Intel® Itanium™ Processor

High Performance On Security Algorithms (RSA Decryption Kernel)

White Paper

Executive Summary

The tremendous growth of the Internet has resulted in an explosion of e-Commerce Web sites. As e-Commerce continues to grow exponentially, security becomes a major issue on the minds of IT managers everywhere.

To secure the e-Commerce environment, companies must deploy solutions at various levels within their computing environment and integrate them into their applications. Web sites use software that relies on security algorithms and protocols to authenticate identities, protect data and monitor transactions. One type of security algorithm is public-key cryptography, which is used widely in Internet-based security technologies. Common protocols such as Secure Sockets Layer (SSL), Public Key Infrastructures (PKI) and Virtual Private Networks (VPN) are examples of security technologies that rely on algorithms based on public-key cryptography. Despite the widespread reliance on these algorithms, however, they do have one significant drawback: They are very compute-intensive and known to have a significant impact on server performance. This is especially true in the case of short transactions, which are typical of e-Commerce.

The Intel® Itanium™ processor, based on the IA-64 architecture, has several features that can help to speed up public-key cryptography. Parallel instruction issue, multiple execution units, 64-bit Integer Multiply-Add instruction, and a large register set enable high performance on public-key cryptography algorithms. Using optimistic performance estimates for competitive products (based on theoretical analyses of their respective instruction sets and architecture) and comparing with actual performance on the Itanium processor, the Itanium processor is nearly 10 times faster than the Sun UltraSPARC III† processor.

The Itanium processor provides performance leadership in executing the public-key algorithms needed for secure e-Commerce transactions, and does so without special hardware assistance. This is an advantage because hardware solutions are costly and increase the form factor of the total server solution.

Because of the potential security vulnerabilities posed by e-Commerce, Web sites need the protection of security-specific software even though such software is widely known to degrade server performance. Until recently, IT managers have been forced to live with the performance trade-off or resort to expensive hardware solutions. Now, performance advancements provided by the Itanium processor enable the integration of additional security features into application software without compromising server performance. This means IT managers can finally eliminate the trade-off between performance and security.

Table of Contents

Table 1. RSA 1024-bit Decryption Performance Comparison

Processor	Clock Frequency	RSA Decryptions Per Second
Itanium™ Processor	660 MHz	1,000*
Sun UltraSPARC III™	600 MHz	130**

* Measured Performance
** Estimate of best case performance based on theoretical analysis

RSA Decryption Kernel Measurements

Background

To ensure that e-Commerce sites are secure, Web sites use security algorithms and protocols to authenticate identities, authorize access, protect data, ensure transaction integrity and monitor and audit transactions. One type of security algorithm is public-key cryptography, which is widely used in Internet-based security technologies.

Public-key cryptography is also known as asymmetric-key cryptography and, as such, differs from symmetric-key cryptography. In symmetric-key cryptography, there is one key, used by the sender for encryption and by the receiver for decryption. This approach introduces potential problems with key distribution. In public-key (or asymmetric-key) cryptography, there are two keys: a public key known to all and a private key known only to the key owner. This approach eliminates any key-

distribution problems since the public key does not need to be hidden. The downside, however, is that compared with symmetric-key cryptography, public-key cryptography is very computationally intensive, which inhibits its use for encrypting large volumes of data. Therefore, the two forms of cryptography are generally used in tandem. The keys for symmetric encryption are exchanged using public-key cryptography, and the actual message is exchanged using the symmetric keys. The most commonly used implementations of public-key encryption are the RSA public-key algorithm, patented by RSA Security Inc., and the protocol known as Secure Sockets Layer (SSL). Some other security technologies that rely on public-key cryptography are Public Key Infrastructures (PKI) and Virtual Private Networks (VPN).

The RSA Algorithm

Named after its inventors (Rivest, Shamir, Adelman) and offered by RSA Security Inc., the RSA algorithm is the most widely used public-key algorithm. It also is computationally intensive. At the core of the computation is the exponentiation of large numbers to large powers. The encryption of a single small message may cost millions of native processor operations. There are alternatives to using the RSA algorithm for public-key encryption, but virtually all of them use a large number multiplication at their core.

To understand large number multiplication, consider computation of the quantity $\mathbf{M^e \bmod n}$, where each of the values is a very large integer, typically 512 or 1024 bits in length. The mod (or modulo) operation computes the remainder after division and is commonly referred to as a reduction, since it reduces the number to be less than **n**. Since the exponent is so large, it is obviously not feasible to complete all of the exponentiation before doing the reduction, because the resulting number would have an astronomical number of bits. So in practice the multiplication steps are interleaved with reductions after each multiplication. The long division used for reduction is a very expensive operation, though, if done by repeated trial division, as by hand.

In 1985, a researcher named Peter Montgomery published a method for doing the multiplication and reduction that does not require trial division. Now known as the Montgomery Product, this method allows the multiplication and reduction to be done as a series of multiplications and additions. The Montgomery Product is used widely for doing modular exponentiation. An excellent summary of the Montgomery Product (and the methods for optimizing it) can be found in [4]. This calculation takes up about 50% of the time required to complete a short secure transaction (typical of e-Commerce).

Secure Sockets Layer

Secure Sockets Layer (SSL) is another important implementation of public-key cryptography. The SSL protocol was originally developed by Netscape† and has been widely accepted for authenticated and encrypted communication between clients and servers on the Web [4]. The SSL protocol has three main purposes:

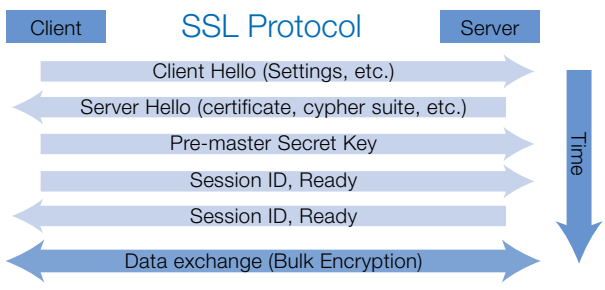
- Server authentication
- Client authentication
- Secure private communications

Server authentication is used to confirm the identity of the server and relies on certificate authorities as a source of trusted information about valid certificates. Client authentication is used to confirm the identity of the client. Though not yet used widely, its use is likely to rise to deal with credit card fraud issues. Secure private communications use encryption to send and receive information.

The SSL protocol uses a combination of public-key and symmetric-key encryption. Symmetric-key encryption is much faster than public-key encryption, but public-key encryption provides more robust authentication techniques. An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, and then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server. The figure below shows the sequence (from top to bottom) of the basic SSL protocol.

SSL is widely known to degrade server performance. From the article “E-Biz

Figure 1. SSL Protocol



Bucks Lost Under SSL Strain" in Internet Week [1], "Recent tests conducted by researcher Networkshop Inc. indicate that powerful Web servers capable of handling hundreds of transactions per second may be brought to a near stand-still by heavy SSL traffic. Some server configurations suffered as much as a fifty-fold degradation in performance from SSL, down to just a few transactions per second, according to analyst Alistair Croll at Networkshop."

Figure 2 shows the contribution of the RSA computation (public-key operations), symmetric data encryption and miscellaneous computations for the transfer of a file of a given size under the SSL protocol. Note that for smaller files, the RSA computation contributes the most time. These results are based on analyses by Intel.

Benefits of Security Algorithm Performance

As previously noted, the impact of security on server performance has been widely reported, particularly in the context of SSL transactions. As Figure 2 shows, a primary source of the performance impact is in the public-key operations. In the past, there were two primary means of addressing this bottleneck: (1) purchasing more servers or (2) using special-purpose hardware to do the public-key computations. Each of these solutions adds cost, both direct (purchase price) and indirect (increased complexity, larger footprint).

SSL and other implementations based on public-key cryptography can be expected to have high performance on Itanium™-based systems. Such performance should enable an increase in server capacity and a decrease in server-response time. The actual capacity increase depends significantly on both the mix of secure vs. non-secure transactions and the size of the transactions. In the best case, we expect to see server capacity to increase by upward of 40 percent over untuned software. This case will apply when there are a high number of short secure transactions. The cost of authentication is incurred only once during a normal SSL transaction. A session may be quite lengthy (e.g., from login to logout), and SSL allows this entire session to be conducted under one authentication. In this case the capacity increase may be minimal.

The improvements in response time are much harder to analyze but are potentially much more dramatic. Since most servers are tuned to operate not at peak capacity but at some average capacity, a significant burst of secure transactions can cause server queues to grow quickly and cause a dramatic increase in response time. The fast authentication capability of the Itanium processor provides faster service times for the queues, thus reducing the potential for unstable situations where the queue is growing faster than it is being serviced. Of course, the benefit will be less apparent when the server is receiving transactions well beneath its capacity.

Several useful discussions of this phenomenon can be found at the Rainbow Technologies ISG Labs Web site at http://isglabs.rainbow.com. (Rainbow is a supplier of cryptographic hardware. We believe that its arguments about the impact of performance improvements in public-key algorithms are valid also for the improvements we have realized on the Itanium processor.)

Test Results

To obtain all performance measurements on the Itanium processor, we used a proprietary test application from RSA Security Inc. This test application was linked with an early version of a security library that RSA Security plans to release.

Based on our analyses of the Montgomery Product, we can now either directly measure or estimate RSA public-key performance. Also included in those analyses is performance data for the Sun UltraSPARC III processor.

Figure 2. Relative component costs for SSL transactions of various sizes

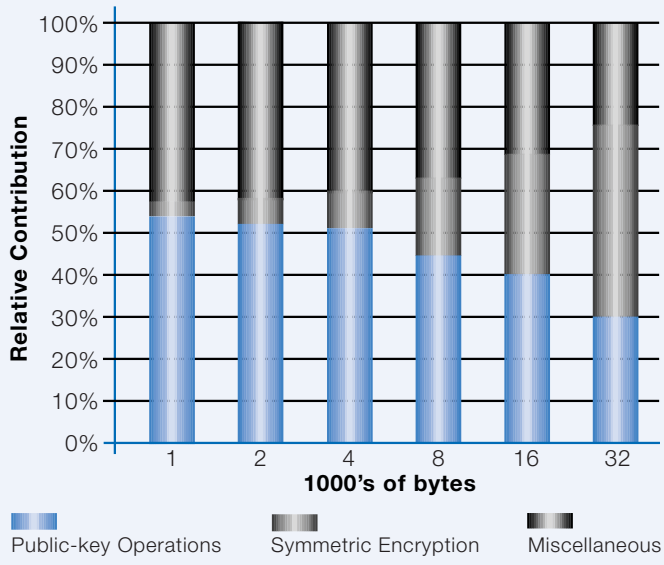


Table 2. RSA 1024-bit Decryption Performance Comparison

Processor	Clock Frequency	RSA Decryptions Per Second
Itanium™ Processor	660 MHz	1,000*
Sun UltraSPARC-III™	600 MHz	130**

* Measured Performance
** Estimate of best case performance based on theoretical analysis

Please note that the measurement results provided in this report are preliminary and were derived from testing done on pre-production hardware. These results do not reflect the performance of the final production-level systems and should not be used to estimate or project production-level performance.

Also note that both software and hardware are expected to change over time, which will change the performance of the system. Finally, performance results may vary considerably depending on the specific workload. The performance gains on particular algorithms will not give the same degree of overall application performance improvement. In particular, the performance gains cited in this report are most relevant in workloads with a high percentage of short, secure transactions.

The Intel® Itanium™ Processor and the Montgomery Product

The Itanium processor has several features that help to accelerate the performance of the Montgomery Product. These include parallel instruction issue, multiple execution units (four integer, four multimedia, two floating-point, two memory and three branch units), large register set and the 64-bit Integer Multiply-Add Instruction (xma).

The 64-bit Integer Multiply-Add instruction produces the upper or lower 64-bit product, executes on either floating-point execution unit, and is fully pipelined. The large register set allows the Montgomery Product operands and intermediate results to be held in registers rather than in memory.

Table 3 shows the parallel instruction execution in the Itanium processor. The algorithm maps into the architecture efficiently, allowing full use of all functional units for the bulk of this computation. This parallel instruction execution continues for most of the Montgomery Product computation.

Table 4 summarizes the Montgomery Product performance results.

Performance of Other Platforms

The Montgomery Product can also be used to compare processor performance. Examining the architecture and implementation details of various microprocessors, their Montgomery Product performance estimates can be calculated. In particular, a performance estimate can be made by comparing the number of integer multipliers, latency of the multipliers, whether or not the multipliers are pipelined, types of integer multiply instructions, number of ALU execution units and number of instructions issued per clock.

The performance of the Itanium processor on the Montgomery Product is compared with the performance of the following processors:

- Compaq† Alpha 21264/21364 processors (Ref. 7)
- Sun† UltraSPARC III processor (Ref. 9)
- IBM† PowerPC 7400 (G4) processor with AltiVec (or Velocity Engine) (Ref. 12)

(Note that the documents used to derive these estimates are listed in the reference section of this document.)

The Alpha architecture defines upper and lower integer multiply instructions much like the Itanium architecture's xmul.u and xmul.l upper and lower integer multiply instructions (but without the multiply-and-add feature). The Alpha 21264/21364 has a single pipelined 64-bit integer multiplier, as compared with the Itanium processor dual pipelined integer multipliers.

The SPARC architecture defines only a single MULX instruction, which multiplies two 64-bit integer values and produces a 64-bit result. There is no method for capturing the upper 64 bits of the result.

Table 3. Itanium™ Processor Parallel Instruction Execution

Unit	Instruction	Function
FPU 0	xma.lu	Integer Multiply with Add
FPU 1	xma.hu	Integer Multiply with Add
Integer 0	Add	Add Partial Products
Integer 1	p = cmp.ltu	Integer Compare for Carry
Memory 0	getf.sig	Move Partial Product from FP Reg to General Reg
Memory 1	(p) add	Predicated Add for Carry

Table 4. Montgomery Product Performance Comparison

Processor	Size	Cycles
Itanium™ processor	512-bit	245
Itanium™ processor	1024-bit	1,220

The UltraSPARC III processor has a single non-pipelined 64-bit integer multiplier, which is a significant performance inhibitor. Each multiply must wait for the previous one to complete.

The PowerPC 7400† (G4) is a 32-bit processor, but still has the power to perform small integer multiplications in the AltiVec unit. The PowerPC G4's AltiVec, or Velocity Engine, extension supports a 4-wide 16-bit multiplication instruction. Four of these instructions plus additions are needed to provide the equivalent of one 64-bit multiplication. For this reason, the performance of this processor also lags that of the Itanium processor.

The performance estimates in Table 5 attempt to reflect an upper bound of the competitive processor performance. The performance estimates were a result of theoretical analyses done without anyone actually having developed code and executed it on the processors. There may be other performance bottlenecks in the implementations, such as a lack of registers or instruction issue limitations. More details are available in Appendix 2: Competitive Analysis Using the Montgomery Product.

Conclusion

Based on current measurements, the Itanium processor 660 MHz provides substantially better performance for the RSA public-key algorithm than what we estimate current competitive processors can provide. We fully expect this performance differential to remain in place as we move toward production-level frequencies. We expect the performance of the Itanium processor 800 MHz to scale linearly from that of the 660 MHz version. Since public-key algorithms are the core of many security applications, Itanium processors should significantly benefit the performance of these applications and enable the integration of additional security features into application software without compromising server performance. This goes a long way towards eliminating the historical trade-offs that IT managers have been forced to make between security and performance.

These performance results are derived from work done at the Intel Microcomputer Labs as part of its mission to enable high-performance computing for independent software suppliers. RSA Security Inc. has committed to incorporate these performance improvements into its future products. These products are used widely as building blocks for security applications. RSA Security's leadership in the security field will help to ensure the proliferation of such performance results into the market. Already, other security suppliers have expressed interest in incorporating the results of this work into their products.

Table 5. 1024-bit Montgomery Product Performance Estimates

Processor	Montgomery Product Performance Estimate
Itanium™processor	1,220 cycles
Alpha 21264	1,800 cycles*
UltraSPARC-III™	12,300 cycles*
PowerPC G4 with AltiVec	14,000 cycles*

* estimates based on theoretical analysis of architecture

References

1. Vergara, Mike, *RSA Security Solutions*, RSA presentation at Intel's SRM Summit, 10/27/99
2. *Understanding Public Key Infrastructure (PKI),* white paper, RSA Security Inc., http://www.rsasecurity.com/products/keon/whitepapers/pki/PKIwp.pdf
3. *E-Biz Bucks Lost Under SSL Strain*, Internet Week, 5/20/99, http://www.internetwk.com/lead/lead052099.htm
4. *Introduction to SSL*, iPlanet Developers, http://docs.iplanet.com/docs/manuals/security/sslin/index.htm
5. *High-Speed RSA Implementation*, TR-201, RSA Laboratories, ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf
6. Van Woudenberg, Scott and Chin, David, *Security Kernel Performance on Merced Processor*, Internal Intel Report
7. Kessler, R.E., *The Alpha 21264 Microprocessor*, IEEE Micro, March-April 1999, pp. 24-36.
8. Gwennap, Linley, *Alpha 21364 to Ease Memory Bottleneck*, Microprocessor Report, Oct. 26, 1998, pp. 12-15.
9. Horel, Tim and Lauterbach, Gary, *UltraSPARC-III: Designing Third-Generation 64-Bit Performance*, IEEE Micro, May-June, 1999, pp. 73-85.
10. Song, Peter, *UltraSparc-3 Aims at MP Servers*, Microprocessor Report, Oct. 27, 1997, pp. 29-34.
11. *VIS Instruction Set User's Manual*, Sun Microelectronics, 805-1394-01, 7/97
12. *Power PC Microprocessor Family: The Programming Environments for 32-bit Microprocessors*, Motorola, MPCFPE32B/AD Rev. 1, 1/97

13. *PowerPC 740/PowerPC 750 RISC Microprocessor User's Manual*, IBM, GK21-02C3-00, 2/23/99

14. MPC7400 RISC Microprocessor Technical Summary - Preliminary, Motorola, MPC7400TS/D, Rev. 0, 8/1999.

Acknowledgments

We would like to thank the people at RSA Security Inc. for integrating our work into their future products and into a testing vehicle suitable for measuring these results.

Appendix 1: System Configuration

The system configuration used in these measurements is outlined in the following text. Measurements were made on an Intel Itanium processor 660MHz-based system with kernels from RSA Security.

Hardware

- Intel Itanium Processor
- BIOS Build 19/PAL16
- 660MHz, 133 MHz system bus, 2x bus (system bus enabled at double pump rate)
- All caches (L1, L2, L3) enabled
- 2MB L3 cache

Software

- Intel® Cross Development SDK Build 5
- Windows† 2000 NT 64-bit

Appendix 2: Competitive Analysis Using The Montgomery Product

The Montgomery Product can also be used to compare processor performance. Examining the architecture and implementation details of various microprocessors, their Montgomery Product performance estimates can be calculated. In particular, comparing the number of integer multipliers, latency of the multipliers, types of integer multiply instructions, number of ALU execution units, and number of instructions issued per clock can help in making estimates.

The performance of the Itanium processor can be compared with the performance of the following processors:

- Compaq† Alpha 21264/21364 processors
- Sun† UltraSPARC III processor
- IBM† PowerPC 7400 (G4) processor with AltiVec (or Velocity Engine)

The following table compares the architectural features of the processors.

The Alpha architecture integer multiply instructions are similar to the ones in the Itanium processor architecture. The SPARC architecture defines only a single MULX instruction, which multiplies two 64-bit integer values and produces a 64-bit result. There is no method for capturing the upper 64 bits of the result.

The PowerPC 7400 is a 32-bit processor, but is still has the power to perform small integer multiplications in the AltiVec unit.

The implementation details of the processors also can be compared, as shown in Table 7.

The Alpha 21264/21364 has a single pipelined 64-bit integer multiplier, as compared with the Itanium processor dual pipelined integer multipliers.

The UltraSPARC III has a single non-pipelined 64-bit integer multiplier, which is a significant performance inhibitor. Each multiply takes a minimum of 6 cycles and must wait for the previous one to complete.

The PowerPC G4's AltiVec, or Velocity Engine, extension supports a 4-wide 16-bit multiplication instruction. Four of these instructions plus additions are needed to provide the equivalent of one 64-bit multiplication. For this reason, its performance also lags that of the Itanium processor.

Table 6. Architectural Feature Comparison

Architectural Feature	Itanium™ Processor	Alpha 21264/ 21364	UltraSPARC-III™	PowerPC G4 with AltiVec
Integer Multiply Instructions	XMA.H, XMA.L	UMULQ, UMULH	MULX	VMULOUH, VMULEUH
Integer Multiplication Width	64 x 64 → 64 upper/lower	64 x 64 → 64 upper/lower	64 x 64 → 64 lower only	Four 16 x 16 → 32
Integer Multiply-and-Add?	Yes	No	No	No
Number of Integer Registers	128	32	8 globals, 8 input, 8 local, 8 output	32 vector registers

Table 7. Implementation Comparison

Implementation Feature	Itanium™ Processor	Alpha 21264/ 21364	UltraSPARC-III™	PowerPC G4 with AltiVec
Instructions Per Clock	6 (4 Int/2 FP)	6 peak, 4 sustainable	4	4
Number and Width of Integer Multiplier	Two 64-bit	One 64-bit	One 64-bit	Four 16-bit
Pipelined Multiplier?	Yes	Yes	No	N/A
Int Multiply Latency	7 cycles	7 cycles	6-9 cycles	N/A
Number of Physical Integer Registers	128	80	8 global/ 24 windowed	32 128-bit

THIS TEST REPORT IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document or by the sale of Intel products. Except as provided in Intel’s Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel retains the right to make changes to its test specifications at any time, without notice.

The hardware vendor remains solely responsible for the design, sale and functionality of its product, including any liability arising from product infringement or product warranty.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, reference www.intel.com/procs/perf/limits.htm or call (U.S.) 1-800-628-8686 or 1-916-356-3104.

The Intel® Pentium® III Xeon™ processors and Intel® Itanium™ processors may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Printed in USA
order number:283585-001
0101/CMD/JH/1K