Processor Hardware Bugs &

Open Source RISC-V Core (Ibex)

Jishnu Das, IIT-BHU
Varanasi, India
jishnuganeshdas@gmail.com

***Abstract* - This report discusses about the various processor hardware bugs, especially Pentium and AMD cores their history. It then discusses the open source RISC-V core Ibex, and gives a brief overview of the core.**

Keywords – RISC-V, Ibex , Hardware bugs.

I. Introduction

Some unpredictable or inaccurate processor behavior is termed a hardware bug, caused by design defects in the processor. They can have serious consequences such as processor crash, data corruption, I/O failure, wrong computation or a processor hang. RISC-V is an open standard instruction set architecture (ISA) based on established reduced instruction set computer principles, developed at UC-Berkeley. RISC-V is provided under royalty-free open-source licenses. Ibex is a RISC-V-based open-source CPU core developed by ETH Zurich and the University of Bologna and presently maintained by the lowRISC foundation. I have introduced some prominent processor bugs and Ibex core, discussing its features and highlighting its main features.

II. Processor Hardware Bugs

The conditions that cause hardware bug can be L1 cache miss (Defect1 of Table1), a snoop request (Defect2 of Table1), and an I/O interrupt with timing information (Defect3 of Table1). Pentium floating-point division [2] bug caused an error in the 9th or the 10th decimal digit, leading to $50 million in chip recalls. Pentium III [3] had a defect, so equipment manufacturers had to stop shipping Intel servers. Prefetch and cache problems in Pentium 4 [4] led to Intel disabling the prefetching in the core. Itanium 2 processors [5] and AMD Athlon 64 [6] have been hit with bugs causing incorrect results. IBM PPC 750GX [7] had circuit errors, causing IBM to reduce clock frequency from rated 1 GHz to 933 MHz. Speculative execution in processors causes security vulnerabilities like Spectre. Out-of-order processors trying to read arbitrary kernel-memory locations cause Meltdown, another security vulnerability.

Defect	Proc.	Defect Description
Defect1	IBM-G3	If the L1 suffers a miss while the power manager is on and the processor is flushing its L2, some L2 lines may get corrupted. [Signal condition: L1WAITMISS & DPM (dynamic power management) & L2FLUSH].
Defect2	P4	If a cache hits on modified data (HITM) while a snoop is going on, and there are pending requests to defer the transaction and to re-initialize the bus, then the snoop is dropped, leading to a deadlock. [Signal condition: SNOOP & HITM & DEFER & BUSINIT].
Defect3	Athl64	When an Adjust after Multiply (AAM) instruction is followed by another AAM within three instructions, or is preceded by a DIV instruction by up to 6 instructions, the ALU produces incorrect results.

Table 1 : Examples of Processor defects

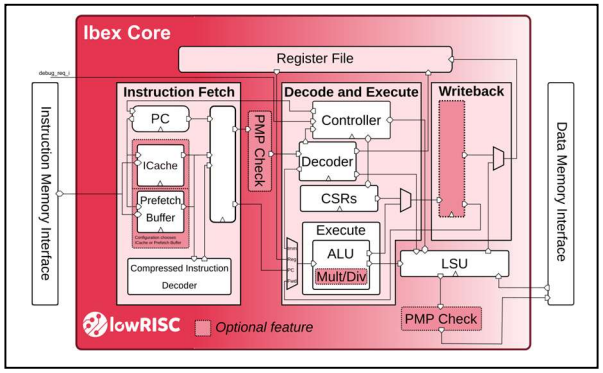

Figure 1 : A block diagram of Ibex core

III. Open Source RISC-V Core : 'Ibex'

Ibex is a 32-bit CPU core written in SystemVerilog, is easily parameterizable and is especially suited for embedded control applications. The block diagram is given in Fig. 1.It supports the Integer (I) or Embedded (E), Integer Multiplication and Division (M), Compressed (C), and B (Bit Manipulation) extensions. It has introduced several configurations - namely micro, small, maxperf and maxperf-pmp-bmful based on the architecture of the multiplier unit and various security features. Ibex is a 2-stage pipelined core but has an extension of adding a 3rd core, the Writeback stage. The two pipelined stages are - Instruction Fetch (IF) and the Instruction Decode and Execute (ID/EX) stage. The IF stage fetches instructions from memory via a prefetch buffer, capable of fetching 1 instruction per cycle if the instruction side memory system allows. The ID/EX stage decodes fetched instruction and immediately executes it, register read and write all occur in this stage. Multi-cycle instructions will stall this stage until they are complete.

References

[1] S. R. Sarangi, A. Tiwari and J. Torrellas, "Phoenix: Detecting and Recovering from Permanent Processor Design Bugs with Programmable Hardware," 2006 39th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO'06), Orlando, FL, USA, 2006, pp. 26-37, doi: 10.1109/MICRO.2006.41.

[2] T. R. Halfhill. The truth behind the Pentium bug : https://www.halfhill.com/byte/1995-3_truth.html.

[3] M. Hachman. Boot-up bug discovered in Intel's desktop Coppermine chips : http://www.my-esm.com , December 1999.

[4] M. Magee. Intel's hidden Xeon, Pentium 4 bugs. : http://www.theinquirer.net , August 2002.

[5] M. Hachman. Bug found in Intel's Itanium 2 could cause data loss. http://www.extremetech.com , May 2003.

[6] Inquirer Staff. AMD Opteron bug can cause incorrect results. http://www.theinquirer.net , June 2004.

[7] Inquirer Staff. IBM Power PC 1GHz chip only runs properly at 933MHz. http://www.theinquirer.net , August 2004.

[8] Ibex Reference Guide : https://ibex-core.readthedocs.io/en/latest/03_reference/index.html