CASPER

CS773-2025-Spring: Computer Architecture for Performance and Security

Lecture 1: Course Logistics

https://www.cse.iitb.ac.in/~biswa/

About Me: ~~Prof./Dr./Mr./Sir~~ Biswa

Member of faculty at CSE-IITB

CASPER group: https://casper-iitb.github.io/

Lectures: Monday/Thursday: 7 PM

Office hours: Please refer to the course webpage https://www.cse.iitb.ac.in/~biswa/courses.html

Email: biswa@cse.iitb.ac.in ([CS773] in the subject)

Office: CC-217 (2nd floor, CC building)

Primary research interests:

Architecture for *performance and security*

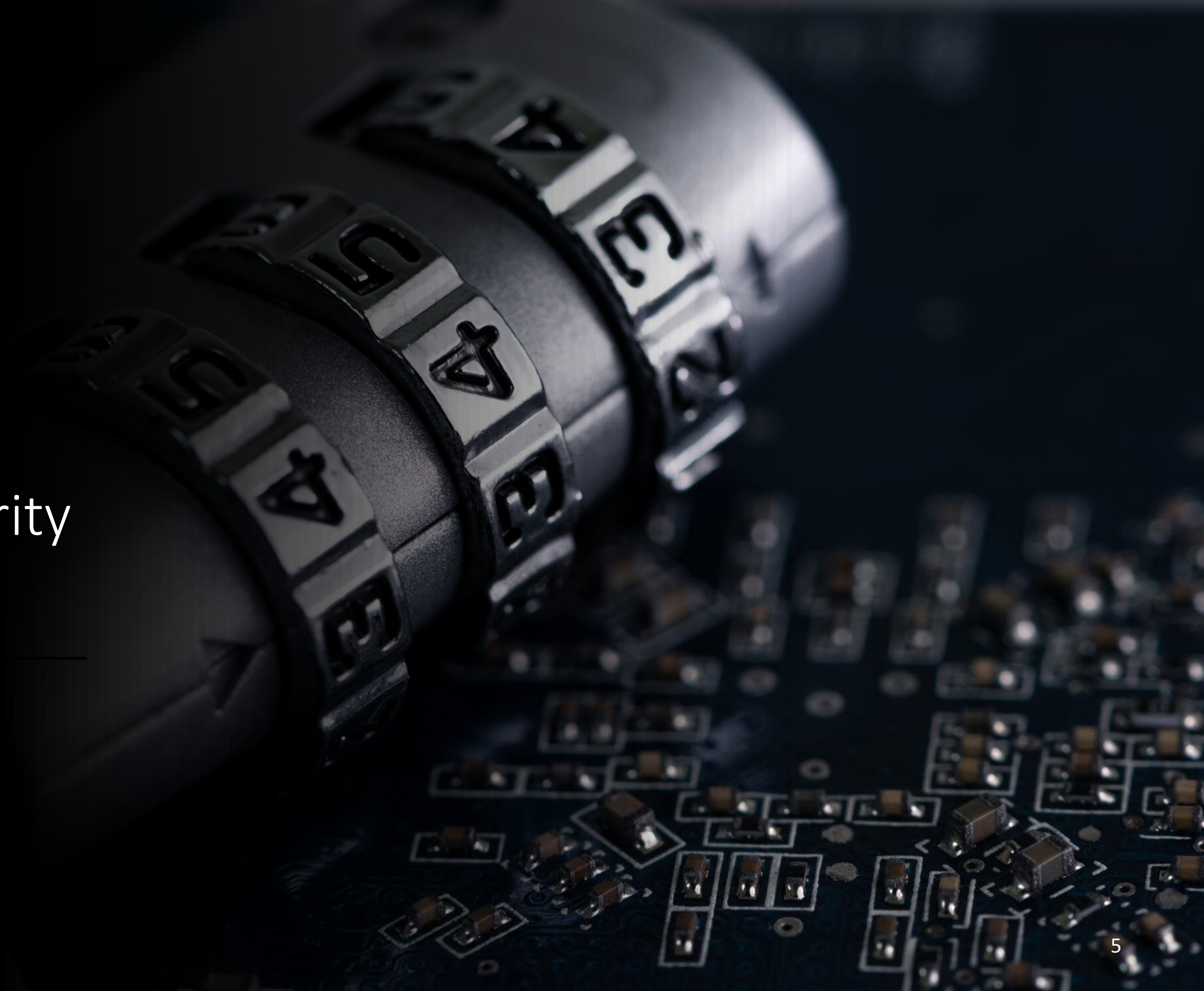
TAs

- Abhishek: Joining Qualcomm Architecture Team
- Prathamesh: Converted from 2-year M.Tech. to 3-year M.Tech. RAP
- Manish: Joining NVIDIA
- Anubhav: Joining MIT hopefully, Intel India Research fellow
- Hrishikesh: EPFL semester exchange

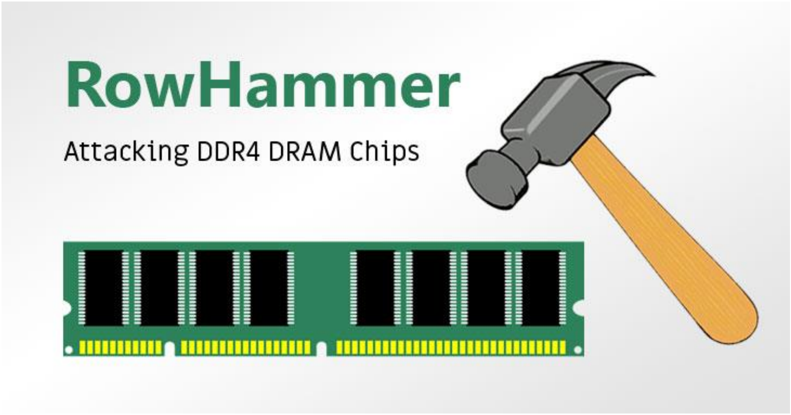
Heard about computer architecture ?

CS773: What is it?

Security and Performance/Security Tradeoffs



Architecture Security: Why?



What Can go wrong?

- You can see secret keys used in crypto libraries ☹
- You can push a billionaire to a millionaire in nanoseconds.
- You can find out who is browsing what at their web browsers, who is running what in an isolated system?

But but but.

You can do all these while the systems stack does not allow you to do.

You can do it because of some mysteries and common sense ideas used in Computer Architecture

It is not Hardware Security ☺

The attacker cannot tamper the hardware physically ☹

Course is also about Mitigation

Security is not for free

But the worlds of Intel, AMD, and Apple cannot sacrifice all that they have done in last 50 years just for architecture security

You are an ML guru. What is CS773 from an ML point of view

✓ Your ML models still run on CPUs and GPUs

We can affect the weights of ML models ☺

Through microarchitecture, can we reverse engineer the ML models: #layers for example ☺

Course Content

- Please check the course website

Assessment Policies

- Mini quizzes = 2 (best of two), Individual = 10
- Mega quizzes (during mid-term and end-term) = best of two, individual = 30
- Two Programming assignments, in next 2 to 2.5 months, individual or group (up to you to decide)=30
- Project (individual or group), up to you to decide=25
- Two minute video on course/course-content = 5

If you do not like exams and assignments

Plan B: Opt only if you are serious about it and can deliver

A research project that can lead to a top conference submission by end of April 2025 – AA grade if you can do that.

Meet me before January 15, if you want to opt for it. I am ok with a large group too.

If you fail, we will grade your progress as per plan A.

Top conferences

Computer Architecture: ISCA, MICRO, HPCA, ASPLOS, PACT

Computer Security: USENIX SECURITY, S&P, CCS, NDSS, Euro S&P

Pre-req (Please drop the course if you feel it is not you)

- Open mind to learn, debate, discuss, and code in C/C++/python
- Interested in asking questions and not only in providing answers ☺
- Ready to spend time in thinking rather than *ing.
- Team player: Trustworthy and professionalism, respecting others' time/suggestions.
- Rest we will take care.

Technically

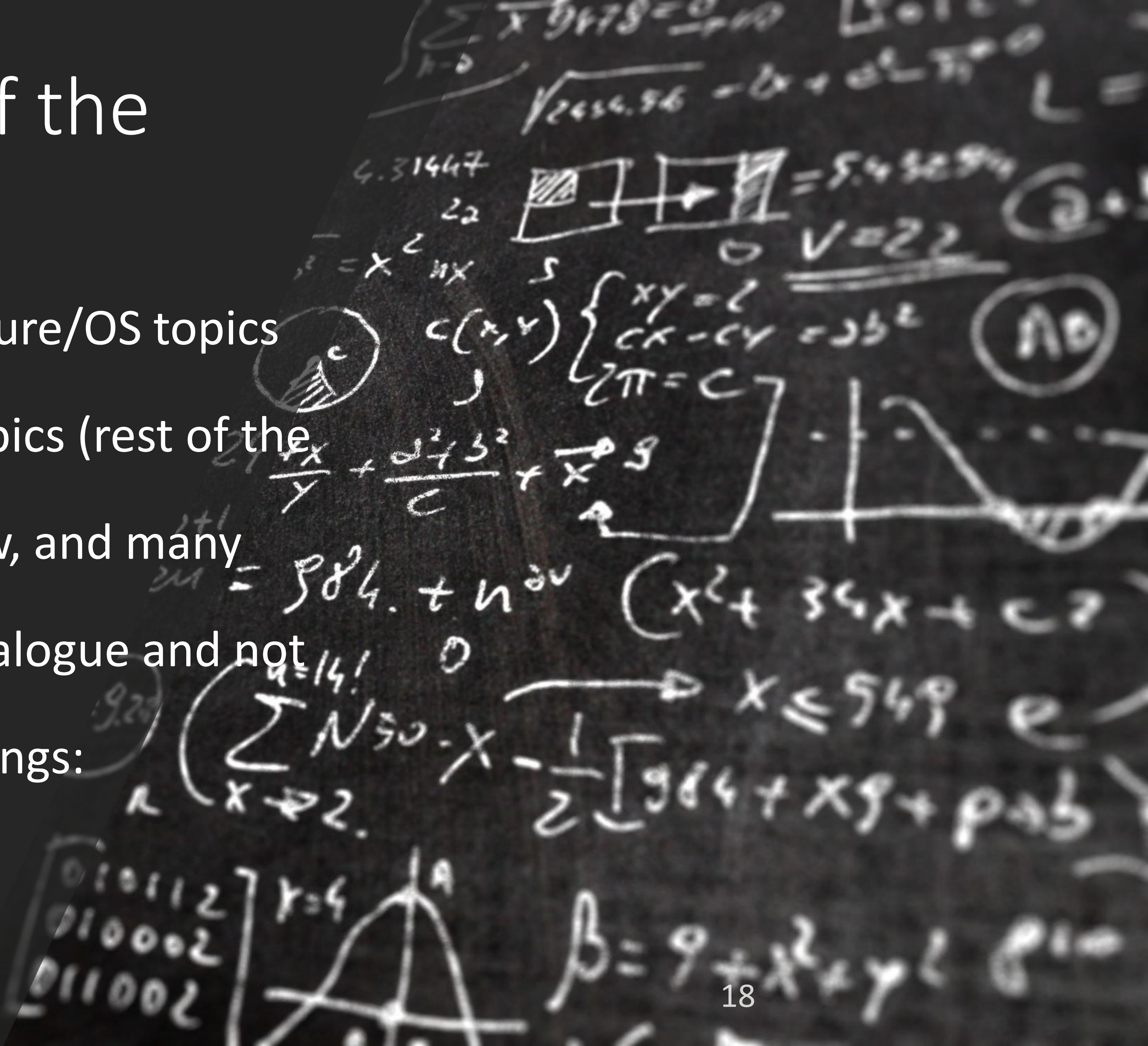
A bit of UG Computer Architecture and a half a bit of OS will be helpful. C/C++/Linux environment

If you know it, it is good

If you do not know it, it is even better.

CS773: Format of the Lectures

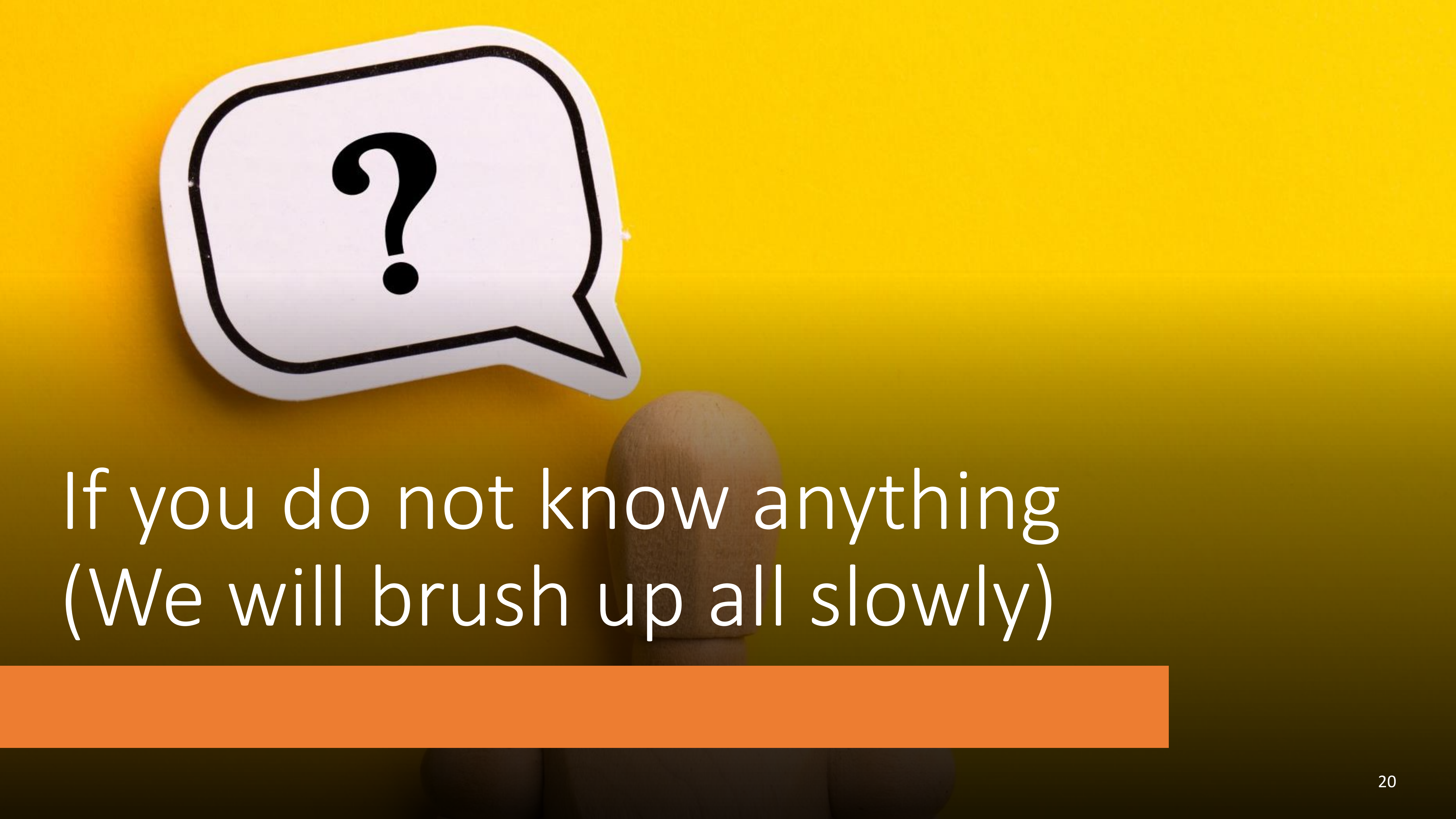
1. Basics of Computer Architecture/OS topics (first few weeks)
2. Advanced state-of-the-art topics (rest of the semester)
3. What can be done? Why, how, and many more
4. Discussion based lectures (dialogue and not monologue)
5. Lectures+discussions+recordings: slides+Chalkboard
6. Guest lectures if possible



Bring your laptop

- For some lectures, we will have hands-on during lecture hours. So, bring your laptop with Linux installed.

- We will inform before time.



If you do not know anything (We will brush up all slowly)

IITB Academic dishonesty protocol (go through it)

https://www.iitb.ac.in/newacadhome/punishments201521July.pdf

https://www.iitb.ac.in/newacadhome/procedures201521July.pdf

More on Assessment

Two Programming Assignments

1st Assignment: Simple one. Not available on web. Goal is to learn how to deliver what is expected with a bit of failure.

#Attack on a real system

2nd Assignment: Mitigations of attacks.

#On tools/simulators

1st Assignment (Coming Soon)

We will have a leaderboard on DDL

Late submissions/penalty

Programming assignments: -2 per day

(Inform TAs at least a week before if you are struggling)

Project checkpoints (I and II):

No late submissions

Projects

PERFORMANCE

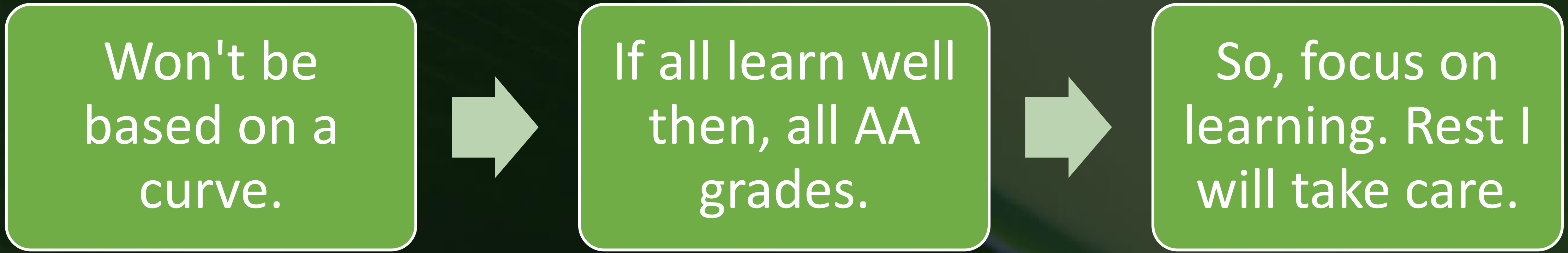
SECURITY

PERFORMANCE AND SECURITY

On real systems, simulators, other tools. We will go through it slowly.

No need to learn all. Depending on your interests, you should learn one (not all)

Grading



Won't be based on a curve.

If all learn well then, all AA grades.

So, focus on learning. Rest I will take care.

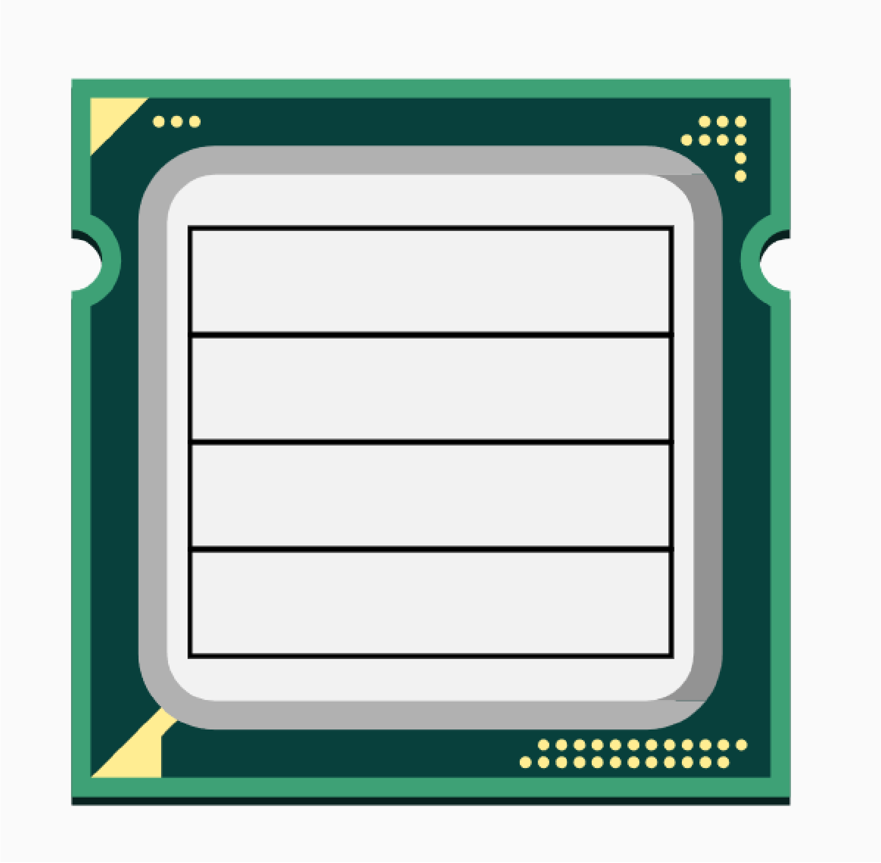
PAUSE

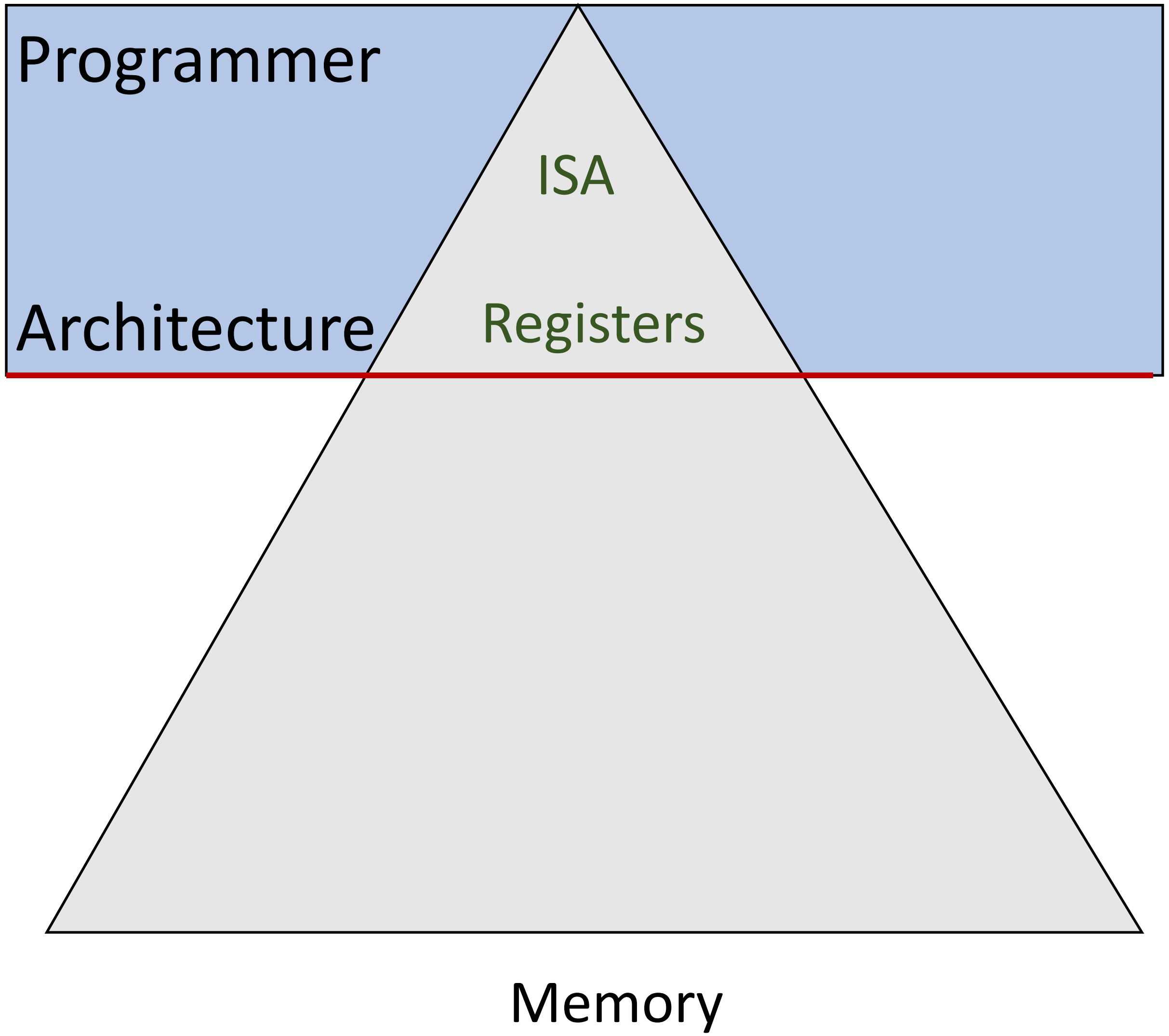
Questions please

Hopefully, some course registrations/drops too ☺

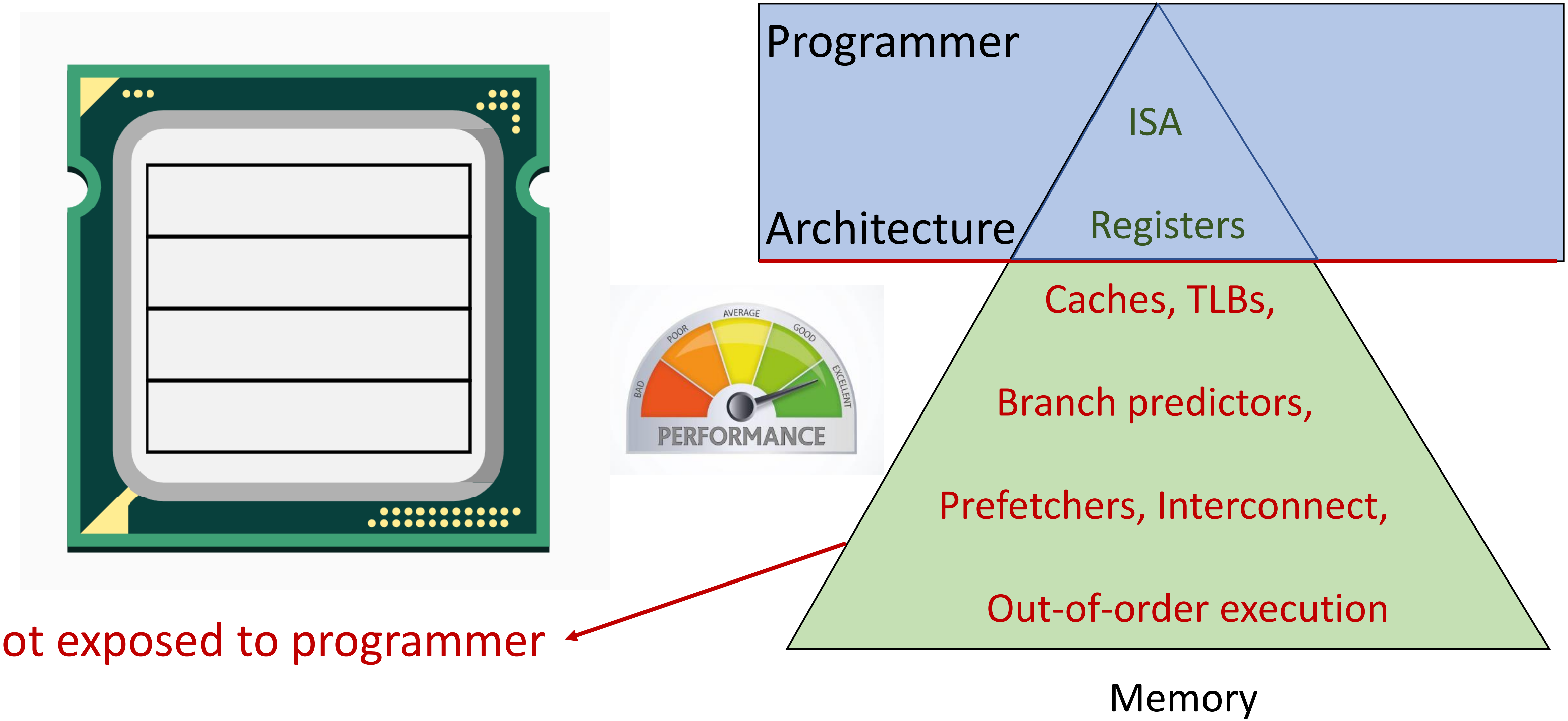
Let’s get Started (Why CS773)

CS773:101



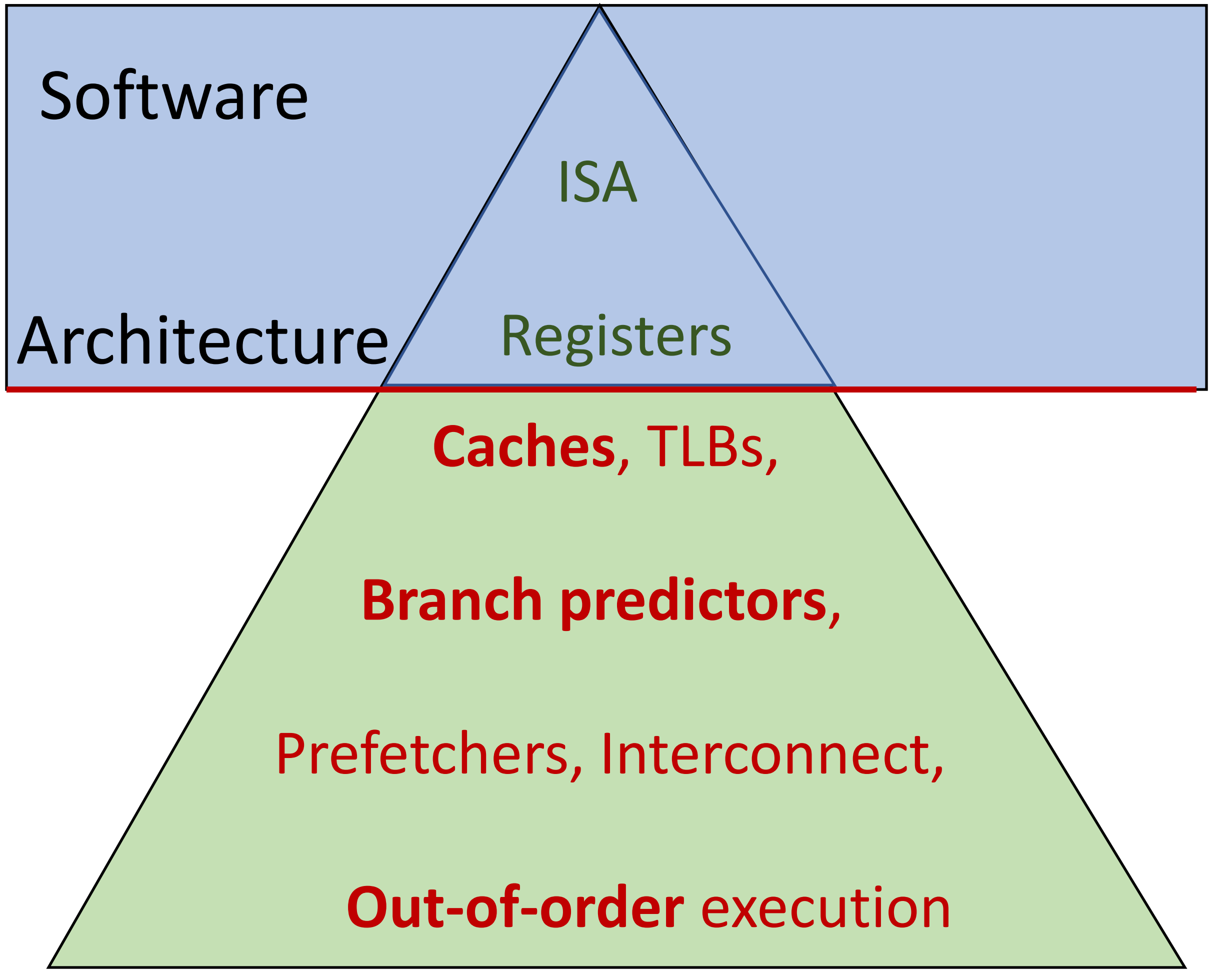


CS773:101



Not exposed to programmer

From Performance to Security



Software

ISA

Architecture

Registers

Caches, TLBs,

Branch predictors,

Prefetchers, Interconnect,

Out-of-order execution

Security (not privacy)

Confidentiality

You do not ***see (READ)*** *what you are not supposed to see*

Integrity

You do not ***change (WRITE)*** *what you are not supposed to see*

Availability

You do not ***affect (DELAY)*** *others (un)intentionally*

Intel Inside; NO; attacks inside ☺

PAUSE (questions)

Drop the Course

It is not a core course. So, no compulsion.

The smaller the number of students, the better (max. 50 around). I am happy, it is just less than 175 so far ☺

By dropping the course, you will help your friends/me who are really interested in this course.

Next Lecture

Brushing up computer architecture-101

Look at CS683 videos:

Lecture 2 (First 15 slides) and

Lecture 4

https://docs.google.com/spreadsheets/d/e/2PACX-1vTZX1W2ALKV9tY39u-ecBYDzLX3XHvVtRnIWtYHTpQmWdGA_K2AIwrLne2jSAZny8-8KxFnuwAyT7fG/pubhtml#

Exam on Thursday ☺

IF THE REGISTRATION COUNT DROPS TO 100, THEN NO EXAM ☺

SO, HELP ME AND YOUR FRIENDS

Thanks