

---

# MUCH SHORTER TITLE

---

SUBTITLE

## LAB REPORT

by

**FELIX BETKE**

3099892

**LENNART HEIN**

3012079

**MELINA HOFFMANN**

2824792

**JAN-NIKLAS SOHN**

3121407

submitted to

RHEINISCHE FRIEDRICH-WILHELMS-UNIVERSITÄT BONN

INSTITUT FÜR INFORMATIK IV

ARBEITSGRUPPE FÜR IT-SICHERHEIT

in degree course

COMPUTER SCIENCE (M.Sc.)

Supervisor: Prof. Dr. Michael Maier  
University of Bonn

Sponsor: Dr. Felix Jonathan Boes  
University of Bonn

Bonn, 31. March 2022

# ABSTRACT

TODO

# CONTENTS

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>2</b>	<b>BACKGROUND</b>	<b>3</b>
2.1	CPU . . . . .	3
2.2	Out-of-order execution . . . . .	3
2.3	Speculative execution . . . . .	5
2.4	Meltdown and Spectre . . . . .	5
2.4.1	Meltdown . . . . .	5
2.4.2	Spectre . . . . .	6
2.4.3	Mitigations . . . . .	6
<b>3</b>	<b>SPECIFICATION OF OUR TASK</b>	<b>7</b>
<b>4</b>	<b>CPU EMULATOR/ BACKEND</b>	<b>8</b>
4.1	CPU Components and our equivalents/ models (10-11 pages) . . . . .	8
4.1.1	CPU . . . . .	8
4.1.2	Instructions and Parser . . . . .	9
4.1.3	Data representation . . . . .	10
4.1.4	CPU frontend . . . . .	10
4.1.5	Memory . . . . .	13
4.1.6	Execution Engine . . . . .	14
4.2	Out of Order Execution (2 pages) . . . . .	15
4.3	Exception- and Fault-Handling (2-3 pages) . . . . .	15
4.3.1	Rollbacks . . . . .	16
4.3.2	Transient Execution Attacks . . . . .	17
4.4	ISA (2 pages) . . . . .	18
4.4.1	Default Instruction Set . . . . .	18
4.5	Config File . . . . .	21
4.5.1	Memory . . . . .	21
4.5.2	Cache . . . . .	22
4.5.3	Instruction Queue . . . . .	22
4.5.4	BPU . . . . .	22
4.5.5	Execution Engine . . . . .	22
4.5.6	UX . . . . .	23
<b>5</b>	<b>USER INTERFACE AND USAGE</b>	<b>24</b>
5.1	Purpose and Inspiration . . . . .	24
5.2	System Requirements and installation . . . . .	24

5.3	Running the program . . . . .	25
<b>6</b>	<b>EVALUATION</b>	<b>26</b>
<b>7</b>	<b>CONCLUSION</b>	<b>27</b>
7.1	Limitations . . . . .	27
7.2	Future Work . . . . .	27
<b>8</b>	<b>CATCHY LAB TITLE</b>	<b>28</b>
8.1	Abstract . . . . .	28
8.2	Introduction (1 page) . . . . .	28
8.3	Brief Theoretical Background (2-3 pages) . . . . .	28
8.4	maybe Specification of the task (1 page) . . . . .	29
8.5	CPU emulator/ backend (17-18 pages) . . . . .	30
8.6	Our Visualisation and Usage/ Frontend (10 pages) . . . . .	32
8.7	Demonstration/ evaluation (7 pages) . . . . .	33
8.8	Conclusion (1 Page) . . . . .	34
	<b>REFERENCES</b>	<b>35</b>
	<b>LIST OF FIGURES</b>	<b>36</b>

# 1 INTRODUCTION

*Felix Betke*

As an advancement over older processors, modern Intel CPUs implement a number of optimization techniques that increase their efficiency. One of which is the concept of out-of-order execution, which takes advantage of the mutual independence of instructions that would normally be executed sequentially. A second optimization technique is called speculative execution and involves the prediction of whether or not a given branch is taken. With either technique, the CPU might encounter cases where the current CPU state must be rolled back to a previous one to ensure correct execution. For out-of-order execution this happens when an instruction raises an exception (e.g. accessing inaccessible memory). For speculative execution, this happens when a branch is mispredicted. An initiated rollback allows some instructions that are currently being executed (in-flight) to continue execution for a short amount of time.

Even though rollbacks are meant to make sure in-flight instructions do not cause any lasting side effects on the microarchitectural state of the CPU, it was discovered that they can affect the contents of caches and other buffers. The disclosure of both Spectre and Meltdown in early 2018 introduced a whole family of vulnerabilities that take advantage of both out-of-order and speculative execution to leak secrets over the processor's caches, or temporarily alter the program flow of other processes. And while the performance losses introduced by software and hardware mitigations are measurable, neither family of vulnerabilities can be exploited as originally presented on a fully patched system. As a result, however, the process of trying to exploit one of the vulnerabilities for the sake of learning how they work in detail can be challenging. Apart from the software, which may be obtained by installing an older version of an operating system that does not implement any mitigations, one must also make sure their CPU is affected by the vulnerabilities and has not yet received any relevant microcode updates from Intel. Often times, this means that a user's personal computer does not meet these requirements.

We design and implement a graphical CPU emulator that supports single-step out-of-order and speculative execution and is vulnerable to select variants of Spectre and Meltdown. While it is a simplification in comparison to real hardware, the emulator allows its users to gain a better understanding of how exactly the two vulnerabilities work and can be exploited. Furthermore, the user may experiment with (ineffective) mitigations or implement their own microcode-programs that are executed once rollbacks are completed. We supply example programs that can be run by the emulator and serve both as an entry point for the user as well as the basis of our evaluation.

Firstly, chapter 2 briefly gives an overview of relevant components of vulnerable Intel CPUs, presents the concepts of out-of-order and speculative execution in greater detail, and introduces both Meltdown and Spectre to which the resulting emulator is designed to be vulnerable. Secondly, chapter 3 further describes the target audience of the emulator and to which variants of the vulnerabilities the emulator is vulnerable, while chapter 4 documents the implementation of the emulator by

describing each main component and explaining how rollbacks are implemented. Additionally, it contains an overview of the set of ISA instructions available to the user. Furthermore, chapter 5 explores the graphical user interface by defining the goals its design is supposed to accomplish and documenting design choices and important features. Chapter 6 provides a demonstration of the emulator, which includes example programs, and determines how effective the implemented mitigations are. Finally, chapter 7 summarizes the other chapters, briefly reflects on how valuable the emulator might be to our target audience, and gives ideas for future improvements.

## 2 BACKGROUND

*Felix Betke*

This chapter briefly covers the theoretical background needed to use the presented emulator and continue its development. The reader is assumed to have an understanding of elementary CPU concepts, such as pipelining and caching.

### 2.1 CPU

*Felix Betke*

A CPU consists of a frontend, an execution engine, and a memory subsystem. As per Intel's Skylake architecture [Wik], the frontend fetches the instructions, maintains a queue of instructions that are to be executed, and decodes them into simpler microinstructions, which are then communicated to the execution engine. Additionally, it is responsible for the branch prediction (see sec. 2.3). [Gru20]

The execution engine consists of multiple sets of execution units, each set being responsible for a specific type of microinstruction, such as loads, stores, or arithmetic. Further, the scheduler allows the execution units to work on independent instructions in parallel, while the reorder buffer makes sure that instructions retire in the correct order. A common data bus (CDB) connects the reorder buffer, scheduler, and execution units. Its purpose is further described in sec. 2.2. [Gru20]

Lastly, the memory subsystem handles all memory accesses of the execution units by maintaining caches and ensuring data is fetched from lower level caches or DRAM if needed [Gru20]. Most importantly, requests to data that is present in the caches is served faster than if it were not.

A visualization of the aforementioned components can be found in fig. 1.

### 2.2 OUT-OF-ORDER EXECUTION

*Felix Betke*

As the name implies, out-of-order execution refers to the idea of executing instructions in a different order than the one in which they are given [Gru20]. With multiple execution units that run in parallel (as described in sec. 2.1), CPUs can take advantage of mutually independent instructions and execute them at the same time.

The basic realization of this concept is provided by Tomasulo's algorithm [Tom67]. It introduces two components, the first of which is the reservation station, which collects the operands of instructions until they are ready to be executed by the execution units. Crucially, the corresponding execution units do not need to wait until all operands are present and can instead compute other instructions. The second component of Tomasulo's algorithm is the Common Data Bus (CDB), which connects all reservation stations and execution units. Whenever a result is computed by an execution unit, the result is broadcast onto the CDB and thus made available to all reservation stations that are



**FIGURE 1:** Simplified overview an Intel Skylake CPU [Gru20, fig. 2.1]. For the memory subsystem, detailed knowledge of the load and store buffers, as well as the TLBs, is not required. The same applies to the allocation queue of the frontend.



waiting for it. This important step ensures that results are not written to registers first, just to be read again by other instructions that need them as operands.

Initially, according to Tomasulo, each set of execution units needed its own reservation station, however, more modern implementations by Intel use a single unified reservation station, called scheduler, that handles all types of instructions, rather than just one [Tom67] [Wik] [Gru20]. This can also be seen in fig. 1.

## 2.3 SPECULATIVE EXECUTION

*Felix Betke*

Speculative execution allows a CPU to predict the outcome of comparisons and other branch instructions. This prevents stalls when waiting for the instruction that determines which branch is taken to finish. Similarly to out-of-order execution, rollbacks are needed in some cases. However, in addition to exceptions, they also occur if a branch was mispredicted. [Gru20]

To predict the outcome of branch instructions, CPUs include a branch prediction unit (BPU) [Gru20]. While available in different configurations, many modern CPUs record the most recent outcomes of a branch with a counter [Gru20] that is either incremented if the branch is taken, or decremented.

## 2.4 MELTDOWN AND SPECTRE

*Felix Betke*

Meltdown [Lip+18] and Spectre [Koc+19] abuse out-of-order and speculative execution to leak data from memory addresses that are normally inaccessible to the attacker over the caches of the CPU.

### 2.4.1 MELTDOWN

On a high level, Meltdown [Lip+18] works by forcing exceptions when reading data inaccessible to the attacker and transiently encoding this data into the cache to retrieve it once the rollback has completed. What enables Meltdown is a small time window between an invalid memory access and the raising of an exception [Lip+18].

The Meltdown-US-L1 variant of Meltdown [Lip+18] to which the presented emulator is vulnerable works by accessing a memory address for which the attacker has no permission. Firstly, the attacker allocates an oracle array and ensures none of its entries are present in the cache. Upon loading the contents of the inaccessible memory location into a register, the attacker uses the value to access the array at a specific offset. When the rollback caused by the access violation has completed, the attacker measures the access time to each of the array entries to determine which one has been accessed. It is important that the data to be stolen is currently cached. While there are numerous other variants of Meltdown that differ from the basic variant mainly by how they force an exception and from which microarchitectural buffer they leak data, these types of attacks are out of scope.

### 2.4.2 SPECTRE

Spectre [Koc+19], on the other hand, relies on the CPU mispredicting a branch and transiently executing instructions that are not part of the correct execution path. This misprediction in a victim process can be induced by maliciously configuring the BPU (sec. 2.3). Depending on the instructions that are wrongfully executed by the victim, traces may later be found in the processor’s cache. Similarly to Meltdown, different variants of Spectre exist. The presented emulator is vulnerable to variant 1 of Spectre, which takes advantage of the CPU mispredicting the outcome of comparison instructions.

### 2.4.3 MITIGATIONS

The mitigations for Meltdown are available in both software and hardware, some of which are implemented in the emulator to allow users to experiment with them and determine their effectiveness. A first, rather simple, mitigation for Meltdown is to disable out-of-order execution [Lip+18], which would completely prevent an attacker from encoding the normally inaccessible data into the cache. Later revisions of Intel’s architectures introduced further mitigations. Although undocumented by Intel, researchers suspect the processor still performs the illegal read, but zeros out the data that is given to dependent instructions before raising an exception [Can+20]. The emulator implements this mitigation, which may be enabled by the user. Other mitigations deployed by operating systems, such as KTPI (or KAISER) [Lip+18], are highly effective, but out of scope, as there exists no operating system.

Unlike Meltdown, Spectre appears to be a design flaw. While one might argue that transiently computing on real values after it is already known an exception will occur is a bug, the behavior abused by Spectre is a direct consequence of speculative execution (sec. 2.3). As a result, an effective yet questionable mitigation is to simply disable speculative execution [Koc+19]. Alternatively, Intel recommends potential victim’s of Spectre v1 to use an “lfence” instruction where appropriate, which ensures prior load instructions retire before continuing, thus effectively disabling speculative execution for certain parts of an application [Int18]. A fence instruction is provided as part of the emulator’s instruction set.

An additional mitigation that works against both Meltdown and Spectre is to flush the entire cache after a rollback. While highly inefficient, it does prevent the retrieval of otherwise inaccessible data after the transient execution phase of the attacks. This mitigation can be realized using the emulator by a sequence of instructions (microprogram) that are executed after each rollback.

### 3 SPECIFICATION OF OUR TASK

todo

## 4 CPU EMULATOR/ BACKEND

In this chapter, we introduce the backend of our emulator program. It contains the elements of our program that emulate actual CPU components. Our emulator is based on information about modern real life CPUs, especially the x86 Intel Skylake architecture [Wik].

In our program, we model the distinct components of a real life CPU with a modular setup making use of the object oriented functionalities of Python3. Breaking up the source code into individual CPU components also makes it easier to understand and maintain. Additionally, we have made simplifications and modifications in comparison to a real life CPU, so the emulator is as clear and easy to understand as possible while still implementing an actual out of order execution and providing the necessary functionality for Meltdown and Spectre attacks.

In this chapter we firstly introduce the components of our CPU emulator, how they work (together) and which part of a real life CPU they emulate sec. 4.1. Then we explain how our emulator provides out of order execution and how it may differ from the general Tomasulo algorithm introduced in sec. 2.2. Subsequently, we show how we implemented rollbacks and exception handling, especially with regards to how our implementation allows for Meltdown and Spectre attacks sec. 4.3. Then we give an overview over our instruction set architecture sec. 4.4. Lastly we show how our emulator can be adapted for different demonstrations and attacks without changing the source code via a config file sec. 4.5.

### 4.1 CPU COMPONENTS AND OUR EQUIVALENTS/ MODELS (10-11 PAGES)

todo

#### 4.1.1 CPU

Felix Betke

The primary purpose of the *CPU* class is to allow all other components to work together. That is, the CPU initializes all other components and provides interfaces to their functions. Most importantly, the *CPU* provides a *tick* function that is called each cycle and does the following: instructions from the instruction queue are fetched from the frontend and forwarded to the execution engine, until either no more slots in the unified reservation station are available, or the instruction queue is empty. It then calls the *tick* function of the execution engine. In case of a rollback, the instruction queue maintained by the frontend is flushed. If configured, a  $\mu$ -program is executed prior to resuming execution. If the rollback was caused by a faulting load instruction, execution is resumed at the next instruction (as described in sec. 4.3). In case a branch was mispredicted, the frontend is notified and refills the instruction queue accordingly. If configured, corresponding microprograms are sent to the instruction queue. Lastly, a snapshot of the current state of the CPU is taken. To provide the UI

with useful information to display to the users, the *tick* function returns an instance of a *CPUStatus* class that contains a boolean indicating if the program has terminated, whether an exception has raised a fault, and a list of instructions that have been issued during this tick.

Other functions exist to load programs from files and initialize the frontend and execution engine accordingly. Further, references to each component are exposed by getter functions to allow the UI to visualize their current state.

The second purpose of the *CPU* class is to provide the snapshot functionality, which allows a user of the emulator to step back to previous cycles. The snapshot list is simply a list that grows at each cycles, where each entry is a deepcopy of the *CPU* instance. To simply be able to deepcopy the *CPU* class, the snapshot list is held separately and not one of its members. Instead, the *CPU* class, and therefore each snapshot, maintains an index to its own entry in the snapshot list. This reference makes traversing the snapshot list one step at a time easier. Due to the low complexity of the programs we expect our users to run, at the moment, no maximum number of available snapshots is configured. To restore snapshots, a static *restore\_snapshot* function exists in the *CPU* class. Crucially, this function returns the deepcopy of an entry of the snapshot list relative to the value of *\_snapshot\_index* of the current instance. This allows users to step back and forth between snapshots. However, manipulating a restored snapshot by calling the *tick* function, for example, discards all more recent snapshots.

#### 4.1.2 INSTRUCTIONS AND PARSER

The general instruction format used by our instruction set is the instruction mnemonic followed by a comma-separated list of instruction operands, as is common in assembly languages. In our instruction set, the instruction mnemonic already determines the exact instruction, including the number and types of its operands. This greatly simplifies parsing. There are three different types of operands in our instruction set:

- *Register* operands specify a register the instruction should operate on. They are introduced by an *r* followed by the decimal register number.
- *Immediate* operands specify a 16-bit immediate value used by the instruction. They take on the usual decimal or hexadecimal form for integer literals, optionally prefixed by a sign.
- *Label* operands specify the destination of a branch instruction. The label referenced has to be defined somewhere in the assembly file, using the label name followed by a colon.

Our instruction set, including all concrete instructions and their semantics, are covered in detail in sec. 4.4. We do not support reading or writing instruction memory. Thus, instructions have no defined in-memory representation.

The instructions of our instruction set are further distinguished based on their *instruction category*. The possible instruction categories are *register-register* instructions, *register-immediate* instructions, *branch* instructions, *load* instructions, *store* instructions, *flush* instructions, and three special categories for the individual *rdtsc*, *fence*, and *flushall* instructions. Our implementation uses *InstructionKind* objects to model the individual instructions of our instruction set. Each such object defines an instruction by its mnemonic, the number and types of its operands, the instruction category it belongs

to, as well as some category-specific information. For register-register and register-immediate instructions, this is the concrete computation performed. For branch instructions, this is the branch condition. And for load and store instructions, this is the width of the memory access.

Grouping similar instructions into categories allows the Execution Engine to handle executed instructions based solely on their instruction category; the Execution Engine does not need to handle every concrete instruction separately. New instructions that match an existing instruction category can be added easily by users, without having to modify the Execution Engine. The mechanisms involved in the Execution Engine are described in detail in sec. 4.1.6.

Our parser is based on an abstract description of the instructions of our instruction set. This description is limited to the instruction's mnemonic and the number and types of its operands. The parser handles all instructions uniformly and has no information about the semantics of any instruction. Operation of the parser is divided into two passes over the input file. The first pass exclusively handles label definitions, which consist of a label name followed by a colon. The parser maintains an internal directory of labels, associating each label name with the immediately following instruction. The second pass parses the actual program, with one instruction per line. After determining the mnemonic and looking up the corresponding instruction, it parses all operands, subject to the rules for operand types described above. Having identified the instruction and parsed all operands, the parser builds an `Instruction` object, which models a concrete instruction in program code. Every `Instruction` object references the `InstructionKind` object of the instruction it represents, and contains the concrete values of all operands. During both passes, the parser skips over any comments, which are lines starting with two slashes (`//`). Performing two passes in this way allows labels to be used both before and after their definition.

### 4.1.3 DATA REPRESENTATION

The data representation used throughout our CPU is based on 16-bit values, called *words*. All CPU registers store a word. All instructions operate on words, and all immediate operands of instructions are words. A minor exception to this are the *store byte* and *load byte* instructions, that truncate a word to an 8-bit byte and zero-extend an 8-bit byte to a word, respectively. See sec. 4.4 for a detailed description of memory operations. Words are interpreted either as unsigned or two's complement signed integer values. However, the distinction between unsigned and signed values is only relevant for the comparison operations used by branch instructions. See sec. 4.4 for a detailed description of branch instructions.

Since our memory model is based on 8-bit *bytes*, words are separated into two 8-bit values when representing them in memory. The two individual bytes of words are stored in memory in little endian order, i.e. the least-significant byte is stored at the lowest memory address. For a detailed description of the mechanics involved in memory operations, see sec. 4.1.5.

### 4.1.4 CPU FRONTEND

In modern CPUs, the CPU frontend provides an interface between code and execution engine. It contains components to fetch and decode the instructions from a cache and supply them to the CPU

in a queue. It is also involved in speculative execution by predicting the result of conditional jumps and supplying instructions to the execution engine accordingly. [Wik]

In our emulator we simplify the components and procedures. We also separate the branch prediction unit (BPU), that manages and predicts the results of conditional jumps, from the rest of the frontend. This makes our code easier to understand and makes potential future changes or additions to the BPU more convenient.

### BRANCH PREDICTION UNIT (BPU)

The BPU of modern CPUs plays a vital role in enabling speculative execution. It stores information about previously executed conditional branch instructions and predicts the outcome of future branch instructions accordingly. The rest of the CPU can then speculatively execute further instructions at an address based on the predicted outcome of the branch instead of stalling until the branch instruction is processed by the execution engine. If the prediction was false, a rollback is performed on the speculatively executed instruction sec. 4.3. If the prediction was true, the execution is overall faster than without speculative execution.

Detailed information about the BPU of our modern base CPU is not widely available [Wik]. In general, the Gshare BPU of modern CPU consists of multiple components. It contains a branch target buffer (BTB) that holds the predicted target addresses for conditional branches. It also uses a pattern history table (PTH), that can be implemented as a 2-bit-saturating counter, and a global history register (GHT) to predict whether a conditional jump will be taken or not. [SCA]

In our emulator, we forgo the BTB entirely. Real life CPUs benefit from stored target addresses since they have to expensively decode each branch instruction before they can work with the target address [Wik]. In our emulator, the parser decodes the jump labels from the assembler code and directly provides them to the frontend, so storing them in an additional buffer is unnecessary sec. 4.1.2. We further forgo the GHT because it is not strictly necessary to execute a Meltdown or Spectre attack. Additionally, our emulator and its behaviour are easier to understand and predict without it, which is important when implementing microarchitectural attacks for didactic purposes. The BPU of our emulator only consists of a PHT, which is enough for simple Spectre-PHT variants [reference-eval-spectre].

The default PHT used in our emulator holds an array called counter of configurable length to store several predictions. The instructions are assigned to different prediction slots by the last bits of their index in the instruction list. For each of the slots, the prediction can take the four different values from zero to three, where zero and one indicate that the branch will probably not be taken and two and three indicate that the branch is likely to be taken.

The source code for our emulator also contains a more simple BPU with only one slot for all instructions. Since the number of slots in the default BPU is freely configurable by the user, this simple BPU is now obsolete.

When the BPU is updated with an actual branch outcome from the execution engine, the prediction in the PHT is updated by a 2-bit counter. This means, that if the prediction was right, the counter remains at or updates to zero (strongly not taken) or three (strongly taken) respectively. If the prediction counter is at zero but the branch is actually taken, the counter is updated to one (weakly

not taken). If it is at a one when the branch is taken, it is directly updated to three. The counter behaves similarly when it has the value two or three and the branch is not actually taken.

## INSTRUCTION QUEUE

In a real life CPU, the overall purpose of the frontend is to provide the execution unit with a steady stream of instructions so the backend is busy as much as possible and therefore efficient. In a modern x86 CPU, the frontend has to fetch x86 macro-instructions from a cache and decode, optimize and queue them repeatedly to provide the backend with a queue of  $\mu$ -instructions ready for issuing in the execution engine. [Wik]

In our emulator, except for the BPU, the functionality of the CPU frontend is bundled in frontend.py. It is significantly simplified compared to a real life x86 CPU, especially since we use only one type of instructions instead of distinguishing between macro- and  $\mu$ -instructions sec. 4.4. They are already provided as a list by the parser, which renders the decoding and optimization steps in the frontend unnecessary sec. 4.1.2.

The main task of our frontend is to act as interface between instruction list provided by the parser and the execution engine sec. 4.1.6. It provides and manages the instruction queue, which holds the instructions that the execution engine should issue next. Conditional branches with their respective BPU predictions are taken into account when filling the queue. This enables speculative execution which is needed for Spectre attacks sec. 2.4.

The central component of our emulated frontend is the instruction queue. In our version, it does not only hold the instructions themselves, but also for every instruction in the queue, the respective index in the instruction list is stored. For branch instructions it also holds the respective branch prediction from the BPU at the time that the instruction was added to the queue. This additional information is needed by the execution engine to handle mispredictions and other exceptions sec. 4.1.6.

When adding instructions to the queue, the frontend selects them from the instruction list, adds the additional information for the execution engine and places them into the instruction queue until the queue's maximum capacity is reached. The frontend maintains a program counter (pc) that points to the next instruction in the list that should be added to the queue. When the frontend encounters a branch instruction and the branch is predicted to be taken, the frontend adjusts the pc to resume adding instructions at the branch target. If a branch was mispredicted, the frontend provides a special function to reset the pc and refill the instruction queue with the correct instructions.

Additionally, the frontend provides a function to add a  $\mu$ -program to the queue. It consists of a list of instructions separate from the parser instruction list. When adding the  $\mu$ -program to the queue, the frontend may exceed the maximum queue capacity. This functionality can be used to implement mitigations against microarchitectural attacks, e.g. by adding a  $\mu$ -program as part of the exception handling after an illegal load [reference-eval-mitigations].

The frontend provides interfaces to both read and take instructions from the queue. It also provides a function that combines taking an instruction from the queue and refilling it, . Additionally, the frontend has an interface for flushing the whole queue at once without taking the instructions from the queue. This can be used when demonstrating mitigations against microarchitectural attacks [reference-eval-mitigations].



The frontend provides further basic interfaces, e.g. for reading the size the instruction queue and reading and setting the pc. These are used by the other components during regular execution, e.g. when issuing instructions to the execution engine, but also to reset the queue to a certain point in the program after an exception has occurred sec. 4.3. Since our emulator only executes one program at a time, the other components can check via another interface whether the frontend has reached the end of the program.

#### 4.1.5 MEMORY

Felix Betke

Memory is primarily managed by the Memory Subsystem (MS). As a simplification over an MS as it is assumed to be used by Intel's Skylake architecture [Wik], our version maintains only a single cache, no load, store, or fill buffers. Further, it maintains the main memory directly. These simplifications are possible, since our objective is to allow users to learn about Meltdown-US-L1 and Spectre v1, none of which rely on any of the MS components we removed in our version. Further, the fact that our CPU consists of a single core only, the MS can directly use the main memory.

To represent the main memory, the class contains a simple array that has  $2^{\text{WordWidth}}$  entries, half of which are initialized to 0. Since our emulator does not run an operating system and therefore does not support paging, a different method is needed to model a page fault that allows attackers to enter the transient execution phase of the Meltdown-US-L1 attack (as explained in sec. 2.4). To solve this, we have decided to make the upper half of the address space (32768 to 65535, by default) inaccessible. Any reads to an address within the upper half result in a fault which causes a rollback a couple of cycles later. Naturally, the value written to the inaccessible addresses is 0x42.

To handle memory accesses, *read\_byte*, *read\_word*, *write\_byte*, and *write\_word* functions are available, which do as their names suggest, optionally without any cache side effects. Each function returns a *MemResult* instance, which contains the data, the number of cycles this operation takes, whether the operation should raise a fault (i.e. memory address is inaccessible), and, if so, in how many cycles this happen. For *write* operations, only the variables regarding faults are of relevance (see sec. 4.1.6).

Other functions that allow the UI to visualize the memory contents are provided. More specifically, *is\_addr\_cached* and *is\_illegal\_access* return whether an address is currently cached and whether a memory access to a specific address would raise a fault, respectively. Further, the MS includes functions that handle the cache management, such as *load\_line*, *flush\_line*, and *flush\_all*.

#### MELTDOWN MITIGATION

As explained in sec. 2.4.3, one of the mitigations implemented by Intel is believed to zero out data illegally read during transient execution. To model this, both the *read\_byte* functions still perform the read operation, but provide 0 as the data in the returned *MemResult*, if the mitigation is enabled. As of now, the read operation still changes the cache, but since only the contents of the inaccessible memory address are cached and not the corresponding oracle entry of the attacker, the mitigation still works. The reason for this is that we believe a consequence of the CPU still performing the illegal read operation but zeroing out the result should have side effects on the cache. If desired, this behavior can be changed easily in the *read\_byte* functions.

## CACHE

To enable attackers to encode transiently read data, the MS maintains a single cache. The number of sets, ways, and entries per line can be configured via the config file (see sec. 4.5). The base *Cache* class firstly initializes all cache sets as an array with each entry holding an array of instances of the *CacheLine* class. There are functions that allow components using the cache to *read*, *write*, and *flush* data given an address and data, if applicable. The *parse\_addr* can be used to obtain the index, tag, and offset of an address. Lastly, the *Cache* class includes functions that allow the UI to visualize its state (*get\_num\_sets*, *get\_num\_lines*, *get\_line\_size*, and *get\_cache\_dump*). Note that the base *Cache* class cannot be used directly, as it does not implement the *\_apply\_replacement\_policy* function.

The *CacheLine* class holds an integer array for the data, a tag, and its own size. Further, functions to *read*, *write*, and *flush* are provided. Lastly, there are functions that set the tag (*set\_tag*) and return whether or not the cache line is currently in use by checking if the tag is set. Contrary to the *Cache* class, the *CacheLine* class can be used directly.

By default, there are three available cache replacement policies that determine which cache line is evicted from a full cache set in case new data should be added. All are implemented by extending the base *Cache* and *CacheLine* classes accordingly. The first policy is the random replacement policy (RR) whose implementation can be found in the *CacheRR* class. This policy simply picks a cache line at random for eviction. Even though the policy introduces noise into the side channel, users may experiment with it for their cache attacks, if they so choose (see sec. 4.5).

The second cache replacement policy is the least-recently-used policy (LRU). By this policy, the cache line to be evicted from a full cache set should be the one whose most recent access was the longest time ago. To achieve this functionality, a new *CacheLineLRU* class updates a *lru\_timestamp* variable each time the *read* or *write* functions are called. This variable is then used by the new *CacheLRU* class in its implementation of the *\_apply\_replacement\_policy* function.

Lastly, the third cache replacement policy is the first-in-first-out (FIFO). In case of a full cache set, this policy picks the cache line that was first populated with data and flushes it. The classes *CacheFIFO* and *CacheLineFIFO* implement the required functions by using a *first\_write* variable.

Even though more complex replacement policies exist, the exact way in which they work is often undocumented [VKM19]. However, we believe our chosen policies are sufficient to understand Meltdown, Spectre, and most cache timing attacks, such as Flush+Reload. New cache replacement policies can easily be added by defining the desired behavior in new cache and cache line classes that inherit from *Cache* and *\_Cache\_Line*, respectively. Further, the constructor of the MS needs to be adjusted to account for the existence of the new policy.

### 4.1.6 EXECUTION ENGINE

The Execution Engine is the central component of a CPU. It is the component responsible for actually performing computations, by executing the stream of instructions provided by the frontend. Just like the Execution Engine of modern x86 processors, our Execution Engine executes instructions out-of-order, i.e. not necessarily in the order of the incoming instruction stream. In order to preserve

the semantics of the program, any data dependencies have to be honored during reordering. For this we use a modified version of Tomasulo's Algorithm, that is described in detail in sec. 4.2.

The Execution Engine contains the Reservation Station with a fixed number of instruction slots. Each slot contains an instruction that is currently being executed. We call such instructions *in-flight*. Our Reservation Station is unified, i.e. each slot can contain any kind of instruction. The same is often found in modern CPUs. The slots of our Reservation Station are also used to model Load Buffers and Store Buffers; the specifics of executing memory accesses are handled by the slots directly instead of separate components. We also have no concept of Execution Units that instructions need to be dispatched to, which means that instructions' ability to execute concurrently is only limited by the number of available slots.

All instructions pass through two phases during execution: In the first phase the instruction is said to be *executing*. It waits for any source operands to become available and computes its result. Once the result is computed, it is made available to waiting instructions, and the instruction transitions to the second phase.

In the second phase the instruction is said to be *retiring*. It determines if it causes a *fault*, which in this case means a *microarchitectural* fault. These can be architecturally visible faults like memory protection violations or architecturally invisible faults like branch mispredictions; both are handled the same way in the Execution Engine. Once the instruction finishes retiring its slot becomes available again and may be used to execute a new instruction.

TODO: Describe concrete execution/retirement behavior for each instruction category?

In each clock cycle only a single instruction may finish execution or retirement. This models the contention of the Common Data Bus, which is used to provide information about computation results inside the Execution Engine and to other components and can only transmit information about a single result each clock cycle.

Besides the Reservation Station, the Execution Engine also contains the Register File, with one entry for each register. Each register entry either contains the concrete value of the register or references a slot of the Reservation Station that will produce the register's value. Since instructions are issued in program order, the state of the register file at a single point in time represents the architectural register state at that point in time, with yet-unknown register values present as slot references.

## 4.2 OUT OF ORDER EXECUTION (2 PAGES)

todo

## 4.3 EXCEPTION- AND FAULT-HANDLING (2-3 PAGES)

*Exceptions* in general are certain conditions that can occur during execution and require handling before execution can be continued. We distinguish between *architectural* and *microarchitectural* exceptions. Architectural exceptions are visible to the program being executed and are usually handled by that program or the underlying operating system. In our CPU simulation there is

no operating system that could handle architectural exceptions, and requiring the program to handle these would increase the complexity of both our CPU and user programs. For this reason architectural exceptions are handled implicitly, by skipping execution of the instruction that caused the exception. After an exception occurred, execution continues with the following instruction instead. The only architectural exceptions present in our CPU are caused by invalid memory accesses, when a memory operation is performed on an inaccessible address.

Microarchitectural exceptions in contrast are not visible to the program being executed and handled directly by the microarchitecture. In our case the only cause for a microarchitectural exception are mispredicted branches.

Both architectural exceptions and microarchitectural exceptions cause what we call microarchitectural *faults*. All microarchitectural faults are handled in the same way inside the Execution Engine; the difference in behavior between architectural exceptions and microarchitectural exceptions is only introduced in the main CPU component, as mentioned in sec. 4.1.1.

#### 4.3.1 ROLLBACKS

As discussed in sec. 4.2, our CPU executes instructions out-of-order. Because of this, special care must be taken when handling microarchitectural faults. In particular, the following effects need to be considered:

- Instructions preceding the faulting instruction in program order might have not yet been executed
- Instructions following the faulting instruction in program order might already have been executed

The abstraction that, from an architectural point of view, instructions are executed in program order has to be preserved. Thus, we have to restore the architectural state from the time the faulting instruction was issued before we can properly handle the fault. This process of restoring the architectural state is called *rollback*. Instructions that follow the faulting instruction in program order, but are executed before the rollback is performed, are said to occur in *transient execution*; they are executed as usual, but afterwards their operation is rolled back.

In our CPU, rollbacks are local to the Execution Engine. In case of a fault, the Execution Engine performs the rollback, and returns information about the fault to the main CPU component. The main CPU component then performs the remainder of the fault handling.

There are two possible approaches to performing rollbacks. The first approach tracks any changes that executed instructions make to the architectural state. When a fault occurs, these tracked changes can be performed in reverse in order to recover the target architectural state. The second approach records a snapshot of the architectural state when the faulting instruction is issued. When a fault occurs, this snapshot can be restored in order to recover the target architectural state. It is not publicly documented what approach real x86 CPUs take to performing rollbacks. Our implementation follows the snapshot-based approach, since it was judged to be easier to implement in a software-based simulator.

In our case, the architectural state that needs to be restored includes the register state and the contents of memory. The state of the cache and the BPU are not considered part of the architectural state and are not restored when performing a rollback. If multiple instructions might cause a fault, the fault that comes first in program order must be the one that is handled. We employ different techniques for ensuring that the register state and the contents of memory have the proper state after the rollback, and for making sure the first fault in program order is handled. These are described in the following sections. Our implementation uses the category of *potentially faulting instructions*, which includes branch instructions and memory operations.

#### RESTORING THE REGISTER STATE

When a potentially faulting instruction is issued, a copy of the current register state is stored in the reservation station slot. As described in sec. 4.1.6, the register state might contain references to other slots of the reservation station. When the instruction actually faults, execution continues normally until all of the slots referenced by the captured register state have finished executing. Then the captured register state contains no more slot references, and can be restored.

#### RESTORING THE CONTENTS OF MEMORY

Storing a snapshot of the contents of memory every time a store instruction is issued would require a lot of space and prevent the rollback from being local to the Execution Engine. Thus, we instead serialize the execution of store instructions with respect to other potentially faulting instructions. When a store instruction is issued, all slots of the reservation station that contain potentially faulting instructions are recorded. Before performing the store operation, execution halts until all of the recorded slots have retired. This ensures that store operations are only performed when it is known that no preceding instructions cause a fault.

#### HANDLING FAULTS IN PROGRAM ORDER

To make sure that faults are handled strictly in program order, we use the same technique as used to avoid having to snapshot and restore the contents of memory, described above. When a potentially faulting instruction is issued, all slots of the reservation station that contain potentially faulting instructions are recorded. When the instruction actually faults, execution continues normally until all of the recorded slots have retired. This ensures that potentially faulting instructions retire strictly in program order.

The techniques described above require waiting on the execution or retirement of preceding instructions. However, except for store instructions waiting for preceding potentially faulting instructions, this is only required in the case when a fault actually occurs. Thus, in the expected case of no faults the out-of-order execution is not unnecessarily restricted.

#### 4.3.2 TRANSIENT EXECUTION ATTACKS

As mentioned above, the state of the cache is not restored during a rollback. Thus, transiently executed instructions can influence the cache in a way that persists beyond the rollback. During normal execution, the state of the cache can then be observed using a timing-based side channel.

This allows using the cache as a transmission channel from the transient execution domain to the usual architectural domain. Such a transmission channel is typically used in Meltdown- and Spectre-type attacks, and integral to their success.

The state of the BPU is similarly not restored during a rollback. Transiently executed instructions can influence the BPU by performing branches, and during normal execution the state of the BPU can be observed using the differences in execution time caused by mispredicted branches. Because of this, the BPU could be used as a transmission channel just like the cache.

The result of a faulting load operation is made available to following instructions before the fault is handled. During transient execution, this result can be transmitted to the architectural domain via a cache-based channel. Thus, Meltdown-type attacks are possible in our CPU simulation.

During the transient execution after a mispredicted branch, memory loads can be performed. In the same transient execution, their result can be transmitted to the architectural domain via a cache-based channel. Thus, Spectre-type attacks are possible in our CPU simulation.

TODO: Reference to Meltdown and Spectre demos performed in the evaluation

## 4.4 ISA (2 PAGES)

Real life Intel x86 CPUs differentiate between two types of instructions or operations. Macro-operations refer to the relatively easily human readable and convenient but complex instructions that are described by the x86 ISA. Their length differs between the instructions. Internally, in the execution units, the CPU works on  $\mu$ -operations, which are small operations of a fixed length. One macro-operation contains one or multiple  $\mu$ -operations. The CPU frontend has to decode the macro-operations into  $\mu$ -operations in an expensive multi step process. sources: [Wik], <https://en.wikipedia.org/wiki/macro-operation>, <https://en.wikipedia.org/wiki/micro-operation>

Our CPU emulator only uses one type of instructions. They are directly read from our assembler code by the parser and passed to the execution engine without further decoding, splitting or replacing sec. 4.1.2, sec. 4.1.4. To show basic Meltdown and Spectre variants, we do not need overly complex instructions, e.g. instructions that contain multiple memory accesses in one or that are used to perform encryption in hardware [ref\_evaluation\_meltdown], [ref\_evaluation\_spectre]. Basic arithmetic operations, memory accesses, branches and a few special operations are sufficient for the demonstrated attacks and are both easy to implement as single instructions and to use in assembler code that should be well understood by the author. Using the same operations throughout the emulator also makes the visualization more clear and easier to follow, e.g. when the same operations appear, one after the other, in the visualization of the assembler code, the instruction queue and the reservation stations [ref\_ui].

### 4.4.1 DEFAULT INSTRUCTION SET

In order that our CPU emulator can recognize and work with an instruction, it has to be registered with the parser sec. 4.1.2. In our default setting default, we register a basic set of instructions with

the parser so students can start writing assembler code and using the emulator right away. This basic instruction set is also used in our example programs in [ref\_UI].

Our relatively small instruction set is based on a subset of the RISC-V ISA. It offers a selection of instructions that is sufficient to implement Meltdown and Spectre attacks as well as other small assembler programs while still being of a manageable size so students can start to write assembler code quickly without spending much time to get to know our ISA. The syntax of the assembler representation is also based on RISC-V (as introduced in the “RISC-V Assembly Programmer’s Handbook” chapter of the RISC-V ISA) [ref\_RISC-V]. If needed, students can add further instructions by registering them with the parser sec. 4.1.2.

In the following subchapters we introduce the instructions of our default ISA. They are grouped according to their respective instruction type in the emulator except for the special instructions which are grouped together sec. 4.1.2. All default instructions are summarized in the appendix into a quick reference sheet [ref\_appendix].

#### ARITHMETIC AND LOGICAL INSTRUCTIONS WITHOUT IMMEDIATE

These are basic arithmetic and logical instructions that operate solely on register values, i.e. both source operands and the destination operand reference registers. For simplicity, we write, for example, Reg1 when referring to the value read from or stored in the register referenced by the first register operand.

Each of these default operations uses the respective python standard operator on our Word class to compute the result, except for the right shifts. For the logical and the arithmetic right shift, the python standard right shift operator is used on the unsigned and the signed version of the register value respectively. When returning the result as a Word, it is truncated to the maximal word length by a modulo operation, if necessary sec. 4.1.3. This means, that any potential carry bits or overflows are effectively ignored.

Arithmetic and Logical Instructions without Immediate		
Instr. Name	Operators	Description
add	Reg1, Reg2, Reg3	Reg1 := Reg2 + Reg3
sub	Reg1, Reg2, Reg3	Reg1 := Reg2 – Reg3
sll	Reg1, Reg2, Reg3	Reg1 := Reg2 << Reg3
srl	Reg1, Reg2, Reg3	Reg1 := Reg2 >> Reg3 logical
sra	Reg1, Reg2, Reg3	Reg1 := Reg2 >> Reg3 arithmetical
xor	Reg1, Reg2, Reg3	Reg1 := Reg2 xor Reg3
or	Reg1, Reg2, Reg3	Reg1 := Reg2 or Reg3
and	Reg1, Reg2, Reg3	Reg1 := Reg2 and Reg3

#### ARITHMETIC AND LOGICAL INSTRUCTIONS WITH IMMEDIATE

These are basically the same instructions as in sec. 4.4.1. The main difference is, that the second source register is replaced by an immediate operand which is set directly in the Assembler code. This immediate is used as the value of a Word in the execution engine, so it is truncated by a modulo operation to be in the appropriate range sec. 4.1.3, sec. 4.1.6.



Arithmetic and Logical Instructions with Immediate		
Instr. Name	Operators	Description
addi	Reg1, Reg2, Imm	Reg1 := Reg2 + Imm
subi	Reg1, Reg2, Imm	Reg1 := Reg2 – Imm
slli	Reg1, Reg2, Imm	Reg1 := Reg2 << Imm
srli	Reg1, Reg2, Imm	Reg1 := Reg2 >> Imm logical
srai	Reg1, Reg2, Imm	Reg1 := Reg2 >> Imm arithmetical
xori	Reg1, Reg2, Imm	Reg1 := Reg2 xor Imm
ori	Reg1, Reg2, Imm	Reg1 := Reg2 or Imm
andi	Reg1, Reg2, Imm	Reg1 := Reg2 and Imm

### MEMORY INSTRUCTIONS

These instructions provide basic interactions with the emulated memory sec. 4.1.5. Load and store instructions exist in two versions, one that operates on Word length data chunks, for convenience, and one that operates on Byte length data chunks, for the fine granular access needed in micro architectural attacks. The flush instruction flushes the cache line for the given address sec. 4.1.5. The address is calculated in the same way for all memory instructions:  $\text{addr} := \text{Reg2} + \text{Imm}$ , and  $\text{addr} := \text{Reg} + \text{Imm}$  for the flush instruction respectively.

Memory Instructions		
Instr. Name	Operators	Description
lw	Reg1, Reg2, Imm	Reg1 := Mem_word[addr]
lb	Reg1, Reg2, Imm	Reg1 := Mem_byte[addr]
sw	Reg1, Reg2, Imm	Mem_word[addr] := Reg1
sb	Reg1, Reg2, Imm	Mem_byte[addr] := Reg1
flush	Reg, Imm	flush cache line of addr

### BRANCH INSTRUCTIONS

All branch instructions compare the values of two source registers. If the comparison evaluates to true, the execution of the program is resumed at the given label in the assembler code. If it evaluates to false, the next instruction in the program is executed. Depending on the instruction, the register values are interpreted as signed or unsigned integers. Labels in the assembler code are automatically resolved by the parser sec. 4.1.2, [rev\_eval\_and\_example\_code].



Branch Instructions		
Instr. Name	Operators	Description
beq	Reg1, Reg2, Label	jump to Label if $\text{Reg1} = \text{Reg2}$
bne	Reg1, Reg2, Label	jump to Label if $\text{Reg1} \neq \text{Reg2}$
bltu	Reg1, Reg2, Label	jump to Label if $u(\text{Reg1}) < u(\text{Reg2})$
bleu	Reg1, Reg2, Label	jump to Label if $u(\text{Reg1}) \leq u(\text{Reg2})$
bgtu	Reg1, Reg2, Label	jump to Label if $u(\text{Reg1}) > u(\text{Reg2})$
bgeu	Reg1, Reg2, Label	jump to Label if $u(\text{Reg1}) \geq u(\text{Reg2})$
blts	Reg1, Reg2, Label	jump to Label if $s(\text{Reg1}) < s(\text{Reg2})$
bles	Reg1, Reg2, Label	jump to Label if $s(\text{Reg1}) \leq s(\text{Reg2})$
bgt	Reg1, Reg2, Label	jump to Label if $s(\text{Reg1}) > s(\text{Reg2})$
bges	Reg1, Reg2, Label	jump to Label if $s(\text{Reg1}) \geq s(\text{Reg2})$

### SPECIAL INSTRUCTIONS

Rdtsc acts like a basic timing instruction. It returns the number of ticks the execution unit has executed so far in the given register.

The fence instruction acts as a fixed point in the out of order execution. All instructions that are already issued in the execution unit at the point of issuing the fence instruction are executed before the fence is executed. No new instructions are issued before the execution of the fence instruction is complete.

Special Instructions		
Instr. Name	Operators	Description
rdtsc	Reg	$\text{Reg} := \text{cyclecount}$
fence	none	add execution fixpoint at this code position

## 4.5 CONFIG FILE

*Felix Betke*

To allow users to change certain parameters of the presented emulator, a configuration file is available. It can be found in the root folder of the project and edited with a regular text editor. This section briefly mentions which parts of the demonstrated emulator can be configured, and why which default values have been chosen.

### 4.5.1 MEMORY

In the “Memory” section, the users may configure how many cycles write operations should take (*num\_write\_cycles*), and how many cycles should be between a faulting memory operation and the corresponding instruction raising a fault (*num\_fault\_cycles*). By default, the former is set to 5 cycles, the latter to 8. While the specific values are not as important, the difference between the number of cycles it takes to perform any faulting memory operation and the number of cycles it takes to raise the fault should be at least 1. Otherwise, the rollback is initiated before dependend instructions can encode the data into the cache for the attacker to retrieve. During our testing, we decided that a difference of at most 3 on a cache miss is sufficient for Meltdown-US-L1 and Spectre v1 to work.

#### 4.5.2 CACHE

In the “Cache” section, users may configure the size of the cache by setting the number of sets, ways, and entries per cache line. For readability when printing, the default value we chose for all values is 4. However, it is important to note that if one were to perform the full Meltdown/Spectre attacks by measuring access times to each oracle entry, a sufficient cache size that ensures accessing an oracle entry does not evict another is required.

Further, the cache replacement policy can be set to either “RR”, for random replacement, “LRU”, for least-recently-used, and “FIFO”, for first-in-first-out. Each policy is explained in sec. 4.5.2. As RR introduces noise, we have decided against using it as the default. Although widely undocumented, Intel’s Skylake architecture is believed to use some kind of specialized version of LRU [VKM19]. For that reason, and since our choice is largely irrelevant as long as users clearly understand how it works, we chose the LRU policy.

The other two values that can be configured are the number of cycles cache hits and misses take. As mentioned in sec. 4.5.1, the specific values are not as important as their differences.

#### 4.5.3 INSTRUCTION QUEUE

The config allows users to configure the size of the instruction queue maintained by the frontend. It determines the maximum number of instructions that can be issued per tick. As the transient execution window is largely determined by cache hits and the number of available entries in the unified reservation station, this choice is not as important. Our testing shows the desired attacks are possible with an instruction queue size of 5. As pointed out in sec. 4.1.4, this limit is ignored in case micro-programs are to be executed.

#### 4.5.4 BPU

Here, the user may configure whether to use the simple BPU, or the advanced one. The difference is that the simple BPU maintains only a single counter, while the advanced one maintains a counter for each program counter value. Additionally, the number of bits used for the counter as well as its initial value can be chosen. By default, we use the advanced BPU with 4 index bits and an initial counter of 2.

#### 4.5.5 EXECUTION ENGINE

The execution engine allows the configuration of the number of available slots in the reservation station. In part, this value determines the width of the transient execution window. We found that with 8 slots, Meltdown and Spectre attacks are possible. Additionally, the number of registers can be configured. Since our instruction set is based on the RISC-V ISA, we chose to offer the same number of registers by default, which is 32 [And17].

#### 4.5.6 UX

The UX can be configured to omit display of certain elements. When selecting to use a large cache, it may be desirable to hide empty cache ways and sets to prevent clutter. By default, we chose to show the empty cache ways so the user can easily see whether or not a cache set is full. We also chose to show the empty cache sets so there is a visual representation of which addresses correspond to certain sets. Another option is to hide the unused reservation station slots. In this case every entry in the reservation station will be numbered. Showing the unused slots may help the user to keep track of bottlenecks in the execution, and is therefore chosen per default. Finally, the user may choose between capitalised or lowercase letters for the registers. By default, we chose to use lowercase letters.

## 5 USER INTERFACE AND USAGE

This chapter focuses on the usage of the application. The user interface and the design choices are described. An instruction on how to prepare the system and how to run the program is given. Furthermore, the application and its features are explained in detail. Finally, we showcase the application in action.

### 5.1 PURPOSE AND INSPIRATION

In order to demonstrate Meltdown and Spectre attacks, this program is designed to visualise the execution of a modern CPU on a microarchitectural level. We implement a simplified model of a CPU to keep focus on the essential parts to understand the demonstrated attacks. At the same time, the CPU needs to show all information required to follow the attack, and offer convenient features to the user.

It was chosen to follow the rough structure of the GNU Debugger GNU [**GDB**] and more specifically the extension Pwndbg [**pwndbg**]. The assumption is that many of the target audience are already well familiar with the GNU Debugger and the Pwndbg extension. GDB and Pwndbg can be interacted with via the command line. Different to other similar solutions, GDB can only be interacted with using commands. Most notable is the ‘context’ screen, which is issued after execution is paused. The context screen prints out the current state of the CPU, including the registers, the stack, a backtrace, and the disassembly.

As with GDB, the emulator can only be interacted with using commands. We further implemented auto-completion and auto-suggestion using the python-prompt-toolkit [**prompt**]. This should lower the difficulty of getting started with a new tool. The emulator also implements a Pwndbg-style context-visualisation, albeit with different elements shown to adapt to the different goal compared to GDB. This ensures most of the relevant information is on the screen at all times.

### 5.2 SYSTEM REQUIREMENTS AND INSTALLATION

The following things need to be installed to run the program:

- Python
- Python-Benedict
- Python-Prompt-Toolkit

To install the required packages, one may use the following command:<sup>1</sup>

---

<sup>1</sup>The requirements file is located in the root directory of the project. In some distributions pip may be called pip3.

```
1 | pip install -r requirements.txt
```

Optionally, the following things can be installed:

- Git

It is recommended to use the program on a Linux system, although Windows functionality is mostly implemented. Further, it's recommended to have a terminal with a width of at least 120 characters.

The following system was used to test the program:

- Debian GNU/Linux 11 (bullseye)
- Python 3.9.10
- Python-Prompt-Toolkit 3.0.28
- Python-Benedict 0.25.0
- Git Commit 419678d33a41eefb0bcd775966dae0418ba51245

### 5.3 RUNNING THE PROGRAM

The syntax for running the emulator from the root folder of the repository is:

```
1 | python -m src.shell <path_to_target_program>
```

If no target program is supplied, the emulator will print system information, along with a help message. The target program may contain instructions as specified in sec. 4.4 (#sec:ISA), separated by linebreaks. Comments can be added to the target program by preceding them with `//`. Furthermore, the `config.yml` file in the root folder can be modified to configure the emulator, see sec. 4.5.

## 6 EVALUATION

todo

## 7 CONCLUSION

*Felix Betke*

Our goal was to create an emulator that allows users to experiment with simplified versions of select Meltdown and Spectre type attacks without access to vulnerable hardware. The choice of Python as the programming language and a limited number of UI libraries ensure our emulator can be used on anything that runs Python, regardless of operating system or architecture. Further, the evaluation (see sec. 6) shows that Meltdown-US-L1 and Spectre v1 attacks are possible given the default configuration and example programs. We document our implementation and provide a user manual in the previous chapters.

### 7.1 LIMITATIONS

While we reached our goals, some limitations of our emulator exist. Firstly, due to not running an operating system, we lack virtual addresses and paging, therefore not fully modelling the Meltdown-US-L1 attack and how exceptions can be forced by user space processes. Secondly, our current implementation of read operations behaves differently than Intel’s CPUs are believed to behave. In our version, if needed data is not present in the cache, instructions stall until the data is available, rather than computing on values taken from other microarchitectural buffers [Sch+19]. As a result, Meltdown-US-L1 is still possible, but in the event the data to be stolen is not cached, users will observe a stall, not a read from other buffers. The reason for this simplification is that the Meltdown-US-L1 attack does not strictly rely on any of those buffers, which we have therefore not modelled. Thus, we are still confident our simplified emulator allows users to better understand the chosen attacks.

### 7.2 FUTURE WORK

One of the obvious improvements would be to make the emulator vulnerable to other Meltdown and Spectre variants. For Meltdown, this would require the addition of new microarchitectural buffers, such as the load, store, or line-fill buffers (see sec. 2.1). For Spectre, a more elaborate BPU (see sec. 2.2 and sec. 2.3) is needed. Other improvements could be to enable users to run multiple programs (attacker and victim), either by context switching or Hyper-Threading. Lastly, one could add further improvements to the UI in regards to visualization and functionality (conditional breakpoints, for example).

## 8 CATCHY LAB TITLE

### 8.1 ABSTRACT

### 8.2 INTRODUCTION (1 PAGE)

```
1 general task/ goal
2     CPU emulator with actual out of order execution, maybe speculative
3     execution and comprehensible implementation and documentation
4     implement different p-architectural features like out-of-order exe.,
5     speculative exe. b.c. we want to observe and demonstrate p-arch.
6     attacks
7 brief context of the task/ goal (e.g. a sentence on Meltdown and why it is
    important to understand it)
8     why is it important to have the emulator: so far no possibility to
9     observe microarchitectural attacks in real life
10    rauscharme Umgebung, die macht was man erwartet
11 structure of the report
```

### 8.3 BRIEF THEORETICAL BACKGROUND (2-3 PAGES)

```
1 premise according to Felix: reader knows SCA lecture -> brief recaps/
2     reminders to reference back to from the other chapters
3
4 ### really brief introduction to CPU
5
6     multiple components
7         maybe mostly via picture
8
9     how they work together
10
11     maybe data-flow from instruction to result
12
13     a lot of hypothticals due to trade secrets
14
15     suggested literature:
16         maybe Gruss Diss. and other works on cbsca
17         maybe textbooks
18         maybe CPU wiki for pictures
19
20 ### out-of-order execution
```



```

20
21     a bit more in depth b.c. this is not content of the sca lecture
22
23     maybe why do we need it/ advantages
24
25     brief explanation of Tomasulo and how it works
26
27     suggested literature:
28         original Tomasulo paper from 1965
29         maybe a more recent/ didactically edited explanation (is this in
30         textbooks?)
31
32     also something about speculative execution
33
34 ### Meltdown and Spectre
35
36     brief introduction to Meltdown (and Spectre) in general
37
38     slightly more in-depth introduction to the Meltdown attack we picked
39     and want to run in our emulator
40
41     highlight the relevant parts of the CPU, maybe mention how they
42     interact in Meltdown (and Spectre)
43
44     mitigations and maybe how successfull they are
45
46     suggested literature:
47         ggf. Dissertation Gruss if we mention basic cbsca
48         Gruss et al. papers on Meltdown and Spectre e.g. https://gruss.cc/
49         files/meltdown.pdf or https://gruss.cc/files/meltdown\_cacm.pdf
50         Canella, Gruss et al. on mititgations https://gruss.cc/files/
51         transient-attacks.pdf

```

## 8.4 MAYBE SPECIFICATION OF THE TASK (1 PAGE)

```

1   rauswerfen, in Introduction mit übernehmen
2
3   emulator to execute and teach Meltdown
4       who is the target audience`
5       which Meltdown attacks specifically
6       etc. further concretisations
7
8   are there existing solutions/ related works?
9       Felix' old emulator? citable?
10      suggested literature:
11          todo

```

## 8.5 CPU EMULATOR/ BACKEND (17-18 PAGES)

```

1 maybe general info e.g. that we wrote it in python, if we used special
   tools/ libraries
2 for everything we implemented:
3     which part of a real life cpu does this model/ how is this done in
   real life cpus
4     briefly how does it work
5     why did we choose to model it like we do
6         nice code structure/ code easy to understand by students
7         some features more or less relevant for meltdown
8         etc.
9     maybe what did we leave out
10    challenges?
11
12 ### CPU Components and our equivalents/ models (10-11 pages)
13
14     modular setup based on real life CPUs and nice coding conventions
15
16     #### CPU
17
18         contains/ controls the rest
19
20         preparation (loading the program, init the rest)
21
22         ticks
23
24         coordinate rollbacks?
25
26     #### Instructions and Parser
27
28         instructions
29
30         parser
31
32     #### Data representation
33
34         how we model and handle data
35
36         byte, word
37
38     #### CPU frontend
39
40         Branch Prediction Unit (BPU)
41
42         Instruction Queue
43
44     #### memory
45

```

```

46         no virtual addresses
47
48         mmu
49
50         how do we store data
51
52         how do we model data access (i.p. wrt Meltdown)
53
54         cache
55
56         what kinds of caches can we represent
57
58         how do we model if something is cached and the access times (i.
59 p. wrt Meltdown)
60
61 ##### Execution Engine
62
63         Reservation Station/ Slots
64
65         unlimited execution units
66
67 ### Out of Order Execution (2 pages)
68
69         our version of out-of-order execution/ Tomasulo
70         how much details on Tomasulo? our choice
71
72         where in our program do we implement which components
73
74         what did we leave out/ do differently
75
76 ### Exceptions and Rollbacks (2-3 pages)
77
78         in particular wrt making Meltdown possible
79
80         general goal/ concept of rolling back after a misprediction or an
81 exception
82
83         snapshots and interaction of the CPU components
84         components that are fully reset after a rollback: cache, BPU
85
86 ### ISA (2 pages)
87
88         overview of ISA
89
90         p-instr. vs. ISA
91         mixture of both in one: only p-code, but more abstract than in real
92         life
93
94         do not need to think about page faults etc. anyways, do not need
95         overly complex instructions

```

```

91
92     reasoning behind the choice of instructions (manageable size and
        instructions (e.g. no divide by zero) balanced with functionality
        particularly wrt Meltdown)
93
94
95     ### config files (1 page)
96
97     what can be configured without changing the source code
98     why these variables? relevant for Meltdown?

```

## 8.6 OUR VISUALISATION AND USAGE/ FRONTEND (10 PAGES)

```

1   ggf. gemäß Anmerkung von Lenni umsortieren: die idee das UI nicht mit in
        die 'unsere designentscheidungen' zu nehmen, sondern im prinzip so als
        Manual abzukapseln finde ich eigentlich ganz gut. Müssen wir aber dann
        mal in der Praxis schauen. Soll ja keine didaktischen begründungen das
        manual zu sehr aufblähen, vllt wird das sinnvoll, dann einen teil des
        UI im "backend" kapitel einzubauen, und dann wirklich ein cleanes
        manual kapitel zu haben
2
3   zwei Strukturierungsmöglichkeiten:
4       z.B. alphabetisch
5       z.B. nach einzelnen Angriffen etc. aufgeteilt und aufeinander aufbauend
6   erklären was technisch passiert nachdem man gezeigt hat wie es aussieht
7   man kann auch explizit sagen, "ich gehe davon aus, dass du GDB kannst,
        daran ist das angelehnt, hier sind die Unterschiede"
8
9   ### general concept
10
11     goal: UI for the emulator with visualisation of CPU/ memory components
        and their contents
12
13     in terminal
14         maybe comparison to existing analysis tool/ debugger gdb
15
16     triggers/ controls the actual emulator
17         overview features, e.g. breakpoints, step-by-step and stepback
18
19     maybe which tools/ libraries were used?
20
21     ### features in more detail and their didactic purpose
22
23     breakpoints, step-by-step, stepback and more
24
25     challenges/ design choices during the implementation

```

## 8.7 DEMONSTRATION/ EVALUATION (7 PAGES)

```

1  what kind of system do we need/ did we use to run this?
2      which python Version?
3      which program version ? git commit
4      other dependencies?
5
6  ### general demonstration
7
8      brief example program showing all the features in a "normal" execution,
        e.g. adding stuff
9
10 ### Meltdown und Spectre demonstration
11
12     #### Example Program Meltdown
13
14         show example program
15
16         maybe compare to example program for real life architecture from
        SCA or literature (Gruss) if available
17
18         explain which Meltdown variant it implements
19
20         briefly highlight which components (we expect to) interact to make
        it work
21
22         how well does it work?
23
24     #### maybe example program spectre
25
26         same as Meltdown
27
28     #### mitigations
29
30         it is known which mitigations exist, here is what we have in our
        emulator:
31
32         what is possible in our program as is
33             planned:    cache flush: microcode -> config file
34                       mfence in assembler (normally in compiler)
35                       aslr directly in program -> config (es gibt ja auch
        mitigations, die keine echte mitigation sind; nice to have -> könnte
        demonstrieren dass es nicht der Fall ist; war eh schon einige Jahre vor
        Meltdown vorhanden/ in Gebrauch; KSLR brachen kann man auch als
        Angriff verkaufen)
36
        flush IQ -> passiert eh schon, ist das überhaupt
        eine echte mitigation?
37
        disable speculation (nice to have, lassen wir weg)
        -> config

```

```

38         out of order -> in config RS mit nur einem Slot
39
40         is our meltdown/ spectre variant still possible?
41         ggf. how does this affect the performance?
42         vorsichtig sein, dass man dann auch die richtige Frage für die
Antwort stellt
43         in real life (already in background)
44         in our program
45
46         what would be the necessary steps/ changes to the program for
further mitigations
47         compare to changes in hardware by the manufacturers

```

## 8.8 CONCLUSION (1 PAGE)

```

1  recap goals
2  main goal of this chapter: to which extend did we reach our goals?
3
4  did we reach the goal of implementing a CPU emulator where a user can
perform a Meltdown attack
5
6  how many Meltdown attacks are possible?
7
8  is Spectre possible?
9
10 mitigations
11     which mitigations did we implement
12     is this a good amount/ sample of real world mitigations or do we miss
important ones?
13     how well do they perform (also in comparison to how they perform in the
real world)
14
15 value to students:
16     how easy to use and convenient do we think our program is?
17     do we think this will be a good tool for teaching?
18     how accessible is it wrt different host architectures?
19     1 überzeugter Satz: wir haben sehr gute Arbeit geleistet und das
Werkzeug ist sehr gut. wenig hin schreiben, damit keiner fragt, ob wir
das nicht weiter evaluieren müssten. nicht weit aus dem Fenster mit
Behauptungen lehnen sondern klar und kurz unsere Meinung formulieren
20
21 further work
22     more (detailed/ realistic) functionality for more Meltdown and Spectre
variants
23     more elaborate BPU with btb (and ghr) for more spectre variants
24     more mitigations
25     maybe nice to have wrt to the visualisation/ general UI functionality/
ISA?

```

## REFERENCES

- [And17] ANDREW WATERMAN, Krste Asanovic: *The RISC-V Instruction Set Manual*. 2017. URL: <https://riscv.org/wp-content/uploads/2017/05/riscv-spec-v2.2.pdf> (visited on 03/19/2022).
- [Can+20] CANELLA, Claudio et al.: “KASLR: Break it, fix it, repeat”. In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. 2020, pp. 481–493.
- [Gru20] GRUSS, Daniel: “Transient-Execution Attacks”. 2020. URL: <https://gruss.cc/files/habil.pdf> (visited on 03/11/2022).
- [Int18] INTEL: *Intel Analysis of Speculative Execution Side Channels*. 2018. URL: <https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Intel-Analysis-of-Speculative-Execution-Side-Channels.pdf> (visited on 03/11/2022).
- [Koc+19] KOCHER, Paul et al.: “Spectre attacks: Exploiting speculative execution”. In: *2019 IEEE Symposium on Security and Privacy (SP)*. 2019.
- [Lip+18] LIPP, Moritz et al.: “Meltdown: Reading Kernel Memory from User Space”. In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018.
- [Sch+19] SCHAIK, Stephan van et al.: “RIDL: Rogue In-flight Data Load”. In: *S&P*. 2019.
- [Tom67] TOMASULO, Robert M: “An efficient algorithm for exploiting multiple arithmetic units”. In: *IBM Journal of research and Development* 11.1 (1967), pp. 25–33.
- [VKM19] VILA, Pepe ; KÖPF, Boris ; MORALES, José F: “Theory and practice of finding eviction sets”. In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019, pp. 39–54.
- [Wik] WIKICHIP: *Skylake Microarchitecture*. URL: [https://en.wikichip.org/wiki/intel/microarchitectures/skylake\\_client](https://en.wikichip.org/wiki/intel/microarchitectures/skylake_client) (visited on 03/10/2022).

## LIST OF FIGURES

- 1    Simplified overview an Intel Skylake CPU [[Gru20](#), fig. 2.1]. For the memory sub-system, detailed knowledge of the load and store buffers, as well as the TLBs, is not required. The same applies to the allocation queue of the frontend. . . . . 4



## STATEMENT OF AUTHORSHIP

I hereby confirm that the work presented in this lab report has been performed and interpreted solely by myself except where explicitly identified to the contrary. I declare that I have used no other sources and aids other than those indicated. This work has not been submitted elsewhere in any other form for the fulfilment of any other degree or qualification.

Bonn, 31. March 2022

---