# 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

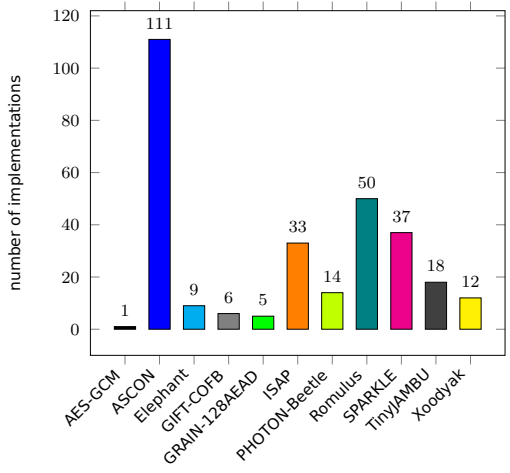
- Automated software implementation benchmarking on MCUs
- 5 target platforms
- 4 architectures (ARM, AVR, Xtensa, RISC-V)
- Evaluation of speed, code size and RAM utilization

- 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)

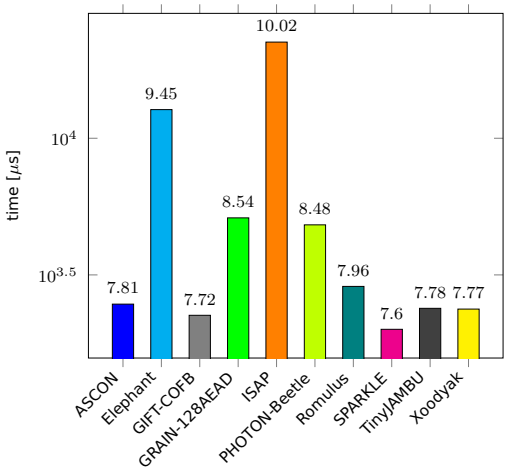


# Results

- Comparison of primary canidates 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

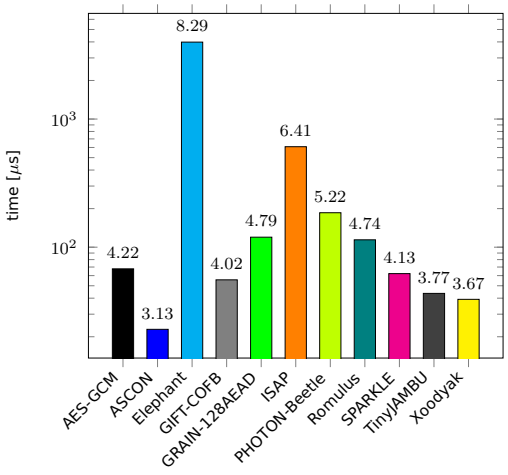
# Results: Speed

Figure: Speed measurements on the Arduino Uno



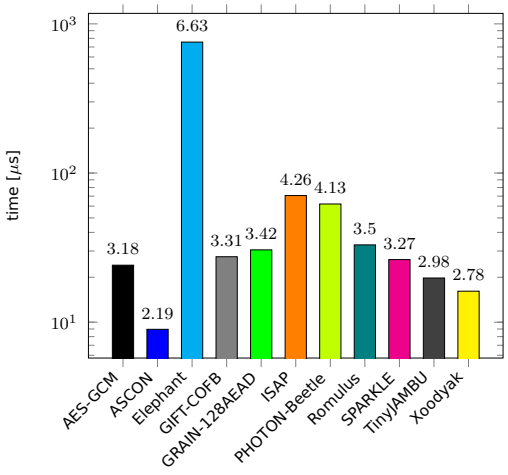
# Results: Speed

Figure: Speed measurements on the ESP32



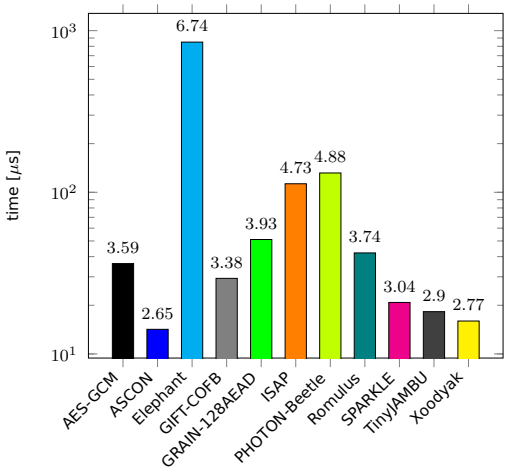
# Results: Speed

Figure: Speed measurements on the Maixduino



# Results: Speed

Figure: Speed measurements on the STM32F7



# Results: Speed

Figure: Speed measurements on the STM32F103

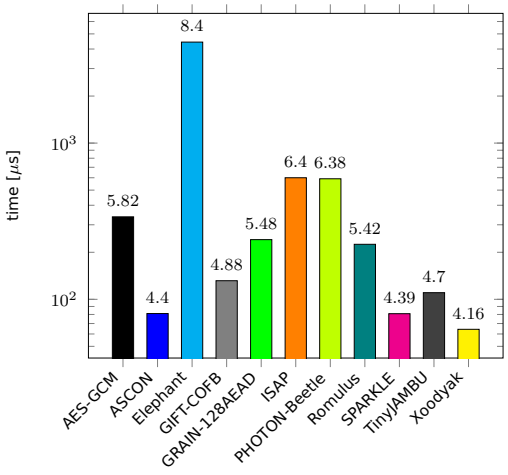
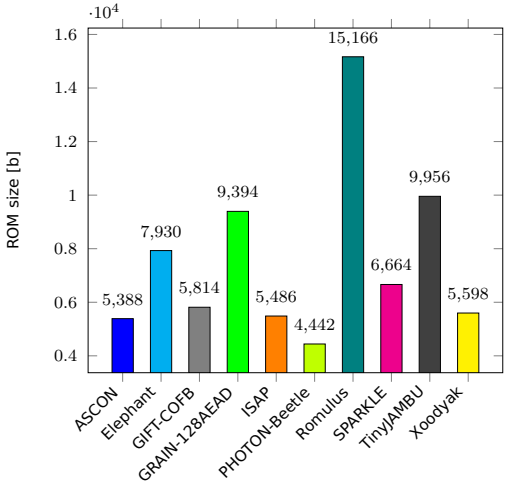


Figure: Code size measurements on the Arduino Uno



# Results: ROM

Figure: Code size measurements on the ESP32

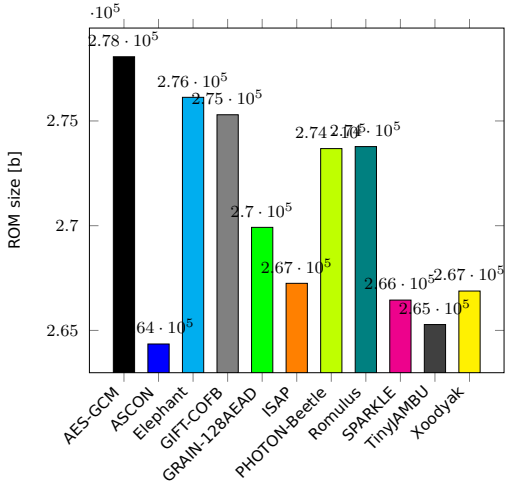


Figure: Code size measurements on the Maixduino

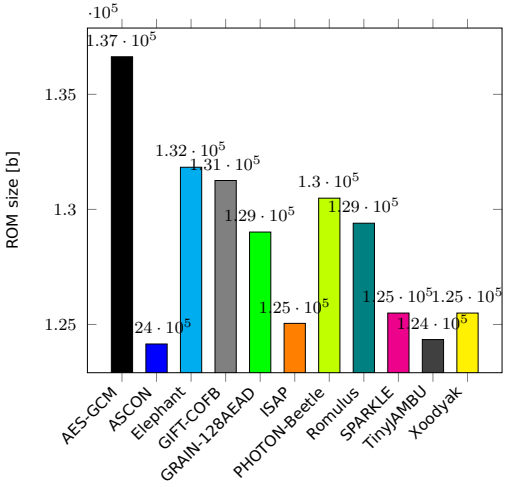


Figure: Code size measurements on the STM32F7

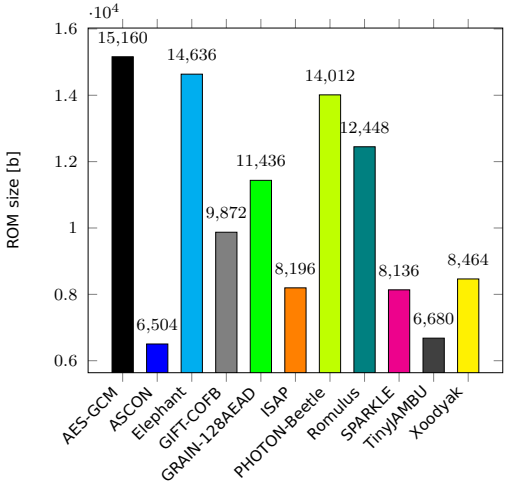
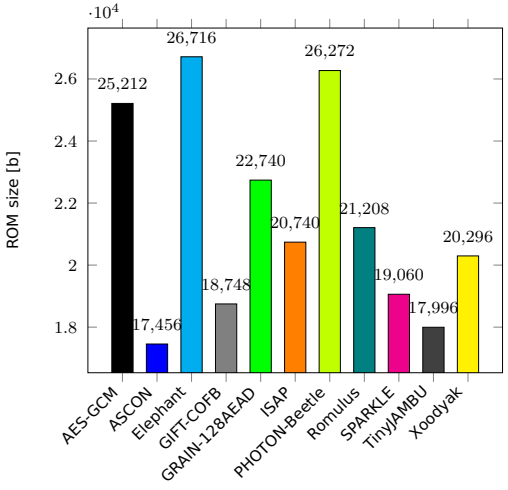
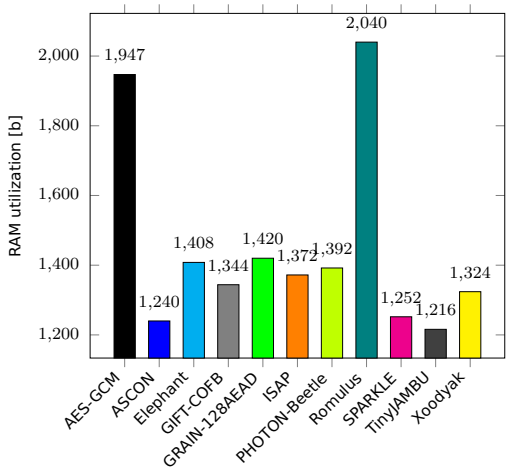


Figure: Code size measurements on the STM32F103



# Results: RAM

Figure: RAM utilization measurements on the STM32F7



# Conclusion: Speed

- 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

# Conclusion: RAM

- 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

# Conclusion

- 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