Standardization Procedure and Timeline

- Publication of the draft standards describing the Ascon family
  - Special Publication (SP) series rather than Federal Information Processing Standards (FIPS) (tentative decision)
  - One or more SP with multiple parts
  - Public comments period of 60 to 90 days

- Renaming possibility

- Tentative timeline: Fall 2023
Which AEAD variants should NIST standardize?

• Ascon-128 (primary)

• Alternatives:
  • Ascon-128a
  • Both Ascon-128 and Ascon-128a
  • Both Ascon-128 and Ascon-128a, with aligned round numbers (b=8)

<table>
<thead>
<tr>
<th>AEAD</th>
<th>Variant</th>
<th>Parameter sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascon-128</td>
<td>128-bit key/nonce/tag</td>
<td></td>
</tr>
<tr>
<td>Ascon-128a</td>
<td>128-bit key/nonce/tag</td>
<td></td>
</tr>
<tr>
<td>Ascon-80pq</td>
<td>160-bit key, 128-bit nonce/tag</td>
<td></td>
</tr>
</tbody>
</table>
Which hash functions/XOFs should NIST standardize?

- Ascon-Hash (primary)
- Alternatives:
  - Ascon-XOF (possibly along with tweaking IV)
  - Both Ascon-Hash and Ascon-XOF
  - For each option: Primary variant (b=12) or A-variant (b=8)?

<table>
<thead>
<tr>
<th></th>
<th>Variant</th>
<th>Parameter sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>Ascon-Hash</td>
<td>256-bit digest</td>
</tr>
<tr>
<td></td>
<td>Ascon-Hasha</td>
<td>256-bit digest</td>
</tr>
<tr>
<td>XOF</td>
<td>Ascon-XOF</td>
<td>Arbitrary length digest</td>
</tr>
<tr>
<td></td>
<td>Ascon-XOFa</td>
<td>Arbitrary length digest</td>
</tr>
</tbody>
</table>
Standards Portfolio

• Ascon may be integrated into NIST’s portfolio of standards beyond the scope of the LWC call

• Additional functionalities: PRF, MAC, DRBG, etc.
Bit Ordering Convention

• Ascon currently follows SHA-2 convention: *most* significant bit in leftmost position
• SHA-3 convention: *least* significant bit in leftmost position

• Should Ascon be specified following SHA-3 convention?
• Larger key sizes

• 64-bit, 96-bit tag size

• Larger nonces

• Support for customization strings

• IVs may need to change to domain separate additional input/output sizes and functionalities
Thanks

• Ascon team
• Bart Mennink for the invited talk
• Presenters
• Sara Kerman for administrative support
• Conference support and AV teams

• Everyone who participated in the LWC standardization process
CONTACT US

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