Silicom
Connectivity Solutions

SILICOM PE3ISCO3 ECC PERFORMANCE TESTS WITH INTEL® 8955

GENERAL

In order to demonstrate the currently available acceleration for Elliptic Curve cryptography, Silicom performed benchmark tests for ECC computations. Using OpenSSL software, with **NIST P256 and P384** (prime) curves implementations, tests were carried out, comparing software-only capability against Intel® 8955 QuickAssist Technology acceleration engine, laid as a lookaside engine on **Silicom PE3iSCO3** PCIe adapter.

TEST DESCRIPTION

Software	Intel® QuickAssist Technology v1.6 software suite (1 instance, 4 processes in dh895xcc_qa_dev0.conf) OpenSSL 1.0.1h with QuickAssist crypto engine Linux (none) 3.6.11-4.fc16.x86_64 #1 SMP Tue Jan 8 20:57:42 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux
Hardware	Intel® 8955 on **Silicom PE3iSCO3** PCIe adapter Intel® Dual Xeon® CPU E5-2670 v2 @ 2.50GHz (2 x 10 cores)

Tests Procedure
Software only
(No acceleration)
	<u>Utility command line invocation</u> –
	`[user@host tests]# taskset 0x3ff openssl speed {ecdhp256, ecdhp384}`
	`[user@host tests]# taskset 0x3ff openssl speed {ecdsap256, ecdsap384}`

Tests Procedure
Accelerated with QuickAssist Technology
	Utility command line invocation –
	`[user@host tests]# taskset 0x3ff openssl speed -engine qat {ecdhp256, ecdhp384}`
	`[user@host tests]# taskset 0x3ff openssl speed -engine qat {ecdsap256, ecdsap384}`

TESTS RESULTS

Tests Results

Software Only

Test #	Summary		Results	
	CPU Cores	Alg. / Curve	Op/S	CPU%
1	1	ECDH P256	2,718	1 core x 100% busy
2	2	ECDH P256	5,332	2 cores x 100% busy
3	4	ECDH P256	10,647	4 cores x 100% busy
4	8	ECDH P256	21,111	8 cores x 100% busy
5	1	ECDH P384	1,236	1 core x 100% busy
6	2	ECDH P384	2,479	2 cores x 100% busy
7	4	ECDH P384	4,949	4 cores x 100% busy
8	8	ECDH P384	9,838	8 cores x 100% busy

Test #	Summary		Results		
	CPU Cores	Alg. / Curve	Op/S		CPU%
			Sign	Verify	
9	1	ECDSA P256	8,304	2,104	1 core x 100% busy
10	2	ECDSA P256	16,627	4,293	2 cores x 100% busy
11	4	ECDSA P256	33,196	8,678	4 cores x 100% busy
12	8	ECDSA P256	66,175	17,279	8 cores x 100% busy
13	1	ECDSA P384	4,391	1,005	1 core x 100% busy
14	2	ECDSA P384	8,741	2,013	2 cores x 100% busy
15	4	ECDSA P384	17,522	4,029	4 cores x 100% busy
16	8	ECDSA P384	35,102	8,139	8 cores x 100% busy

Tests Results

Accelerated with QuickAssist Technology (QAT) Using Intel® 8955 on Silicom PE3iSCO3

Test #	*Summary (Alg. / Curve)*	*Results*	
		Op/S	*CPU%*
17	ECDH P256	54,810	1 core x 5% busy
18	ECDH P384	30,250	1 core x 4% busy

Test #	**Summary (Alg. / Curve)**	**Results**		
		Op/S		CPU%
		Sign	Verify	
19	ECDSA P256	40,005	17,302	1 core x 5% busy
20	ECDSA P384	30,825	9,906	1 core x 5% busy

CONCLUSIONS

ECDH – Intel® 8955 on both curves under test (P256 and P384), surpasses 8 CPU cores (as well as 10 CPU cores) performance (see Figure 1). As a result, a complete CPU socket is "returned" to the system, for general purpose processing, while Intel® 8955 upholds all crypto work.

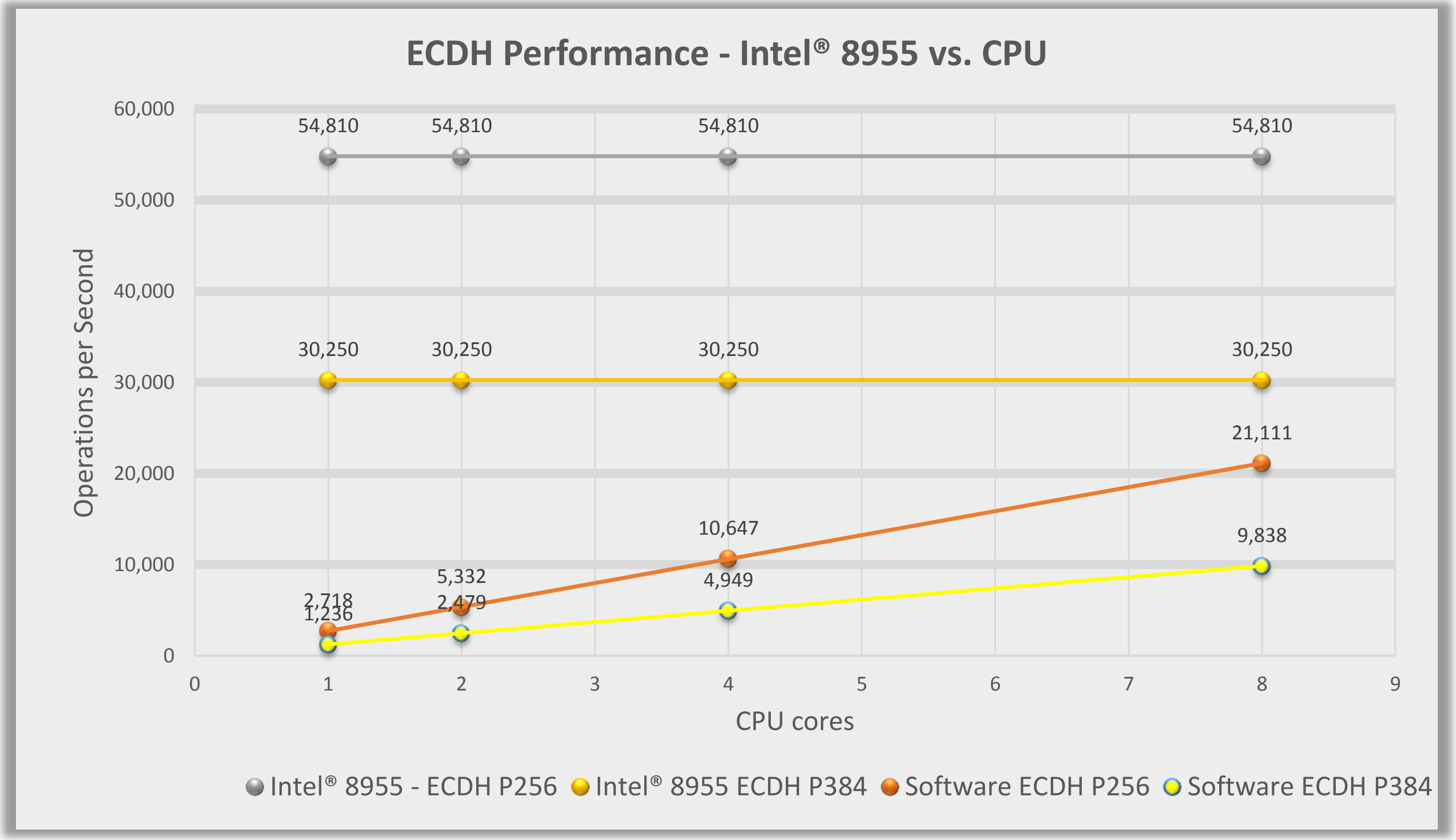

Figure 1 - ECDH Performance

ECDSA – Similarly, with digital signing, Intel® 8955 enables CPU cycles savings, while performing the crypto work of 4, 5, and 8 CPU cores (see Figure 2 and Figure 3). These cores that needed to spend 100% of their cycles on crypto work, are freed almost in full for general processing.

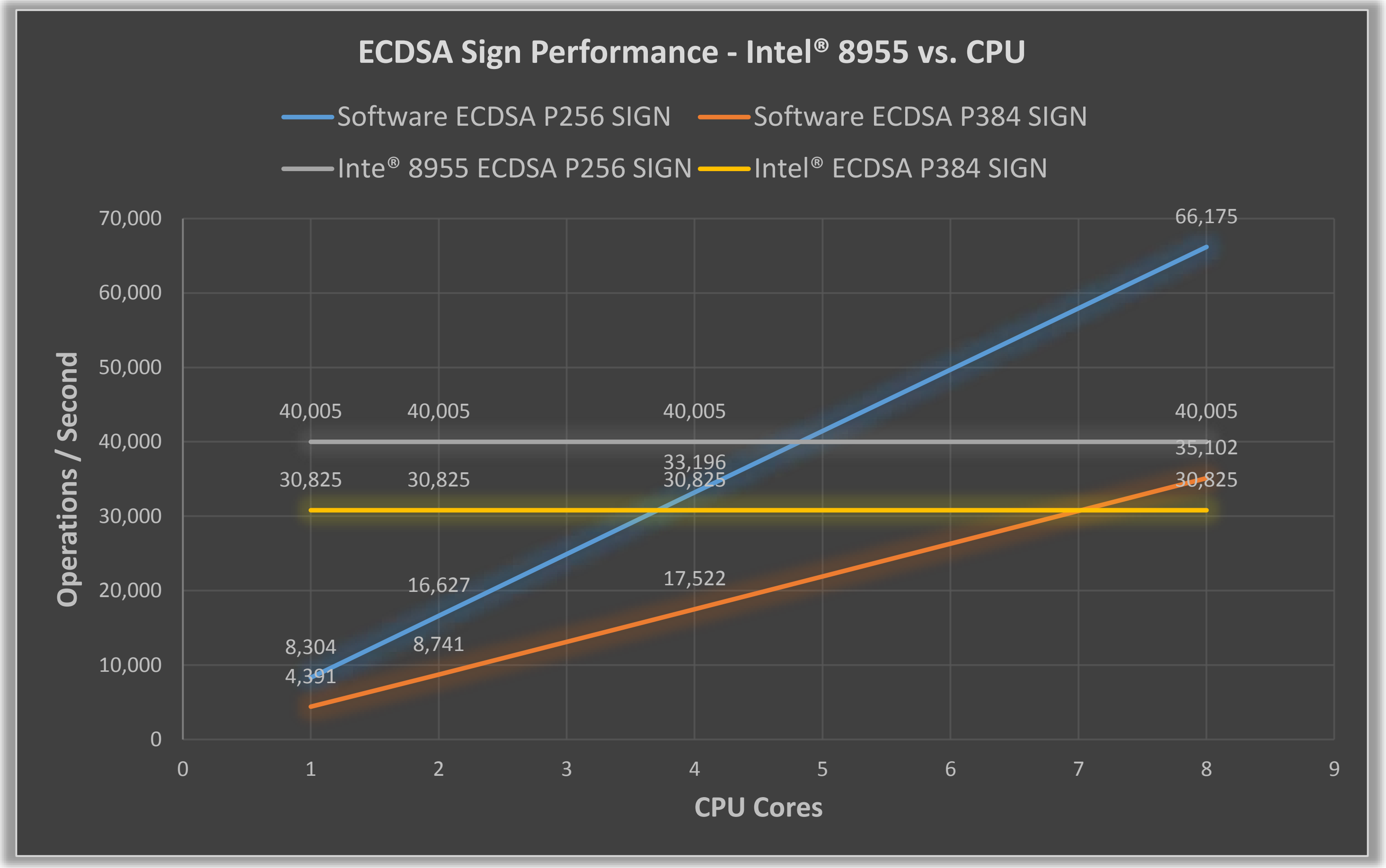

Figure 2- ECDSA Sign Performance

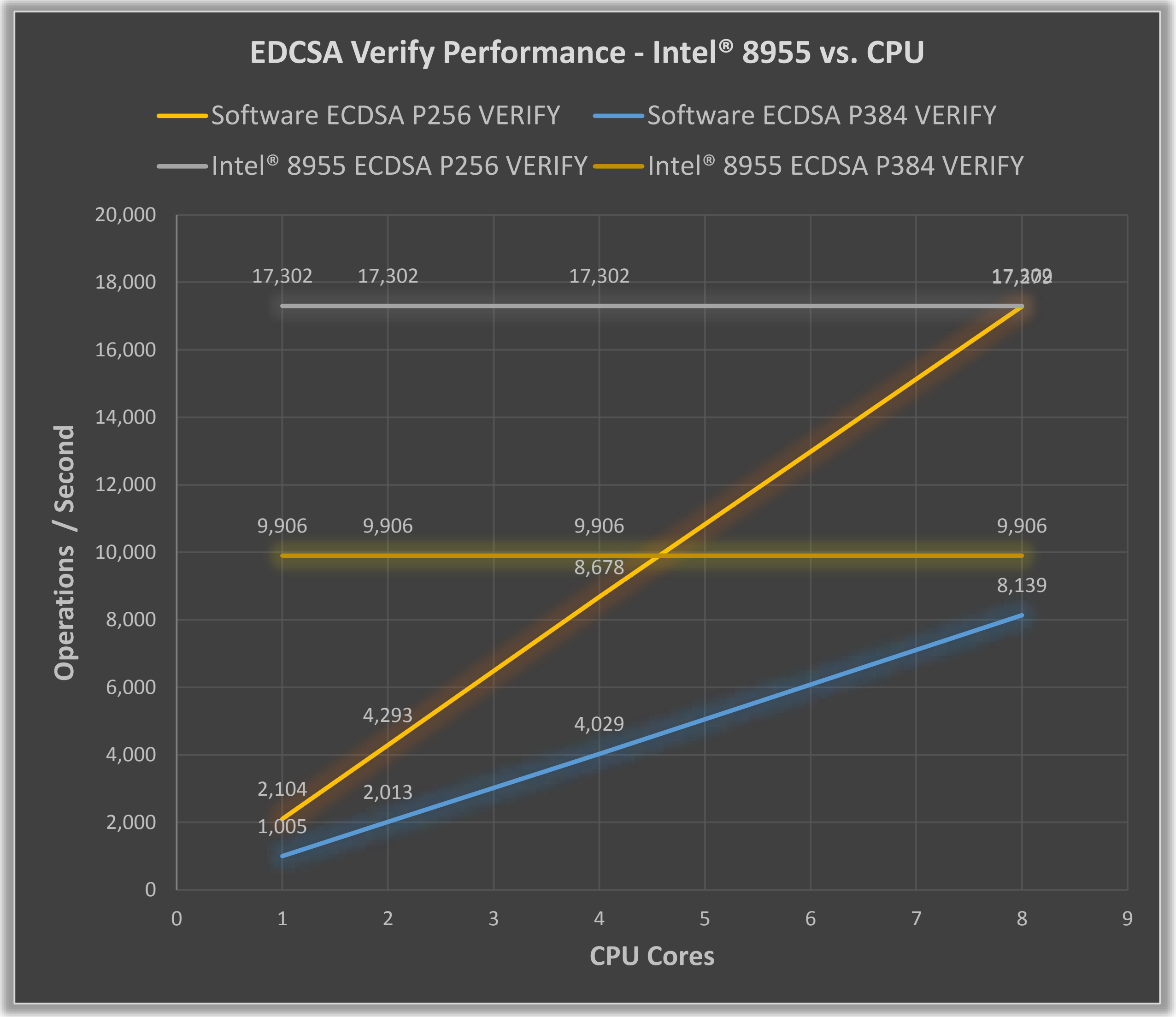

Figure ECDSA Verify Performance

Silicom ltd., 14 Atir Yeda St., Kefar Sava 4464323, ISRAEL

sales@silicom.co.il www.silicom-usa.com