

# The Advantages of IA-64 for Security Applications

Information for Software Developers

intel®

The features of the IA-64 architecture and its first microprocessor implementation, the Intel® Itanium™ processor, prove particularly useful for accelerating the performance of security applications in relation to the public and private algorithms while eliminating the bottlenecks and expense.

## The Challenge

Appropriate security is central to successful e-Business, both for external company Web sites and for internal company networks. Encryption algorithms lie at the heart of security systems, scrambling information to prevent it from being intercepted and read by anyone but a recipient with a proper key.

There are two major varieties of encryption algorithms. The most familiar variety is the symmetric (or private key) algorithm. With symmetric encryption, both parties agree on a key for the message to be encrypted (e.g., a password), and the algorithm uses this same key at both ends of the conversation to scramble and then unscramble the message. This is analogous to two people having identical keys to a padlocked box. The sender locks the box with his key, and the receiver unlocks it with his key. But there's a major problem with e-Commerce—transporting the key without exposing it to unfriendly eyes while it travels through the network. To solve this problem, the second kind of algorithm, called an asymmetric (or public key) algorithm was invented. This is analogous to a padlock that requires different keys for locking and unlocking. The key for locking is made available to

everyone, but only the receiver has a key that can unlock the box. However, the performance of public key algorithms is the major performance bottleneck in most e-Commerce situations.

Security algorithms (public and private) can be added at a variety of layers—hardware, operating system and applications. Instances of such implementation include:

- Establishing protected communications between a Web server and client for transmitting credit card information
- Authenticating users within a company to log in to desktops, file servers, databases or e-mail systems
- Authorizing users within a company
- Protecting confidentiality between internal corporate networks and people outside the network, such as telecommuters or supply-chain partners, via Virtual Private Networks (VPNs)
- Protecting implementation of basic network infrastructure, such as TCP/IP
- Protecting storage of information on a server or client
- Protecting confidential e-mail

For example, an e-Commerce transaction in which a customer orders a product from a Web site involves multiple security operations. First, the e-Commerce system must verify the customer's identity using a password or token, a process called authentication. Second, the system must encrypt any confidential information passing between the customer and the Web server. Due to all the various levels of security, encrypting and decrypting can be extremely time-consuming.

RSA, a leading data security company, claims the speed of one of its primary algorithms with modest security is only 21.6 kilobits per second on an Intel® Pentium® processor running at 90 MHz. By contrast, most Web servers connected to a T1 line send data at 1.54 megabits per second; internal corporate servers connect to dozens of clients at 10 to 1,000 megabits per second.

In addition, the performance of encryption operations represents a critical bottleneck that acts as a barrier to protected networks. Encrypting all network traffic from a client or server requires significant processor resources. The microprocessors must encrypt and decrypt each and every piece of data sent over the wire, a process that requires a significant amount of computing resources. For example, Web servers running the Secure Sockets Layer (SSL) encryption protocol (used for receiving page requests and transmitting protected Web pages) face a 10-20x performance hit over Web servers that are not running SSL.

Like Web servers, servers handling multiple VPN sessions will face a similar bottleneck due to encryption performance, since every TCP/IP packet sent and received by the machine must be encrypted or decrypted. These operations can be offloaded in some cases to dedicated, encryption accelerating hardware, but this dedicated hardware is typically expensive. Moreover, the application or operating system performing the encryption must have the proper interfaces to recognize and take advantage of this specialized hardware.

## IA-64 Architecture's Contribution to the Solution

The IA-64 architecture offers a number of features that will reduce the overhead required for protected communications, e-Business and e-Commerce:

- **64-Bit Arithmetic:** Traditional encryption algorithms take blocks of data and perform certain operations on those blocks, employing the key. Since algorithms such as DES employ 64-bit or larger, sized data blocks and keys larger than 32-bit implementations can now benefit from the IA-64 architecture due to the ability to perform 64-bit arithmetic operations. IA-64 processors can thus move and manipulate public and private key indexes in fewer steps than 32-bit processors.
- **Parallelism:** IA-64 provides parallel execution units that, when scheduled properly by the compiler, can deliver faster performance by executing multiple instructions per clock cycle. Getting more executions per clock improves performance on looping algorithms, a central part of encryption computations. The multiplication of large numbers is run in parallel, meaning that for significant portions of the algorithm, up to six instructions can be executed simultaneously. This increase for public key algorithms is very significant.
- **Predication:** The performance of a microprocessor suffers a very large penalty when it mis-predicts the results of a branch or an "if" statement, because the processor has to flush and reload the content of its instruction pipeline. The IA-64 architecture improves branch handling

by minimizing branches in the code through the use of qualifying predicates and increasing branch prediction hit rates for the remaining branches through branch predict instructions.

- **Loop Handling Optimizations:** The IA-64 architecture provides a branch operator that allows for perfect prediction of loop termination for counted loops, eliminating these mis-predicts penalties.

The IA-64 architecture also supports modulo scheduling, a software pipelining technique that allows a compiler to schedule loop iterations in parallel, rather than sequentially. Traditional compilers use techniques such as loop unrolling, which greatly expand the memory footprint and take up valuable space in the processor caches. The IA-64 architecture instead provides a feature called register rotation, which allows each iteration of a loop to use its own set of automatically renamed registers.

Without automatic renaming, the registers would have to be renamed by the compiler (increasing code size as described above) and the processor would stall. The stall occurs because the registers would have to wait for the first iteration of the loop to finish before starting the second iteration, since the loop code of both iterations of the loop writes to the same registers. With automatic renaming, iterative loops can be run in a pipelined, parallel fashion with a small memory footprint.

Most security algorithms consist of many loop iterations. The IA-64 architecture's features accelerate loop-handling performance and can greatly increase the throughput of encryption algorithms.

- **Very large set of registers:** With 128 integer registers, 128 floating point and eight branch registers, which represents a significant increase over IA-32 and RISC microprocessors, data commonly referenced by the encryption algorithms can be stored in the registers. Thus, a smaller amount of data must be accessed from memory. This useful feature eliminates the potential stall of the processor due to waiting for such data to come from memory. In addition, the large number of registers can accommodate more complex encryption algorithms, which would be painstakingly slow if intermediate results had to constantly be moved back and forth between memory and registers.
- **Large Physical Memory for Security Caching:** Enterprises with very large directory services for managing user IDs, security tokens, contact information or other secure data will need to support quick user authentication and authorization for thousands (Fortune 50 internal users) to multi-millions (telephone, Web sites and credit card companies) of users. Directory services built around 64-bit in-memory databases will prove useful for providing fast processing of security algorithms.

## Summary

Encrypting network traffic to prevent interception or tampering can be a processor-intensive operation, because encryption algorithms (public and private) consist largely of small loops with many arithmetic operations. Network servers that don't benefit from hardware accelerators face bottlenecks due to the overhead of encrypting many streams of information and incur great expenses. The IA-64 architecture delivers the features to allow security applications to benefit significantly. The Intel® Itanium™ processor offers new architectural features such as sophisticated loop handling, 64-bit arithmetic and improved instruction parallelism. Security applications optimized for IA-64 architecture and Itanium will deliver the performance needed for today's demanding e-Business infrastructures.



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. 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 may make changes to specifications and product descriptions at any time, without notice.

The Intel® Itanium™ processor 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.