

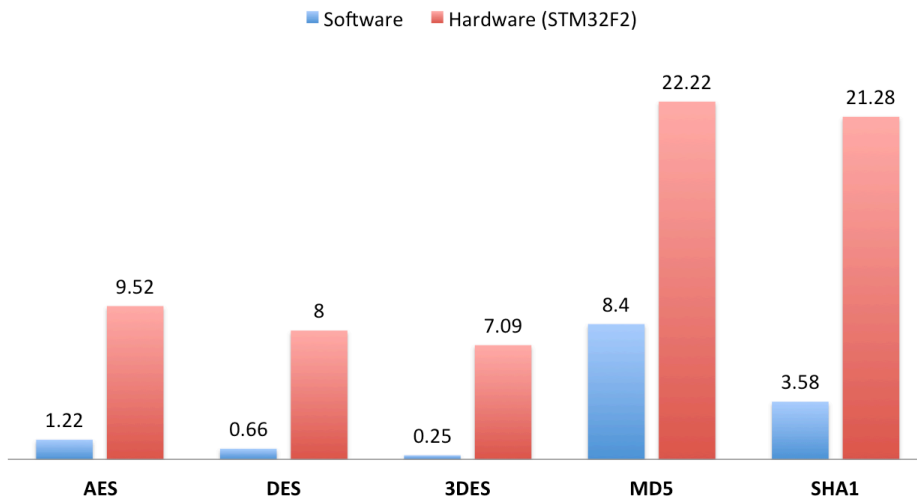


## wolfSSL + STM32

STM32 Hardware Encryption, RNG, and STM32CubeMX Support

The wolfSSL embedded SSL/TLS library now has support for the hardware-based cryptography and random number generator offered by the STM32F2/F4 processor, and support for both STM32CubeMX and the STM32 HAL.

CTaoCrypt Algorithm Speeds (MB/s)



### STM32 Hardware Crypto:

- AES (CBC, CTR)
- DES (ECB, CBC)
- 3DES
- MD5
- SHA1



### STM32 Hardware Crypto Support

Using wolfSSL with the STM32F2, applications can see substantial speed improvements when using hardware accelerated cryptography versus using wolfSSL's standard software crypto implementation. The following benchmarks were gathered from the wolfCrypt benchmark application running on the **STM3221G-EVAL** board (STM32F2) using the **STM32F2 Standard Peripheral Library** and **FreeRTOS**. For details regarding the STM32F2 cryptography and hash processors, please see the STM32Fxx Standard Peripheral Library documentation, or STM32CubeMX with HAL.

### Perfect for your Embedded Device

wolfSSL is a fully-featured, progressive, and easy-to-use SSL/TLS library perfect for resource constrained systems. With a footprint size of 20-100kB, runtime memory usage of 1-36 kB, and support for a large number of operating systems, it is the perfect solution for securing your embedded project today.

### Learn More

For more information about using wolfSSL with the STM32 processor, please contact us at [info@wolfssl.com](mailto:info@wolfssl.com), or visit our website [www.wolfssl.com](http://www.wolfssl.com).

[www.wolfssl.com](http://www.wolfssl.com)

Copyright © 2017 wolfSSL Inc. All Rights Reserved