ACORN
Different Design Approaches:

- Fast
  - AES-NI (AEGIS)
  - SIMD (MORUS)

- Lightweight
  - Mode (JAMBU)
  - Dedicated (ACORN)
ACORN: design

• ACORN-128
  • Based on bit-oriented stream cipher
  • Encryption and authentication share the same state
  • Small state
    • 293-bit (the minimum is 256-bit)
  • IV should not be reused
  • 128-bit key, 128-bit IV, 128-bit tag
ACORN: design

• Tweaks
  • Key is introduced into 1664 steps in initialization in v2 (128 steps in v1)
  
  • Initialization: 1792 steps (v2) : 1536 steps (v1)
  • Assoc. Data Padding: 256 steps (v2) : 512 steps (v1)
  • Message padding: 256 steps (v2) : 512 steps (v1)
  • Finalization: 768 steps (v2) : 256 steps (v1)

• Rationale for tweaks: to provide protection against nonce-reuse
  • Non-invertible initialization so that the key cannot be recovered directly from the state (the state can be recovered when nonce is reused in encryption/decryption)
  • More steps in the initialization so as to increase the difficulty of recovering the key from the state
Figure 1.1: The concatenation of 6 LFSRs in ACORN-128. $f_i$ indicates the overall feedback bit for the $i$th step; $m_i$ indicates the message bit for the $i$th step.
• Initialization
  • Key and IV are injected into the state bit by bit
  • Consists of 1792 steps

• Process associated data
  • Each step one bit
  • Padding is fixed as 256 bits: 1 0^{255} (without padding to fixed length block, so suitable for bit-oriented hardware implementation)

• Process plaintext
  • Each step one bit
  • Padding is fixed as 256 bits: 1 0^{255}

• Finalization
  • Run the cipher for 768 steps
  • The last 128 keystream bits are the tag

• Two control bits are applied to the cipher to separate associated data, plaintext and the finalization
ACORN: Security

• Encryption: Analysis is the same as stream cipher analysis (no security weakness found when nonce is not reused)

• Authentication: with the use of the concatenated LFSRs, the security analysis of authentication can be done much easier
  • To eliminate the difference being injected into the state, the success rate is $2^{-189}$
ACORN: Performance

• Hardware
  • Bit-oriented design, suitable for hardware implementation
    • Expected to be slightly more costly than Trivium (hardware area)
  • Fast implementation is possible due to 32 parallel steps
  • Small state-size: 293 bits
  • Energy efficient
    • Simple circuits
    • Encryption and authentication share most of the operations

• Major difference between ACORN and TriviA-ck
  • ACORN’s encryption and authentication share the same state and operations
    => smaller state and less computations
ACORN: Performance

- Software speed on Sandy Bridge

<table>
<thead>
<tr>
<th>Size (B)</th>
<th>64B</th>
<th>128B</th>
<th>256B</th>
<th>512B</th>
<th>1024B</th>
<th>2048B</th>
<th>4096B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>72.1</td>
<td>41.5</td>
<td>26.3</td>
<td>18.6</td>
<td>14.7</td>
<td>12.8</td>
<td>11.9</td>
</tr>
</tbody>
</table>
Conclusions

• **ACORN**
  • A new design very different from the other candidates
  • Lightweight
  • Reasonably fast due to 32 parallel steps
  • ACORN-128 provides 128-bit encryption and authentication security

• **ACORN v2**
  • Protection against nonce-reuse in encryption/decryption so that the key cannot be directly recovered from the state

• **ACORN provides a new approach to design lightweight MAC (using bit-oriented registers)**