JAMBU
A Lightweight Authenticated Encryption Mode

Hongjun Wu  Tao Huang

Nanyang Technological University

DIAC 2016, Nagoya
26 Sep 2016
JAMBU
Comparison between AEGIS, MORUS, JAMBU, ACORN

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

Lightweight
- Mode (JAMBU)
- Dedicated (ACORN)
No tweak to the JAMBU mode for the third round

Update in JAMBU v2.1 document
  • Add authentication security proof for nonce reused in JAMBU
  • Add hardware performance of JAMBU
Outline

• Design Motivation
• The JAMBU Authenticated Encryption Mode
• JAMBU Features
• AES-JAMBU and SIMON-JAMBU
• Security of JAMBU
• Performance of JAMBU
• Conclusion
Design Motivation

• To design a **lightweight AE mode**
  • Use simple operations
    • Only XOR is used
  • Introduce small extra state size.
  • For $2n$-bit block size, the extra state sizes are

<table>
<thead>
<tr>
<th></th>
<th>CCM</th>
<th>GCM</th>
<th>OCB3</th>
<th>EAX</th>
<th>CPFB</th>
<th>COLM</th>
<th>SILC</th>
<th>CLOC</th>
<th>JAMBU</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Size</td>
<td>4n</td>
<td>6n</td>
<td>6n</td>
<td>8n</td>
<td>6n</td>
<td>8n</td>
<td>4n</td>
<td>4n</td>
<td>3n</td>
</tr>
<tr>
<td>Increments</td>
<td>2n</td>
<td>4n</td>
<td>4n</td>
<td>6n</td>
<td>4n</td>
<td>6n</td>
<td>2n</td>
<td>2n</td>
<td>n</td>
</tr>
</tbody>
</table>

**smallest**
The JAMBU Mode:
– Initialization

Block cipher: $2n$ bits block size
IV: $n$ bits
The JAMBU Mode:
– Process Associated Data

Data block size: $n$ bits
Pad the associated data with: $10^*$
The JAMBU Mode: – Process Plaintext

Data block size: $n$ bits
Pad the plaintext with: 10
The JAMBU Mode:
- Finalization

Tag: $n$ bits
## Parameter sets

<table>
<thead>
<tr>
<th>Order</th>
<th>Name</th>
<th>Key size (bits)</th>
<th>IV size (bits)</th>
<th>State size (bits)</th>
<th>Tag size (bits)</th>
<th>Use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>SIMON-JAMBU96/96</td>
<td>96</td>
<td>48</td>
<td>144</td>
<td>48</td>
<td>Lightweight/Defense in depth</td>
</tr>
<tr>
<td>Secondary</td>
<td>SIMON-JAMBU64/96</td>
<td>96</td>
<td>32</td>
<td>96</td>
<td>32</td>
<td>Lightweight/Defense in depth</td>
</tr>
<tr>
<td>Tertiary</td>
<td>SIMON-JAMBU128/128</td>
<td>128</td>
<td>64</td>
<td>192</td>
<td>64</td>
<td>Lightweight/Defense in depth</td>
</tr>
<tr>
<td>Quaternary</td>
<td>AES-JAMBU</td>
<td>128</td>
<td>64</td>
<td>192</td>
<td>64</td>
<td>Defense in depth/Lightweight</td>
</tr>
</tbody>
</table>
JAMBU Features

• Use the existing block ciphers directly
• Lightweight mode
  • Only $n$-bit extra state is introduced (for $2n$-bit block size)
  • Only simple XORs are introduced at each step
• Reasonably strong when IV is misused
• Use only block cipher encryption in both encryption and decryption
Security of JAMBU

• Encryption
  • **When IV is unique**
    • similar to the CFB mode
  • **When IV is reused and the first $i$ plaintext blocks are the same**
    • it is obvious that the security of the $(i + 1)$-th plaintext block is insecure when nonce is reused.
    • the $(i + 2)$-th block is also insecure according to the analysis by Thomas Peyrin, Siang Meng Sim, Lei Wang, and Guoyan Zhang (FSE 2015)
    • the blocks after $(i + 2)$-th plaintext blocks are secure
Security of JAMBU

• Authentication
  • \( n \)-bit tag
  • Provide \( n \)-bit security when message size is no more than \( 2^{n/2} \) bits and nonce is misused
    • Note that the nonce reuse security for spongeWrap with \( 2n \)-bit permutation, \( n \)-bit message block size, the authentication security is \( n/2 \)-bit when nonce is misused.
  • We show in our security proof that for adversary making at most \( q \) queries with at most \( l \) blocks of message in each query
    \[
    Adv_{JAMBU}^{auth} \leq \frac{3q^2l^2}{2^{2n}} + \frac{2q^2l}{2^{2n}} + \frac{5q^2}{2^{2n+1}} + \frac{q(l+2)}{2^{2n+1}}
    \]
Performance of JAMBU

• Software
  • Around half of the speed of underlying block cipher
  • JAMBU is not designed for high-speed applications

Table. Software performance of JAMBU (Intel Core i7-4770 Haswell)

<table>
<thead>
<tr>
<th></th>
<th>64B</th>
<th>128B</th>
<th>256B</th>
<th>512B</th>
<th>1024B</th>
<th>4096B</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIMON-JAMBU96/96</td>
<td>83.24</td>
<td>62.78</td>
<td>57.21</td>
<td>54.79</td>
<td>53.21</td>
<td>51.94</td>
</tr>
<tr>
<td>SIMON-JAMBU64/96</td>
<td>124.72</td>
<td>95.67</td>
<td>84.93</td>
<td>79.67</td>
<td>76.93</td>
<td>75.08</td>
</tr>
<tr>
<td>SIMON-JAMBU128/128</td>
<td>76.11</td>
<td>58.26</td>
<td>49.55</td>
<td>45.61</td>
<td>43.06</td>
<td>41.45</td>
</tr>
<tr>
<td>AES-JAMBU</td>
<td>24.41</td>
<td>17.08</td>
<td>13.41</td>
<td>11.57</td>
<td>10.65</td>
<td>9.98</td>
</tr>
</tbody>
</table>
Performance

• Hardware
  • JAMBU mode requires the least amount of extra state comparing to other AE modes
  • FPGA results of SIMON-JAMBU96/96 on Xilinx Virtex-7 (CAESAR hardware API)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>434 MHz</td>
</tr>
<tr>
<td>Area in Slices</td>
<td>375 Slices</td>
</tr>
<tr>
<td>Area in LUTs</td>
<td>1254 LUTs</td>
</tr>
<tr>
<td>Throughput</td>
<td>385 Mbits/s</td>
</tr>
<tr>
<td>Throughput/slice</td>
<td>1.028 Mbits/Slice</td>
</tr>
<tr>
<td>Throughput/LUT</td>
<td>0.307 Mbits/LUT</td>
</tr>
</tbody>
</table>
Conclusion

• Main features of JAMBU
  • Strong authentication security when nonce is misused
  • CFB-type encryption security when nonce is misused
  • Probably the most compact authenticated encryption mode

• **No tweak** to the JAMBU mode in the third round

• Update
  • Authentication security proof in the nonce-reuse cases
  • FPGA performance of JAMBU
Thanks for your attention!