wolfSSL / wolfCrypt Asynchronous Support

With Intel QuickAssist or Cavium Nitrox III/V crypto hardware

The wolfSSL / wolfCrypt libraries support asynchronous (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	Native C	ASM*	Quick Assist	Nitrox V
RSA 2048 public	2,199	35,857	187,754	140,699
RSA 2048 private	196	1,166	37,521	8,266
DH 2048 key gen	577	2,296	54,781	
DH 2048 key agree	571	1,976	82,803	
ECDHE 256 agree	1,136	16,782	48,691	10,503
ECDSA 256 sign	1,107	41,192	46,930	22,165
ECDSA 256 verify	1,662	13,208	26,932	7,361

Symmetric MB/sec	Native C	ASM*	Quick Assist	Nitrox V
AES-128-CBC-Enc	282	844	2,518	238
AES-128-CBC-Dec	287	6,018	2,513	238
AES-128-GCM	68	3,099	2,519	133
SHA	552	567	2,704	
SHA-224	246	474	2,209	
SHA-256	246	474	2,045	
SHA-384	373	689	1,688	
SHA-512	374	689	1,682	

Performed on an Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 12GB RAM, Single Thread, wolfSSL v3.14.4 on QuickAssist DH895xCC (1 MB) and Cavium Nitrox V CNN5560-900-C45
** ASM: Assembly speedups (AXV/AVX2/AESNI/RDRAND/SP-ASM)*

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-1, SHA-2, SHA-3 and HMAC.
- Hardware simulator for testing/evaluation
- DRBG and NRBG

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.