Current and Future Efforts in Benchmarking NIST LWC Ciphers

Sebastian Renner, Enrico Pozzobon and Jürgen Mottok

Laboratory for Safe and Secure Systems, OTH Regensburg
October 20, 2020
Table of Contents

- Statistics
- Current State of Work
- Results
- Lessons Learned
- Feature Requests
- Future Work
- Discussion
300+ different implementations tested (2nd round)
9-10 implementations/candidate (avg.)
Ranging from 1 to 37 implementations
► Results published at lwc.las3.de
► Maintenance of public cipher repository
► Cipher submission form
5 Boards supported (incl. RISC-V)
Highlighting of ’main’ variants
Basic test vector/time plots
Which implementations are comparable?
What impact does the platform have?
Different levels of optimization
Inner-family vs. inter-family
Every result can be compared on the web
Figure: Speed measurements of xoodyak on the STM32F103
Figure: Speed measurements of giftcofb128v1 on the STM32F7
Results: Speed

![Graph showing speed measurements of isapk128av20 on the STM32F103]

Figure: Speed measurements of isapk128av20 on the STM32F103

- ref: 5,879.11 µs
- rhys: 3,717.85 µs
- opt32-armv6m: 2,467.18 µs
- opt32-armv7m: 2,217.23 µs
Figure: Speed measurements on the STM32F103
Figure: ROM size measurements of giftcofb128v1 on the STM32F7
Results: ROM

Figure: ROM size measurements on the STM32F103
**Figure:** RAM usage measurements on the STM32F7
Lessons Learned

- Automate as much as possible
- The closer a deadline, the more submissions
- Cache matters
- Keep track of every change (git)
Feature Requests

- Provide access to log files
- Calculate a combined metric (Speed/ROM/RAM)
- Provide speed in cycles/byte
Future Work

- Provide more versatile visual representations of the test results
- Extend test setup to collect power traces to facilitate SCA
- Create & benchmark masked/protected implementations