



JK Lakshmipat University, Jaipur
Institute of Engineering and Technology
End Term Examination, B.Tech., VII Semester

Introduction to Hardware Security (CS1255)

Duration: 2.5 hours

MM: 40

Roll Number:

Instructions to Students:

1. Do not write anything other than your roll number on the question paper.
2. Mention all the assumptions for your answers clearly.
3. Calculators are permitted.

There are three questions in this paper with sub-parts. You have to attempt all the questions.

1. Fill in the Blanks Questions:

(1 x 5 - COs 1, 3, 4, 5, 6)

- (a) A Trojan that activates only when a specific sequence of events occurs uses a _____ trigger.
- (b) A Physical Unclonable Function (PUF) generates a unique response to a given _____.
- (c) In fault injection attacks, attackers intentionally introduce glitches in voltage or _____ to alter circuit behavior.
- (d) The metric used to measure the difference between responses of different PUF devices is called _____.
- (e) In the supply chain, adding unique identifiers to chips helps prevent device _____.

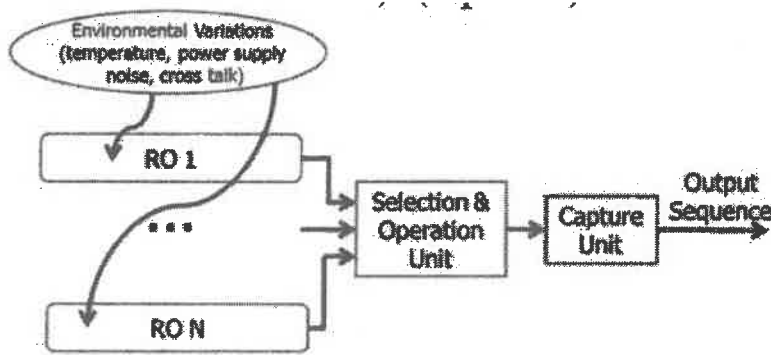
2. Short Answer Questions:

(4 x 6 - COs 3,4,6)

- (a) What is digital watermarking? How is digital watermarking different from digital fingerprinting? Explain with examples.
- (b) A hardware security team is testing a 128-bit Physical Unclonable Function (PUF) to determine whether it is suitable for use in secure authentication systems. During evaluation, they obtain the following results:
 - The average intra-Hamming distance measured from repeated responses of the same device is 5.3 bits.
 - The average inter-Hamming distance measured across multiple devices is 60.5 bits.
 - For one device, 70 out of 128 bits in its response are '1'.

Compute the Bit Error Rate (BER), the Reliability of the PUF, the Uniqueness of the PUF, and the Uniformity.

- (c) The main concern in the present semiconductor era is that even if the cryptographic algorithms are mathematically strong, attackers may still extract secret keys using side-channel attacks (SCA). Explain the different types of SCA that could be used by an attacker to extract secret information from the device. Your answer should include at least four major SCAs, along with a short explanation of how each attack works and what type of physical information it exploits.
- (d) A semiconductor company suspects that some of its fabricated ICs contain Hardware Trojans (HTs). List the main characteristics used to classify HTs.
- (e) Identify the following structure and determine the nature of the output sequence. Justify your answer.



- (f) Consider the following scenario and determine:
 - (i) an attack on the system,
 - (ii) a suitable countermeasure (U/G).

Scenario: Secure Shell (SSH) provides encrypted and authenticated communication. Each time a user presses a key, the SSH client immediately sends an encrypted packet. Researchers have shown that the time interval between key presses leaks information. For example, the interval between typing “a” then “j” is shorter than between “z” and “1” because different fingers and key distances are involved.

3. Long Answer Questions:

(6+5 - CO 4, 6)

- (a) A toy block cipher computes:

$$C = S(P) \oplus K$$

where:

- P is a 4-bit plaintext,
- K is a 4-bit secret subkey (unknown),
- $S(\cdot)$ is a 4-bit S-box,
- C is the resulting 4-bit ciphertext.

The attacker measures Hamming Weight (HW), as HW proportional to power consumption: You are given 10 samples of plaintexts, ciphertexts, and measured power (HW). Your task is to recover the secret key using Differential Power Analysis (DPA).

Given Inverse S-Box (4×4, Hex Format)

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S^{-1}(x)$	3	E	5	8	7	D	1	B	6	0	F	4	9	2	C	A

Collected Power Trace Data

Sample	C (Ciphertext, bin)	Measured Power $\alpha \cdot \text{HW}$
1	0001	2
2	1010	3
3	1101	3
4	0011	2
5	1111	4
6	1001	2
7	1000	1
8	0110	2
9	1011	3
10	1110	3

For each trace:

$$P_{\text{Guess}} = S^{-1}(C \oplus K_{\text{Guess}})$$

Compute:

1. For key $K = D$ and $K = 9$, compute the predicted intermediate plaintext value.
2. Compute the predicted selection bit (choose LSB).
3. Partition the power traces into two groups (bins):

$$\text{Bin 0: } b = 0, \quad \text{Bin 1: } b = 1$$

4. Compute the difference of means:

$$\Delta = \text{mean}(\text{Bin 1}) - \text{mean}(\text{Bin 0})$$

5. Identify the correct key.

- (b) A digital circuit consists of **10,000 gates** and normally consumes an average dynamic power of

$$P_{\text{normal}} = 42.8 \text{ mW.}$$

A Hardware Trojan (HT) is suspected. The attacker has inserted:

- a combinational trigger of 12 gates, activated when a rare 8-bit sequence occurs,
- a payload of 20 gates that toggle only when the trigger activates.

Trace No.	Input Pattern Probability	Measured Power (mW)
1	0.25	42.9
2	0.10	42.8
3	0.40	42.9
4	0.07	43.2
5	0.28	42.9
6	0.05	43.2
7	0.12	42.8
8	0.03	43.2

Table 1: Collected Power Traces

When activated, the Trojan's dynamic power contribution per toggling gate is:

$$P_{\text{gate}} = CV^2f = 0.004 \text{ mW per gate.}$$

The defender performs statistical side-channel power analysis. Eight power traces were collected:

The trigger activates only when the input probability satisfies:

$$\text{Probability} < 0.1.$$

Perform the following:

1. Compute the dynamic power contributed by the Trojan payload.
2. Identify which traces show Trojan activation.
3. Compute the expected power during Trojan activation:

$$P_{\text{expected}} = P_{\text{normal}} + P_{\text{HT}}.$$

4. For the above-computed Trojan-activated traces, compare the measured power with the expected power.