University of Moratuwa
Faculty of Engineering
Department of Electronic & Telecommunication Engineering

EN2031 - Fundamentals of Computer Organization and Design

Dissectors
Processor Dissection Report

Group Members	
Index No	**Name**
210015M	R.N.Abeywardhane
210031H	A.A.W.L.R.Amarasinghe
210705E	M.P.D.N.Wickramasingha

Abstract

This report presents an in-depth investigation and comparative analysis of two distinct processors, the Intel Xeon Platinum from the CISC (Complex Instruction Set Computer) architecture and the Cortex-M23 from the RISC (Reduced Instruction Set Computer) architecture. The study delves into various aspects of these processors, including their instruction set architecture, instruction set, micro-architecture, ALU (Arithmetic Logic Unit) functions, cache memory, memory interfacing, and timing related to memory.

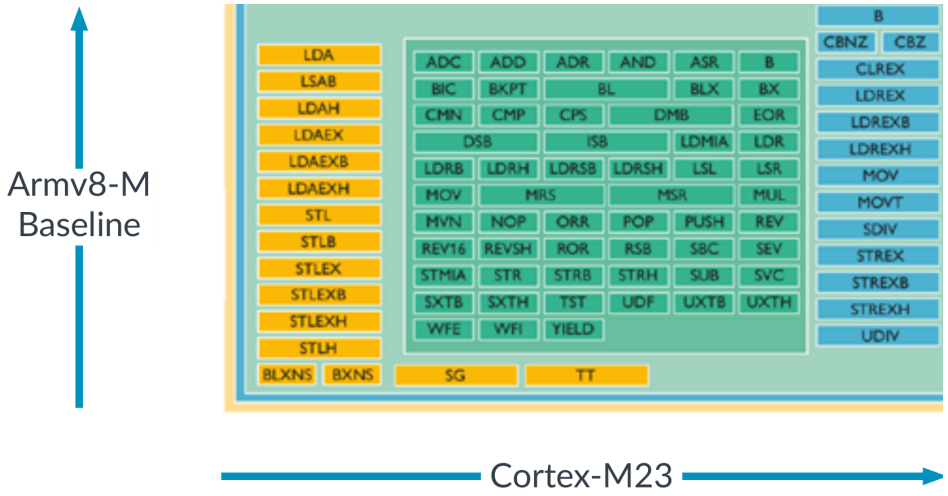
The Intel Xeon Platinum processor, a representative of the CISC architecture, is known for its high-performance capabilities and extensive instruction set. In contrast, the Cortex-M23 processor, adhering to the RISC architecture, is designed for energy-efficient and embedded applications with a focus on security.

ARM Cortex-M23 Processor

Instruction Set Architecture

Instruction Set

- The Cortex-M23 processor uses the ARMv8-M baseline architecture.
- It is a 32-bit RISC architecture with a focus on low-power and embedded applications.
- It is compatible with the Thumb-2 instruction set, which offers 32-bit performance and a high code density.
- To improve system security, the processor additionally offers an optional Security Extension.



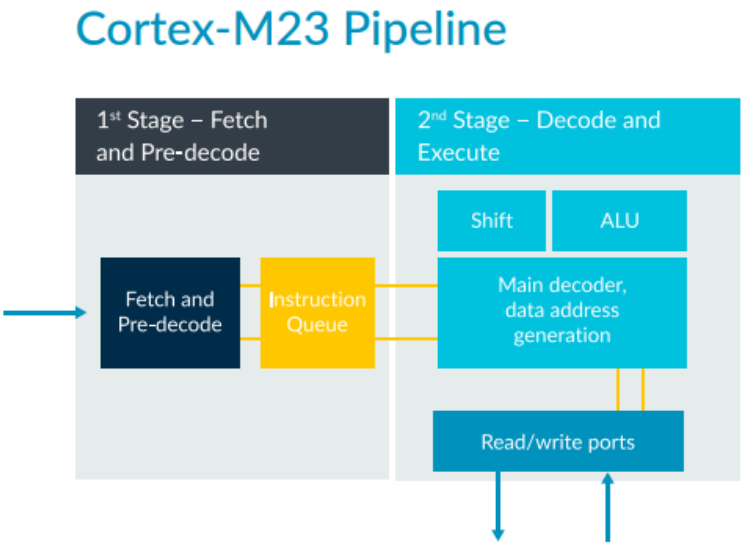
Instructional Classes and Formats

- The CPU supports a wide range of RISC architecture commands.
- It contains load/store instructions, arithmetic and logic instructions, branch instructions, and other instructions.
- The Thumb-2 instruction set's instruction format often contains a 16-bit encoding.
- It allows for efficient memory use.

Micro-Architecture

Data Path

- The Cortex-M23 processor has two stages of execution.
- It has an easy-to-use data path that supports load/store operations, ALU operations, and control flow instructions.
- The two-stage pipeline enables quick instruction execution.



Controller

- The processor's controller manages the execution of instructions and control signals within the pipeline.
- It decodes instructions and manages instruction fetch, execute, and write-back stages.

ALU Functions

- The processor includes an ALU (Arithmetic Logic Unit) that performs various arithmetic and logic operations as required by the instruction set.

Operation	Description	Assembler	Cycles
Logical	AND	ANDS <Rd>, <Rd>, <Rm>	1
	Exclusive OR	EORS <Rd>, <Rd>, <Rm>	1
	OR	ORRS <Rd>, <Rd>, <Rm>	1
	Bit clear	BICS <Rd>, <Rd>, <Rm>	1
	Move NOT	MVNS <Rd>, <Rm>	1
	AND test	TST <Rn>, <Rm>	1

- This comprises addition, subtraction, logical AND, OR, shifting, and other operations.

Cache Memory and Memory interface

- The Cortex-M23 processor does not have a built-in cache memory as it is designed for low-power and area-optimized embedded applications.
- It can also be equipped with optional Memory Protection Units (MPUs) for secure and non-secure memory regions, enabling access control.
- It allows single-cycle I/O access for peripherals that are strongly connected.
- It enables quick access to GPIO and other I/O devices.

Timing Related to Memory

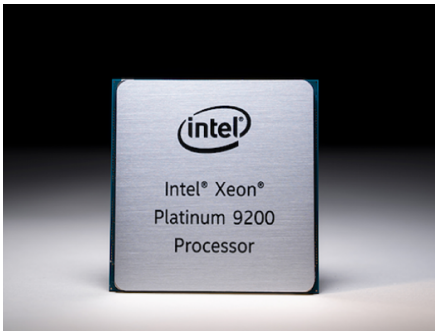
- The processor provides deterministic and fixed-latency interrupt handling, ensuring that time-critical applications can rely on consistent timing.
- The processor supports various memory protection mechanisms, such as MPU and SAU allowing for safe memory access and control.
- Wait For Interrupt (WFI) and Wait For Event (WFE) instructions provide low-power sleep modes on the processor.
- These are essential for embedded system power efficiency.

The Cortex-M23 CPU is made for highly embedded, energy-efficient applications that prioritize security. It interacts with external memory components, has a straightforward two-stage pipeline. It supports a variety of instructions from the Thumb-2 instruction set.

Applications with different security requirements can use it because of its adjustable features, which include memory protection units and the Security Extension. Its predictable interrupt handling and low-power modes further improve its viability for real-time and low-power applications.

Intel Xeon Platinum Processor

Intel Xeon Platinum processors come under the product collection of Intel Xeon scalable processors. These processors are intended for scalable servers and data center applications, therefore offering a wide range of performance options and advanced features. Within the Xeon family, the platinum processor is considered as the high end processor offering multiple cores(12,28,56…), higher clock speeds and advanced security, memory and I/O capabilities.

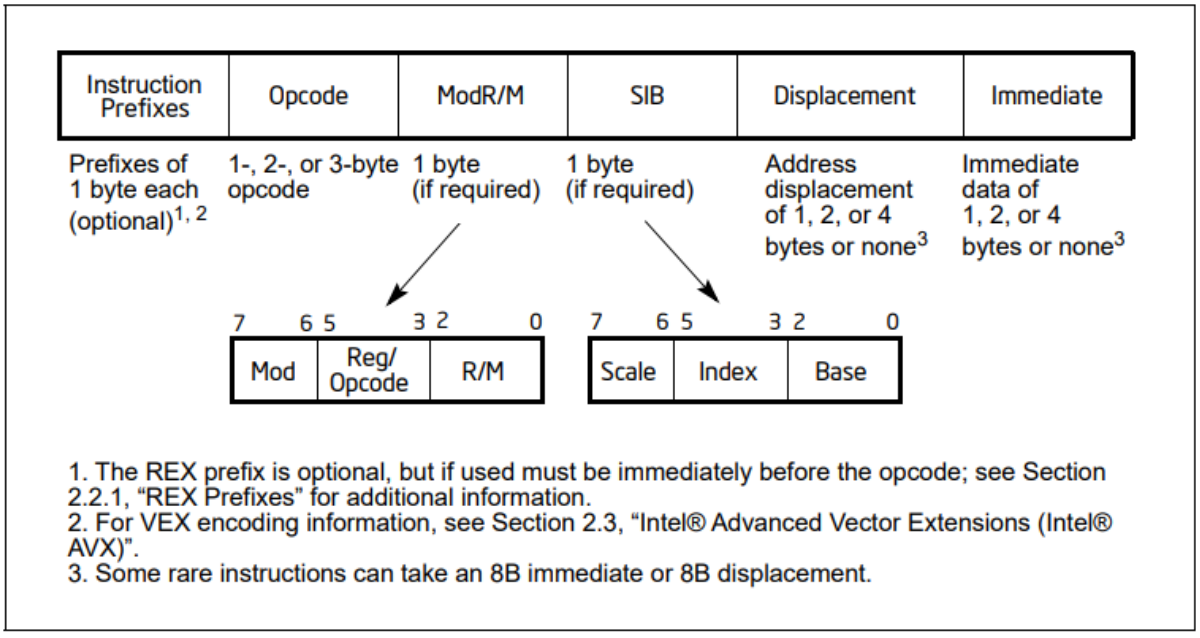


Instruction Set Architecture

Intel Xeon Platinum processors include the IA-32 and Intel® 64 instruction set architecture. The architecture encompasses both the 32bit IA-32 architecture and the 64bit Intel 64(x84-64) architecture. The instruction set is quite complex and has a large number of instructions due to the long history and evaluation of these architectures. The Xeon Platinum processor comes with four additional **instruction set extensions,** which are SSE(Streaming SIMD Extensions)4.2, Intel® AVX (Advanced Vector Extensions), Intel® AVX2, Intel® AVX-512.

Instruction Format

ISA primarily uses variable length instructions. The ISA common instruction format can be shown as below. ISA instruction encodings are subsets of the format shown below.



Intel 64 and IA-32 architectures instruction format

Basic Instruction classes available in intel64 IA-32 ISA

1. Arithmetic and Logic instructions

Opcode	Instruction	Op/ En	64-bit Mode	Compat/ Leg Mode	Description
04 ib	ADD AL, imm8	I	Valid	Valid	Add imm8 to AL.
05 iw	ADD AX, imm16	I	Valid	Valid	Add imm16 to AX.
05 id	ADD EAX, imm32	I	Valid	Valid	Add imm32 to EAX.

2. Data transfer instructions

Opcode	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
88 /r	MOV r/m8, r8	MR	Valid	Valid	Move r8 to r/m8.
REX + 88 /r	MOV r/m8[1], r8[1]	MR	Valid	N.E.	Move r8 to r/m8.
89 /r	MOV r/m16, r16	MR	Valid	Valid	Move r16 to r/m16.

3. Control transfer instructions

Opcode	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
EB cb	JMP rel8	D	Valid	Valid	Jump short, RIP = RIP + 8-bit displacement sign extended to 64-bits.
E9 cw	JMP rel16	D	N.S.	Valid	Jump near, relative, displacement relative to next instruction. Not supported in 64-bit mode.

4. Bit Manipulation Instructions

Opcode	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
A8 ib	TEST AL, imm8	I	Valid	Valid	AND imm8 with AL; set SF, ZF, PF according to result.
A9 iw	TEST AX, imm16	I	Valid	Valid	AND imm16 with AX; set SF, ZF, PF according to result.
A9 id	TEST EAX, imm32	I	Valid	Valid	AND imm32 with EAX; set SF, ZF, PF according to result.

5. String Instructions

Opcode	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
A6	CMPS *m8, m8*	ZO	Valid	Valid	For legacy mode, compare byte at address DS:(E)SI with byte at address ES:(E)DI; For 64-bit mode compare byte at address (R|E)SI to byte at address (R|E)DI. The status flags are set accordingly.

6. Floating Point instructions

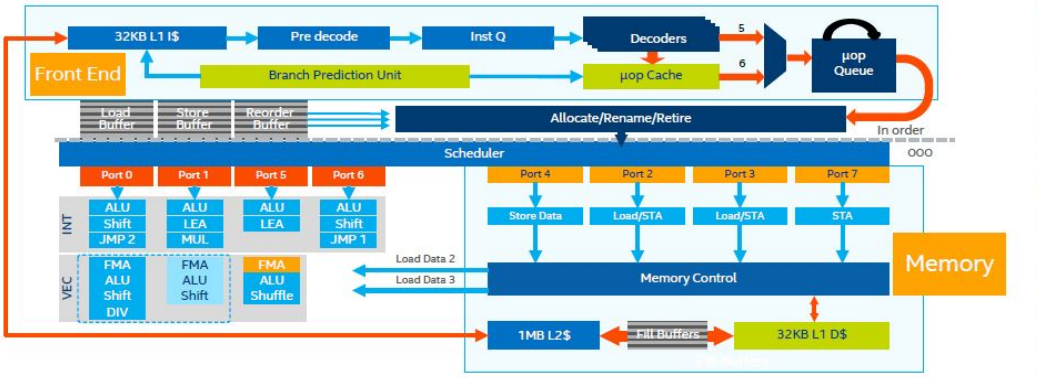
Opcode	Instruction	64-Bit Mode	Compat/ Leg Mode	Description
D8 /1	FMUL m32fp	Valid	Valid	Multiply ST(0) by m32fp and store result in ST(0).
DC /1	FMUL m64fp	Valid	Valid	Multiply ST(0) by m64fp and store result in ST(0).
D8 C8+i	FMUL ST(0), ST(i)	Valid	Valid	Multiply ST(0) by ST(i) and store result in ST(0).

7. SIMD(Single instruction, Multiple Data) instruction

Micro-Architecture

Micro-architecture is the physical realization of an ISA. This includes the design of instruction pipeline, caching, datapath etc. Intel Xeon Platinum processors use intel x86-64(intel 64) microarchitecture.

Data Path and Controller



ALU Functions

Intel 64 and IA-32 instructions support a wide range of ALU functions. Here are some common ALU functions performed.

- Addition, Subtraction, Division, Multiplication
- Bitwise Logic Operations
- Shifts and Rotates
- Comparison
- Increment and decrement
- Bit Manipulation
- Conditional Jump

Cache Memory and memory interfacing

1. Cache
    a. Intel Xeon platinum processors include L1, L2 and L3 caches. Additionally it includes two separate L1 caches for instructions(L1i) and data(L1d).
    b. Many Xeon Platinum processors include a larger, shared L3 cache that serves multiple cores. This L3 cache helps improve data sharing between cores and can significantly reduce memory latency for frequently accessed data.
2. Memory interfacing
    a. This processor supports multiple memory channels. And this supports DDR4-2666 (varies from processor to processor) memory type. Therefore maximum memory speed is 2666MHz(varies from processor to processor). And the processor can access 768GB(varies from processor to processor) of

memory which is required for data-intensive applications such as virtualization and large-scale databases.

Timing related to memory

- In order to address memory access latency the L1,L2 and L3 cache memories in the Intel Xeon Platinum processor have been carefully optimized. And they are continuously being optimized for newer versions as well.
- Intel Xeon platinum processors have high end memory access speeds(2666MHz, 3200MHz) because they are required for data-intensive applications such as virtualization and large-scale databases.
- Intel Xeon platinum processors come with ECC-Error Checking Code memory which adds an additional layer of error checking and correction, which can introduce a slight increase in memory access latency but ensures data integrity.
- Xeon Platinum processors typically support multiple memory channels. This allows concurrent memory access, increase in memory bandwidth and therefore increasing the overall system performance.

Comparison of ARM Cortex-M23 Processor & Intel Xeon Platinum

The difference between Intel Xeon Platinum and Cortex- M23 processors lies in their use cases, target applications, performance, power consumption, architecture, and many more things. But first, these two processors have been built for different purposes, so most of the features included in these two processors are so different.

Use Cases:

- Intel Xeon Platinum is designed for high-performance server usages and data center applications. It is used in a data center setting to manage difficult complicated workloads.
- Cortex-M23 is Designed for low-power, embedded, and IoT applications. It is generally employed in small, battery-operated devices and focuses primarily on energy efficiency. As a result, it requires less power than an Intel Xeon Platinum processor.

Microarchitecture:

- Because Intel Xeon Platinum is produced on advanced process nodes like 10nm and 14nm, it offers a high-performance, sophisticated out-of-order execution microarchitecture appropriate for server applications. designed to execute sophisticated instructions.
- ARM built the Cortex-M23, which has an energy-efficient microarchitecture and a straightforward in-order pipeline for the above mentioned applications. It is produced using older, low-power process nodes, such as 28nm and 40nm.

Instruction Set Architecture (ISA):

- Intel Platinum Processor uses the complex instruction set computing (CISC) architecture of the x86 ISA. It offers a rich set of complex instructions.
- Cortex M23 uses the reduced instruction set computing (RISC) architecture of the ARMv8-M ISA. designed to execute instructions more simply and power-efficiently.

Operating System Support:

- Because Intel Xeon Platinum is capable of handling complicated server applications, it is compatible with a wide range of operating systems, including virtualization platforms, Linux, and Windows Server.
- Real-time operating systems such as FreeRTOS or specially designed firmware for certain embedded applications are usually used to power Cortex-M23 devices.

Memory Hierarchy:

- Intel Xeon Platinum memory has high-speed memory interfaces, and supports large memory capacities, large multi-level caches including L1, L2, and sometimes L3 caches, designed to minimize memory latency and improve performance. It operates with faster memory access times and higher memory bandwidth.
- Cortex-M23 typically has a simplified memory hierarchy with smaller caches, often with just L1 caches or even no caches depending on the specific implementation. It is designed for smaller memory footprints and low-power consumption. It operates with slow memory access times but is optimized.

Power Consumption:

- Depending on the model, the Thermal Design Power of an Intel Xeon Platinum CPU can vary from 70W to over 400W. Because of its high performance and several cores, this processor uses more power.
- Extremely low power consumption typically in the micro- or milliwatt-range makes the Cortex-M23 perfect for battery-operated or energy-efficient products.

Task Allocation

Index No	Name	Contribution
210015M	R.N.Abeywardane	Intel Xeon Platinum Processor
210031H	A.A.W.A.R.Amarasinghe	ARM Cortex-M23 Processor
210705E	M.P.D.N.Wickramasinghe	Comparison of the two processors