

Unit 9 - Week 8

Course outline

How does an NPTEL online course work?

Week 1

Week 2

Week 3

Week 4

Week 5

Week 6

Week 7

Week 8

Power Analysis Attacks

Hardware Trojans

FANCI : Identification of Stealthy Malicious Logic

Detecting Hardware Trojans in ICs

Protecting against Hardware Trojans

Side Channel Analysis

Fault Attacks on AES

Demo: Cache-timing based Covert Channel - Part 1

Demo: Cache-timing based Covert Channel - Part 2

Demo: Cache timing attack on T-table implementation of AES

Quiz : Practice Assignment 8

Quiz : Assignment 8

Week 8 Feedback

Download Videos

Text Transcripts

Assignment 8

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment.

Due on 2020-03-25, 23:59 IST.

1) A CMOS inverter is a combination of a PMOS and an NMOS connected in series having the same input.

1 point

- True
 False

No, the answer is incorrect.
Score: 0

Accepted Answers:
True

2) Power Analysis can be used to predict keys of ciphers like RSA and AES

1 point

- True
 False

No, the answer is incorrect.
Score: 0

Accepted Answers:
True

3) In Power Consumption models, the Hamiltonian Distance and Manhattan distance Models are commonly used.

1 point

- True
 False

No, the answer is incorrect.
Score: 0

Accepted Answers:
False

4) High value of Pearson's correlation coefficient means that the attacker's prediction is far from the actual key value

1 point

- True
 False

No, the answer is incorrect.
Score: 0

Accepted Answers:
False

5) I. There are special libraries which have cells/gates that consume power uniformly for different operations
II. DRECON is an Algorithmic approach to solve the Power Attacks on ciphers

1 point

- I- True,II-False
 I- False,II-False
 I- True,II-True
 I- False,II-True

No, the answer is incorrect.
Score: 0

Accepted Answers:
I- True,II-True

6) Underfeeding Voltage and Varying temperature may lead to a skipping of instruction causing a fault in the circuit

1 point

- True
 False

No, the answer is incorrect.
Score: 0

Accepted Answers:
True

7) Let O and O' be the output of a main and redundant circuit used in redundancy based countermeasures for fault attacks. Which of the following is true for the circuit to be not faulty

1 point

- O or $O' = 1$
 O xor $O' = 1$
 O and $O' = 1$
 O or $O' = 0$

No, the answer is incorrect.
Score: 0

Accepted Answers:
 O or $O' = 0$

8) Clock glitch attack leads to Setup and hold time violation in the flops of a circuit

1 point

- True
 False

No, the answer is incorrect.
Score: 0

Accepted Answers:
True

9) Introducing a Stuck at 0 faults in the last round of a 256 bit cipher X is the easiest and most economic

1 point

- True
 False

No, the answer is incorrect.
Score: 0

Accepted Answers:
False

10) In the 1980s when NASA sent spaceships to the space they saw abnormal behaviour in the digital circuitry of the spaceship. This was mainly caused due to

1 point

- Radiation
 Laser Beams
 Clock Glitch
 The Force

No, the answer is incorrect.
Score: 0

Accepted Answers:
Radiation