Next Steps in NIST Lightweight Cryptography Standardization

Meltem Sönmez Turan
NIST Lightweight Cryptography Team

September 27, 2023
NIST Lightweight Cryptography Standardization Project

**PROCESS**
Public competition-like process with multiple rounds like AES, SHA3 and PQC standardization

**GOAL**
Develop new guidelines, recommendations and standards optimized for constrained devices

**SCOPE**
Authenticated Encryption and (optional) hashing for constrained software and hardware environments
Initial Phase  
(July 2015 – August 2018)

Call for Candidates  
(August 2018 – April 2019)

Round 1  
(April 2019 – August 2019)

Round 2  
(August 2019 – March 2021)

Final Round  
(March 2021 – June 2023)
Two workshops (2015, 2016) to get feedback on target applications, industry need, requirements, etc.

Publications:
- NISTIR 8114 Report on Lightweight Cryptography
- (White paper, retired) Profiles for the Lightweight Cryptography Standardization Process
Submission Requirements and Evaluation Criteria

**Deadline:** February 2019
56 First-round candidates

Evaluation only based on security

**NIST IR 8268** explains how 32 candidates (out of 56) were selected to move forward to the second round.
Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – June 2023)

Initial Phase
(July 2015 – August 2018)

Call for Candidates
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

32 Second-round candidates

Two workshops (2019, 2020)

NIST IR 8369 explains how 10 finalists were selected to move forward to the final round.
Ten finalists

- Ascon
- Photon-Beetle
- Elephant
- Romulus
- GIFT-COFB
- Sparkle
- Grain-128AEAD
- TinyJambu
- ISAP
- Xoodyak

Two workshops

NIST IR 8454 explains the selection of Ascon.

Initial Phase (July 2015 – August 2018)

Call for Candidates (August 2018 – April 2019)

Round 1 (April 2019 – August 2019)

Round 2 (August 2019 – March 2021)

Final Round (March 2021 – June 2023)
Selection of Ascon

In February 2023, NIST announced the Ascon family as the winner.

- High security margin, large number of third-party analysis
- Primary choice for lightweight applications in the final CAESAR portfolio
- No design tweaks
- Performance advantages over NIST standards (AES-GCM and SHA-2) in hardware and software
- Implementation and design flexibility
- Mode-level protection mechanism against leakage and lower additional cost for protected implementations
- Support for additional functionalities XOF, dedicated MAC, in addition to Hash
• AEAD and hashing scheme (fixed or variable output length)
• Main component: 320-bit permutation instantiated with different constants and number of rounds for different variants
• AEAD: MonkeyDuplex mode with keyed initialization and finalization
• Hash: Sponge construction

The primary AEAD variant of Ascon family
<table>
<thead>
<tr>
<th>Variant</th>
<th>Parameter sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascon-128</td>
<td>128-bit key/nonce/tag</td>
</tr>
<tr>
<td>Ascon-128a</td>
<td>128-bit key/nonce/tag</td>
</tr>
<tr>
<td>Ascon-80pq</td>
<td>160-bit key, 128-bit nonce/tag</td>
</tr>
<tr>
<td>Ascon-Hash</td>
<td>256-bit digest</td>
</tr>
<tr>
<td>Ascon-Hasha</td>
<td>256-bit digest</td>
</tr>
<tr>
<td>Ascon-XOF</td>
<td>Arbitrary length digest</td>
</tr>
<tr>
<td>Ascon-XOFa</td>
<td>Arbitrary length digest</td>
</tr>
</tbody>
</table>

**Current tentative decisions:**

- Either Ascon-128 or both Ascon-128 and Ascon-128a
- Do not include Ascon-80pq
- XOF standardization instead of hash functions
• Publication of the draft standards describing the Ascon family (later in 2023)
  • Special Publication (SP) series rather than Federal Information Processing Standards (FIPS)
    (tentative decision)

• Public comments period of 60 to 90 days
CONTACT US

lightweight-crypto@nist.gov

PUBLIC FORUM lw-forum@list.nist.gov

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

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