3rd Round Ciphers Evaluation on Microcontrollers

Sebastian Renner, Enrico Pozzobon and Jürgen Mottok

Laboratory for Safe and Secure Systems, OTH Regensburg
May 9, 2022
Table of Contents

- Benchmarking Environment
- Implementation Overview
- Results
- Discussion
- Conclusion
Automated software implementation benchmarking on MCUs

5 target platforms

4 architectures (ARM, AVR, Xtensa, RISC-V)

Evaluation of speed, code size and RAM utilization
- Result updates available at lwc.las3.de
- Maintenance of public cipher repository
- Implementation submission via form/mail (lwc@las3.de)
Implementation Overview

- 295 implementations for 3rd round candidates
- 85 ARM-optimized variants
- 10 specific AVR implementations
- 12 submissions optimized for Xtensa/ESP32
Figure: Implementations tested per candidate (for every variant)
Comparison of primary candidates only (in this talk)
Best (primary) implementation for each test case is chosen
Speed/ROM test case on 5 platforms
RAM utilization measurement taken only on the STM32F7
Basic AES-GCM implementation to compare to LWC ciphers
Figure: Speed measurements on the Arduino Uno
Figure: Speed measurements on the ESP32
**Figure:** Speed measurements on the Maixduino

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time [µs]</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-GCM</td>
<td>3.18</td>
</tr>
<tr>
<td>ASCON</td>
<td>2.19</td>
</tr>
<tr>
<td>Elephant</td>
<td>3.31</td>
</tr>
<tr>
<td>GIFT-COFB</td>
<td>3.42</td>
</tr>
<tr>
<td>ISAP</td>
<td>4.26</td>
</tr>
<tr>
<td>Romulus</td>
<td>4.13</td>
</tr>
<tr>
<td>SPARKLE</td>
<td>3.5</td>
</tr>
<tr>
<td>TinyJAMBU</td>
<td>3.27</td>
</tr>
<tr>
<td>Xoodyak</td>
<td>2.98</td>
</tr>
</tbody>
</table>
Figure: Speed measurements on the STM32F7

![Graph showing speed measurements of various cryptographic algorithms on the STM32F7]

- AES-GCM: 6.74 µs
- ASCON: 3.59 µs
- Elephant: 2.65 µs
- GIFT-COFB: 3.38 µs
- ISAP: 3.93 µs
- PHOTON-Beetle: 4.73 µs
- Romulus: 4.88 µs
- SPARKLE: 3.74 µs
- TinyJAMBU: 3.04 µs
- Xoodyak: 2.77 µs
Figure: Speed measurements on the STM32F103

Results: Speed
**Figure:** Code size measurements on the Arduino Uno

[Bar chart showing code size measurements for various algorithms on the Arduino Uno.]
Figure: Code size measurements on the ESP32
**Figure:** Code size measurements on the Maixduino

![Bar chart showing code size measurements for various AEAD algorithms.](image)

- AES-GCM: $1.37 \cdot 10^5$ (1.37MB)
- ASCON: $1.32 \cdot 10^5$ (1.32MB)
- Elephant: $1.31 \cdot 10^5$ (1.31MB)
- GIFT-COFB: $1.29 \cdot 10^5$ (1.29MB)
- ISAP: $1.25 \cdot 10^5$ (1.25MB)
- ISAP-Beetle: $1.25 \cdot 10^5$ (1.25MB)
- Romulus: $1.25 \cdot 10^5$ (1.25MB)
- SPARKLE: $1.24 \cdot 10^5$ (1.24MB)
- TinyJAMBU: $1.24 \cdot 10^5$ (1.24MB)
- Xodyak: $1.29 \cdot 10^5$ (1.29MB)
Figure: Code size measurements on the STM32F7
Figure: Code size measurements on the STM32F103
Figure: RAM utilization measurements on the STM32F7
AES-GCM outperforms at least 3 LWC algorithms on each speed test case

Xoodyak, TinyJAMBU and ASCON always outperform (our) AES-GCM in throughput

SPARKLE/GIFT-COFB also deliver above average speeds
- AES-GCM ranks last in code size on 3 of 4 platforms (3rd to last on the 4th)
- ASCON, TinyJAMBU, SPARKLE and Xoodyak rank overall best in code size (for non-AVR)
- ISAP performs well regarding binary size
- An AVR-optimized implementation of PHOTON-Beetle ranks 1st on the Arduino Uno
- Reference implementations are slow but often have little code size
AES-GCM ranks 2nd to last in RAM utilization

TinyJAMBU, ASCON, SPARKLE, Xoodyak and GIFT-COFB form the top half

The overall differences in RAM are rather small compared to other metrics
- AES-GCM is outperformed by some LWC ciphers in any test case
- Similar ciphers reach top ranks in almost every benchmark
- Performance is highly dependent on the optimization level of the implementation