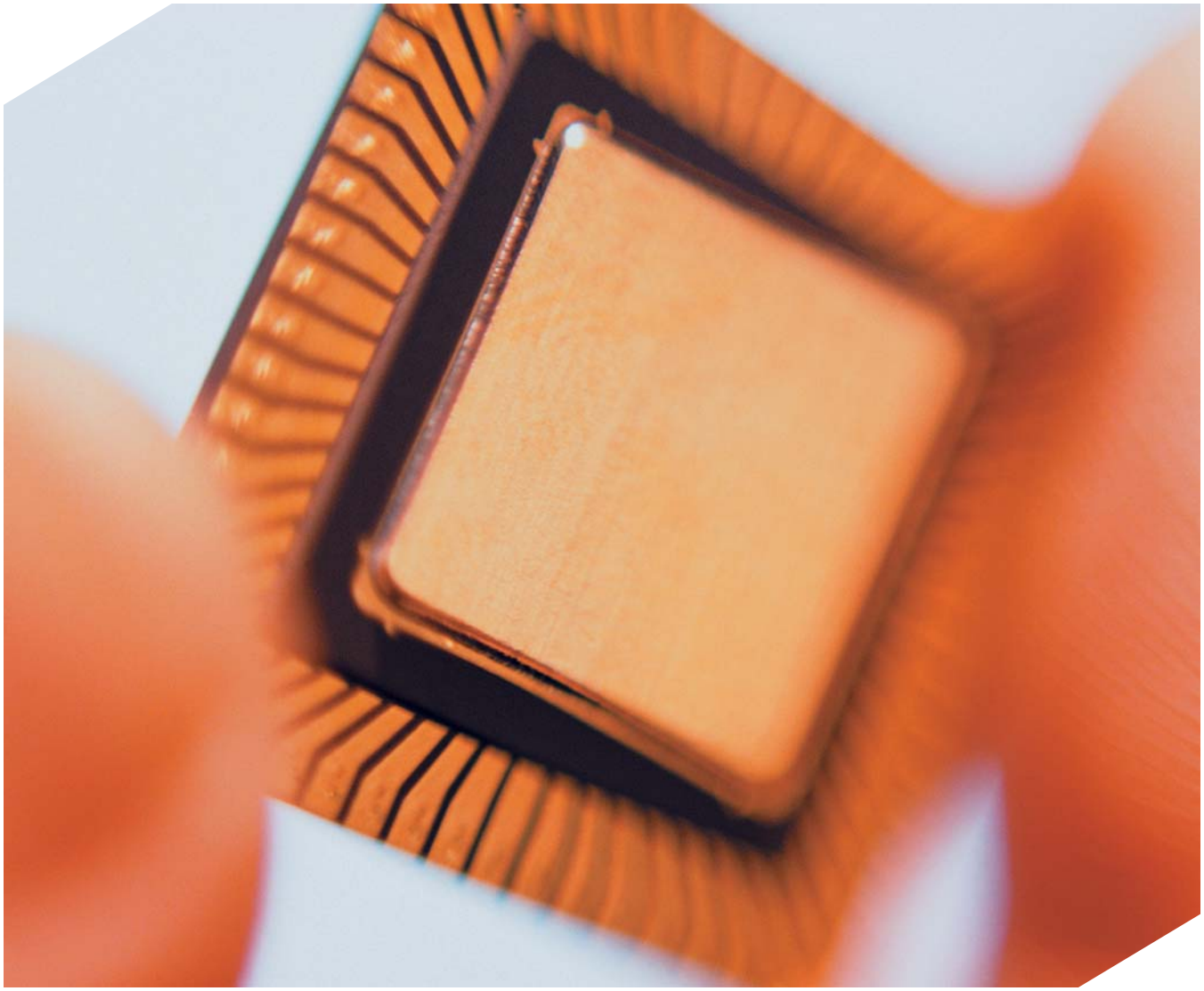
Understanding Cryptographic Performance.



Freescale Semiconductor
White Paper

Matthew Short: 512.996.5814
Geoffrey Waters: 512.996.5815
February 25, 2005

Launched by Motorola
freescale™
semiconductor

Performance Methodology

RAW PERFORMANCE

Freescale Semiconductor defines cryptographic raw performance as the bandwidth of a cryptographic execution unit as measured from the unit's input FIFO, through the algorithm accelerator, and into the unit's output FIFO. This number assumes that the execution unit has been set up prior to measurement and varies only as a function of operating frequency and the execution unit selected. When multiple operations are performed on the same data (encryption and authentication), the measurement is made from the input FIFO of the first execution unit to the output FIFO of the second.

BUS LIMITED PERFORMANCE

Bus limited performance is cryptographic throughput as measured from the time a cryptographic hardware unit's DMA begins reading external memory until the DMA has placed final data and context in external memory. The latency of each bus transaction is assumed to be relatively worst case for every transaction and does not necessarily take into account the pipelined nature of the bus architecture. For Freescale Semiconductor's security architecture, this performance benchmark includes the fetch of descriptors, encryption keys, IVs, HMAC keys, plain text, the write back of cipher text, the HMAC, any preserved context and a DONE write back. The measurement varies as a function of bus frequency and packet size but is not a function of the execution unit selected. It should also encompass DRAM latency, memory controller characteristics and bus arbitration mechanism. The performance should then be scaled by the percentage of the bus that can be allocated to cryptographic processing, usually between 10% and 33%.

CPU LIMITED PERFORMANCE

CPU limited performance takes into consideration the instructions per packet needed for protocol and driver processing. CPU bandwidth limitations are estimated by multiplying CPU frequency by the CPU's instructions per clock and then dividing by the estimated instructions per packet. The instructions per packet for IPsec processing, including driver overhead, is highly implementation-dependent, but, for the purpose of this analysis, is estimated to vary between 6000 and 20000 IPP. The CPU limit should then be scaled by the percentage of the CPU that can be dedicated to protocol processing, typically 40% and 75%. The packets per second estimate is then multiplied by packet size to determine throughput in Mbps.

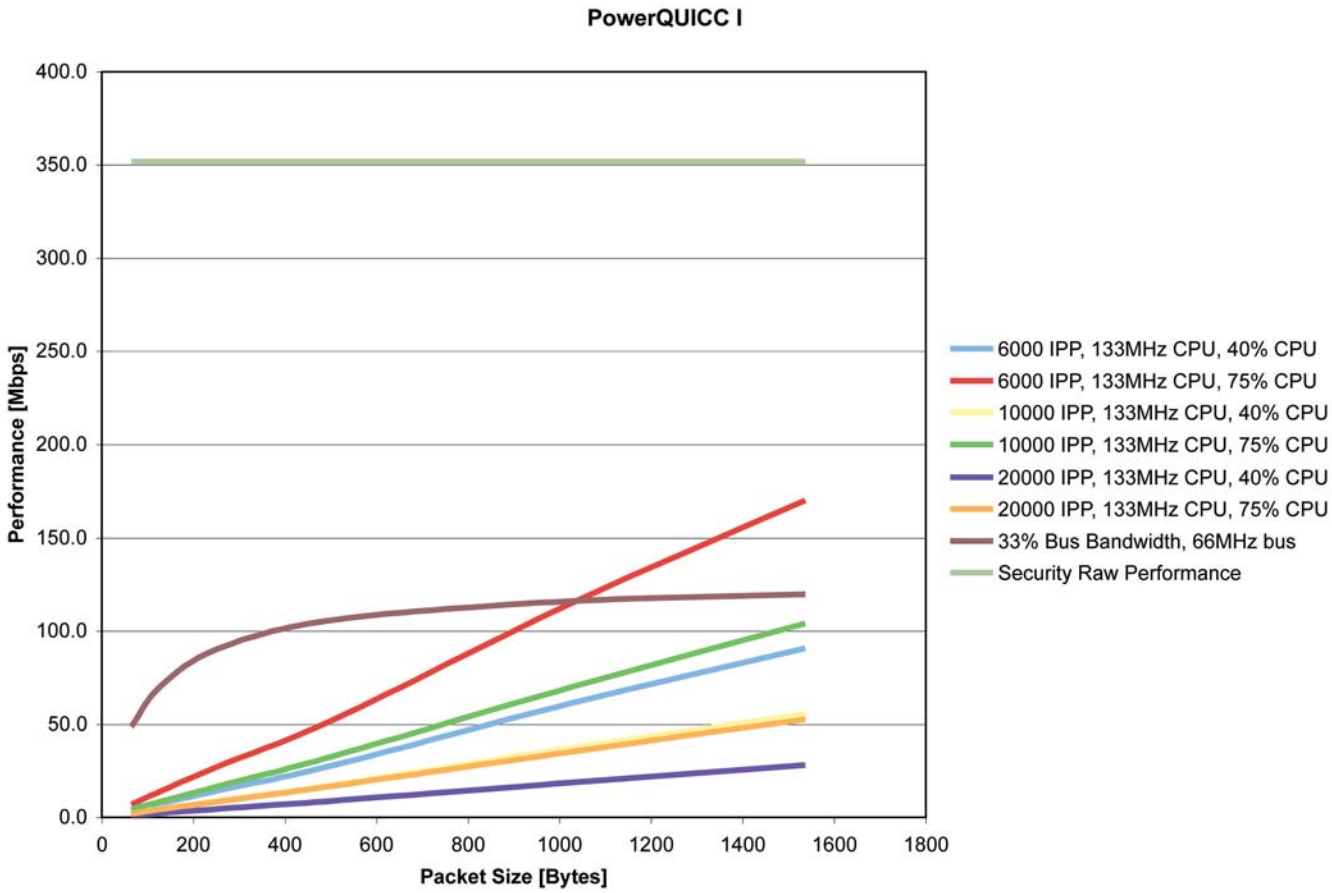
OVERALL SYSTEM PERFORMANCE

The overall system performance will therefore be the smaller of the three numbers for any given packet size. Performance tends to be core limited at small packet sizes, bus limited at large packet sizes and potentially limited by the cryptographic core in some high-performance systems. Freescale Semiconductor strives to not only provide the highest credibility performance number, but also to demonstrate a methodology that customers can apply to their specific systems.

PowerQUICC™ I Integrated Communications Processors

Table 2 shows the security performance for PowerQUICC™ I integrated communications processors, which contain a PowerPC™ core.

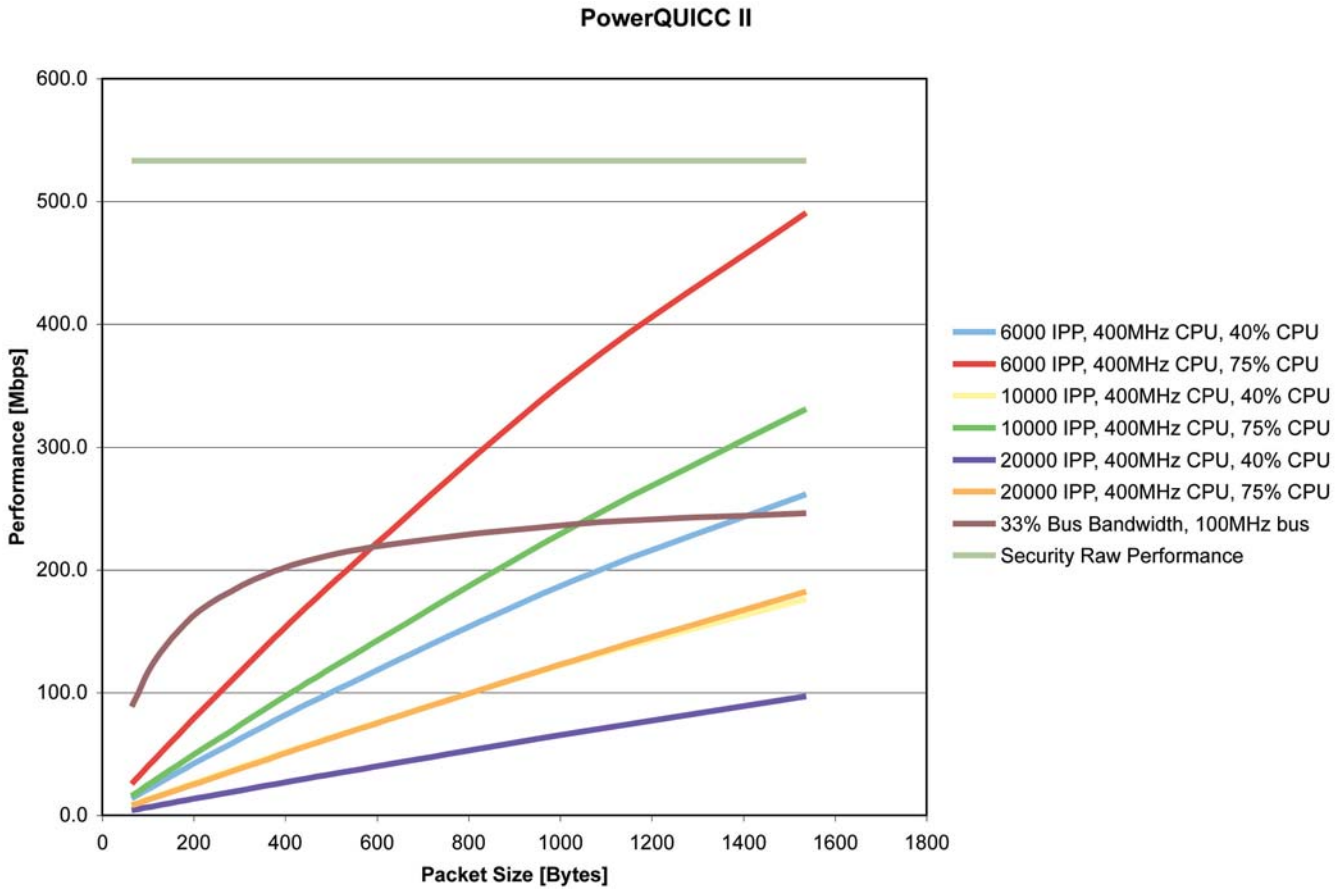
Measurement Point	64B [Mb/s]	128B [Mb/s]	256B [Mb/s]	512B [Mb/s]	1024B [Mb/s]	1536B [Mb/s]
6000 IPP, 133MHz CPU, 40% CPU	3.8	7.5	14.7	28.5	61.3	90.8
6000 IPP, 133MHz CPU, 75% CPU	7.1	14.0	27.6	53.4	115.0	170.3
10000 IPP, 133MHz CPU, 40% CPU	2.3	4.6	9.1	17.8	37.3	55.6
10000 IPP, 133MHz CPU, 75% CPU	4.4	8.6	17.1	33.5	70.0	104.2
20000 IPP, 133MHz CPU, 40% CPU	1.2	2.4	4.6	9.2	18.9	28.2
20000 IPP, 133MHz CPU, 75% CPU	2.2	4.4	8.7	17.3	35.4	52.9
33% Bus Bandwidth, 66MHz bus	48.8	70.6	91.0	106.4	116.2	119.9
Security Raw Performance	352.0	352.0	352.0	352.0	352.0	352.0



PowerQUICC II™ Integrated Communications Processors

Table 3 shows the security performance for PowerQUICC II™ integrated communications processors, which contain a PowerPC core.

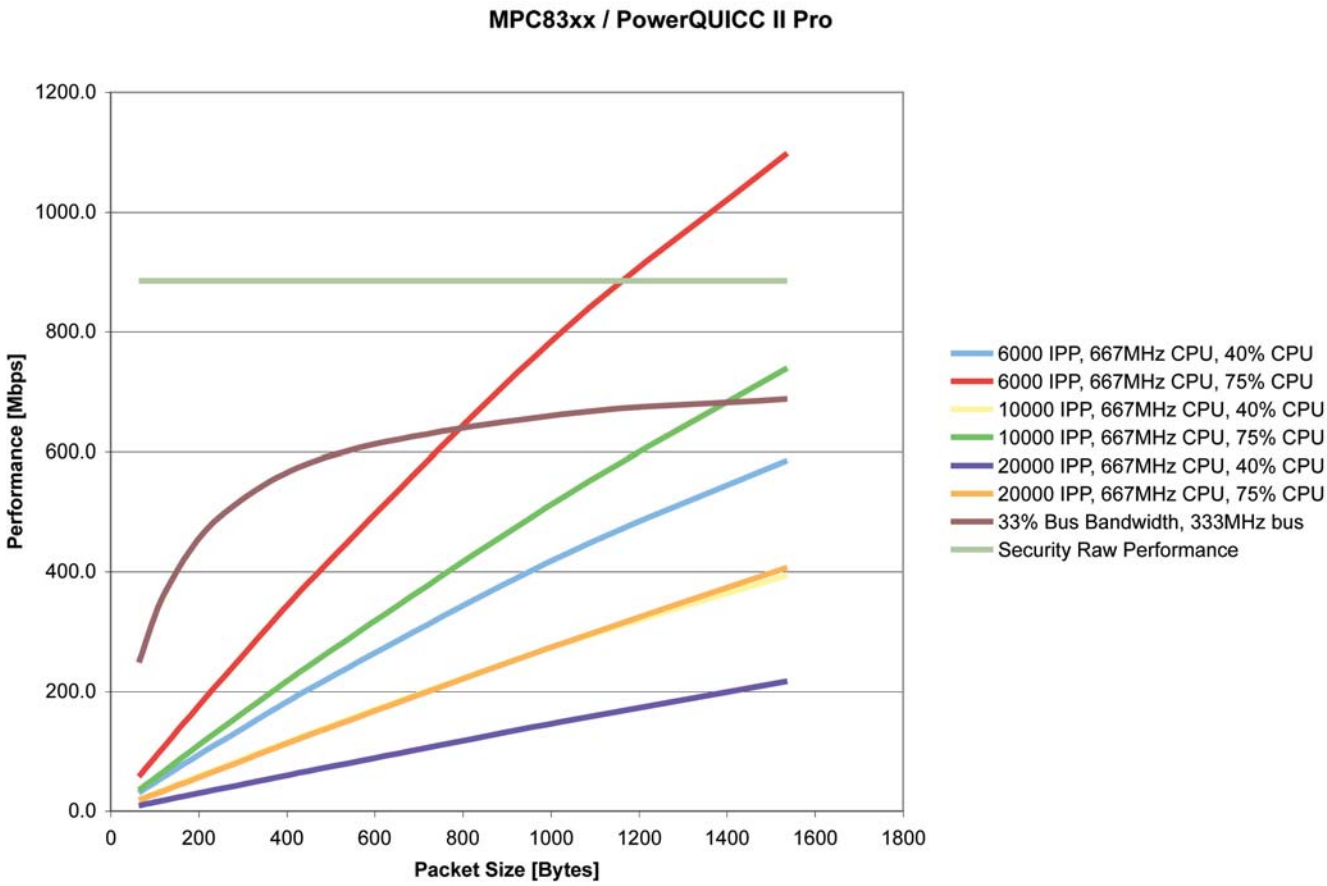
Measurement Point	64B [Mb/s]	128B [Mb/s]	256B [Mb/s]	512B [Mb/s]	1024B [Mb/s]	1536B [Mb/s]
6000 IPP, 400MHz CPU, 40% CPU	13.8	27.3	53.5	102.9	190.9	261.8
6000 IPP, 400MHz CPU, 75% CPU	25.9	51.2	100.4	102.9	358.0	490.8
10000 IPP, 400MHz CPU, 40% CPU	8.6	17.0	33.6	65.6	125.0	176.5
10000 IPP, 400MHz CPU, 75% CPU	16.1	32.0	63.0	122.9	234.3	331.0
20000 IPP, 400MHz CPU, 40% CPU	4.4	8.8	14.4	34.4	67.0	97.3
20000 IPP, 400MHz CPU, 75% CPU	8.3	16.4	32.6	64.5	125.7	182.5
33% Bus Bandwidth, 100MHz bus	88.9	133.3	177.8	213.3	237.0	246.2
Security Raw Performance	533.3	533.3	533.3	533.3	533.3	533.3



MPC83xx PowerQUICC II™ Pro Integrated Communications Processors

Table 4 shows the security performance for MPC83xx PowerQUICC II™ Pro integrated communications processors, which contain a PowerPC core.

Measurement Point	64B [Mb/s]	128B [Mb/s]	256B [Mb/s]	512B [Mb/s]	1024B [Mb/s]	1536B [Mb/s]
6000 IPP, 667MHz CPU, 40% CPU	30.8	60.9	119.4	229.6	426.8	586.1
6000 IPP, 667MHz CPU, 75% CPU	57.7	114.2	223.8	430.6	800.3	1098.9
10000 IPP, 667MHz CPU, 40% CPU	19.1	37.9	74.9	146.2	278.9	394.6
10000 IPP, 667MHz CPU, 75% CPU	35.8	71.1	140.5	274.2	523.0	739.8
20000 IPP, 667MHz CPU, 40% CPU	9.8	19.5	38.8	76.6	149.4	217.2
20000 IPP, 667MHz CPU, 75% CPU	18.4	36.6	72.8	143.7	280.2	407.2
33% Bus Bandwidth, 333MHz bus	248.5	372.8	497.0	596.4	662.7	688.2
Security Raw Performance	885.3	885.3	885.3	885.3	885.3	885.3



PowerQUICC III Integrated Communications Processors

Table 5 shows the security performance for PowerQUICC III integrated communications processors, which contain a PowerPC core.

Measurement Point	64B [Mb/s]	128B [Mb/s]	256B [Mb/s]	512B [Mb/s]	1024B [Mb/s]	1536B [Mb/s]
6000 IPP, 833MHz CPU, 40% CPU	70.4	140.8	282.0	526.8	897.2	1126.8
6000 IPP, 833MHz CPU, 75% CPU	132.0	264.0	528.8	987.8	1682.3	2112.8
10000 IPP, 833MHz CPU, 40% CPU	43.2	86.4	172.8	345.6	650.0	854.8
10000 IPP, 833MHz CPU, 75% CPU	81.0	162.0	324.0	648.0	1218.8	1602.8
20000 IPP, 833MHz CPU, 40% CPU	20.7	41.4	82.7	163.8	306.7	424.6
20000 IPP, 833MHz CPU, 75% CPU	38.8	77.6	155.1	307.1	575.0	796.1
33% Bus Bandwidth, 333MHz bus	248.5	372.8	497.0	596.4	662.7	688.2
Security Raw Performance	885.3	885.3	885.3	885.3	885.3	885.3