Silicom Ltd.
Connectivity Solutions

Intel® Crypto Technology Accelerates WolfSSL Embedded SSL library

Intel® QuickAssist technology adapters made by Silicom bring performance surge

Feb. 2017

WolfSSL is a lightweight and portable C language based SSL/TLS library that is fast, and rich in feature set [1], such as FIPS support, smart cards support and external crypto engines support.

WolfSSL's main advantage lies in its remarkable efficiency. WolfSSL team took it one step further and enhanced the package operation with the integration of Intel® based QuickAssist crypto acceleration technology.

Being a strong partner of Intel, as well as being an Intel network builder, Silicom manufactures complete line of QuickAssist PCIe adapters, of all generations.

Benchmarking WolfSSL against Intel® QuickAssist adapter made by Silicom, yielded tremendous improvement in performance. In fact, not only does WolfSSL outperform common open source packages as a pure software package, WolfSSL could also squeeze out even better numbers out of same QuickAsssit adapter compared to common open source SSL/TLS projects.

As it comes to operation with co-processors in general, also with QuickAssist the best mode of operation is by asynchronous crypto functions calls. And indeed, WolfSSL team successfully managed to remodel the I/O operation of the basic package to work in an asynchronous mode with QuickAssist, thus working in the best mode with it.

Hardware	
Server	Intel(R) dual Xeon(R) CPU E5-2440 v2 @ 1.90GHz
Adapter	Silicom QAT PE3iSCO3 with Intel® 8955 chipset

Table 1 - Hardware setup

Software
CentOS 7.0 Linux
Intel QuickAassist v2.6-60
WolfSSL v3.10.0

Table 2 – Software setup

The test of which results are brought herein focuses on asymmetric encryption (RSA [2] and ECC [3]), that pauses the highest burden on standard x86 CPUs.

The results are outright and very convincing. Two threads of test application using WolfSSL managed to reach the peak performance of the QuickAssist engine with asymmetric encryption (see Table 3).

Algorithm	Threads	WolSSL w/ QuickAssist	WofSSL on x86
RSA 2K	4	41K	400
ECC256	4	53K	600

Table3 - Tests results

Indeed, unlike QuickAssist assisted WolfSSL, the software only version of WolfSSL scales up with CPU cores, where the QuickAssist version reach the peak quite early in the game. However, reaching a peak as high as seen in Table 3 with QuickAssist is beyond the capability of standard CPU, regardless of core count or software package. Evidently, overall performance is improved by using QuickAssist, while a large portion of CPU cycles is relieved for further business logic processing.

REFERENCES

[1] http://www.wolfssl.com

[2] https://simple.wikipedia.org/wiki/RSA_(algorithm)

[3] https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

Silicom ltd., 14 Atir Yeda St., Kefar Sava, ISRAEL
sales@silicom.co.il www.silicom-usa.com