

Application Brief

CC27xx HSM 时序基准



Zhitao Wu

简介

CC27xx 是德州仪器 (TI) 的无线微控制器器件系列，集成了硬件安全模块 (HSM)，可提供硬件加速的加密功能。嵌入式固件工程师和安全架构师可以使用本文档来帮助为物联网 (IoT)、智能家居、工业自动化和无线传感器应用设计互联产品，在这些应用中安全和能效都至关重要。

本文档测试 CC2745 的时序性能基准，该器件是一款 TI 无线微控制器，集成了专用硬件安全模块 (HSM) 以加速加密操作。HSM 从主 CPU 转移了安全工作负载。

测试过程测量了 AES-128、SHA-256 和 ECC-256 操作的时序数据。所有时序测试均使用德州仪器 (TI) 的 SimpleLink™ 低功耗 F3 软件开发套件 (SDK) 版本 9.20.00.81 和 PG2.0 器件上的 HSM 固件版本 3.4.5 进行，除非另有说明。结果包括根据测试数据得出的核心建议以及 HSM 硬件加速与 MbedTLS 软件之间的比较。

这些数据可帮助设计团队选择适当的加密路径：使用 HSM 硬件处理大吞吐量（在较大的有效载荷下速度提升达 2.5 倍），使用软件回退处理对延迟敏感的小数据包用例。

时序比较：HSM 硬件与 MbedTLS 软件

在 PG2.0 器件上，在 HSM 固件版本为 3.4.5 的 SDK 9.20.00.81 上进行了测量。结果表明，对于较大的有效载荷，HSM 硬件可提供比 MbedTLS 软件明显更好的吞吐量。

表 1. AES-CBC-128

数据大小	加密			解密		
	HSM 硬件 (μs)	MbedTLS 软件 (μs)	软件与硬件比率	HSM 硬件 (μs)	MbedTLS 软件 (μs)	软件与硬件比率
16 字节	124	34	0.27 × (小数据量下软件更快)	122	84.5	0.69 × (小数据量下软件更快)
128 字节	124	134.5	1.08 × (硬件更快)	123.5	204	1.65 × (硬件更快)
256 字节	127	232.5	1.83 × (硬件更快)	125.5	328	2.61 × (硬件更快)

表 2. SHA-256

数据大小	HSM 硬件 (μs)	MbedTLS 软件 (μs)	软件与硬件比率
3 字节	110.5	70	0.63 × (小数据量下软件更快)
65 字节	109	125.5	1.15 × (硬件更快)
252 字节	110	279.5	2.54 × (硬件更快)

表 3. ECDSA- SECP-256

操作	HSM 硬件 (ms)	MbedTLS 软件 (ms)	软件/硬件比率
签名	23.63	1062	44.94 × (硬件更快)
验证	41.50	4017	96.8 × (硬件更快)

核心发现

CC2745 HSM 提供了硬件加速的加密操作。根据基准数据得出了以下核心发现：

- AES-128 加密或解密延迟约为 124 至 127 μ s，表明限制延迟的是 HSM 操作本身，而非驱动器接口。SHA-256 可能呈现类似的模式。
- 尽管 ECC-256 签名 (约 24ms) 和验证 (约 41ms) 是开销最大的操作，但其性能仍优于 MbedTLS 软件实现。
- 对于更大的有效载荷，HSM 硬件性能优于 MbedTLS 软件：
 - AES-CBC 加密在 256 字节时速度提升约 1.83 倍，解密速度提升约 2.61 倍
 - SHA-256 在 252 字节时速度提升约 2.5 倍
 - 在小数据量 (小于约 30 字节) 时，由于 HSM 初始化开销，MbedTLS 软件实现更快

总体而言，HSM 适用于需要批量加密吞吐量以及基于 ECDSA 的签名和验证的应用。对于小数据量 (小于 16 - 30 字节) 且对延迟敏感的操作，设计可采用软件回退方式。

参考资料

1. 德州仪器 (TI)，[CC274xR-Q1](#)、[CC274xP-Q1](#) 汽车级 SimpleLink™ 低功耗 Bluetooth® 无线 MCU 数据表

商标

SimpleLink™ is a trademark of Texas Instruments.

所有商标均为其各自所有者的财产。

重要通知和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做任何明示或暗示的担保，包括但不限于对适销性、与某特定用途的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他安全、安保法规或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 [TI 销售条款](#)、[TI 通用质量指南](#) 或 [ti.com](#) 上其他适用条款或 TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

版权所有 © 2026，德州仪器 (TI) 公司

最后更新日期：2025 年 10 月