Memory

starting in 5:00

Dr. Goran Soldar
Dr. Khuong An Nguyen

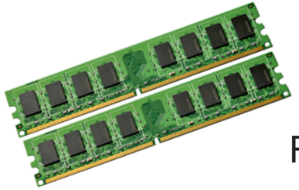
Memory (Human vs Computer)

Date of birth

Short term memory

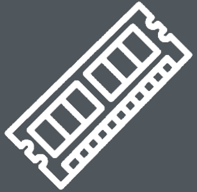
Long term memory

ROM



RAM

HDD



Internal memory

External memory

Data protection

1 | Internal memory

2 | External memory

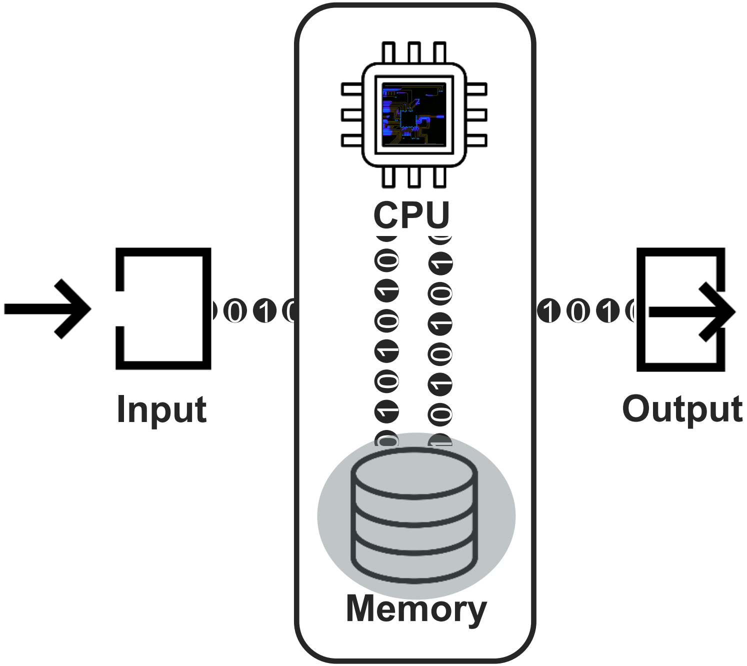
3 | Data protection techniques

Internal memory

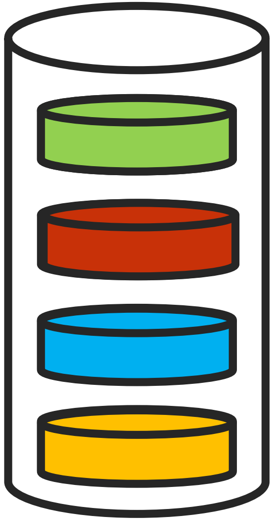
External memory

Data protection

von Neumann architecture



Short-term memory



Short-term memory

Give me some data !

CPU

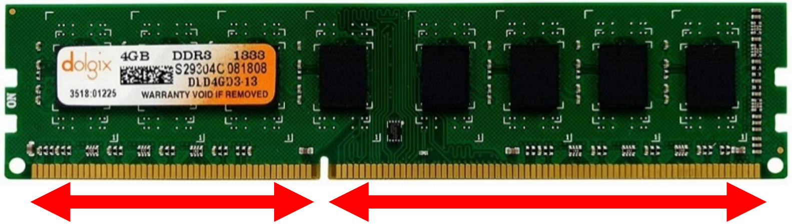
1. Pre-loading programs in short-term memory.
2. Executing quickly and continuously.
3. Data could be accessed in any order.

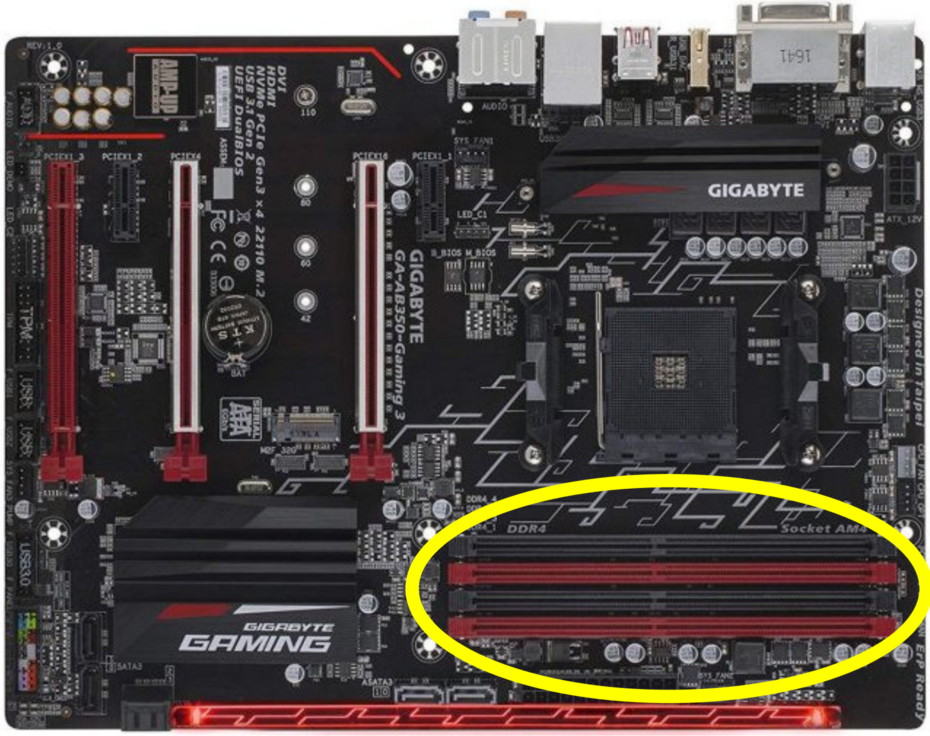
Internal memory

External memory

Data protection

RAM





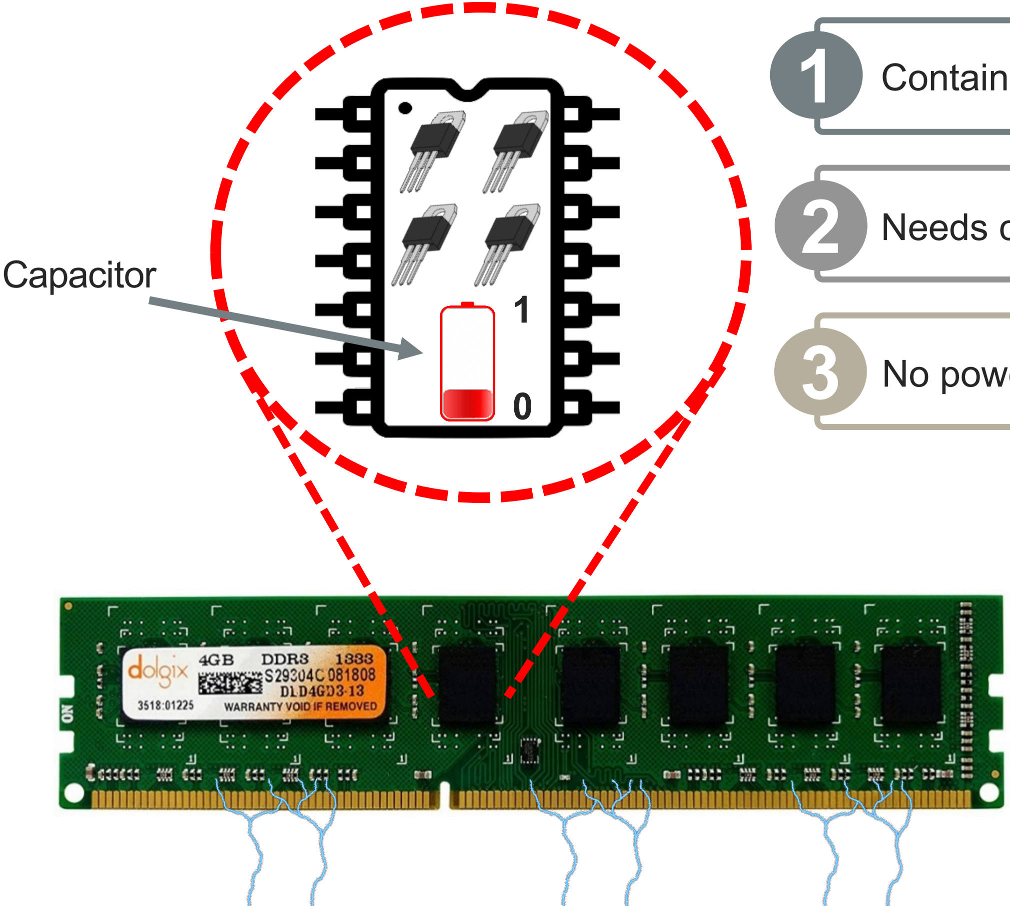
DIMM slots
(Dual Inline Memory Module)

Internal memory

External memory

Data protection

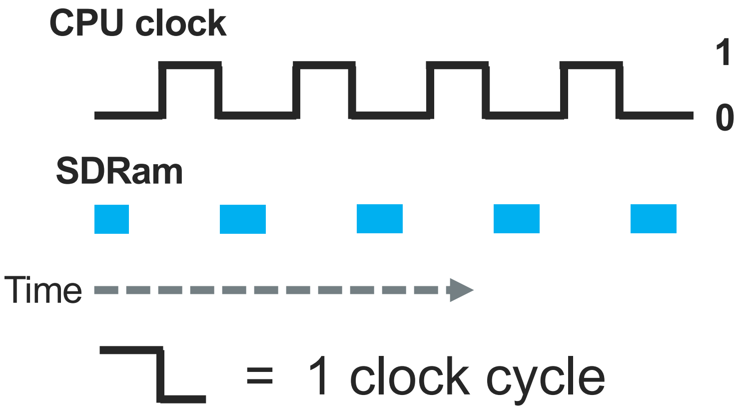
Dynamic RAM



1. Contains transistors and capacitors.
2. Needs constant electric refreshed.
3. No power = Data loss.

Synchronous Dynamic RAM

1. Design of modern computer RAM.
2. Operating synchronously with the CPU clock.
3. Faster than asynchronous DRAM.

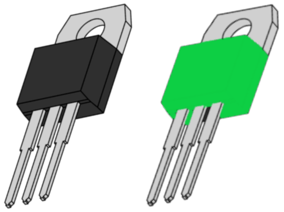


Internal memory

External memory

Data protection

Single-bit error



0 1

"Hello"

	H	e	l	l	o
ASCII	72	101	108	108	111
Binary	01001000	01100101	01101100	01101100	01101111
1-bit mistake	01001001	01100001	01101110	01101110	01100111
	I	a	n	n	g

Internal memory

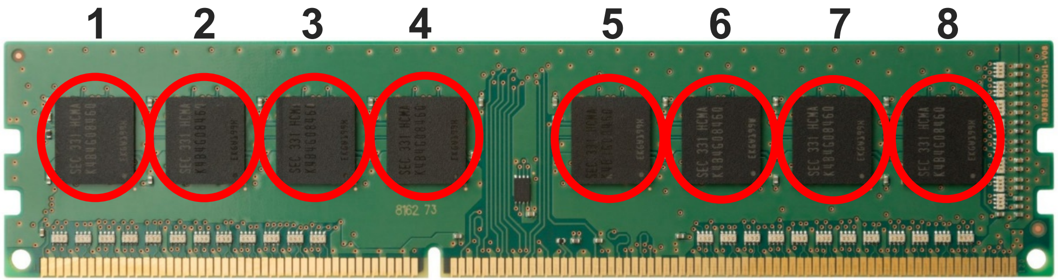
External memory

Data protection

ECC

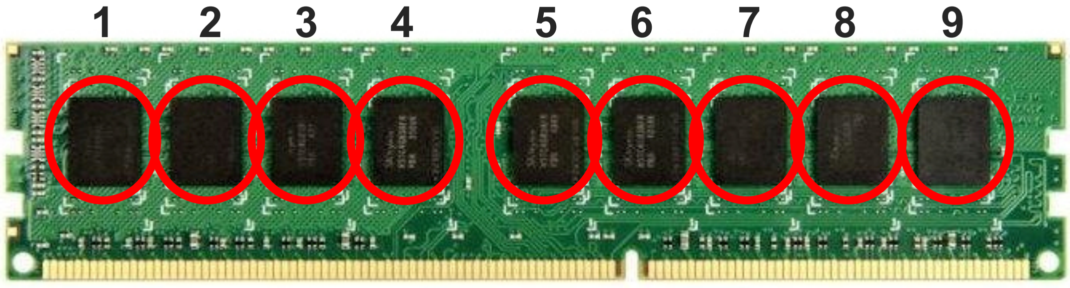
1. Error Correcting Code.
2. Detecting if errors happened in RAM, and makes corrections.
3. Mostly used in servers.

Non-ECC RAM



8 memory chips

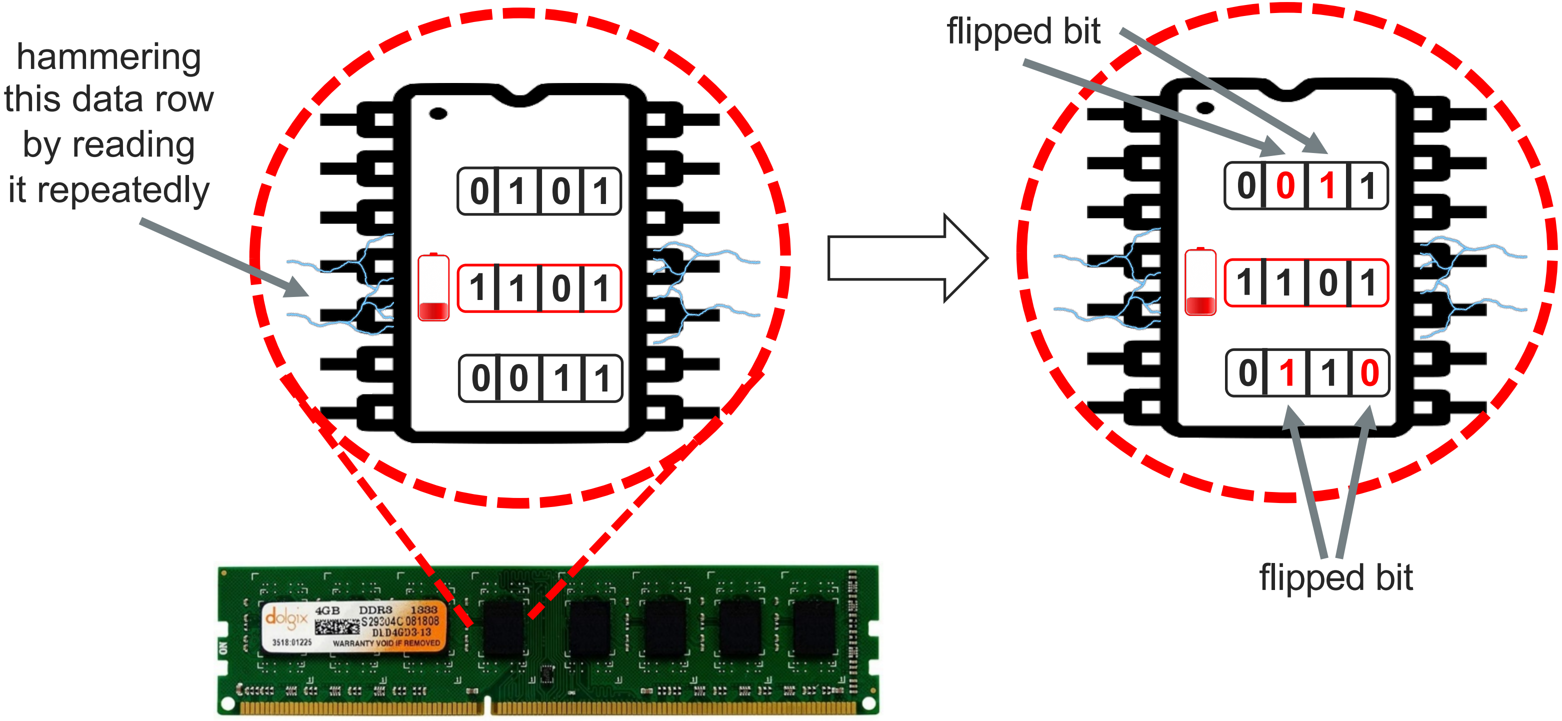
ECC RAM



9 memory chips

RowHammer

1. Bits (data) in DRAM can be consistently induced to flip.
2. >80% of current DRAM are vulnerable.



Internal memory

External memory

Data protection

RowHammer

1. DRAM cells are designed too close to each other.
2. Each cell is not electrically isolated.
3. Accessing one cell affects its neighbourhood cells.

CPU

RAM

```
loop:
   mov (X),  %eax
   mov (Y),  %ebx
   clflush (X)
   clflush (Y)
   mfence
   jmp loop
```

Code : https://github.com/CMU-SAFARI/rowhammer

Further reading

Kim, Y., et al. 2014. “Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors”. ACM SIGARCH Computer Architecture News, 42(3), pp.361-372.

RowHammer (recent exploits)

- **2015** : Gain kernel privileges on x86-64 Linux when run as an unprivileged userland process.
https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

- **2016** : Gain control of smartphone deterministically
Van Der Veen, V., et al, 2016. Drammer: Deterministic rowhammer attacks on mobile platforms.
In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 1675-1689).

- **2016** : Gain unrestricted access to systems of website visitors
Gruss, D., et al. 2016. Rowhammer. js: A remote software-induced fault attack in JavaScript.
In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 300-321). Springer.

- **2019** : Stealing 2048-bit crypto key
https://arstechnica.com/information-technology/2019/06/researchers-use-rowhammer-bitflips-to-steal-2048-bit-crypto-key

- **2020** : Gain access through network requests.
Lipp, M., et al, 2020. Nethammer: Inducing rowhammer faults through network requests.
In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 710-719). IEEE.
(if you do enough load the memory of a remote server, you could cause the memory on the server to flip).

RowHammer (solutions)

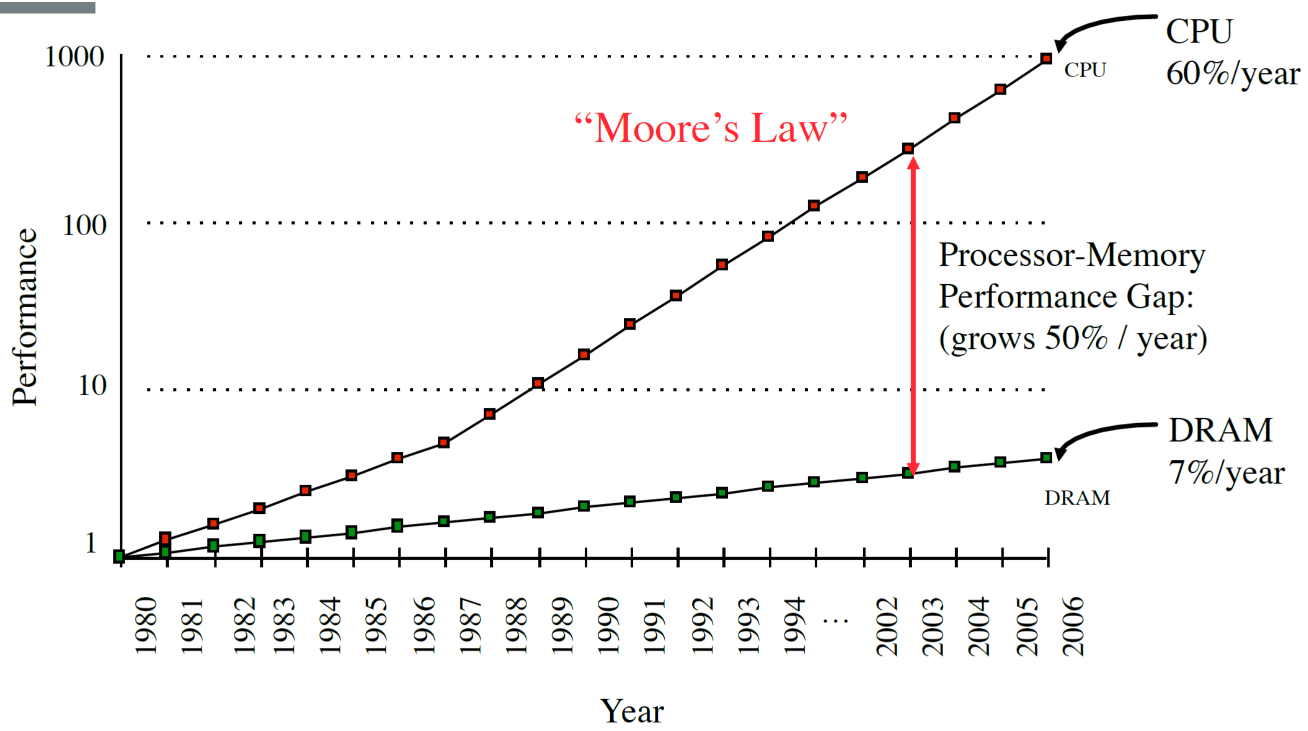
1. Designs better DRAM chips (expensive).
2. Changing refresh frequency (performance).
3. Access control (power, complexity).

Internal memory

External memory

Data protection

Speed : CPU vs RAM



Further reading

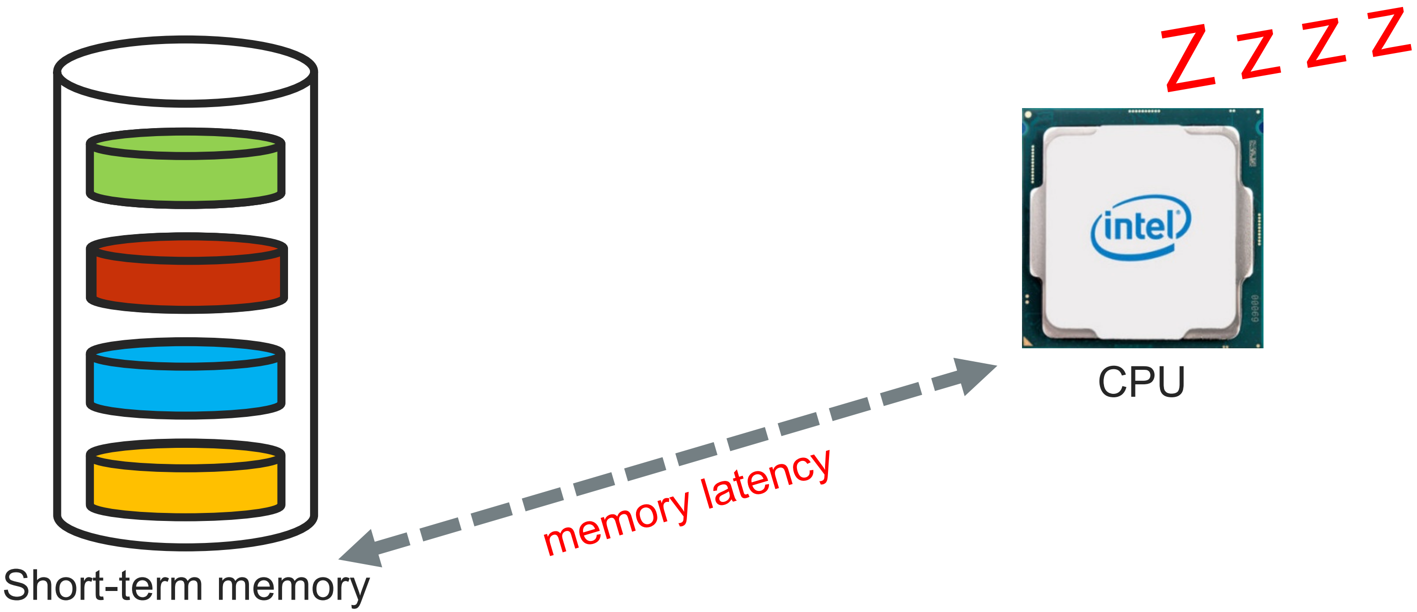
Bahi, M. and Eisenbeis, C., 2011. High performance by exploiting information locality through reverse computing. In 23rd International Symposium on Computer Architecture and High Performance Computing (pp. 25-32). IEEE.

Internal memory

External memory

Data protection

CPU bottleneck

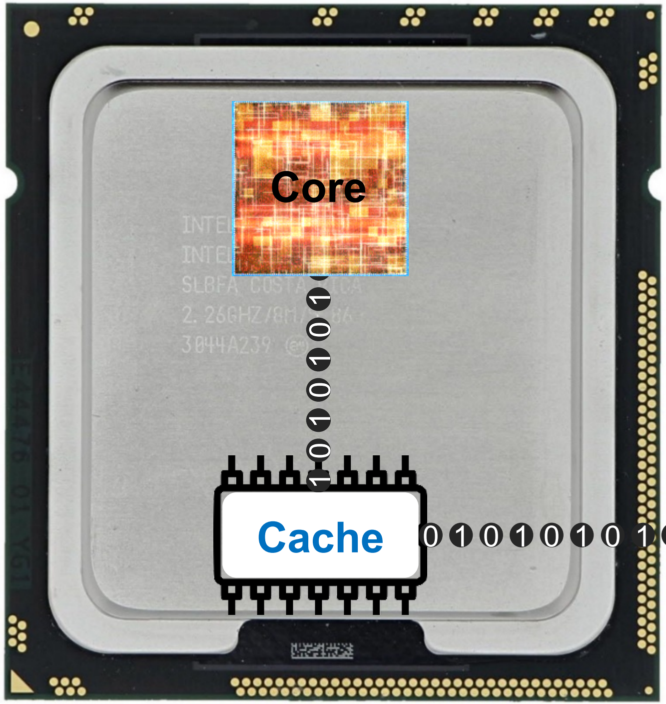


Internal memory

External memory

Data protection

Static RAM (benefits)

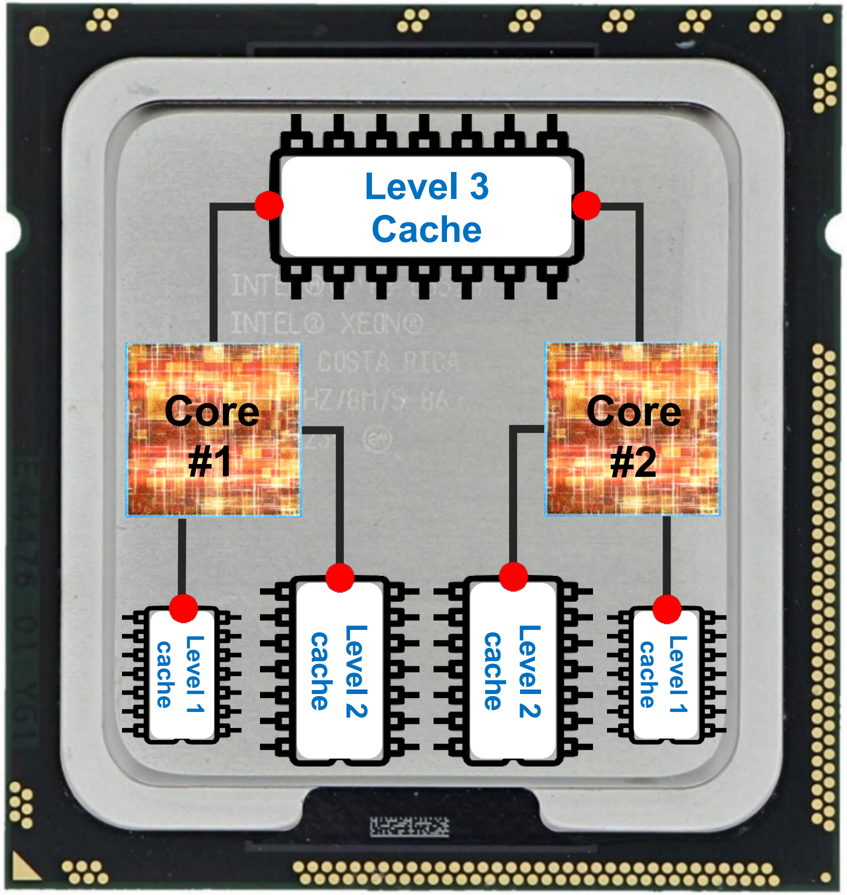


1. Much faster than DRAM & SDRAM.
2. Need no constant electric refreshing.
3. Is built directly inside the CPU.

Static RAM (shortcomings)

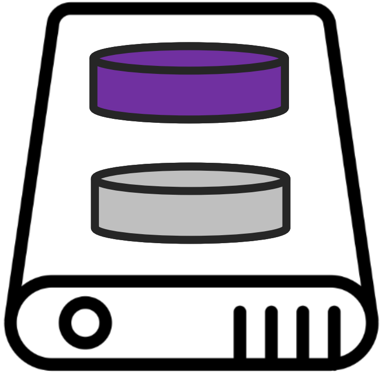
1. Much more expensive than DRAM & SDRAM.
2. Tiny storage capacity (i.e. a few MBs in modern CPUs).
3. Big physical space (i.e. 3 times bigger than DRAM & SDRAM).

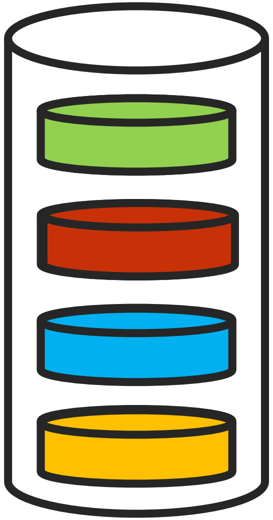
3 levels of cache



1. Level 1 & 2 caches are dedicated to each core.
2. Level 3 cache is shared.
3. Capacity increases, but speed decreases as cache level goes up.

Virtual memory





1. Big program may not fit in RAM.
2. Part of the program is kept in the virtual memory.
3. Slowly transferred to RAM afterwards.

External memory

Problem: RAM can only hold data when there is electricity.

HDD

CD/DVD

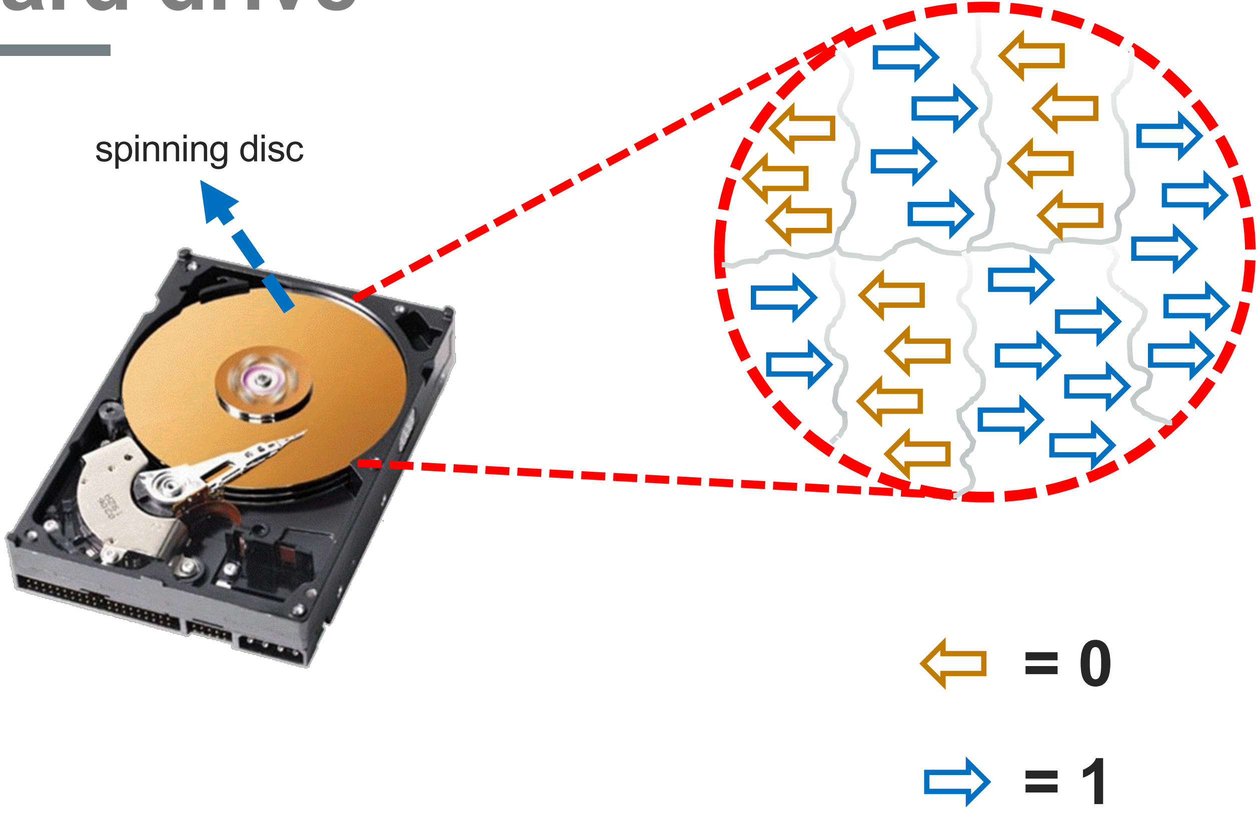
SSD

Internal memory

External memory

Data protection

Hard drive

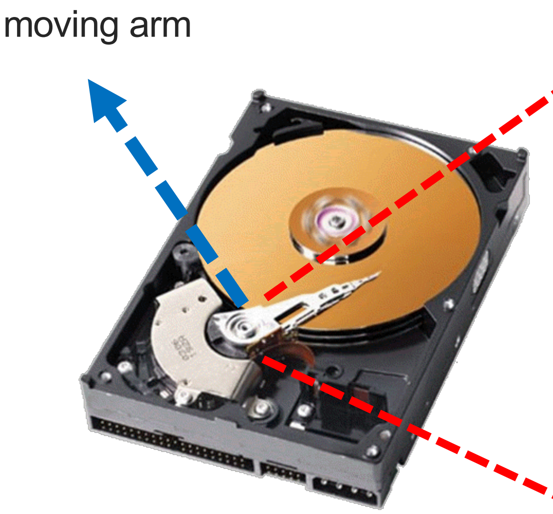


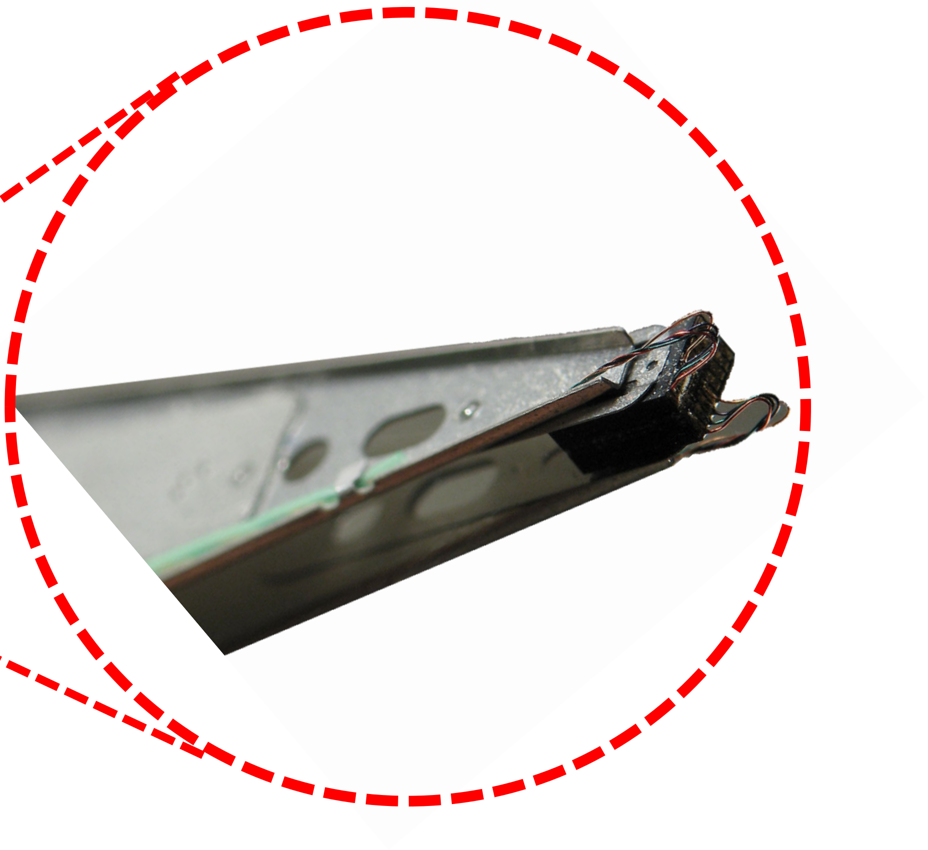
Internal memory

External memory

Data protection

Hard drive



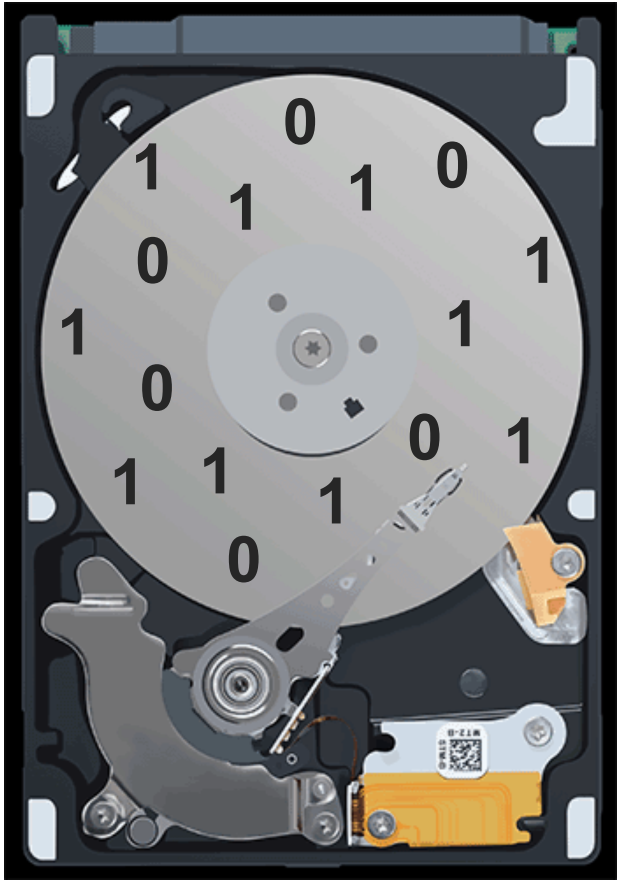


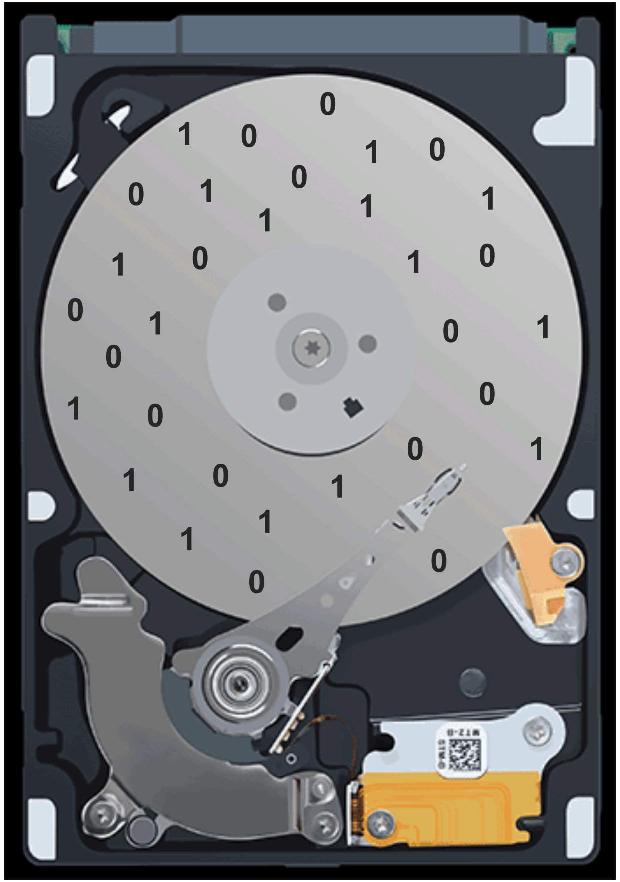
Internal memory

External memory

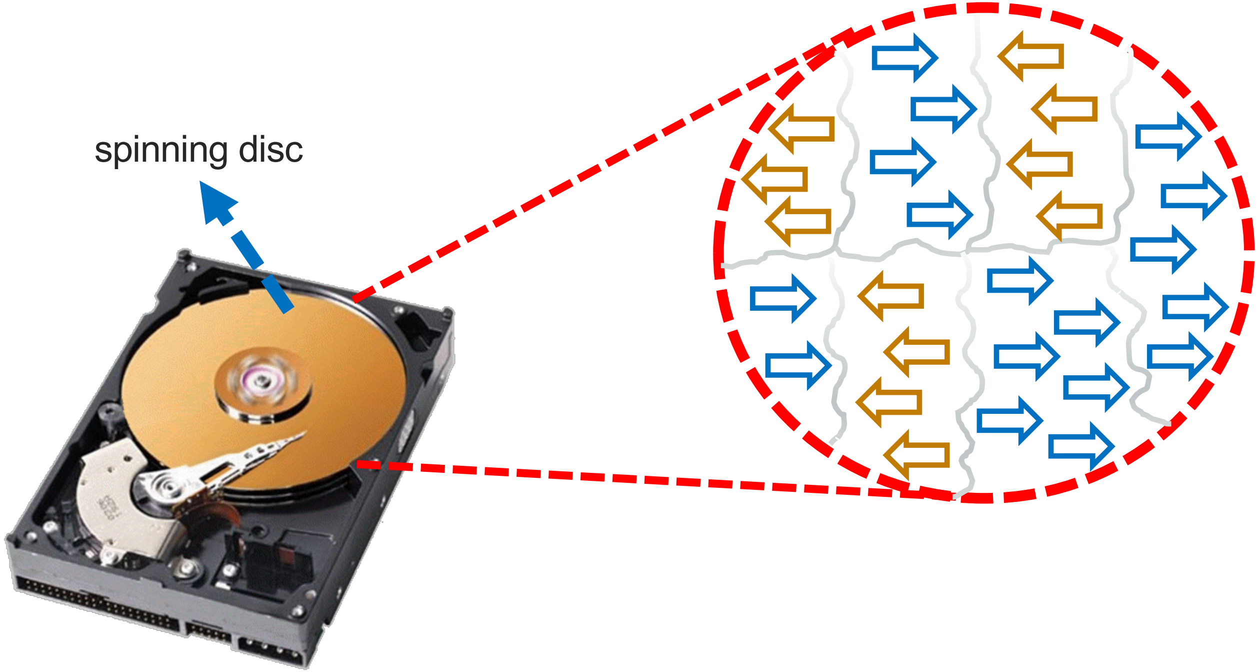
Data protection

Hard drive’s area density





Superparamagnetic effect

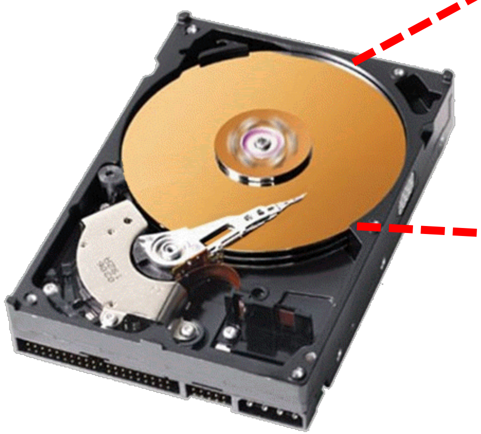


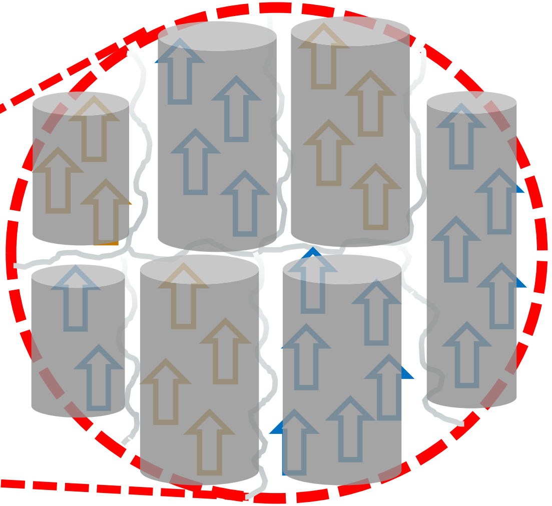
Internal memory

External memory

Data protection

Solution





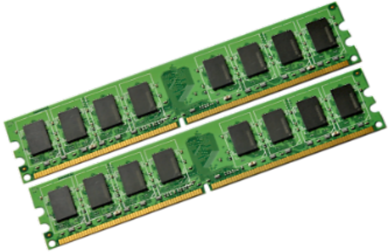
1. Creating a cylinder shape for each section (bit).
2. Increasing the section's height.
3. Keeping the cross section small.

Internal memory

External memory

Data protection

HDD vs RAM



HDD	**RAM**
Cheap	Expensive
Slow	Fast
Using moving heads	No moving part

Internal memory

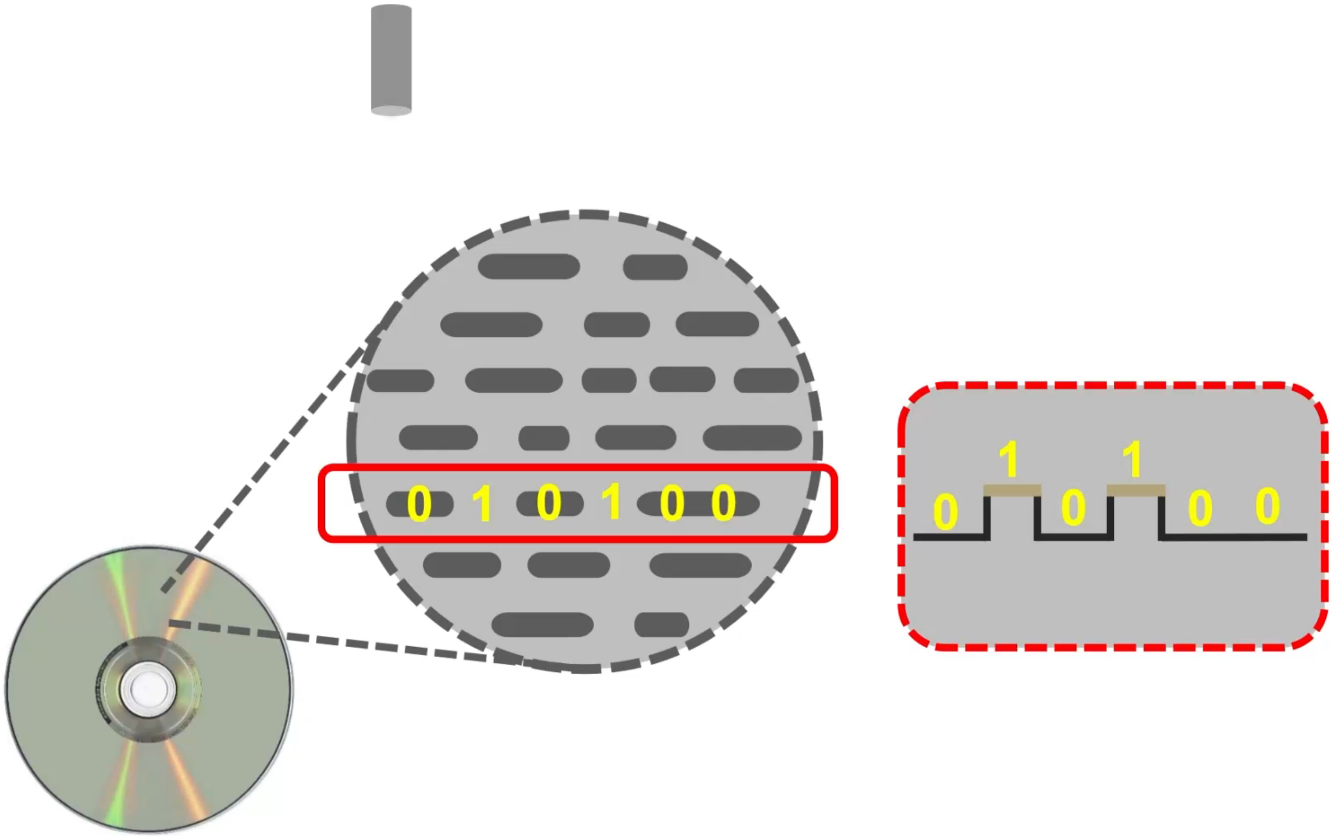
External memory

Data protection

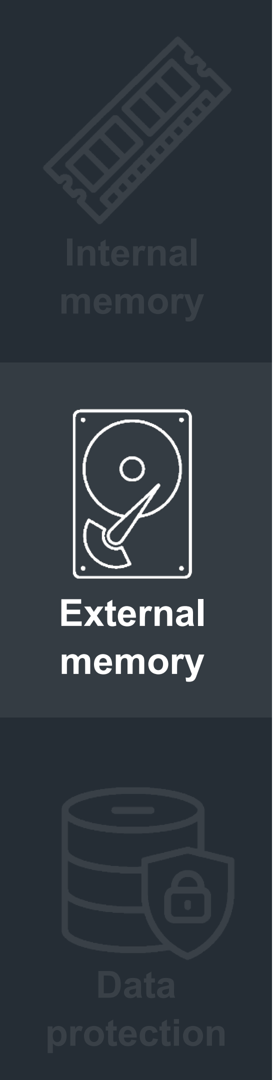
Optical media

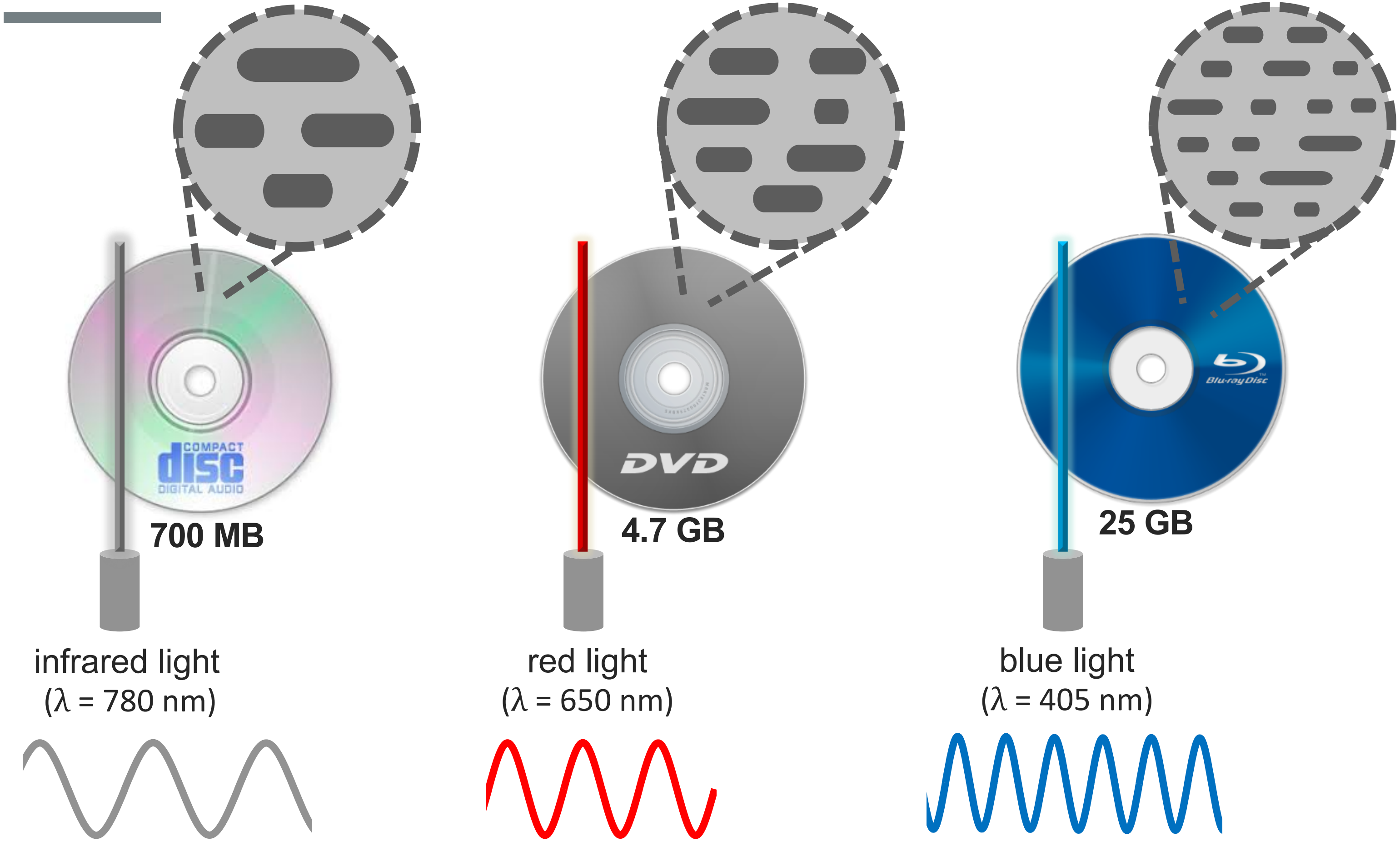
1. Spinning disc.
2. Coated with reflective materials.

Optical media



Optical media





Internal memory

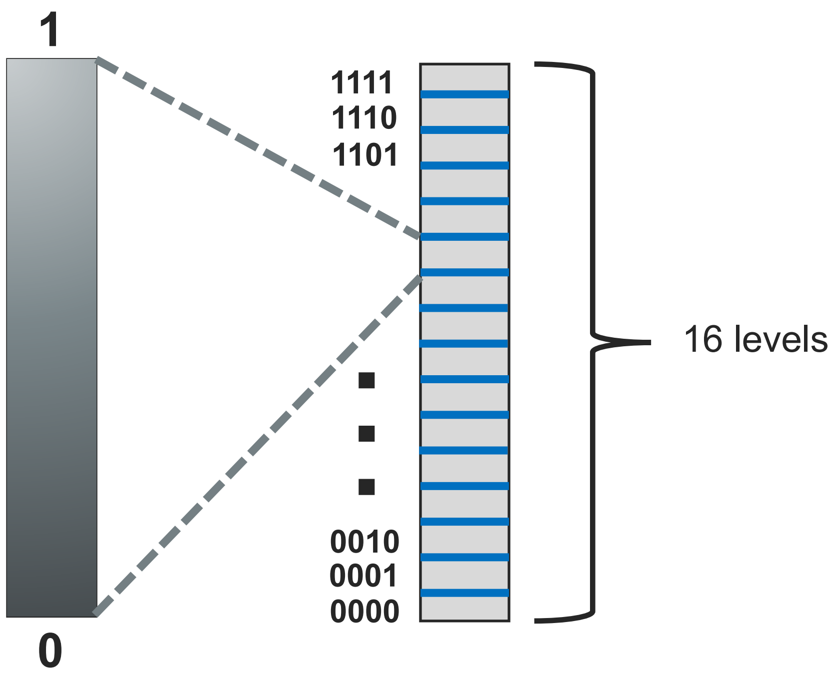
External memory

Data protection

Solid state drive

1. Has no moving parts.
2. Based on floating gate transistors.

Solid state drive



Internal memory

External memory

Data protection

SSD vs HDD

SSD

Instant data access

Fast data random access

Low energy consumption

Completely silent

More expensive per GB

Lower capacity

HDD

Delay while drive spins up

Loses information without power

Higher energy consumption

Noises from moving parts

Cheaper per GB

Higher capacity

RAID

1. Redundant Array of Independent Disks.
2. A technique to prevent data loss.
3. RAID 0, 1, 5, 6, 10.

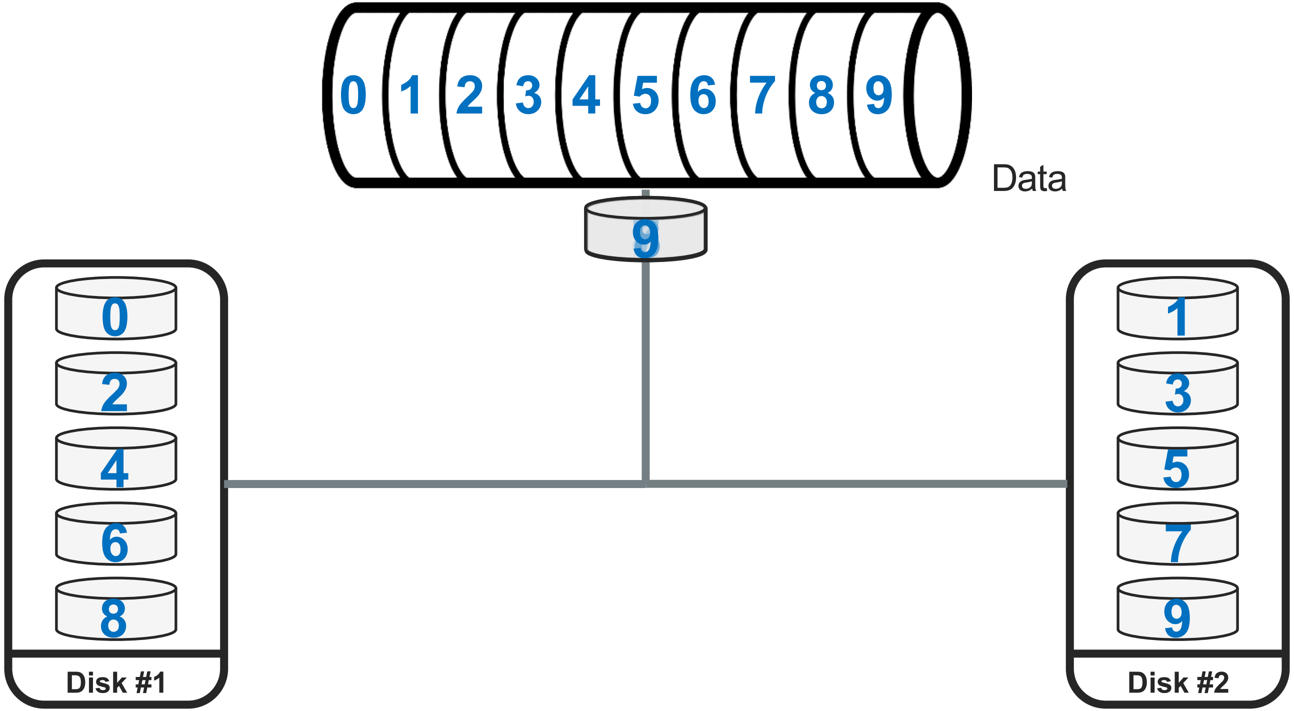
Internal memory

External memory

Data protection

RAID 0

1. Perhaps should not be called RAID.
2. Actually increasing the chance of data loss.
3. Data are spread across disks.



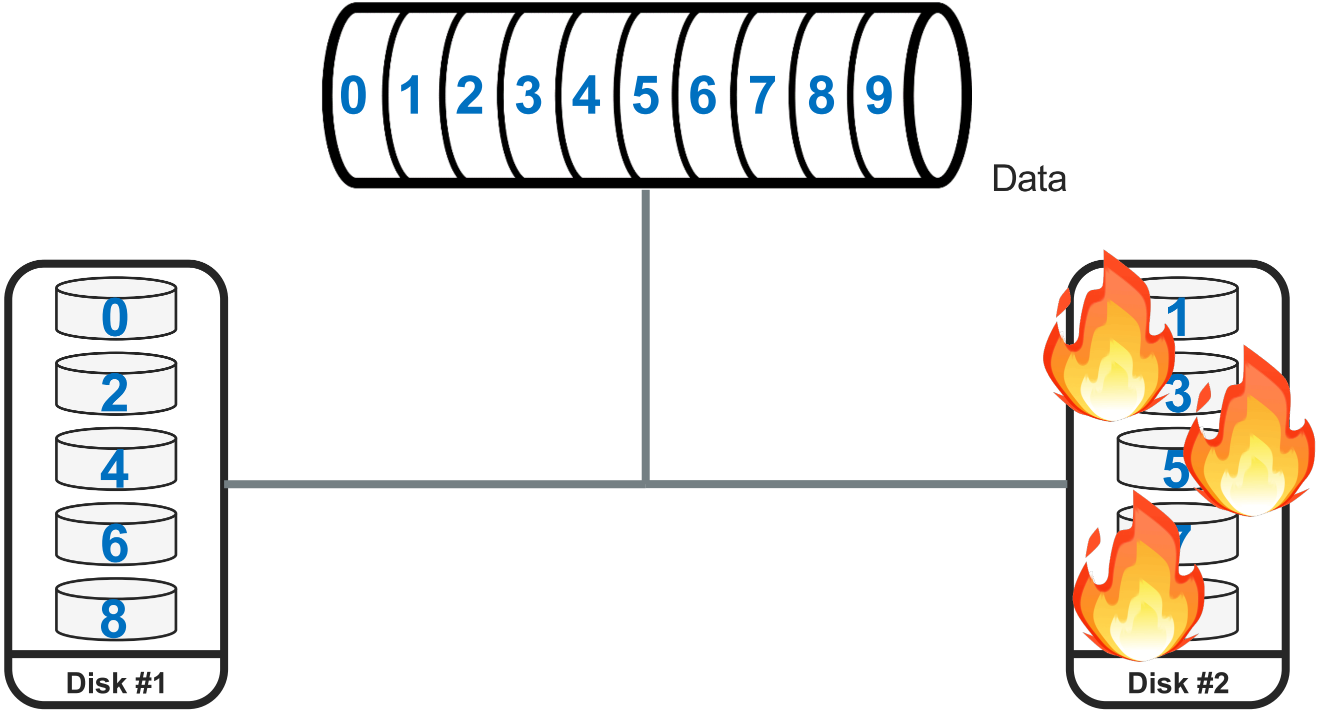
Internal memory

External memory

Data protection

RAID 0

Problem: Cannot restore the original data if one disk is damaged.



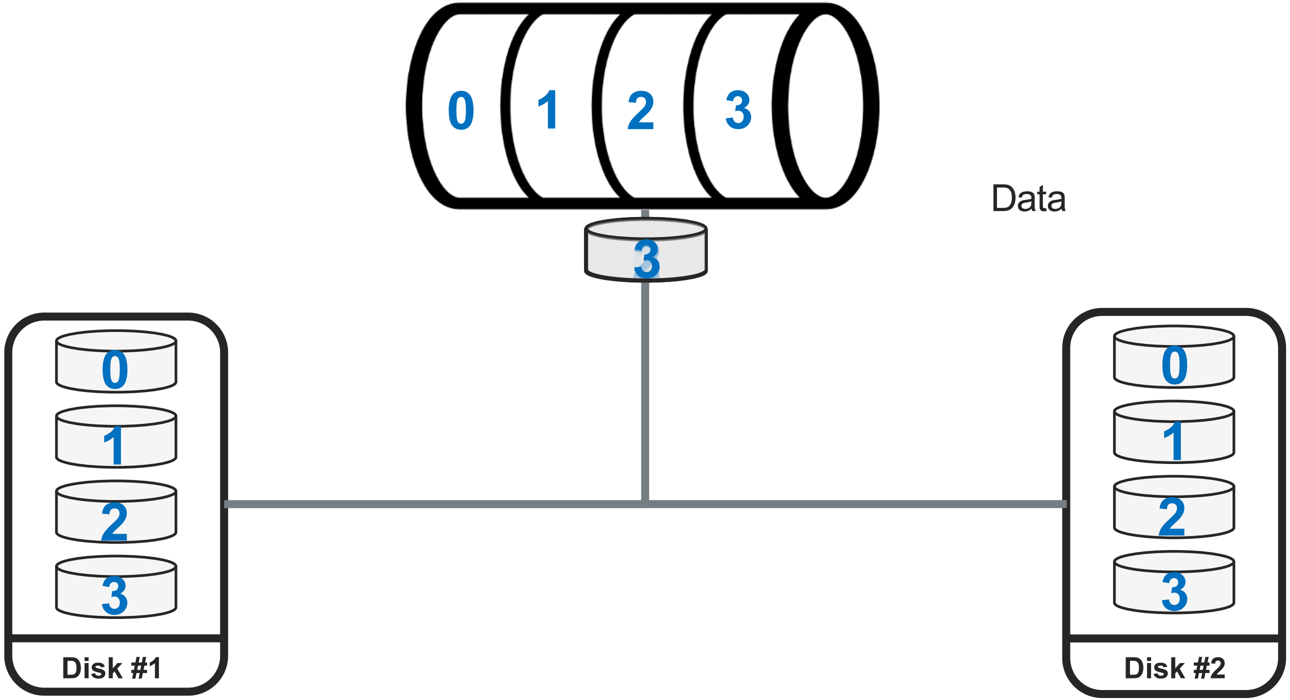
Internal memory

External memory

Data protection

RAID 1

1. Data is duplicated on multiple disks.
2. Similar to keeping a full back-up of the original data.



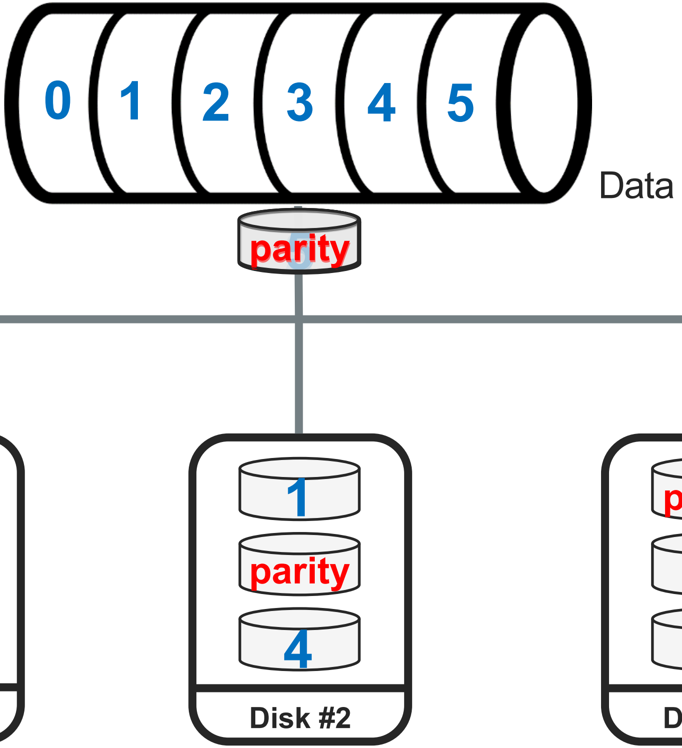
Internal memory

External memory

Data protection

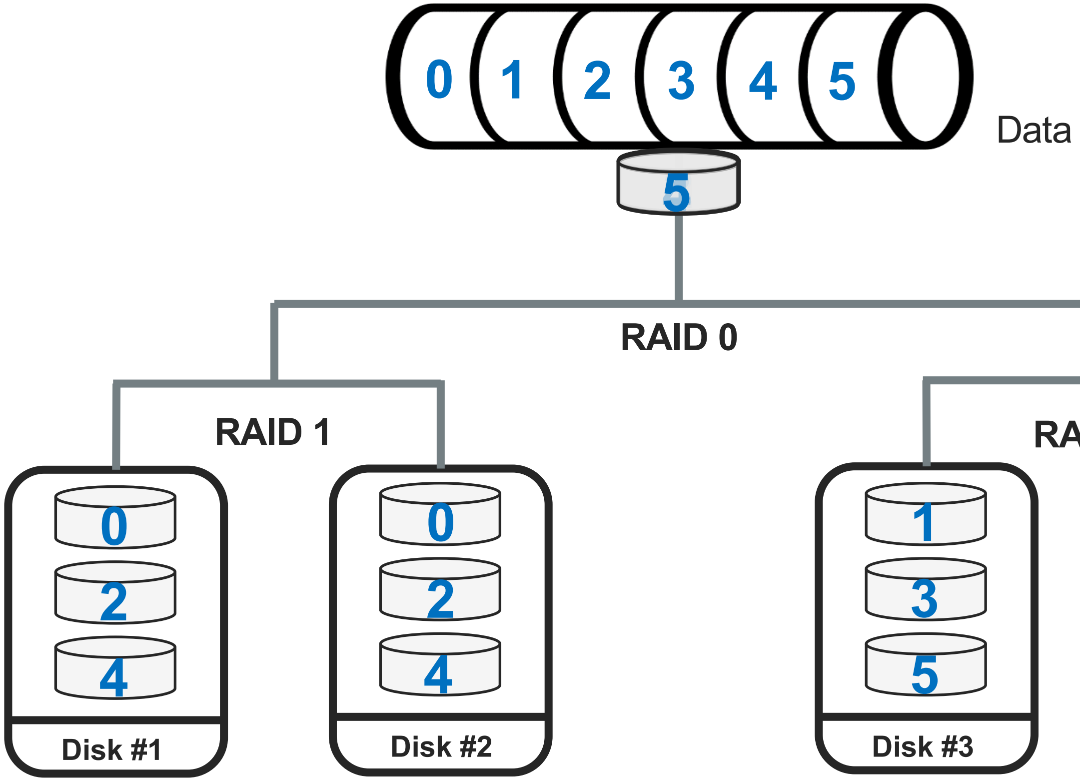
RAID 5

1. Requires at least 3 disks.
2. Data is spread across all disks, along with ‘parity’ information.
3. One whole disk is used to store ‘parity’.



RAID 10

1. A combination of RAID 0 & RAID 1.
2. Requires at least 4 disks.
3. Just 50% of total capacity is available.

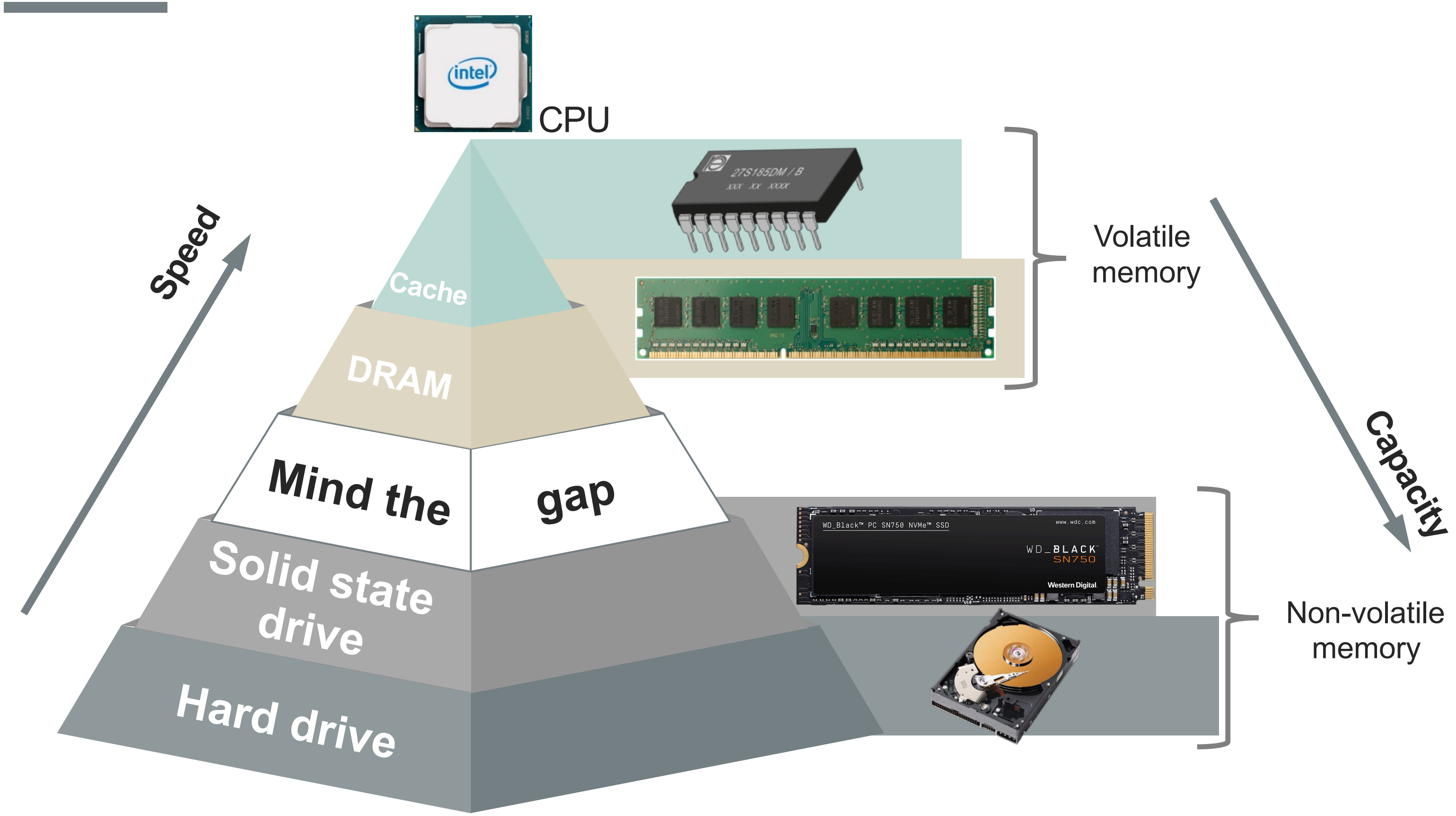


Internal memory

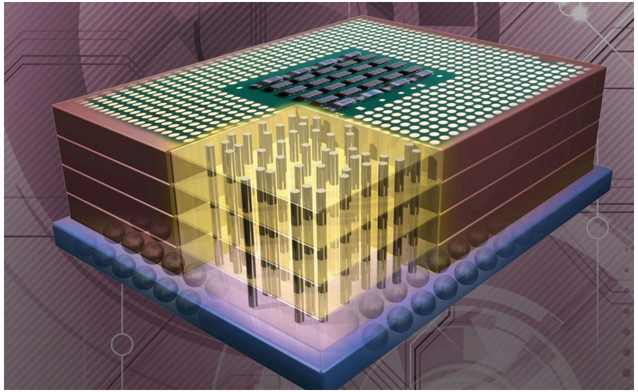
External memory

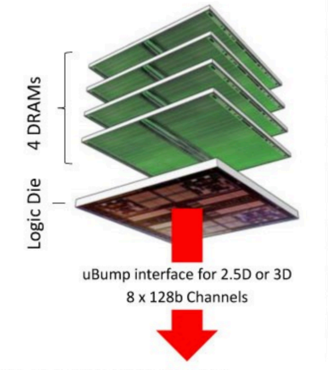
Data protection

Memory hierarchy



FUTURE OF MEMORY





STACKED HBM

dram on top of CPU

Computing logic inside memory layers

Processing in memory (PIM)

Data close to CPU

Post von Neumann Computing

Internal memory

Questions, feedback

Cockcroft building
C519 (Khuong)
C537 (Goran)

K.A.Nguyen@brighton.ac.uk
G.Soldar@brighton.ac.uk

https://khuong.uk

"No one will need more than 640 KB of memory for a personal computer."

— ***Bill Gates, 1981***