ACORN v3
A Lightweight Authenticated Cipher

Hongjun Wu
Nanyang Technological University
Different Design Approaches:

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

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

• ACORN-128
  • Based on bit-oriented stream cipher
  • Encryption and authentication share the same state
  • Small state
    • 293-bit (37 bits more than the minimum 256-bit)
  • IV should not be reused
  • 128-bit key, 128-bit IV, 128-bit tag
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.
ACORN: design

• Tweak for Round 3
  • Function \( ch \) is moved from the nonlinear feedback function to the output filtering function

\[
\begin{align*}
  k_{S_i} &= S_{i,12} \oplus S_{i,154} \oplus \text{maj}(S_{i,235}, S_{i,61}, S_{i,193}) \oplus ch(S_{i,230}, S_{i,111}, S_{i,66}); \\
  f_i &= S_{i,0} \oplus (\sim S_{i,107}) \oplus \text{maj}(S_{i,244}, S_{i,23}, S_{i,160}) \oplus (c_{a_i} \& S_{i,196}) \oplus (c_{b_i} \& k_{S_i});
\end{align*}
\]

• Rationale for the tweak:
  • Better balance between the feedback function and the output filtering function
    • The feedback function consists of 6 LFSRs and the overall nonlinear feedback.
  • Larger security margin against guess-and-determine attack
• 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

- Security of initialization (1792 steps)
  - Strong against differential analysis
    - probability is less than $2^{-200}$ for 400 steps
ACORN: Security

• Security of initialization (1792 steps)
  • Strong against cube analysis (as the cube size $n$ increases from 17 to 32, the number of steps increases from 931 to 974, less than 3 steps per one cube increment)

<table>
<thead>
<tr>
<th>$n$</th>
<th>steps</th>
<th>$n$</th>
<th>steps</th>
<th>$n$</th>
<th>steps</th>
<th>$n$</th>
<th>steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>669</td>
<td>17</td>
<td>931</td>
<td>25</td>
<td>955</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>736</td>
<td>18</td>
<td>933</td>
<td>26</td>
<td>957</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>781</td>
<td>19</td>
<td>933</td>
<td>27</td>
<td>961</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>796</td>
<td>20</td>
<td>938</td>
<td>28</td>
<td>964</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>806</td>
<td>21</td>
<td>942</td>
<td>29</td>
<td>965</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>843</td>
<td>22</td>
<td>949</td>
<td>30</td>
<td>966</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>852</td>
<td>23</td>
<td>950</td>
<td>31</td>
<td>972</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>869</td>
<td>24</td>
<td>954</td>
<td>32</td>
<td>974</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ACORN: Security

• Security of encryption
  • Strong against statistical analysis
    • nonce used only once
    • nonlinear state update function
  • Strong against guess-and-determine attack
    • Complexity larger than $2^{200}$ (of the attack that attempts to recover the state from linear equations)
ACORN: Security

• Authentication
  • with the use of 6 concatenated LFSRs, it is expensive to eliminate a difference in the state.
  • To eliminate the difference being injected into the state through ciphertext or associated data, the success rate is $2^{-181}$
ACORN: Performance

• Hardware performance on FPGA Virtex 7 (Tao Huang)
  • 499 LUTs, 3.4 Gbps (implementing 8 steps)
    • Currently much smaller than other CAESAR candidates
    • About the same speed of AES-GCM, but 7 times smaller than AES-GCM.
  • 979 LUTs, 11.3 Gbps (implementing 32 steps)
ACORN: Performance

• Software speed on Intel Skylake (Intel Core i7-6550U, ultrabook cpu)
  • Faster than AES-GCM on the microprocessors with no AES instructions

<table>
<thead>
<tr>
<th></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>encryption</td>
<td>38.2</td>
<td>23.2</td>
<td>15.4</td>
<td>11.8</td>
<td>11.2</td>
<td>8.8</td>
<td>8.2</td>
</tr>
<tr>
<td>decryption</td>
<td>37.8</td>
<td>22.1</td>
<td>14.3</td>
<td>10.5</td>
<td>8.4</td>
<td>7.5</td>
<td>7.1</td>
</tr>
</tbody>
</table>
ACORN: Features

• Lightweight
  • Based on bit-oriented stream cipher (small data path)
  • Message length is not needed for authentication and verification
    • Do not need to implement circuits to count the message length
    • Do not need to pad the message to full blocks

• 32 steps can be computed in parallel in software and hardware

• High security
  • 128-bit encryption security
  • 128-bit authentication security
Conclusions

• ACORN
  • Lightweight
  • Reasonably fast due to 32 parallel steps
  • 128-bit encryption and authentication security