MORUS
A Fast Authenticated Cipher

Hongjun Wu       Tao Huang

Nanyang Technological University

DIAC 2016, Nagoya
26 Sep 2016
MORUS
Different Design Approaches:

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

- Lightweight
  - Mode (JAMBU)
  - Dedicated (ACORN)
Design Motivation and Main Features

• To design a high-speed authenticated cipher:
  • No AES-NI
  • Make use of the SIMD (SSE2, AVX2) instructions

• Features
  • Fast in software: 0.69 cpb on Haswell
  • Fast in hardware: 95.8 Gbps on Xilinx Virtex 7
    250 Gbps on 65 nm ASIC (ETH implementation)
  • Nonce-based
Changes in MORUS v2

• Tweaks are **only** applied to the *finalization* of MORUS
  • Remove *register $S_3$* in the message word of finalization
  • Change the *tag generation* to the same way as the keystream generation
    • Increase the number of steps from 8 to 10 (compensating the change in tag generation)

• Rationale for tweaks
  • Improve the hardware efficiency of MORUS
## MORUS: Parameters

<table>
<thead>
<tr>
<th></th>
<th>State size (bits)</th>
<th>Key size (bits)</th>
<th>Tag size (bits)</th>
<th>Plaintext size (bits)</th>
<th>AD size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MORUS-1280-128</td>
<td>1280</td>
<td>128</td>
<td>128</td>
<td>&lt;2^{64}</td>
<td>&lt;2^{64}</td>
</tr>
<tr>
<td>MORUS-640-128</td>
<td>640</td>
<td>128</td>
<td>128</td>
<td>&lt;2^{64}</td>
<td>&lt;2^{64}</td>
</tr>
<tr>
<td>MORUS-1280-256</td>
<td>1280</td>
<td>256</td>
<td>128</td>
<td>&lt;2^{64}</td>
<td>&lt;2^{64}</td>
</tr>
</tbody>
</table>
MORUS: State and Operations

• State organization
  • MORUS-1280: five 256-bit words
  • MORUS-640: five 128-bit words

• Operations:
  • XOR, AND, SHIFT
  • Rotl\_128\_32(x, n): Divide a 128-bit block x into 4 32-bit words, rotate each word left by n bits.
  • Rotl\_256\_64(x, n): Divide a 256-bit block x into 4 64-bit words, rotate each word left by n bits.
MORUS: State Update
(Overview)

One step: 5 rounds
MORUS: Initialization

• Load IV, key and constants into the initial state
• Update state: 16 steps
• Key is XORed to the state at the end of the initialization
MORUS: Keystream Generation

• State $S = \{S_0, S_1, S_2, S_3, S_4\}$

• For MORUS-640:
  • $keystream = S_0 \oplus (S_1 << 96) \oplus (S_2 \& S_3)$

• For MORUS-1280:
  • $keystream = S_0 \oplus (S_1 << 192) \oplus (S_2 \& S_3)$
MORUS: Finalization (**Tweaked!**)  

**MORUS v1**  
- State update: **8** steps  
- Message  
  \[ S_3 \oplus (adlen||msglen) \]  
- Tag generation  
  \[ S_1 \oplus S_2 \oplus S_3 \oplus S_4 \]  

**MORUS v2**  
- State update: **10** steps  
- Message  
  \[ (adlen||msglen) \]  
- Tag generation  
  \[ S_0 \oplus (S_1 \ll C^\ast) \oplus (S_2 \& S_3) \]  

* \( C = 96 \) for MORUS-640;  
  \( C = 192 \) for MORUS-1280
## MORUS: Security Goal

<table>
<thead>
<tr>
<th></th>
<th>Confidentiality (bits)</th>
<th>Integrity (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MORUS-640-128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>MORUS-1280-128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>MORUS-1280-256</td>
<td>256</td>
<td>128</td>
</tr>
</tbody>
</table>

DIAC 2016 MORUS
Security of MORUS: Initialization

• Algebraic degree
  • After 10 steps, the algebraic degree exceeds 256

• Differential cryptanalysis
  • differential probability $< 2^{-256}$
Security of MORUS: Encryption

• Guess-and-determine attack
  • state size of MORUS is at least five times of key size
  • keystream generation function
    • state bits are not directly known to the adversary
Security of MORUS: Finalization

• Internal state collision
  • Probability < $2^{-128}$

• Differential forgery attack on the finalization
  • 10 steps, differential probability < $2^{-256}$
Security of MORUS

**Remark** on the analysis by Mileva et al. in BalkanCryptSec 2015

- Not that relevant to the security of MORUS
- Collison on the state update function: assuming special difference in the state – unrealistic
- Distinguisher in nonce-reuse scenarios – excluded in our security claim
- “differential bias” – becomes invalid when a different key is used
MORUS: Hardware Performance

• State update function of MORUS is designed to be fast in hardware
  • AND and XOR gates are used
  • Short critical path
MORUS: Hardware Performance

• Current implementation on FPGA using CAESAR API
  • Virtex 7, Xilinx Vivado 2016.2

<table>
<thead>
<tr>
<th></th>
<th>Area (Slice)</th>
<th>Area (LUT)</th>
<th>Frequency (MHz)</th>
<th>TP (Gbps)</th>
<th>TP/LUT (Mbps/LUT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MORUS-640</td>
<td>681</td>
<td>2129</td>
<td>342.4</td>
<td>43.8</td>
<td>20.6</td>
</tr>
<tr>
<td>MORUS-1280</td>
<td>1045</td>
<td>3746</td>
<td>370.4</td>
<td>95.8</td>
<td>25.6</td>
</tr>
</tbody>
</table>
MORUS: Hardware Performance

Comparison between MORUS-1280 v1 and MORUS-1280 v2

- Area (LUT)
- Throughput (Gbps)
- Throughput/LUT (Mbps/LUT)
MORUS: Hardware Performance

- Performance on ASIC: high throughput/area
  (Michael Muehlberghuber and Frank K. Gürkaynak, DIAC 2015)
• Performance on ASIC: high throughput (250Gbps) (Michael Muehlberghuber and Frank K. Gürkaynak, DIAC 2015)
MORUS: Software Performance

- Speed on Haswell, AVX2 is used in MORUS-1280

<table>
<thead>
<tr>
<th></th>
<th>16B</th>
<th>64B</th>
<th>512B</th>
<th>1024B</th>
<th>4096B</th>
<th>16384B</th>
</tr>
</thead>
<tbody>
<tr>
<td>MORUS-640(EA)</td>
<td>40.64</td>
<td>10.35</td>
<td>2.30</td>
<td>1.72</td>
<td>1.30</td>
<td>1.19</td>
</tr>
<tr>
<td>MORUS-640(DV)</td>
<td>38.47</td>
<td>10.13</td>
<td>2.30</td>
<td>1.72</td>
<td>1.29</td>
<td>1.18</td>
</tr>
<tr>
<td>MORUS-1280(EA)</td>
<td>45.32</td>
<td>10.38</td>
<td>1.85</td>
<td>1.24</td>
<td>0.80</td>
<td>0.69</td>
</tr>
<tr>
<td>MORUS-1280(DV)</td>
<td>45.74</td>
<td>10.66</td>
<td>1.91</td>
<td>1.28</td>
<td>0.81</td>
<td>0.70</td>
</tr>
</tbody>
</table>
MORUS: Software Performance

• Faster than AES-GCM on Haswell (1.03 cpb)
• Almost the same as MORUS v1 for long message

• Reasons:
  • Benefits from SIMD
  • Removed the redundant operations in the cipher
Conclusion

• **MORUS**
  • The fastest candidate on the platforms with SIMD but with no AES-NI (0.69 cpb with AVX2)
  • The most efficient candidate in hardware
    MORUS-1280: 95.88 Gbps, 3764 LUTs, 25.6 Mbps/LUT

• **MORUS v2**
  • Tweaked finalization to reduce hardware area. Throughput/Area is increased by **28%**
Thanks for your attention!