Backup

J7 Crypto HWA Performance

Crypto HWA Performance

- The table shows the performance of each crypto core in the running at 250 MHz
- Some devices may support higher speeds
- ‘Adjusted Throughput’ column includes 25% de-rating for software overhead impact on the theoretical numbers.

Module Name	Block size (Bits)	Cycles per Block	Modes overhead	Freq (MHz)	Theoretical Throughput (Mbits/sec)	Adjusted Throughput (Mbits/sec))	Remark
AES core	128	15	1	250	2,000	1,500	AES 256-bit key numbers, worst case
3DES core	64	14	1	250	1,067	800	3DES 3 key numbers, worst case
Galois Multiplier	128	8	1	250	3,556	2,667	Galois multiplier core used for GCM mode
AES -CCM - 128/192 bits AES Key	128	13	1	250	1,143	857	In CCM mode, AES is run twice for same block.
AES -CCM - 256 bits AES Key	128	15	1	250	1,000	750	In CCM mode, AES is run twice for same block.
SHA1 core	512	84	1	250	1,506	1,129	Same numbers with keyed hash (HMAC)
MD5 core	512	68	1	250	1,855	1,391	Same numbers with keyed hash (HMAC)
SHA2-256 core	512	68	1	250	1,855	1,391	Same numbers with keyed hash (HMAC)
SHA2-512 core	1024	84	1	250	3,012	2,259	Same numbers with keyed hash (HMAC)

Table 22: Encryption and Authentication Core Performance Data

Encryption & Hashing Performance (2 of 2)

- Measured performance in system with packet DMA
- Performance increases with packet sizes (lower overhead per packet)

						A72 - Src, Dest & Context in DDR				MCU R5 - Src, Dest & Context in DDR			
						Throughput (Mbps*)				Throughput (Mbps*)			
		Cipher Mode	Auth Mode	KeySize (bits)	AuthKeySize (bits)	PKTSIZE = 64	PKTSIZE = 512	PKTSIZE = 1024	PKTSIZE = 2048	PKTSIZE = 64	PKTSIZE = 512	PKTSIZE = 1024	PKTSIZE = 2048
1	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_NULL	128	0	1024	2730	3360	3692	356	1771	2114	2184
2	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_NULL	128	0	910	2520	3048	3542	409	1820	2148	2319
3	Tx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_NULL	128	0	1024	1524	1820	2048	409	1424	1659	2032
4	Rx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_NULL	128	0	819	1489	1724	1985	431	1456	1680	2048
5	Tx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_NULL	256	0	910	1285	1579	1736	409	1365	1560	1846
6	Rx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_NULL	256	0	819	1260	1506	1702	431	1337	1579	1899
7	Tx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_HMAC_SHA1	128	160	409	862	1008	1096	372	963	1110	1317
8	Rx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_HMAC_SHA1	128	160	409	897	1040	1129	372	992	1120	1297
9	Tx Channel	sa_CipherMode_GCM	sa_AuthMode_NULL	128	0	630	978	1129	1213	409	1040	1260	1440
10	Rx Channel	sa_CipherMode_GCM	sa_AuthMode_NULL	128	0	630	992	1139	1254	431	1057	1285	1489
11	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_GMAC	0	192	682	1524	1795	2080	431	1310	1542	2016
12	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_GMAC	0	192	682	1456	1747	2048	409	1310	1598	2001
13	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_GMAC_AH	0	128	682	1524	1820	2064	409	1365	1618	1899
14	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_GMAC_AH	0	128	682	1489	1747	2048	455	1365	1618	2016
15	Tx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	128	0	630	910	1040	1129	409	978	1202	1372
16	Rx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	128	0	585	873	985	1052	431	978	1149	1291
17	Tx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	192	0	585	840	936	989	431	923	1101	1219
18	Rx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	192	0	585	789	885	932	431	897	1057	1170
19	Tx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	256	0	546	762	840	879	409	862	992	1120
20	Rx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	256	0	546	728	799	832	431	829	978	1057
21	Tx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	256	0	546	753	840	876	431	862	992	1110
22	Rx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	256	0	512	712	804	832	455	829	970	1065
23	Tx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	256	0	546	780	851	879	390	885	992	1120
24	Rx Channel	sa_CipherMode_CCM	sa_AuthMode_NULL	256	0	546	736	804	834	431	840	978	1074
25	Tx Channel	sa_CipherMode_AES_CBC	sa_AuthMode_HMAC_MD5	256	160	273	590	720	796	303	744	856	981
26	Rx Channel	sa_CipherMode_AES_CBC	sa_AuthMode_HMAC_MD5	256	160	273	648	757	811	315	753	862	1000
27	Tx Channel	sa_CipherMode_DES_CBC	sa_AuthMode_HMAC_SHA2_224	64	256	431	851	1000	1074	372	963	1129	1260
28	Rx Channel	sa_CipherMode_DES_CBC	sa_AuthMode_HMAC_SHA2_224	64	256	431	873	970	1040	390	936	1101	1213
29	Tx Channel	sa_CipherMode_3DES_CBC	sa_AuthMode_HMAC_SHA2_256	192	256	390	618	740	809	356	736	868	978
30	Rx Channel	sa_CipherMode_3DES_CBC	sa_AuthMode_HMAC_SHA2_256	192	256	390	630	724	780	390	744	840	953

Encryption & Hashing Performance (2 of 2)

- Measured performance in system with packet DMA
- Performance increases with packet sizes (lower overhead per packet)

						A72 - Src, Dest & Context in DDR				MCU R5 - Src, Dest & Context in DDR			
						Throughput (Mbps*)				Throughput (Mbps*)			
		Cipher Mode	Auth Mode	KeySize (bits)	AuthKeySize (bits)	PKTSIZE = 64	PKTSIZE = 512	PKTSIZE = 1024	PKTSIZE = 2048	PKTSIZE = 64	PKTSIZE = 512	PKTSIZE = 1024	PKTSIZE = 2048
31	Tx Channel	sa_CipherMode_3DES_CBC	sa_AuthMode_NULL	192	0	682	799	851	868	409	949	1057	1134
32	Rx Channel	sa_CipherMode_3DES_CBC	sa_AuthMode_NULL	192	0	682	753	804	821	455	897	1008	1074
33	Tx Channel	sa_CipherMode_DES_CBC	sa_AuthMode_HMAC_SHA2_384	64	256	455	897	1101	1208	372	1040	1236	1387
34	Rx Channel	sa_CipherMode_DES_CBC	sa_AuthMode_HMAC_SHA2_384	64	256	455	949	1074	1165	390	1024	1180	1351
35	Tx Channel	sa_CipherMode_3DES_CBC	sa_AuthMode_HMAC_SHA2_512	192	256	409	642	753	811	356	799	929	1048
36	Rx Channel	sa_CipherMode_3DES_CBC	sa_AuthMode_HMAC_SHA2_512	192	256	409	682	762	799	390	809	916	1020
37	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_CMAC	0	128	682	1260	1542	1724	431	1310	1472	1783
38	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_CMAC	0	128	682	1260	1506	1702	431	1310	1489	1859
39	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_MD5	0	128	409	771	845	897	390	949	1083	1170
40	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_MD5	0	128	409	771	851	897	409	963	1092	1165
41	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_NULL	0	0	910	2730	3360	3692	431	1638	2016	2114
42	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_NULL	0	0	1024	2520	3048	3495	431	1724	1985	2240
43	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_CMAC	0	192	630	1213	1409	1542	409	1260	1456	1759
44	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_CMAC	0	192	630	1170	1379	1542	409	1260	1472	1747
45	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_MD5	0	0	292	704	804	870	315	862	1048	1134
46	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_MD5	0	0	292	704	804	873	315	897	1048	1139
47	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_SHA1	0	0	431	1057	1224	1337	409	1236	1394	1659
48	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_SHA1	0	0	431	1040	1213	1337	409	1285	1424	1648
49	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_SHA2_256	0	0	512	1236	1456	1618	390	1337	1598	1795
50	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_SHA2_256	0	0	512	1260	1472	1618	431	1365	1579	1872
51	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_HMAC_MD5	0	160	221	642	766	845	256	819	992	1110
52	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_HMAC_MD5	0	160	221	636	766	845	256	829	985	1110
53	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_HMAC_SHA2_256	0	256	390	1149	1394	1569	409	1260	1506	1771
54	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_HMAC_SHA2_256	0	256	390	1149	1379	1569	431	1260	1542	1820
55	Tx Channel	sa_CipherMode_NULL	sa_AuthMode_HMAC_SHA2_512	0	512	409	1456	1846	2064	390	1365	1702	2097
56	Rx Channel	sa_CipherMode_NULL	sa_AuthMode_HMAC_SHA2_512	0	512	409	1489	1771	2048	390	1365	1771	2080
57	Tx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_HMAC_SHA1	128	160	315	819	978	1069	327	936	1120	1266
58	Rx Channel	sa_CipherMode_AES_CTR	sa_AuthMode_HMAC_SHA1	128	160	315	851	1008	1083	341	963	1129	1310

Crypto HWA Performance – PKA-ECDSA

- The table below shows the performance of the PKA module (EIP29t2) when running ECDSA sign and verify operation using multiple instructions that consist of multiply, scale, modinv, add instruction.
- The sign numbers have been adjusted for 30% software delay, and the verify numbers have been adjusted for 20% software delay.
- An updated firmware that includes single-step sign and verify instruction is now available which produces higher ECDSA performance with reduced CPU overhead.
  - P-256 curve: ~550 verifies/sec (@ 300 MHz)

Algorithm	Curve	Sign (ops/sec)	Verify (ops/sec)
ECDSA	P-192	1116	638
ECDSA	P-224	879	502
ECDSA	P-256	706	404
ECDSA	P-384	337	193
ECDSA	P-521	157	90
ECDSA	K-163	1885	1077
ECDSA	K-233	984	562
ECDSA	K-283	690	394
ECDSA	K-409	342	195
ECDSA	K-571	181	104
ECDSA	B-163	1880	1074
ECDSA	B-233	979	559
ECDSA	B-283	687	392
ECDSA	B-409	344	196
ECDSA	B-571	180	103

Table 23: PKA ECDSA Performance

Crypto HWA Performance – PKA-RSA

- The table contains information on the number of clocks needed to perform various modular exponentiation (ModExp & ModExp-CRT) operations.
- The ModExp operation uses the PKCP and LNME engines for its calculations.
- The raw performance values do not include the time needed to write the input vectors into or read output vector from PKA RAM.
- The adjusted values include a 25% overhead.
- Software overhead on the Host is not included.

Operation	SW overhead	HW ops	Exp (bits)	Mod (bits)	#Odd powers	#clocks	Ops/sec @ 300 MHz (raw)	Ops/sec @ 300 MHz (w/25% ovhd)
DSA2 sign 160	host + seq.	ExpMod	160	512	1	21,652	13,855	10,391
DSA(2) sign 160	host + seq.	ExpMod	160	512	4	19,885	10,309	7,732
DSA(2) verify 160	host + seq.	2x ExpMod	160	512	1	43,304	6,927	5,195
DSA(2) verify 160	host + seq.	2x ExpMod	160	512	4	39,770	7,543	5,657
DH(1) key neg 180	host + seq.	ExpMod	180	1024	1	62,019	4,837	3,628
DH(1) key neg 180	host + seq.	ExpMod	180	1024	4	55,565	5,399	4,049
RSA sign/encr/decr 512	sequencer	ExpMod	512	512	1	67,530	4,441	3,331
RSA sign/encr/decr 512	sequencer	ExpMod	512	512	4	57,559	4,876	3,657
RSA sign/encr/decr 1024	sequencer	ExpMod	1024	1024	1	344,530	871	653
RSA sign/encr/decr 1024	sequencer	ExpMod	1024	1024	4	291,328	1,030	772
RSA sign/encr/decr 2048	sequencer	ExpMod	2048	2048	1	2,354,023	126	95
RSA sign/encr/decr 2048	sequencer	ExpMod	2048	2048	4	1,965,693	152	114
RSA sign/encr/decr 3072	sequencer	ExpMod	3072	3072	1	8,015,735	37	28
RSA sign/encr/decr 3072	sequencer	ExpMod	3072	3072	4	6,685,589	44	33
RSA sign/encr/decr 4096	sequencer	ExpMod	4096	4096	1	17,915,156	16	12
RSA sign/encr/decr 4096	sequencer	ExpMod	4096	4096	4	15,043,318	19	14
RSA sign/decr CRT(1,3) 512	sequencer	2x ExpMod	256	256	1	41,671	7,199	5,399
RSA sign/decr CRT(1,3) 512	sequencer	2x ExpMod	256	256	4	36,686	8,177	6,133
RSA sign/decr CRT(1,3) 1024	sequencer	2x ExpMod	512	512	1	144,721	2,073	1,555
RSA sign/decr CRT(1,3) 1024	sequencer	2x ExpMod	512	512	4	122,950	2,451	1,838
RSA sign/decr CRT(1,3) 2048	sequencer	2x ExpMod	1024	1024	1	722,171	415	311
RSA sign/decr CRT(1,3) 2048	sequencer	2x ExpMod	1024	1024	4	603,916	496	372
RSA sign/decr CRT(1,3) 4096	sequencer	2x ExpMod	2048	2048	1	4,824,315	62	47
RSA sign/decr CRT(1,3) 4096	sequencer	2x ExpMod	2048	2048	4	4,010,816	74	56
RSA verify 512	sequencer	ExpMod	17	512	1	3,286	91,296	68,472
RSA verify 1024	sequencer	ExpMod	17	1024	1	8,011	37,448	28,086
RSA verify 2048	sequencer	ExpMod	17	2048	1	27,144	11,052	8,289
RSA verify 3072	sequencer	ExpMod	17	3072	1	59,719	5,023	3,767
RSA verify 4096	sequencer	ExpMod	17	4096	1	107,290	2,796	2,097
RSA verify 512	sequencer	ExpMod	3	512	1	2,107	142,382	106,786
RSA verify 1024	sequencer	ExpMod	3	1024	1	4,901	61,211	45,908
RSA verify 2048	sequencer	ExpMod	3	2048	1	16,474	18,210	13,657
RSA verify 4096	sequencer	ExpMod	3	4096	1	66,200	4,532	3,399

1) For DH & CRT, the Sequencer performs all SW operations inside the PKA engine.

2) For DSA, the Sequencer does not perform all operations inside the PKA engine, for example random number generation has to be done via the Host processor and a TRNG.

3) For CRT, two exponentiations are done sequentially, the cycle count mentioned is the total of the cycles needed for these two operations and includes pre/post-processing.