Application Brief

CC27xx HSM Timing Benchmarks

Zhitao Wu

Introduction

The CC27xx is a Texas Instruments' wireless microcontroller device family with an integrated hardware security module (HSM) providing hardware-accelerated cryptography. Embedded firmware engineers and security architects can use this document to help design connected products for internet of things (IoT), smart home, industrial automation, and wireless sensor applications where security and energy efficiency are both critical.

This document tests the timing performance benchmark for the CC2745, a TI wireless microcontroller that integrates a dedicated hardware security module (HSM) for accelerating cryptographic operations. The HSM offloads security workloads from the main CPU.

The testing process measured timing data for AES-128, SHA-256, and ECC-256 operations. All timing tests were run using Texas Instruments' SimpleLink™ Low Power F3 software development kit (SDK) version 9.20.00.81 with HSM firmware version 3.4.5 on PG2.0 silicon unless otherwise noted. The results include key recommendations drawn from the testing data and comparisons between HSM hardware acceleration and MbedTLS software.

The data enables design teams to select the appropriate crypto path: HSM hardware for bulk throughput (up to 2.5 times faster at larger payloads) and software fallback for small-packet, latency-sensitive use cases.

Timing Comparison: HSM Hardware vs MbedTLS Software

Measurements were taken on SDK 9.20.00.81 with HSM firmware of 3.4.5 on PG2.0 silicon. The results show that HSM hardware delivers significantly better throughput than MbedTLS software for larger payloads.

Table 1. AES-CBC-128

Data Size	Encryption			Decryption		
	HSM HW (µs)	MbedTLS SW (µs)	SW to HW Ratio	HSM HW (µs)	MbedTLS SW (µs)	SW to HW Ratio
16 bytes	124	34	0.27 × (SW faster at small sizes)	122	84.5	0.69 × (SW faster at small sizes)
128 bytes	124	134.5	1.08 × (HW faster)	123.5	204	1.65 × (HW faster)
256 bytes	127	232.5	1.83 × (HW faster)	125.5	328	2.61 × (HW faster)

Table 2. SHA-256

Data Size	HSM HW (µs)	MbedTLS SW (µs)	SW to HW Ratio
3 bytes	110.5	70	0.63 × (SW faster at small sizes)
65 bytes	109	125.5	1.15 × (HW faster)
252 bytes	110	279.5	2.54 × (HW faster)

Table 3. ECDSA- SECP-256

Op	HSM HW (ms)	MbedTLS SW (ms)	SW/HW Ratio
Signing	23.63	1062	44.94 × (HW faster)
Verification	41.50	4017	96.8 × (HW faster)

Key Findings

The CC2745 HSM provides hardware-accelerated cryptographic operations. The benchmark data produced the following key findings:

- AES-128 encryption or decryption latency is approximately 124 to 127µs, indicating that the HSM operation restricts the latency rather than the driver interface. SHA-256 can show a similar pattern.
- Even though ECC-256 signing (approximately 24ms) and verification (approximately 41ms) are the most expensive operations, these operations still outperform MbedTLS software.
- For larger payloads, HSM hardware outperforms MbedTLS software:
  - AES-CBC encryption is approximately 1.83 times faster at 256 bytes and decryption is approximately 2.61 times faster
  - SHA-256 is approximately 2.5 times faster at 252 bytes
  - At small data sizes (less than approximately 30 bytes), MbedTLS software is faster due to HSM initialization overhead

Overall, the HSM is appropriate for applications requiring bulk cryptographic throughput and ECDSA based signing and verification. For latency-sensitive operations on small data (less than 16–30 bytes), designs can implement a software fallback.

References

1. Texas Instruments, *CC274xR-Q1, CC274xP-Q1 Automotive SimpleLink™ Bluetooth® Low Energy Wireless MCU* datasheet

Trademarks

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale, TI’s General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Last updated 10/2025