

# 6.595

# Secure Hardware Design

**Mengjia Yan**

Spring 2026



# Who Built This Course?



**Mengjia Yan**  
Professor



**Joseph Ravichandran**  
TA Spring 2022 + CA 2023  
Lab and Recitation Design  
(Spectre, ASLR Bypasses,  
CPU Fuzzing, Physical Attacks)



**Peter Deutsch**  
TA Spring 2023  
Lab Design  
(Rowhammer)



**Yuheng Yang**  
Lab and Recitation Design  
(Formal Verification)



**Willian Liu**



**Miles Dai**  
TA Fall 2020  
(Cache Attacks)



**Jack Cook**  
Lab Design  
(Website Fingerprinting)



**Miguel Gomez-Garcia**  
Lab Design  
(Rowhammer)



**Shixin Song**

# Course Staff



Instructor: Mengjia Yan

- [mengjia@csail.mit.edu](mailto:mengjia@csail.mit.edu)
- Office: 32-G840
- Office Hours: Friday 2:30pm–3:30pm



Course Assistant: Taylor Braun

- Email: [shd-staff@mit.edu](mailto:shd-staff@mit.edu)

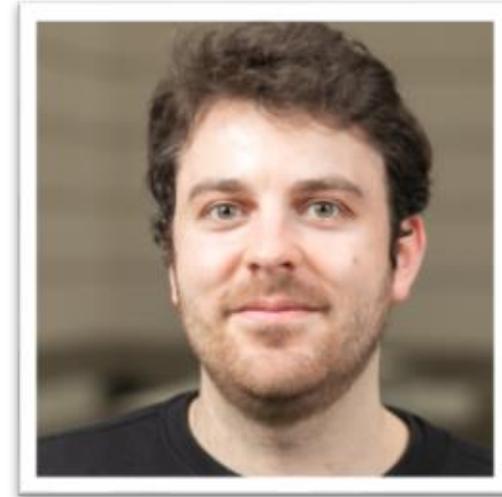
# TAs



Kelly Xu



Kosi Nwabueze



Vincent Ulitzsch

Email: [shd-staff@mit.edu](mailto:shd-staff@mit.edu)

Office: 32-G786

## Office Hours (32-G7 Lobby)

- Tuesdays 11:30am–1:30pm (Kelly)
- Wednesdays 2:30pm–4:30pm (Kosi)
- Extra office hours before Lab Due Dates

No office hours  
in Week 1.

# Today's Agenda

1. Course Overview: What can you learn from this course?
2. Course Logistics: assignments, labs, grading, etc.
3. Enrollment Cap Selection Process
4. Review basic architecture materials (from 6.1910 [6.004])

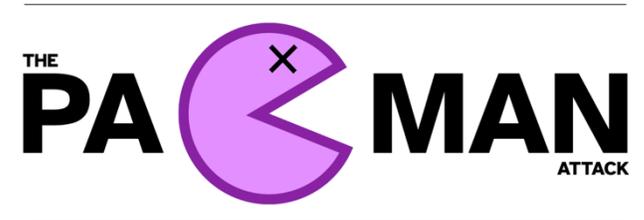
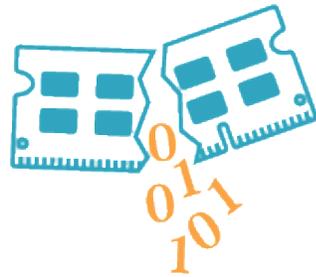
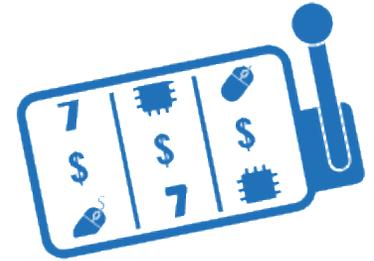
# Course Overview



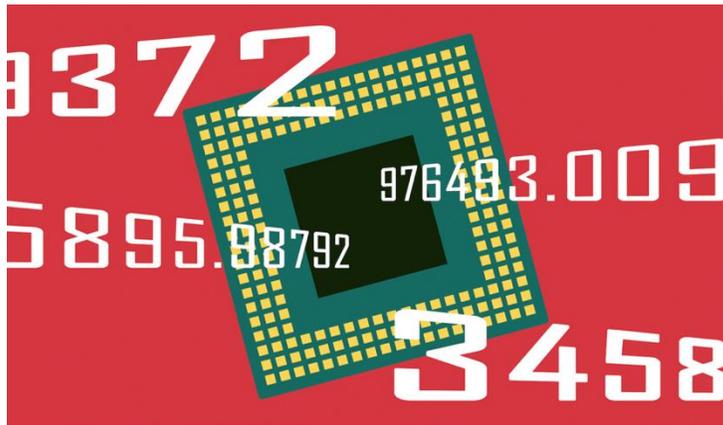
# Hardware Attacks on The Spotlight



FORESHADOW

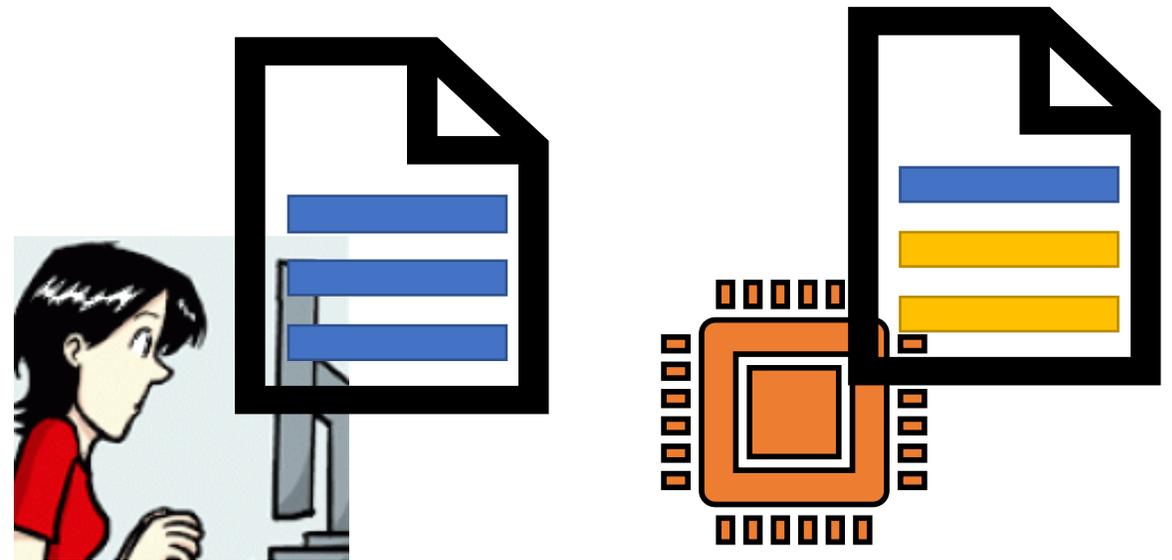


# Hardware Bugs



Pentium FDIV bug

# Hardware Design Choices



Conceptual speculative execution vulnerabilities

# Mitigation Choices

- A) A comprehensive mitigation that can block all the attacks in a specific category
- B) An ad-hoc mitigation that can block some but not all the attacks in the category

**Which one do you choose?**

But what if?

A) is 15% slower than B) and also consumes 1.5x more energy than B)

# What mitigation has been deployed?

The screenshot shows the Intel Software Security Guidance website. The header includes the title "Software Security Guidance" and a navigation menu with items: Overview, Advisory Guidance, Best Practices, Disclosure Documentation, Feature Documentation, and More Information. The main content area is titled "Advisory Guidance" and includes a sub-header "Overviews and one-page descriptions of security advisories along with recommended mitigations for affected environments." Below this, there is a link to "Find industry-wide severity ratings in the National Vulnerability Database." and four severity level icons: Critical (red), High (orange), Medium (yellow), and Low (grey). A table lists two advisories:

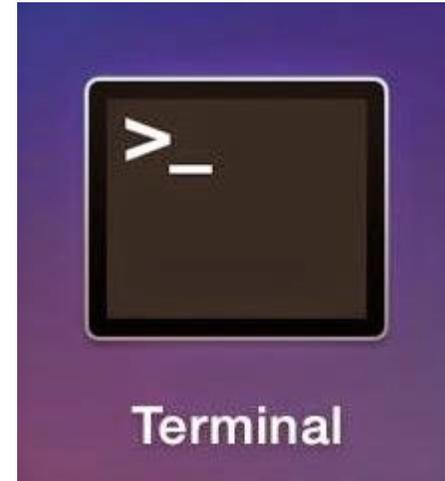
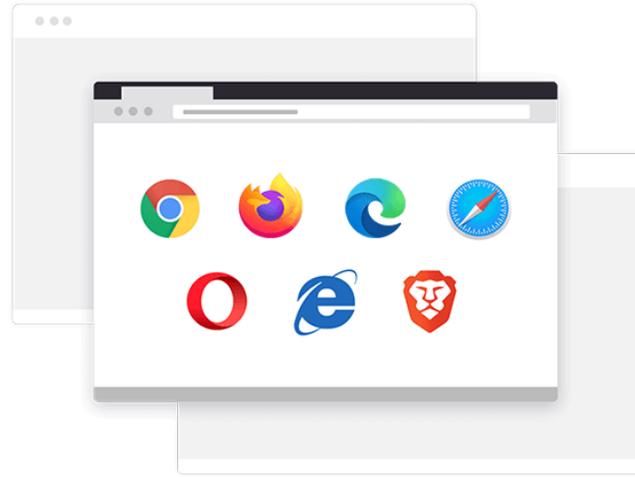
CVSS	Title	CVE	SA	Severity	Disclosure Date
6.0	Stale Data Read from Legacy xAPIC	CVE-2022-21233	INTEL-SA-00657	Medium	2022-08-09
5.5	Post-Barrier Return Stack Buffer Predictions	CVE-2022-26373	INTEL-SA-00706	Medium	2022-08-09

<https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/advisory-guidance.html>

# Hardware Security Features



# What programmers see?



A computer system

# System Abstractions

Programs



**Virtual  
Machine**

System Software (virtual memory, process, I/O) <- 6.1810[6.828]



**Instruction Set  
Architecture (ISA)**

Computer Architecture (caches, core, pipelining)

<- 6.1910[6.004], 6.5900[6.823]

Digital Circuits (combinational and sequential circuits)



**Digital  
Abstraction**

Analog Circuits; Devices (transistors) <- 6.6010 [6.374]

# Abstraction Hides Details

- Program 1

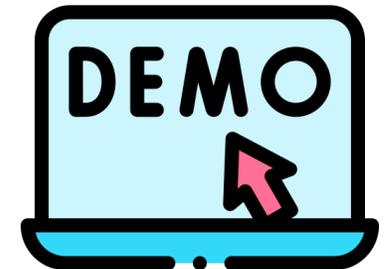
```
for (i=0; i<=1000; i++){  
    sum += n;  
}
```

How many instructions will be executed?

- Program 2

```
printf("hello world\n");
```

- (A) Hundreds ( $\approx 10^2$ )
- (B) Thousands ( $\approx 10^3$ )
- (C) Tens of thousands ( $\approx 10^4$ )
- (D) More

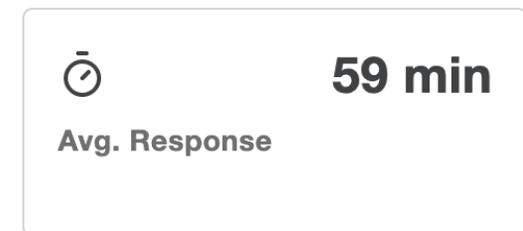
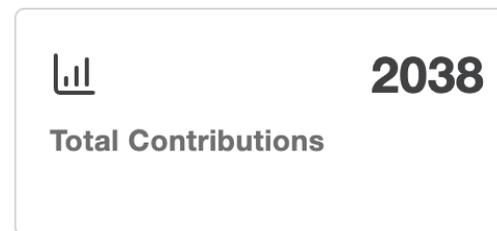
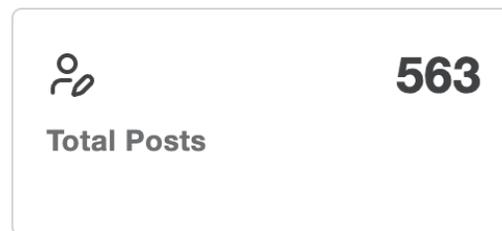


# Course Logistics: Lectures, Paper Discussion, Grading



# Three Websites

- Course website: <https://shd.mit.edu/2026/>
  - All the course policy, grading details, lecture slides, lab handouts, etc.
- Piazza: Announcements and Q&A
- Gradescope and Github Classroom: Submit your lab assignments and homework

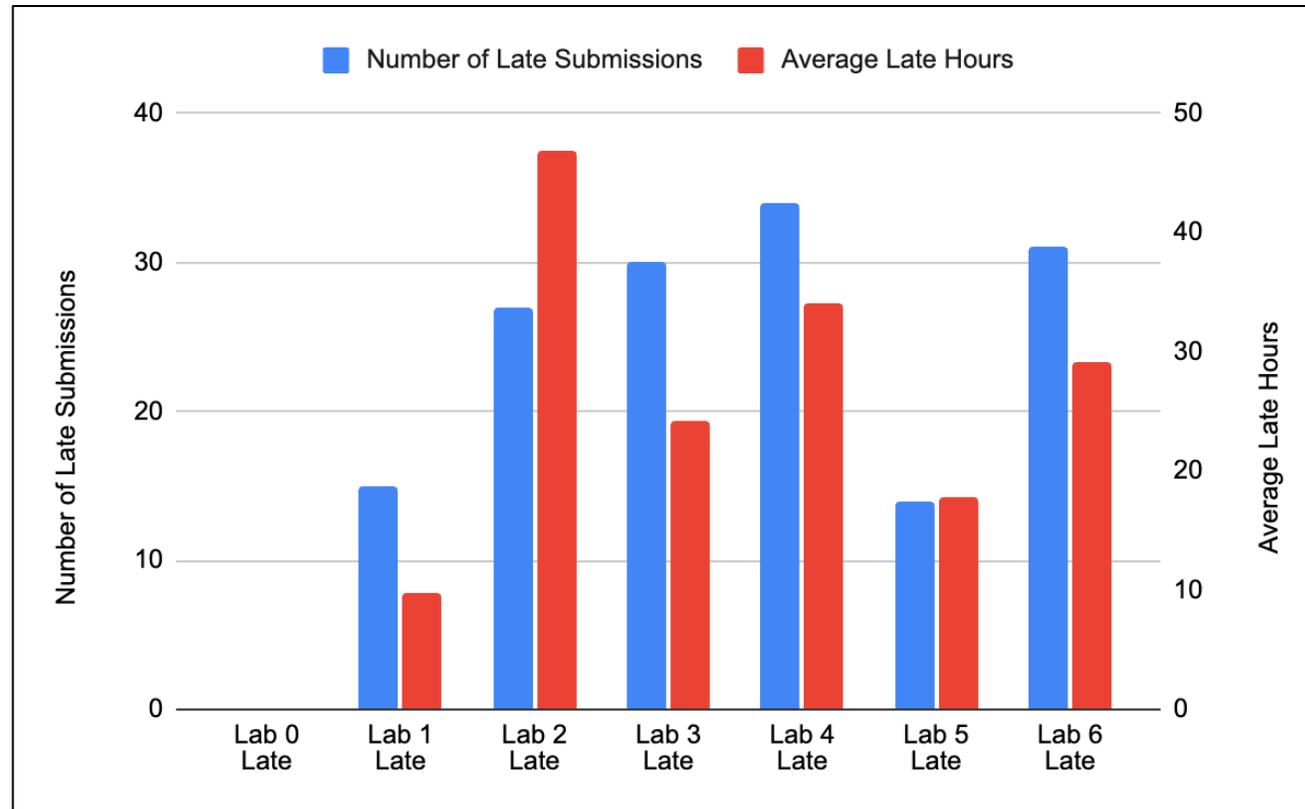


*Piazza stats of SHD 2025*

**Now let's navigate  
the course website**

# Labs

- Read late policy carefully on the website.



Late days usage statistics in Spring 2025

# Exam (NEW)

- Close-book, in-class exam.
- Length: 80 min
- Date: May 6
  
- We do not accept accommodations for conflicts with other classes.
  
- Preparation materials are lecture slides, recitation materials, and lab materials. No pset.

# Enrollment Cap Selection Process

- Due to hardware constraints, enrollment is capped at **96** students
- You must attend the first lecture and fill in a short poll.
- You must satisfy the prerequisite 6.1910
  - If you are an MIT student and have taken 6.1910, you automatically satisfy pre-req
  - If not, please submit submit proof of equivalent background or other more advanced course you have taken at MIT via Piazza by **noon Tuesday Feb 3rd**.
- Random lottery.
- Results will be out before **Tuesday Feb 3rd 5pm**.

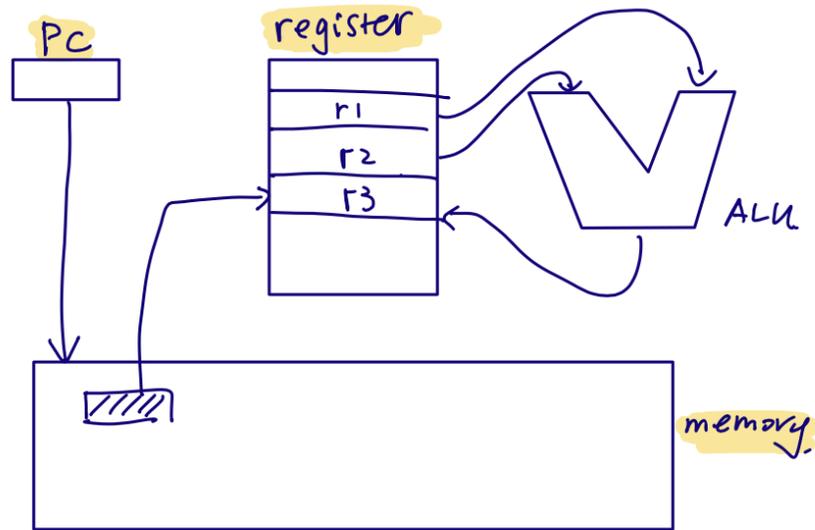
# Review

## Basic Architecture Concept

- ISA and Pipelined Processors
- Virtual Memory

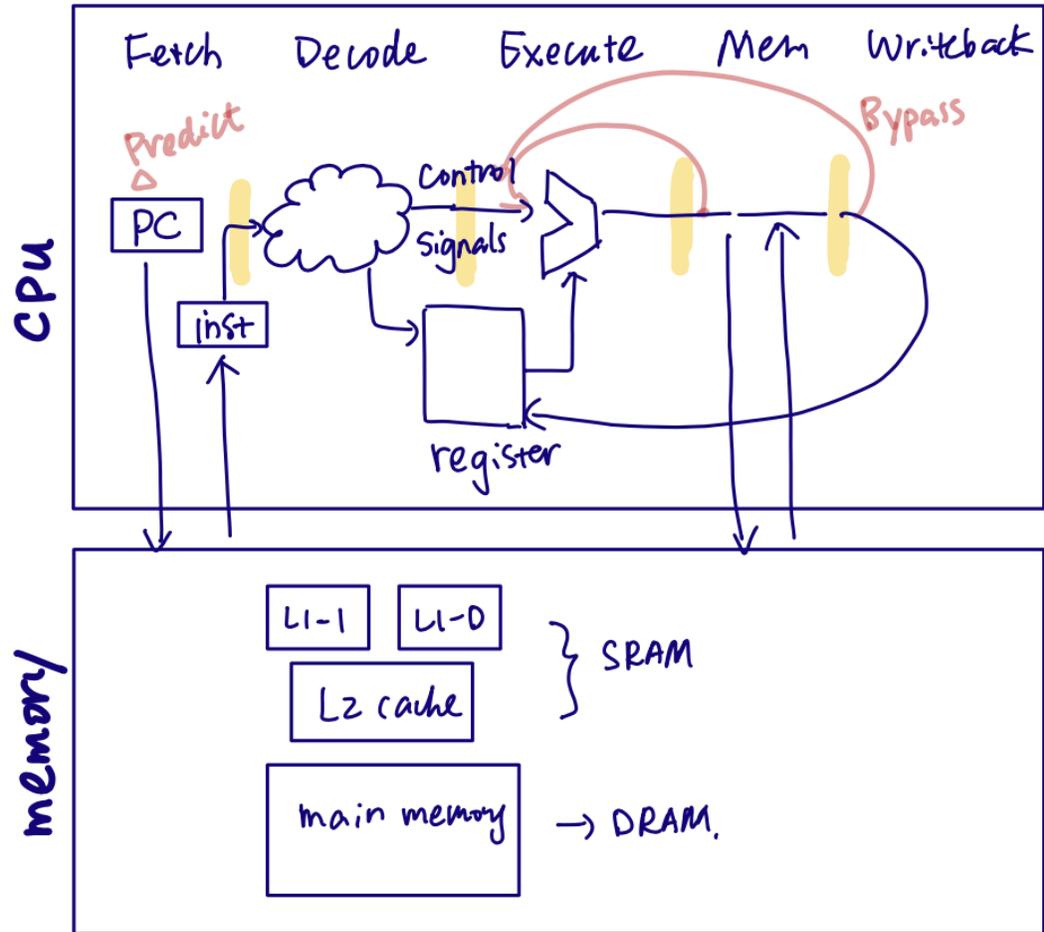


# ISA and A Pipelined Processor



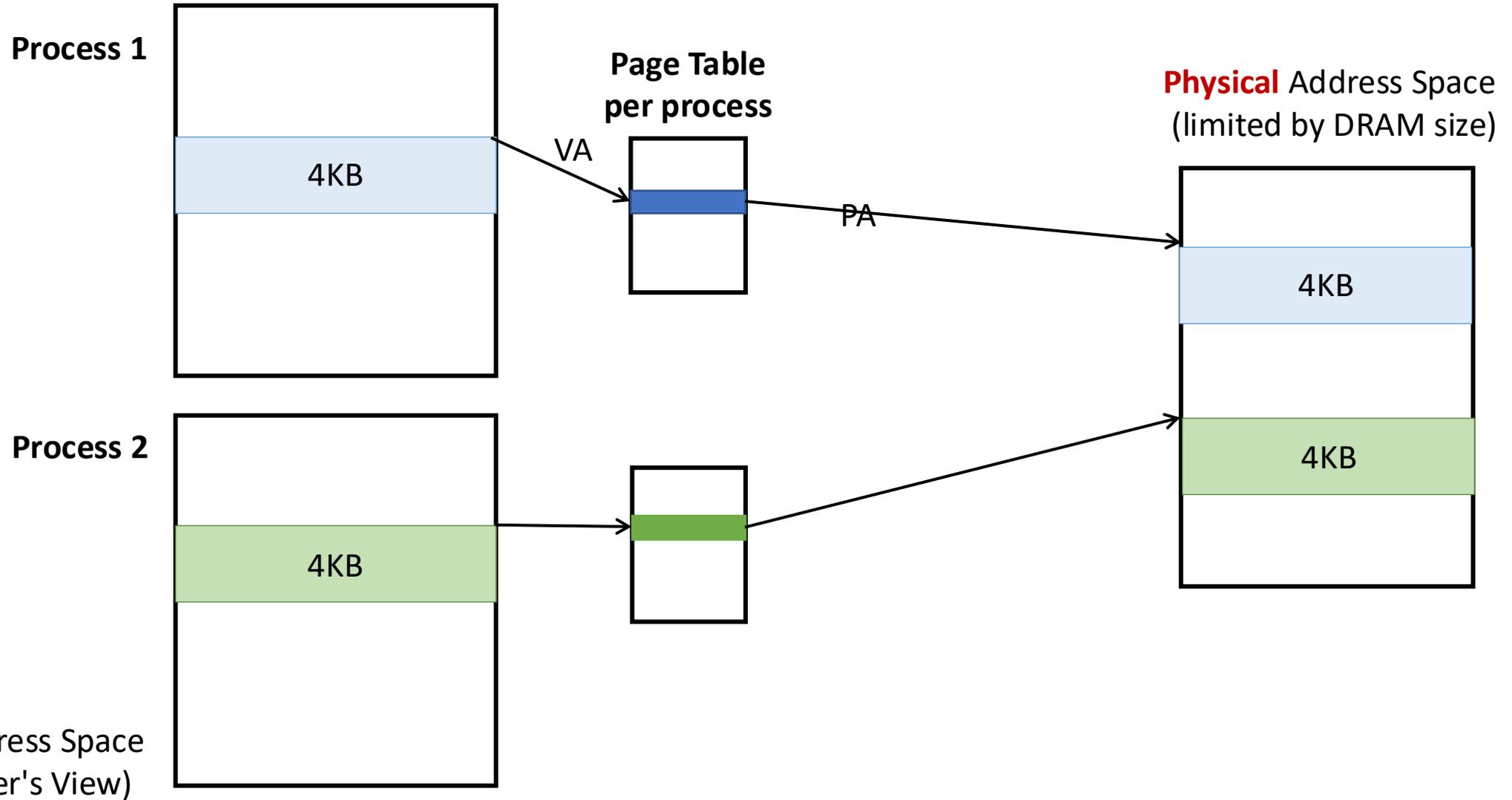
inst: Add r3, r1, r2.

Software's View of the Processor



A 5-stage Pipelined Processor

# Virtual Address & Address Mapping



**Virtual** Address Space  
(Programmer's View)

# Next: Side Chanel Overview

