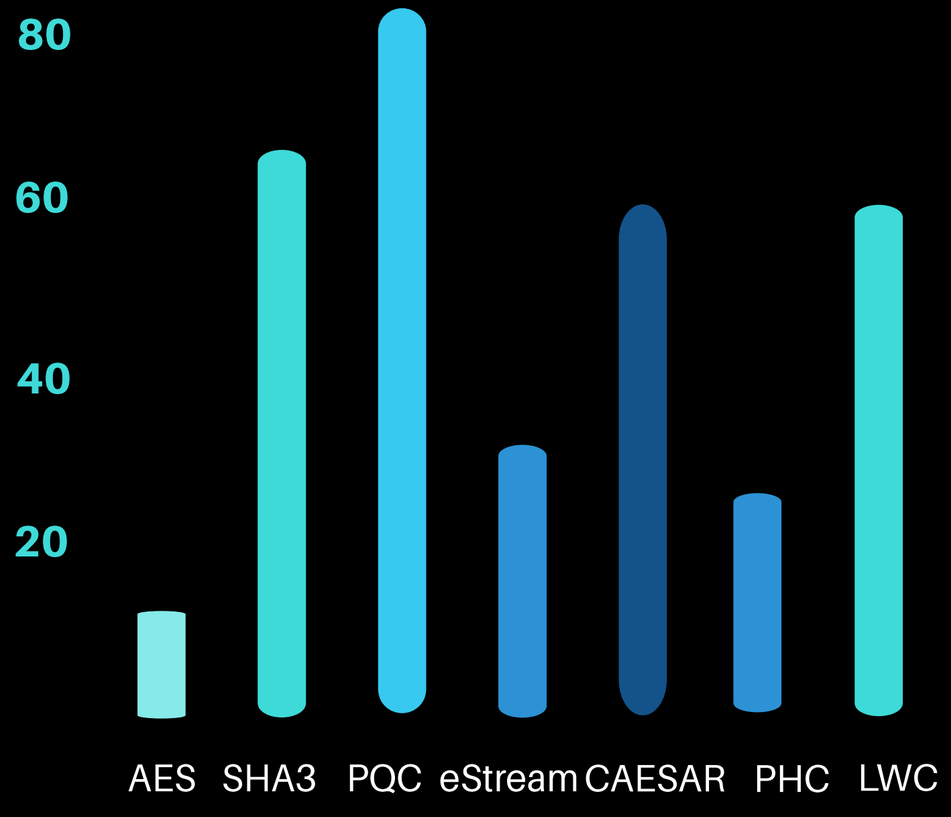
SCOPE

Authenticated Encryption and (optional) hashing for constrained software and hardware environments

TIMELINE

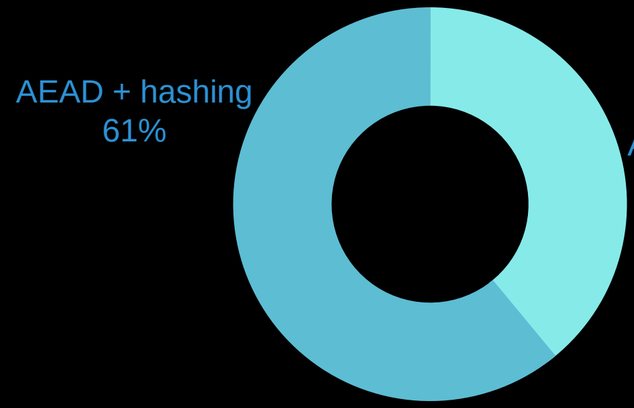
Multi-year
2015 First workshop
2021 Winner selection (tentative)

56 ROUND 1 CANDIDATES



NUMBER OF SUBMISSIONS

FROM 25 COUNTRIES



FUNCTIONALITY

32 ROUND 2 CANDIDATES

ACE	Gimli	Oribatida	SPIX
ASCON	Grain-128aead	Photon-Beetle	SpoC
COMET	HyENA	Pyjamask	Spook
DryGascon	ISAP	Romulus	Subterranean
Elephant	KNOT	SAEAES	Sundae-GIFT
ESTATE	LOTUS&LOCUS	Saturnin	TinyJambu
ForkAE	mixFeed	Skinny-AEAD&Hash	Wage
GIFT-COFB	ORANGE	Sparkle	Xoodyak

END OF ROUND 1

After four months, NIST selected 32 Round 2 candidates.

SECURITY CONCERNS

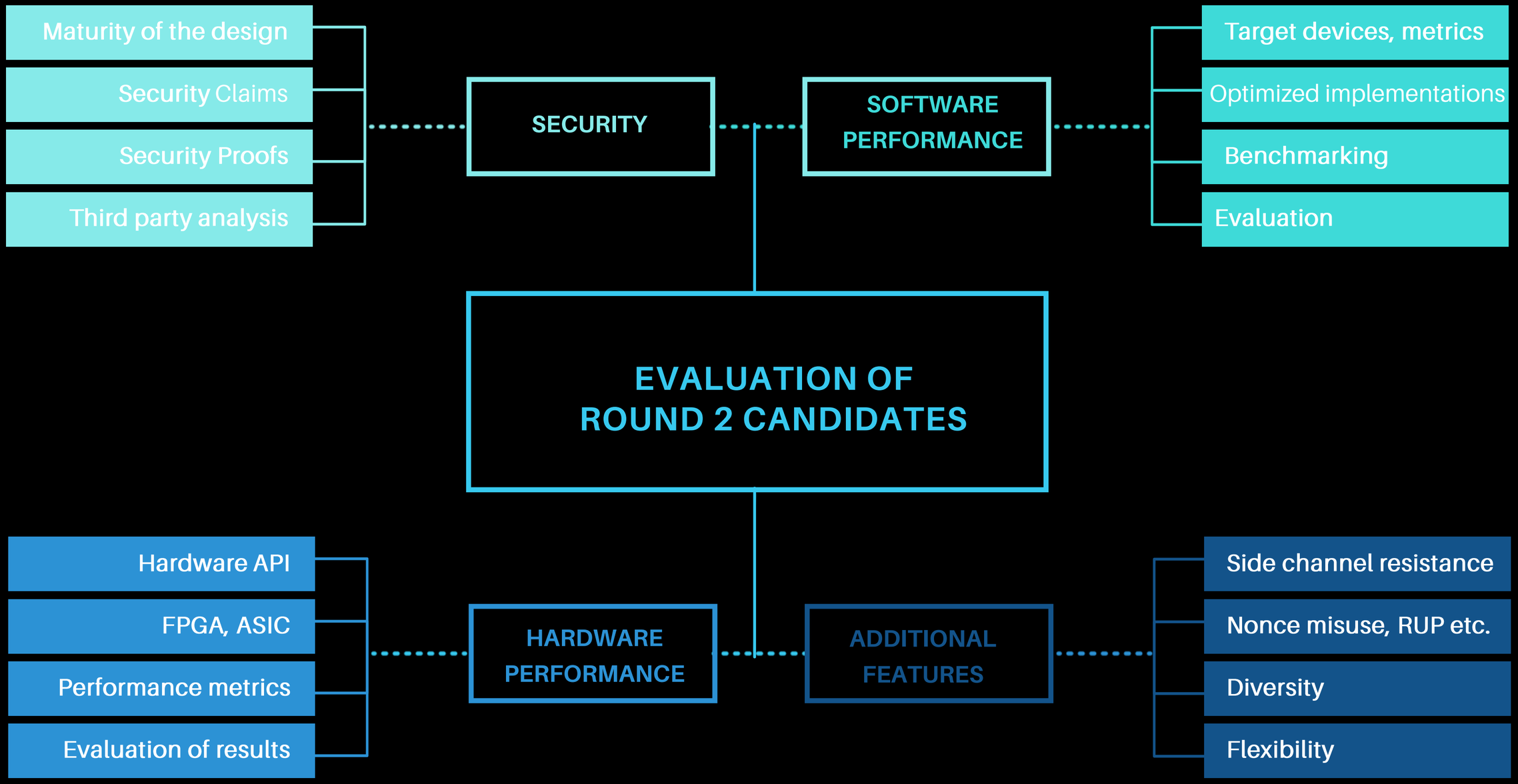
e.g., distinguishing attacks, practical tag forgeries etc.

STATUS REPORT

NISTIR 8268

Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry A. McKay
Çağdaş Çalık
Donghoon Chang
Larry Bassham


EVALUATION OF ROUND 2 CANDIDATES
SECURITY
Maturity of the design
Security Claims
Security Proofs
Third party analysis
SOFTWARE PERFORMANCE
Target devices, metrics
Optimized implementations
Benchmarking
Evaluation
HARDWARE PERFORMANCE
Hardware API
FPGA, ASIC
Performance metrics
Evaluation of results
ADDITIONAL FEATURES
Side channel resistance
Nonce misuse, RUP etc.
Diversity
Flexibility

NEXT STEPS

Announcement of the finalists

December 2020 (tentative)

Publishing the round 2 status report

January 2021 (tentative)

Evaluation of the finalists

January 2021 – December 2021

Selection of the winner(s)

December 2021

Standardization

January 2022 - ...

CONTACT

lightweight-crypto@nist.gov

WEBSITE

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

PUBLIC FORUM

lwc-forum@list.nist.gov