Effectively implement AES for EFI/Tiano based on IA-32 Platform

Chen, Tianzhou  He, Zhenjie  Hu, Wei
College of Computer Science, Zhejiang University, Hangzhou 310027, China

1. Introduction

The Advanced Encryption Standard (AES) is one of the most important algorithms in modern cryptography. Although fully defined in terms of functionality, AES requires best exploitation to achieve optimum performance on specific architectures.

Generally even highly optimized SW solutions are magnitude slower than dedicated HW solutions. Our work concentrates on Extensible Firmware Interface (EFI) as the next generation firmware technology contains much more benefits than legacy BIOS. To combine the unusually high speed with platform universality, we present a new usage model of AES for EFI/Tiano Framework based on IA-32.

2. Design and Implementation Strategies

The Intel NetBurst architecture is a new 32-bit micro-architecture allows processors to operate at significantly higher clock speeds and performance levels, which introduce many new advanced features. One important feature is the ability to operate on 128-bit packed integers in XMM registers provides greater flexibility and greater throughput when performing SIMD operations on packed integers. This capability is particularly useful for applications including AES. To speed up processing and improve cache usage, the SSE2 extensions offer several new instructions that allow application programmers to control the cache ability of data. These instructions provide the ability to stream data in and out of the registers without disrupting the caches and the ability to pre-fetch data before it is actually used. By manipulating memory management translation tables, it is possible to assign the AES substitution tables to the data cache. This ensures that there will be no interference by other data structures or applications on the data cache, and once loaded, substitution tables will always remain there.

The round transformation can be combined in a single set of table lookups, allowing for very fast implementations on processors with word length or above. In the key expansion stage, pre-computing and storing entire key in table-lookup, and then finding the desire round key is much fast than repeat computing it, which accelerate the speed when processing mass data. EFI is a public industry specification that describes a set of abstract programmable interfaces between firmware and OS. Tiano is a firmware infrastructure that is designed to take advantage of the abstraction inherent in EFI which introduces many contemporary design principles of computer science. Driver eXecution Environment (DXE) is the phase where most of the system initialization is performed, also providing an environment for program execution. Fig. 1 shows AES implementation.

We select typical IA-32 processors, Pentium 4 and Celeron D with two distinct SW platforms, EFI/Tiano (Release 6), and OS (Windows XP) to do experiment for comparing the performance. As a result, we found that the former much better than that latter, reaching at a speed of almost twice times fast.

3. Conclusion

In this work, the new advanced feature of universal IA-32 for AES are identified and appropriately exploited. A new usage model of AES implementation within EFI/Tiano framework based on IA-32 is formulated. It is a compact implementation, preserves the flexibility of AES algorithm, especially, it exhibits performance advantage evidently.