JAMBU
A Lightweight Authenticated Encryption Mode

Hongjun Wu    Tao Huang

Nanyang Technological University
JAMBU
Comparison between AEGIS, MORUS, JAMBU, ACORN

Fast

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

Lightweight

- Mode (JAMBU)
- Dedicated (ACORN)
JAMBU: Design Goal

• Design Goal:
  • To design a **lightweight AE mode**
• The previous AE modes are not that lightweight
  • For n-bit block size, the extra state sizes are

<table>
<thead>
<tr>
<th>Mode</th>
<th>Extra State Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCM</td>
<td>n-bit (authenticate-then-encrypt)</td>
</tr>
<tr>
<td>GCM</td>
<td>2n-bit</td>
</tr>
<tr>
<td>OCB3</td>
<td>2n-bit</td>
</tr>
<tr>
<td>EAX</td>
<td>3n-bit</td>
</tr>
<tr>
<td>JAMBU</td>
<td>0.5n-bit</td>
</tr>
</tbody>
</table>
JAMBU: Design

- JAMBU is a light-weight block cipher authenticated encryption mode
  - Benefits
    - Use the existing block ciphers directly
    - Light-weight mode
      - Only \( n/2 \) extra state is introduced (for \( n \)-bit block size)
      - Only simple XORs are introduced at each step
    - Reasonably strong when IV is misused
  - It is not computationally efficient
    - The computational cost is twice that of CBC encryption
JAMBU: Initialization

Block cipher: n–bit block size
IV: n/2-bit
JAMBU: Process associated Data

Data block size: $n/2$ bits
Pad the associated data with: $10^*$
JAMBU: Process plaintext

Data block size: n/2 bits
Pad the plaintext with: 10*
JAMBU: Finalization

Tag: n/2-bit
JAMBU: Security

• Encryption: as secure as CFB mode
• Authentication
  • n/2-bit tag
  • Provide **n/2-bit security** when \(2^{n/2}\) message blocks get protected

• The nonce misuse in JAMBU affects security, but JAMBU is still reasonably strong

• We performed security analysis of JAMBU
  • security proof will be provided later
JAMBU mode: Performance

• Any strong block cipher can be used in JAMBU

• In our submission, we used AES as an example
  • The speed of AES-JAMBU is about half that of AES-CBC

• The hardware area cost of JAMBU is very close to that of the underlying block cipher
  • I guess that **JAMBU is probably the most compact AE mode** in the CAESAR competition
Conclusion

• JAMBU: A lightweight authenticated encryption mode
  • Reasonably strong when nonce is misused
  • Probably the most compact authenticated encryption mode