Presented at the Research Congress 2013
De La Salle University Manila
March 7-9, 2013

DEMYSTIFYING INTEL® IVY BRIDGE MICROARCHITECTURE

Roger Luis Uy
College of Computer Studies, De La Salle University

Abstract: Tick-Tock is a model introduced by Intel ® Corporation in 2006 to show the improvement of its chip development. Every "tick" is the die-shrink of the current microarchitecture, while every "tock" is the new microarchitecture. During the 2nd quarter of 2012, Ivy Bridge Microarchitecture was introduced as the 22-nm die shrink (the "tick") of the Sandy Bridge microarchitecture (the "tock"). Ivy Bridge-based microprocessors are multi-core processor which place emphasis on minimizing thermal dissipation of processor and providing architecture innovation rather than raw processor speed. Ivy Based-processor comes in three variations – for desktop, for mobile and for server usage. Difference among them lies in the number of core in a processor, the clock frequency, the Thermal Design Power (TDP), the cache memory size and architectural innovations. This research paper will survey the Ivy Based-processor and classify them accordingly. Survey will be based from the Intel's official website (ark.intel.com). At the same time, independent website (www.cpu-world.com) will be used to counter-check the specifications and to obtain additional information. A freeware software, called CPU-Z (www.cpuid.com) is used to gather information of the processor and provide information such as the name and number of the processor, internal and external clock rate, clock multiplier, supported instructions and cache information. Once the survey and classification is done, we can gain information on which type of applications can be used on which type of microprocessor.

Key Words: Computer Architecture, processor architecture, Ivy Bridge microarchitecture, architectural innovation

1. INTRODUCTION

Tick-Tock is a model introduced by Intel ® Corporation in 2006 which serve as the roadmap for microprocessor development (Intel 2013). Every "tick" represents finding improvement in the manufacturing process of the processor with the goal of increasing transistor density and improving thermal problem. On the other hand, every "tock" represents finding improvement and innovation in processor microarchitecture. It is expected that there will at least be a "tick" or a "tock" every year.

The current improvement involves a "tick" improvement. During the 2nd quarter of 2012, Intel ® Ivy Bridge microarchitecture was introduced. This microarchitecture is the improve model of the previous microarchitecture codename "Sandy Bridge". Some of the key improvement includes introduction of tri-gate (3D) planar transistor and the reduction of transistor die size to 22-nm . Tri-gate (3D) transistor uses lesser voltage which translates to less power consumption and less current leakage as compare to the 2D planar transistor which is used by Sandy Bridge microarchitecture (Doyle et al., 2003).

Decrease in transistor die size translates to higher transistor density. This allows improvement in the architectural innovations. Some of them are as follows:

a.) Improvement in integrated graphics – There are two versions of integrated graphics: the lower end

Intel HD Graphics 2500 and the high end Intel HD Graphics 4000. Improvement will involve support to 3D graphics, Direct X 11 and Open Compute (Open CL). The execution units of the HD Graphics 4000 also increases to 16 from the previous 12.

b.) Introduction of a new random number generator instruction (RdRAND) to work hand-in-hand with the processor's random number generator. This is used mainly in cryptography and security

In terms of implementation, the Ivy Bridge microarchitecture introduces the 3rd generation Core i3, Core i5, Core i7, Celeron, Pentium and Xeon processor and it comes with three variants – desktop, mobile and server. Intel Core i5, Core i7 and the mobile Core i7 was introduced initially on April 29, 2012. It was followed by Xeon on May 14, 2012, mobile core i3 and i5 during the 2nd quarter of 2012, Pentium and mobile Pentium during the 3rd quarter of 2012. Celeron and mobile Celeron will be introduced during the 1st Quarter of 2013. The difference among the implementation lies in the number of core in a processor, the clock frequency, the Thermal Design Power (TDP), the cache memory size and the architectural innovations. This research paper will survey the Ivy Based-processor and classify them accordingly. Once the survey and classification is done, we can gain information on which type of applications can be used on which type of microprocessor. Survey will be based from the Intel's official website (ark.intel.com). At the same time, independent website (www.cpu-world.com) will be used to counter-check the specifications and to obtain additional information. A freeware software, called CPU-Z (www.cpuid.com) is used to gather information of the processor and provide information such as the name and number of the processor, internal and external clock rate, clock multiplier, supported instructions and cache information.

2. Methodology

As single-core processors are getting faster, the dual problems of heat dissipation and efficient use of Instruction Level Parallelism (ILP) has now become a major problems. Major chip developers such as Intel have shifted to multi-core processor. Multi-core processor has a lower clock rate than single-core processors. Various architectural innovations have been incorporated to offset the lower clock rate. These innovations have been incorporated to provide value-added performance to the multi-core processor. The following sub-sections defined some of the architectural innovations used in Ivy Bridge-based processor.

2.1 Turbo Boost

Turbo Boost is a technology in which the processor can go beyond its base clock rate. This can be done when the operating system request for the highest performance level of the processor (Intel, 2008). The increase in clock rate is subject to the thermal and electrical limitation of the processor as well as the number of processor core active at that time. The clock rate of the processor increases by an increment of 100MHz. The specification of a processor gives the base clock rate and the number of increments that a processor can increase given the number of core that are active at that time. For example, Core i7-3770 has a base frequency of 3.4GHz (3400MHz) and a turbo rating of 3/4/5/5. The first number denotes the number of multiples of 100Mhz supported when four cores are active, the second number is for the number of multiples when three cores that are active, the third number if two cores are active and the fourth number if a single core is active. Thus, if only single or two cores are active, the clock rate can go as high as 3400Mhz + (5*100MHz) = 3900MHz or 3.9GHz. Note that turbo boost cannot be controlled by user, it is dynamically adjusted by the operating system only.

2.2 Hardware Virtualization

Hardware virtualization technology allows multiple operating systems to simultaneously share hardware resources in a safe and efficient manner (Neigher, et al. 2006). In software virtualization, a single operating system is solely in-charge of all hardware platforms. In hardware virtualization, instead of operating system, there is a software layer called virtual-machine monitor (VMM) which is in-charge of arbitrating access to

the hardware resources. Thus, multiple operating systems act as guest to the VMM and the VMM provides each guest operating system a set of virtual platform interfaces known as virtual machine.

2.3 Trusted Execution Technology

Trusted execution technology is a hardware level support to attest the authenticity of a platform and its operating system and assures that an authentic operating system starts in a trusted environment (Greene, 2012). When the platform or computer powers on, the hardware level starts a chain of trust by validating a known digitally signed module as provided by the chipset.

2.4 vPro

vPro technology is a platform that provides security and manageability on a hardware level (Levy, 2008). Manageability and security includes identity protection, data protection, threat management, hardware-assisted virtualization, secure computing in the cloud and remote repair. This platform includes processor, chipset and network interface card as well as other architectural innovation such as hardware virtualization, active management and trusted execution technology.

2.5 Hyperthreading

Hyperthreading technology is a technique in which a single physical processor appears as two logical processes (Marr, 2002). This is done by duplicating the architectural state but sharing the same physical execution resources. Architectural state refers to all the registers in a processor – general-purpose, control, advanced programmable interrupt controller. Physical execution resources refer to the execution unit, cache memory, address bus, data bus and the like. From the software point of view, each architectural state is therefore viewed as if it is a separate processor. Thus, in terms of parallelism, it can be viewed as Simultaneous Multi-Threading (SMT) – Multiple instructions operating on separate data in parallel. Note that operating system should also be SMT-aware or else in will not be able to take advantage of the Hyperthreading technology.

2.6 AES-NI

Advanced Encryption Standard New Instructions (AES-NI) is a set of 6 instructions that deals with encryption and decryption using AES standard. The AES standard is an encryption and decryption standard adopted by U.S. government and is to be use by software developer to protect network traffic and personal data. (Gueron, 2012). Software developer uses AES-NI instructions to access hardware level AES support. It therefore accelerates the execution of AES-based algorithm.

The AES algorithm works by encrypting a fixed block size of 128-bit of plain text in several rounds to produce the final encrypted text. The number of rounds can be 10, 12 or 14 depending on the key length (i.e., 128-bit, 192-bit or 256-bit). These instructions provide an integrated single instruction in lieu of multiple instructions software solution. The 6 new instructions are as follows: AESENC (performs a single round of encryption), AESENCLAST (performs last round of encryption), AESDEC (performs a single round of decryption), AESDECLAST (performs last round of decryption), AESKEYGENASSIST (use to generate round keys for encryption, AESIMC (performs conversion of encrypted round key to a form useable for decryption).

3. Results and Analysis

3.1 Desktop Implementation

Desktop implementation of Ivy Bridge microarchitecture has the highest clock speed and the highest cache memory available. Table 1 summarizes the implementation of desktop-based implementation in terms of number of cores, Hyper-Threading support, Turbo Boost support, Cache memory, integrated graphics support and range of TDP.

Table 1: Summary of Desktop Implementation of Ivy Bridge Microarchitecture

Model	# of cores	Hyperthreading	Turbo Boost	Cache Memory	Integrated Graphics	TDP (w)
Celeron	2	No	No	2MB	HD Graphics	35, 55
Pentium	2	No	No	3MB	HD Graphics	35, 55
Core i3	2	Yes	No	3MB	HD Graphics 2500, HD Graphics 4000	35, 55
Core i5	4	No	Yes	6MB	HD Graphics 2500, HD Graphics 4000	35, 45, 65 ,77
Core i7	4	Yes	Yes	8MB	HD Graphics 4000	45, 65, 77

Both Celeron and Pentium are almost identical in the following aspects: dual-core configuration, no Hyper-threading and integrated graphics does not support 3D graphics. The only difference lies in the cache memory - Celeron has 2MB while Pentium has 3MB of cache memory. This configuration is suitable for usage related to common business productivity tools and internet access activity. Even though Core i3 is a dual-core configuration, but it support Hyper-Threading and its integrated graphics supports 3D graphics. This configuration is best suited for applications that require light to medium graphics applications. Both, Core i5 and Core i7 are quad-core configuration. But Core i5 does not support Hyper-Threading while Core i7 supports Hyper-Threading. Both should be suitable for processor intensive applications such as Computer-Aided Design, video manipulation and heavy graphics applications.

3.2 Mobile Implementation

Mobile implementation of Ivy Bridge microarchitecture has the highest integrated graphics capability as compare to its desktop equivalent. Although, clock rate and cache memory is lower as compare to its desktop equivalent. Table 2 summarizes the implementation of mobile-based processor in terms of number of cores, Hyper-Threading support, Turbo Boost, cache memory, integrated graphics support and range of TDP. Since the concern of mobile implementation is the battery life, the TDP of the processor is lower than that of the desktop equivalent. Surveying the table information, some implementations have TDP as low as 7 watts only.

The mobile implementation of Celeron and Pentium is almost identical with the desktop implementation except for the lower TDP. As with desktop, both Celeron and Pentium are almost identical in the following aspects: dual-core configuration, no Hyper-threading and integrated graphics does not support 3D graphics. The only difference lies in the cache memory - Celeron has 2MB while Pentium has 3MB of cache memory. As with desktop, except for the mobility aspect, this configuration is suitable for usage related to common business productivity tools and internet access activity. Core i3 is a dual-core configuration with Hyper-Threading support. Its integrated graphics supports 3D graphics. This configuration is best suited for applications that require light to medium graphics applications. Unlike the desktop implementation, Core i5 is dual-core configuration and is almost identical to the mobile Core i3 except for the Turbo boost support. Core i7 has two configurations – dual-core and

quad-core version. The dual-core Core i7 is almost identical to mobile Core i5 except for a higher clock rate. I f cost is the overriding factor, Core i5 should be a better choice as compare to the dual-core Core i7. Finally, the quad-core Core i7 has both Hyper-threading and Turbo Boost support. As with the desktop configuration, this is best suited for graphics and processor intensive applications such as Computer Aided Design, video manipulation and heavy graphics applications.

Table 2: Summary of Mobile Implementation of Ivy Bridge Microarchitecture

Model	# of cores	Hyperthreading	Turbo Boost	Cache Memory	Integrated Graphics	TDP (w)
Celeron	2	No	No	2MB	HD Graphics	17, 35
Pentium	2	No	No	3MB	HD Graphics	10, 17, 35
Core i3	2	Yes	No	3MB	HD Graphics 4000	7,17,35
Core i5	2	Yes	Yes	3MB	HD Graphics 4000	7,17,35
Core i7	2	Yes	Yes	4MB	HD Graphics 4000	7,17, 25, 35
Core i7	4	Yes	Yes	8MB	HD Graphics 4000	35,45,55

3.3 Server Implementation

Currently, the only server implementation available is the Core i3-derived server known as Xeon E3. Server implementation of Ivy Bridge microarchitecture has the highest clock speed and the highest cache memory available. Integrated graphics is optimized and certified for professional applications such as Autodesk and Adobe. Table 3 summarizes the server implementation of in terms of number of cores, Hyper-Threading support, Turbo Boost, cache memory, integrated graphics support and range of TDP.

The Xeon E3 supports both dual-core and quad-core configurations. The Dual-core configuration supports hyper-threading support while the quad-core configuration supports with or without hyper-threading. Dual-core configuration has 3MB cache while quad-core configuration has 8MB Cache. TDP is the highest among implementation, with some model as high as 87 watts. Xeon-based processors support ECC memory, as such it is best suited for server setup. Besides cost factor, there should be no reason why server-based processor cannot be used as home based desktop. Besides being used as a server, it can also be used in a compute-intensive environment.

Table 3: Summary of Server Implementation of Ivy Bridge Microarchitecture

Model	# of cores	Hyperthreading	Turbo Boost	Cache Memory	Integrated Graphics	TDP (w)
Xeon E3	2, 4	Yes	Yes	3MB, 8MB	HD Graphics P4000	17, 45, 69, 77, 87

4. Conclusion

Ivy bridge-based processor having a clock rate of at least 2 GHz and couple this with architectural innovations equate to one having the power of a supercomputer in their desktop. But all will come to naught, if there is no software developed to take advantage of it. This paper provides an overview of the architectural innovations and the implementation that are currently available. The next step will be to for software developer to realize the innovations and to develop compiler, software and operating systems to take advantage of it.

5. Bibliography

Doyle, B., Boyanov, B. & Datta, S. (2003). Tri-Gate Fully-Depleted CMOS Transistors: Fabrication, Design and Layout. Digest of Technical Papers. 2003 Symposium on VLSI Technology. 133-134.

Greene, J. (2012). Intel Trusted Execution Technology (White Paper). 1-8, from http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf

Gueron, S. (2012). Intel Advanced Encryption Standard (AES) New Instruction Set (White paper). 1-93, from http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-aes-instructions-set

Intel (2008). Intel® Turbo Boost Technology in Intel Core Microarchitecture Based Processors. White Paper. 1-10, from http://www.intel.com.

Intel (2013). *Intel Tick Tock Model*. Retrieved February 1, 2013, from http://www.intel.com/content/www/us/en/silicon-innovations/intel-tick-tock-model-general.html

Levy, O.,Kumar, A.& Goel, P. (2008). Advanced Security Features of Intel vPro. *Intel Technology Journal*. 12(4). 229-238.

Marr, D., Binns, F. & Hill, D (2002). Hyperthreading Technology Architecture and Microarchitecture. *Intel Technology Journal*. 6(1). 4-15.

Neigher, G., Santoni, A.& Leung, F. (2006). Intel Virtualization Technology: Hardware Support for Efficient Processor Virtualization. *Intel Technology Journal*. 10(3). 167-178.