Benchmarking Software Implementations of 1st Round Candidates of the NIST LWC Project on MCUs

Sebastian Renner, Enrico Pozzobon and Jürgen Mottok

Laboratory for Safe and Secure Systems, OTH Regensburg

November 3, 2019
Table of Contents

- Goals
- Framework
- Test Setup
- Test Cases
- Platforms
- Results
- Conclusion & Future Work
Goals

- Obtain performance figures for all NIST LWC candidates
- Provide results on popular embedded platforms
- Test as many cipher variants as possible (per platform)
- Fair comparison, i.e. no change of ref. implementations
- High degree of automation
- Easy extensibility
- Written in C, Python and Bash
- Common test procedure for all platforms
- MCU-specific template (platformIO/STM32CubeMX)
- Fully automated compilation and test routine
- Measurements are taken directly on the DUT
- Use of NIST test vectors and API
Test vectors sent and verified over stdout/stdin

Submitted Algorithms

MCU-specific template

C/C++/Arduino project structure

adapter.py

MCU

UART

JTAG / SWD

MCU

Measurements from probes

Test vectors sent and verified over stdout/stdin

Logs

Test Vectors

Git

Circuit

Figure: Core components and data flow of the test framework
- SEGGER J-Link
- Saleae logic analyzer
- GPIO pull up/down for signaling
Figure: Benchmark Test Setup
Average over 1089 generated NIST test vector en- and decryptions

Expected PT and CT are compared to the results

`nocrypt` memcpyp “algorithm“

AES-GCM implementation stripped out of mbedTLS for reference
Test Cases: ROM Footprint

- `nocrypt` template size as baseline
- Compilation with optimization for speed (where possible)
- Bash script to determine code size
Conducted only on the STM32 F746ZG
RAM gets filled with a known pattern
Memory dumped after execution of algorithm(s)
Consecutive untouched memory segments are seen as “unused memory”
nocrypt is used as a reference
Tested Platforms

- Arduino Uno R3: 8 bit ATmega328P MCU, 16 MHz clock, 32 KB flash
- STM32F1 “bluepill”: 32 bit ARM Cortex-M3 core, 72 MHz clock, 64 KB flash
- STM32 NUCLEO-F746ZG: 32 bit ARM Cortex-M4, 216 MHz clock, 1MB flash
- Espressif ESP32 WROOM: 32 bit Xtensa LX6 MCU, 240 MHz clock, 4 MB flash
Figure: Ten fastest implementations on the STM32 F746ZG
Results: ROM

Figure: Ten smallest implementations on the STM32 F746ZG
Results: RAM

**Figure:** Ten least RAM-intensive implementations on the STM32 F746ZG
Figure: Test results for top ciphers per test case on the STM32 F746ZG
Use of plain reference implementations

Some cipher variants have not been tested (e.g. optimized implementations)

The level of protection against SCA/FI was not taken into account
Development of an easily extensible LWC performance evaluation tool for embedded devices

Successful test of 200+ cipher variants (enc/dec test case)

AES-GCM is neither best nor worst in all test cases
Future Work

- Extension of evaluation tool
- Determine why some tests failed
- SCA/FI attacks & countermeasures on e.g. fastest candidates