Mid Term Practice Exam

Spring 2025

Problem 1: Indicate if the following statement is True/False.

1. Third-party hardware IPs can create trust issues in modern system-on-chip design.
2. Product cipher is always stronger than its individual components used separately.
3. Implementation of asymmetric key cryptography is typically more complex and resource-hungry than symmetric ones.
4. One time pad (OTP) is mathematically breakable.
5. In case of a strong block cipher, we cannot even start decoding ciphertext C before receiving the entire C.
6. A PUF can be used for detecting counterfeit ICs.
7. Error Correction Code (ECC) can be used to improve robustness for signatures in a PUF.
8. A ring oscillator (RO) PUF is a delay based PUF (i.e. it converts delay variation in transistors and interconnects into digital signature).
9. A true random number generator (TRNG) circuit needs to rely on random environmental noise.
10. Active metering does not require communication between design house (IP owner) and foundry.

Problem 2: Explain:

2.1 What is a Caesar Cipher?

2.2 How can a Caesar Cipher be attacked?

Problem 3: What is:

1. Hardware Vulnerability?

2. Integrity?

3. A Cloned IC?

4. A Remarked IC?

5. The difference between asymmetric and symmetric systems?

Problem 4: Hardware Threats

An integrated circuit design and fabrication process can involve three major entities namely IP Vendor, System Integrator, and Fabrication. List all the security and trust issues associated with each of these entities.

IP Vendor:

System Integrator:

Manufacturer:

Problem 5: PUFs

a. What is a Physical Unclonable Functions (PUF)?

b. What are the qualities desired for PUFs and the metrics used to measure PUF quality?

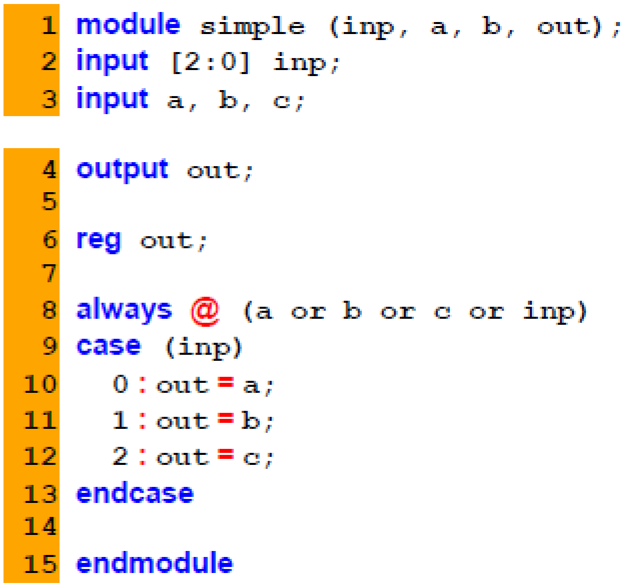
c. What is the difference between watermarking and fingerprinting? For chip authentication, what is preferred and why?

Problem 6: Physical attacks and hardware implementation in FPGA.

a. What is an invasive attack?

b. What is a non-invasive attack?

c. In the following Verilog Code, indicate what input (*inp*) condition is don't care for output variable *out*. How can modify the code to use it as a watermark for the IP?



```
module simple (inp, a, b, out);
input [2:0] inp;
input a, b, c;
output out;

reg out;

always @ (a or b or c or inp)
case (inp)
   0 : out = a;
   1 : out = b;
   2 : out = c;
endcase

endmodule
```

Problem 7: Testing

1. What is Yield?

2. Briefly describe common ways to test chips for defects.

Problem 8: Counterfeit ICs

There are two major test techniques used for counterfeit IC detection, namely electrical test and visual inspection. Briefly describe each of these techniques.

Visual Inspection:

Electrical Test:

Problem 9: Hardware metering

Explain Passive and active metering.

Passive metering:

Active metering:

What were the common issues with some of the hardware metering techniques such as EPIC, logic barriers, etc?: