Hardware Security

# Homework 1 - Solution

Student Number: Name:

**Problem 1. (10+10+10pt)** Manufacturing cost

Given the following table, answer the following questions.

| Chip | Die size ($cm^2$) | Estimated defect rate (per $cm^2$) | Transistors (millions) |
|---|---|---|---|
| IBM Power5 | 3.89 | 0.0030 | 276 |
| Sun Niagara | 3.80 | 0.0075 | 279 |
| AMD Opteron | 1.99 | 0.0075 | 233 |

(a) If a 300mm diameter wafer is used to manufacture each chip, how many dies are there in a die?

$$\text{Dies per wafer (IBM Power5)} \approx \frac{\pi \times (30\,/\,2)^2}{3.89} - \frac{\pi \times 30}{\sqrt{2 \times 3.89}} = 147.92$$

$$\text{Dies per wafer (Sun Niagara)} \approx \frac{\pi \times (30\,/\,2)^2}{3.80} - \frac{\pi \times 30}{\sqrt{2 \times 3.80}} = 151.82$$

$$\text{Dies per wafer (AMD Opteron)} \approx \frac{\pi \times (30\,/\,2)^2}{1.99} - \frac{\pi \times 30}{\sqrt{2 \times 1.99}} = 307.96$$

(b) If the wafer yield is 100% and the process-complexity factor is 12, what is the die yield of each chip?

$$\text{Die yield (IBM Power5)} = \frac{1}{(1 + 0.0030 \times 3.89)^{12}} = 0.87$$

$$\text{Die yield (Sun Niagara)} = \frac{1}{(1 + 0.0075 \times 3.80)^{12}} = 0.71$$

$$\text{Die yield (AMD Opteron)} = \frac{1}{(1 + 0.0075 \times 1.99)^{12}} = 0.83$$

(c) If the wafer cost is the same, which chip can be manufactured at the lowest cost?

$$\text{Cost of die (IBM Power5)} = \frac{Cost\ of\ wafer}{147.92 \times 0.87} = 0.0077 \times Cost\ of\ wafer$$

$$\text{Cost of die (Sun Niagara)} = \frac{Cost\ of\ wafer}{151.82 \times 0.71} = 0.0092 \times Cost\ of\ wafer$$

$$\text{Cost of die (AMD Opteron)} = \frac{Cost\ of\ wafer}{307.96 \times 0.83} = 0.0038 \times Cost\ of\ wafer$$

AMD Opteron can be manufactured at the lowest cost.

**Problem 2. (10+10pt)** Reliability

Let us suppose a system consists of four components. MTTF and MTTR of each component is given in the following table.

| | Component A | Component B | Component C | Component D |
|---|---|---|---|---|
| MTTF | 1,000 hours | 500 hours | 200 hours | 500 hours |
| MTTR | 8 hours | 20 hours | 16 hours | 5 hours |

(a) Compute the MTTF of the system as a whole, under the assumption that the lifetimes are exponentially distributed and that failures are independent.

$$\mathrm{FailureRate} = \frac{1}{1000} + \frac{1}{500} + \frac{1}{200} + \frac{1}{500} = \frac{10}{1000} = 0.01$$

$$\mathrm{MTTF} = \frac{1}{\mathrm{FailureRate}} = 100\ (hours)$$

(b) We want to lengthen the MTTF by adding on redundant component. The cost of adding one component is the same for all components. Adding which component results in the longest MTTF?

$$MTTF_{PairA} = \frac{1{,}000^2}{2 \times 8} = 62{,}500$$

$$FailureRate_{PairA} = \frac{1}{62500} + \frac{1}{500} + \frac{1}{200} + \frac{1}{500} = 0.0090$$

$$MTTF_{PairB} = \frac{500^2}{2 \times 20} = 6{,}250$$

$$FailureRate_{PairB} = \frac{1}{1000} + \frac{1}{6250} + \frac{1}{200} + \frac{1}{500} = 0.0081$$

$$MTTF_{PairC} = \frac{200^2}{2 \times 16} = 1{,}250$$

$$FailureRate_{PairC} = \frac{1}{1000} + \frac{1}{500} + \frac{1}{1250} + \frac{1}{500} = 0.0058$$

$$MTTF_{PairD} = \frac{500^2}{2 \times 5} = 25{,}000$$

$$FailureRate_{PairD} = \frac{1}{1000} + \frac{1}{500} + \frac{1}{200} + \frac{1}{25{,}000} = 0.0080$$

Answer: Component C

**Problem 3. (10+10pt)** Amdahl's Law

When making changes to optimize part of a processor, it is often the case that speeding up one type of instruction comes at the cost of slowing down something else. For example, if we put in a complicated fast floating-point unit, that takes space, and something might have to be moved farther away from the middle to accommodate it, adding an extra cycle in delay to reach that unit. The basic Amdahl's law equation does not take into account this trade-off.

(a) If the new fast floating-point unit speeds up floating-point operations by, on average, 2×, and floating-point operations take 20% of the original program's execution time, what is the overall speedup (ignoring the penalty to any other instructions)?

$$Speedup_{Basic} = \frac{1}{0.8 + \frac{0.2}{2}} = 1.11$$

(b) Now assume that speeding up the floating-point unit slowed down data cache accesses, resulting in a 1.5× slowdown (or 2/3 speedup). Data cache accesses consume 10% of the execution time. What is the overall speedup now?

$$Speedup_{Trade-off} = \frac{1}{0.7 + \frac{0.2}{2} + \frac{0.1}{2/3}} = 1.05$$

**Problem 4. (10+10pt)** Cache optimization

You are investigating the possible benefits of a way-predicting L1 cache. Assume that a 64 KB four-way set associative single-banked L1 data cache is the cycle time limiter in a system. As an alternative cache organization you are considering a way-predicted cache modeled as a 64 KB direct-mapped cache with 80% prediction accuracy. It takes two cycles for cache hits and ten cycles for cache misses. A correctly predicted way access that hits in the cache takes one cycle, and three cycles, otherwise (mispredicted). The cache hit rate for a certain workload suite is 0.96 for direct mapped, and 0.98 for four-way set associative cache.

(a) What is the average memory access time (AMAT) of the current four-way set associative cache?

$AMAT_{Current} = 0.98 \times 2 + 0.02 \times 10 = 2.16$

(b) What is the average memory access time (AMAT) of the way-predicting cache?

$AMAT_{Way-predicting} = 0.96 \times (0.8 \times 1 + 0.2 \times 3) + 0.04 \times 10 = 1.744$

**Problem 5. (10pt)** Memory

Whenever a computer is idle, we can either put it in stand by (where DRAM is still active) or we can let it hibernate. Assume that, to hibernate, we have to copy just the contents of DRAM to a nonvolatile medium such as Flash. If reading or writing 64 bytes to Flash requires 2.56 μJ and DRAM requires 0.5 μJ, and if idle power consumption for DRAM is 1.6 W (for 8 GB), how long should a system be idle to benefit from hibernating in terms of energy consumption? Assume a main memory of size 8 GB.

Energy consumption of hibernating $= (2.56 + 0.5) \times 10^{-6} \times 8 \times 10^{9} \div 64 = 382.5\ (J)$

Energy consumption of waking up = Energy consumption of hibernating

$382.5 \times 2 \div 1.6 = 478.125\ (s)$