

Understanding Cryptographic Performance

by: Matthew Short and Geoffrey Waters
NCSG

1 Performance Methodology

1.1 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.

1.2 Bus Limited Performance

Bus limited performance is cryptographic throughput as measured from the time a cryptographic hardware unit's DMA begins reading external memory, to the time the DMA has placed final data and context in external memory. The latency of each bus transaction is assumed to be the 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, and plaintext, and the write back of ciphertext, 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

This document contains information on a new product. Specifications and information herein are subject to change without notice.

© Freescale Semiconductor, Inc., 2004. All rights reserved.

**For More Information On This Product,
Go to: www.freescale.com**

Coldfire Security Performance

be scaled by the percentage of the bus that can be allocated to cryptographic processing, usually between 10% to 33%.

1.3 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 6000-10000 IPP. The CPU limit should then be scaled by the percentage of the CPU that can be dedicated to protocol processing, typically 40% to 75%. The packets per second estimate is then multiplied by packet size to determine throughput in Mbps.

1.4 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 to demonstrate a methodology that any customer can apply to their specific system.

2 Coldfire Security Performance

Table 1 shows the security performance for Coldfire.

Table 1. 266 MHz CPU, 266MHz Bus

Measurement Point	64B [Mbps]	128B [Mbps]	256B [Mbps]	512B [Mbps]	1024B [Mbps]	1536B [Mbps]
6000 IPP, 40%CPU	13.6	27.2	54.5	109.0	217.9	326.9
6000 IPP, 75% CPU	25.5	51.1	102.1	204.3	408.6	612.9
7500 IPP, 40%CPU	10.9	21.8	43.6	87.2	174.3	261.5
7500 IPP, 75% CPU	20.4	40.9	81.7	163.4	326.9	490.3
10000 IPP, 40%CPU	8.2	16.3	32.7	65.4	130.7	196.1
10000 IPP, 75% CPU	15.3	30.6	61.3	122.6	245.1	367.7
33% BUS Bandwidth	166.3	240.8	310.4	362.8	396.3	408.8
Security Raw Performance	352.0	352.0	352.0	352.0	352.0	352.0



THIS PAGE INTENTIONALLY LEFT BLANK

Freescale Semiconductor, Inc.

HOW TO REACH US:**USA/Europe/Locations not listed:**

Freescale Semiconductor Literature Distribution
P.O. Box 5405, Denver, Colorado 80217
1-800-521-6274 or 480-768-2130

Japan:

Freescale Semiconductor Japan Ltd.
Technical Information Center
3-20-1, Minami-Azabu, Minato-ku
Tokyo 106-8573, Japan
81-3-3440-3569

Asia/Pacific:

Freescale Semiconductor H.K. Ltd.
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T. Hong Kong
852-26668334

Learn More:

For more information about Freescale Semiconductor products, please visit <http://freescale.com>

Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductor products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Freescale Semiconductor reserves the right to make changes without further notice to any products herein. Freescale Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters which may be provided in Freescale Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals" must be validated for each customer application by customer's technical experts. Freescale Semiconductor does not convey any license under its patent rights nor the rights of others. Freescale Semiconductor products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Freescale Semiconductor product could create a situation where personal injury or death may occur. Should Buyer purchase or use Freescale Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold Freescale Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Freescale Semiconductor was negligent regarding the design or manufacture of the part.

Freescale™ and the Freescale logo are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners.
© Freescale Semiconductor, Inc. 2004.