wolfSSL / wolfCrypt Asynchronous Support

With Intel QuickAssist or Cavium Nitrox III/V crypto hardware

The wolfSSL / wolfCrypt libraries support asyncronous (non-blocking) crypto using hardware acceleration with the Intel QuickAssist adapter and Cavium Nitrox III/V. This allows greatly increased performance on server platforms requiring high connection rates and throughput.

Performance Benchmarks

Asymmetric ops/sec	SW (CPU)	SW (AESNI)	HW QAT	Times Faster
RSA 2048 public	14,140	14,262	209,909	14.85
RSA 2048 private	1,145	1,149	41,999	36.68
DH 2048 key gen	3,833	3,849	112,491	29.35
DH 2048 key agree	3,784	3,799	95,129	25.14
ECDHE 256 agree	5,029	5,262	55,117	10.96
ECDSA 256 sign	4,900	5,450	46,798	9.55
ECDSA 256 verify	7,201	8,527	28,917	4.02

Symmetric MB/sec	SW (CPU)	SW (AESNI)	HW QAT	Times Faster
AES-CBC Enc	978	4,809	2,932	3.00
AES-CBC Dec	1,020	23,021	2,882	2.83
AES-GCM	108	5,045	2,903	26.88
3DES	161	160	1,511	9.39
MD5	3,452	3,444	2,309	0.67
SHA	1,716	1,720	5,068	2.95
SHA-224	986	1,277	2,392	2.43
SHA-256	972	1,274	1,941	2.00
SHA-384	1,312	1,286	2,020	1.54
SHA-512	1,317	1,875	1,908	1.45

Performed on an Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 12GB RAM, with QuickAssist DH895xCC (1 MB)

Asynchronous Features

wolfSSL:

- Client and Server (SSL/TLS)
- Public Key infrastructure – Handshake / PKI (RSA, ECC, DH)
- Encryption/ Decryption
- Hashing / HMAC
- Certificate Signing and Verification

wolfCrypt:

- PKI: RSA public/private (CRT/non-CRT), ECDSA/ECDH, DH
- Cipher: AES CBC/GCM, DES3
- Digest: MD5, SHA, SHA224, SHA256, SHA384, SHA512 and HMAC.
- Hardware simulator for testing/evaluation

Design: The implemention is similar to epoll, which ensures that no function call will block. If a call would block waiting on hardware then "WC_PENDING_E" is returned and the hardware must be polled. For wolfSSL polling is done with either "wolfSSL_CTX_AsyncPoll" or "wolfSSL_AsyncPoll". For wolfCrypt polling is done with "wolfAsync_EventQueuePoll" or "wolfAsync_EventPoll".

Learn More

For more information on the wolfSSL asynchronous features or to evalaute it, please contact us at info@wolfssl.com.