Name: _____________________________________________

Problem 1 – What this course is all about  ________________/15
Problem 2 – Reliable system design   ________________/12
Problem 3 – Secure and safe systems   ________________/12
Problem 4 – Application-specific processors ________________/8
Problem 5 – Papers and presentations   ________________/12

TOTAL         ________________/59

Attempt to solve all the problems in this exam. Use your time wisely, and pay attention to
the point distribution. Think before you plunge, if you are spending too much time on one
part, move on to another one. All problems are divided in multiple parts; each part is
independent from the others.

If you need more space to work out some the problems, use the backside of the exam sheets
using a statement like “Go to back of page 6”. When in doubt, state any assumption you
make. Show all your work, you will get partial credit for partial answers. Good luck!

HONOR PLEDGE:
“I have neither given not received aid on this exam, nor have I concealed any violations of
the Honor Code.”

Signature: _____________________________________________
1. **What this course is all about – 15 points**

[Hint: Don’t write an essay. You should answer with just a few sentences per question.]

1A. **(3 points)** (i) Give two examples of a permanent silicon fault. (ii) The rate of permanent silicon faults is widely believed to rise in the near future. Why is this the case?

1B. **(3 points)** Give two reasons why resiliency analysis (i.e., simulating a design to discover its ability to correct faults) is much more costly than performance analysis (i.e., simulating a design to see how fast it runs)?

1C. **(3 points)** Checkpointing techniques are often used in the implementation of resiliency mechanisms. (i) What special capability does a checkpointing mechanism provide? (ii) If I add a checkpointing mechanism to my processor design, will it be protected against transient faults? If yes, why, if no, why not?
1D. (3 points) (i) Why are high-quality random numbers needed to build secure systems? (ii) Describe three sources of high-quality "randomness".

1E. (3 points) When designers need to optimize performance, power and cost at the same time, they will often rely on an application-specific design. (i) Why do application-specific designs scale so well? Give an example to support your answer. (ii) In class, we talked about one major trend that threatens the future success of application-specific designs. (iii) What is this trend, and why might it end the benefits of application-specific design?
2. Reliable System Design – 12 points

The following questions are related to reliable system design techniques from the papers we read this semester.

2A. (4 points) The RiVIVal paper uses two techniques to tolerate process variation (i.e., voltage interpolation and variable latency). (i) What is process variation and why does it occur? Process variation can be random (i.e., unique for any particular device) or spatially correlated (i.e., devices near each other have the same variation). (ii) Which of these two types of variability is best tolerated with voltage interpolation, and why? (iii) Which of these two types of variability is best tolerated with variable latency, and why?

2B. (4 points) (i) Describe an example that conveys the trade-off between system reliability and power consumption? (ii) How does Wilkerson’s adaptive cache design provide reliability at very low power?
2C. (4 points) (i) Why do traditional design techniques have large voltage margins? (ii) How does the POWER7 design eliminate much of the voltage margin? (iii) Can the design eliminate all of the voltage margin? If yes, how? If no, why not?
3. Secure and Safe Design – 12 points

The following questions are related to secure and safe design techniques from the papers we read this semester.

3A. (4 points) The SCRAP paper described a signature-based technique to protect against code reuse attacks. (i) What is a code reuse attack, and under what circumstances is it used? (ii) What is a false positive, and why are they problematic for this technique?

3B. (4 points) The MemTracker paper describes a hardware-based technique to detect memory access errors. (i) How does MemTracker provides efficient access to memory state values? (ii) How is it that MemTracker might miss a temporal access error (e.g., accessing heap storage after it has been freed)?
3C. (4 points) (i) Describe two cache-based side-channels that can leak secret information out of a processor. (ii) How does Wang and Lee’s randomization technique lessen the possibility of cache side-channel attacks?
4. Application-Specific Processor Design - 8 points

The following questions are related to application-specific design techniques from the papers we read this semester.

4A. (4 points) Despite requiring 100’s of Watts of power to operate, modern GP-GPUs are remarkably energy-efficient designs. (i) Describe two features of the Fermi architecture that make the design more energy-efficient than a conventional CPU. (ii) Divergent threads occur when threads within a warp go different directions on a branch. Why does this reduce the execution efficiency of the Fermi architecture?

4B. (4 points) The Composite Core design works to reduce the overheads of switching between heterogeneous cores. (i) What are these overheads, specifically? (ii) When does the Composite Core design perform better: when the system wants to switch cores frequently or rarely? And why is this so?
5. Papers and Presentations – 12 points

5A. (6 points) Possessing a well-developed skill for presentation will serve you in any walk of life. Please give three pitfalls to avoid when presenting technical research.

5B. (6 points) Of the papers we reviewed this semester, which would you consider primarily a paper presenting a “solution” to a problem, or an “analysis” to make a case for a problem, or “both”. Mark the papers below with an “S” for solution paper, “A” for an analysis paper, or “B” for both.

- (____) Active Management of Timing Guardband to Save Energy in POWER7, MICRO-2011.
- (____) Designing and implementing malicious hardware, LEET 2008.
- (____) Composite Cores: Pushing Heterogeneity into a Core, MICRO 2012.