Constant-Time Bitsliced Rijndael-256 on ARM Cortex-M4: On the Limitations of Fixlicing Beyond AES-128

IIUM Engineering Journal • Article • *Open Access* • 2026 • DOI: 10.31436/iiumej.v27i2.4405

Lestari, Andriani Adi [a] ; Suryadi, MT [b] ; Ramli, Kalamullah [a] ; Gunawan, Teddy Surya [c] ; Agustina, Esti Rahmawati [d] ; +1 author

[a] Department of Electrical Engineering, Universitas Indonesia, Faculty of Engineering, Depok, 16424, Indonesia

Abstract

Wider-block ciphers are increasingly needed in high-volume applications, because 128-bit blocks in modes such as Galois/Counter Mode (GCM) limit each invocation to roughly 64 GiB of plaintext per key-nonce pair, forcing complex re-keying strategies. Rijndael-256, the 256-bit-block variant of Rijndael with a 256-bit key, has therefore attracted renewed interest as a natural wider-block companion to Advanced Encryption Standard (AES). At the same time, 32-bit ARM Cortex-M microcontrollers dominate the IoT and embedded landscape, yet, to the best of our knowledge, no constant-time software implementation of Rijndael-256 targeting this platform has been published. This paper addresses that gap. We present a constant-time bitsliced implementation of Rijndael-256 on the ARM Cortex-M4 and provide a systematic structural analysis explaining why fix slicing, the technique that achieves the best-known AES-128 performance on this platform, becomes suboptimal

when applied to Rijndael-256. Specifically, the irregular ShiftRows offsets (0, 1, 3, 4) of Rijndael-256 break the uniform register rotation exploited by fix slicing, requiring eight distinct MixColumns compensation variants instead of four. We demonstrate that these compensation variants cost 3.00 × as much as executing an explicit, in-place ShiftRows routing using ARM's bitfield instructions. Our macro-inlined assembly variant achieves 6,199 cycles (193.7 cycles/byte) at -O2, including packing and unpacking. We provide benchmarks across five compiler optimization levels, constant-time verification over 10^6 samples via DUDECT (maximum t-statistic well below the vulnerability threshold), and per-component cycle breakdowns, showing that the optimal bitslicing strategy is inherently cipher-specific and architecture-dependent.

Author keywords

ARM Cortex-M4; bitslicing; constant-time implementation; fix slicing; Rijndael-256

Corresponding authors

Corresponding author	K. Ramli
Affiliation	Department of Electrical Engineering, Universitas Indonesia, Faculty of Engineering, Depok, 16424, Indonesia
Email address	kalamullah.ramli@ui.ac.id

Abstract

Author keywords

Corresponding authors

About Scopus

What is Scopus