**Assignment 4**

Question 1 :

Various DRAM performance techniques are :

1) DRAMs added timing signals that allow repeated accesses to the row buffer without another row access time.

2) The second major change was to add a clock signal to the DRAM interface, so that the repeated transfers would not bear that overhead. *Synchronous DRAM* (SDRAM) is the name of this optimization.

3) Third, to overcome the problem of getting a wide stream of bits from the memory without having to make the memory system too large as memory system density increased, DRAMS were made wider.

4) The fourth major DRAM innovation to increase bandwidth is to transfer data on both the rising edge and falling edge of the DRAM clock signal, thereby doubling the peak data rate. This optimization is called *double data rate* (DDR).

Low power consumption in SDRAM.

* In the most advanced DDR3 SDRAMs the operating voltage has been dropped to 1.35 to 1.5 volts, significantly reducing power versus DDR2 SDRAMs.
* Introducing banks.
* In addition to these changes, all recent SDRAMs support a power down mode, which is entered by telling the DRAM to ignore the clock.

I would choose

* SDRAM: Introduced *banks*, breaking a single SDRAM into 2 to 8 blocks (in current DDR3 DRAMs) that can operate independently.
* Doubling the peak data rate. This is done by increasing the bandwidth to transfer data on both rising and falling edge of the DRAM clock. This is called DOUBLE DATA RATE (DDR).

I would ignore

* Wider DRAMS. Since it increase the power consumption.

**Question 2 :**

PROTECTION THROUGH VIRTUAL MEMORY.

1. Page based virtual memory with a translation lookaside buffer that caches page table entries.
2. Limit what a process can access when running a user process yet allow an operating system process to access more.
3. Provide at least two modes, indicating whether the running process is a user process or an operating system process. This latter process is sometimes called a **kernel process or a supervisor process.**
4. Provide a portion of the processor state that a user process can use but not write.
5. Introducing a mechanism in which processor can go from user mode to supervisor mode and vice-versa.
6. Giving a mechanisms to limit memory accesses to protect the memory state of a process without having to swap the process to disk on a context switch.
7. Provide TLB to translate addresses.

PROTECTION THROUGH VIRTUAL MACHINE ARCHITECTURE.

1. Supports isolation and security.
2. The sharing of a single computer among many unrelated users, such as in a datacenter or cloud.
3. Increases in the raw speed of processors which makes VM overhead acceptable.
4. VM supports different ISAs so that software from the departing ISA to be used until it can be ported to the new ISA.
5. Guest virtual machines run on emulated hardware, which means that the virtual machine monitor has access to all of a guest virtual machine’s state. This includes registers, memory, disk contents, and other I/O device state (such as the video or sound buffer). By dealing with the VMM, security services can monitor all activities on a guest VM from outside.
6. Easier to manipulate the state of a virtual machine than the state of a physical machine.
7. Virtual machine technology makes it possible to recognize an malicious application by testing it on a “cloned” machine and see whether this application behave normally.
8. **System Virtual Machines**. This gives a illusion that users of a VM have an entire computer to themselves, including a copy of the operating system.
9. **Virtual Machine Monitor (VMM).** It is the software that support VM. It determines how to map virtual resources to physical resources.

The main requirements that an architect must fulfil to create a robust virtual machine to prevent security lapses are:

1. Provide a software interface to guest software, it must isolate the state of guests from each other, and it must protect itself from guest software.(Done by VMM).
2. Guest software should behave on a VM exactly as if it were running on the native hardware, except for performance-related behaviour or limitations of fixed resources shared by multiple VMs.
3. Guest software should not be able to change allocation of real system resources directly.

**Question 3:**

A)

Access times generally increase as cache size and associativity are increased.

the access time for the faster L1 cache is assumed to be 1.

Access time = Hit time + Mis Rate\*Miss Penalty

1 way Access time = 1+0.037\*12

= 1.44

2 way Access time = 1.16+0.031\*12

= 1.532

4 way access time = 1.38+0.030\*12

= 1.74

Relative access time of 2-way = 1.532/1.44

= 1.061

Relative access time of 4 -way = 1.74/1.44

= 1.205

B)

Access time = Hit time + Miss Rate\*Miss Penalty

1-way Access time = 1+(0.037+0.028)\*12

=1.78

2-way Access time = 1.16+(0.031+0.006)\*12

= 1.604

4-way access time = 1.38+(0.030+0.0005)\*12

=1.746

**Therefore 2-way Access time is better.**

**C)**

Access time = Hit + Miss rate \* Miss Penalty

1-way access time = 1.2+0.02\*12

= 2.252

2-way access time = 1.16\*2+0.019\*12

= 2.548

4-way access time = 1.38\*2+0.019\*12

= 2.988

**Therefore 1-way Access time is better.**

**Question 4:**

Time =  total power require to hibernate and wake up / total idle time power

given

64 byte to FLASH require 2.56uj.

so , 8\*10^9 bytes(8GB) require 128\*10^7J.

given

64 byte to DRAM require 0.5nj.

So, 8\*10^9 bytes(8GB) require 625\*10^5J.

Idle power consumption = 1.6W for 8 GB

Time = [(2.56\*10^-6 + 0.5\*10^-9)\*2\*8\*10^9 ] / (64\*1.6)

= 400 seconds.