Computer Science and Engineering

Course work portal

powered by Moodle v2x

Hardware Security

Home > My courses > Previous Years > 2020 > Spring Semester (2020-21) > Hardware Security > Class Test 3 > Class Test 3

Started on	Monday, 12 April 2021, 5:01 PM
State	Finished
Completed on	Monday, 12 April 2021, 6:05 PM
Time taken	1 hour 4 mins
Grade	**15.00** out of 43.00 (**35**%)

Question 1

Complete

Mark 3.00 out of 5.00

Flag question

Mr. Spillover wants to attack the AES by inducing a single byte fault on the first byte in the 8th round of execution. However, while inducing the fault, he spills it in multiple bytes as shown in the figure below. He goes to Prof. Pacifier for help. Prof. Pacifier says that he will still be able to extract the key. Explain how the attack will still work briefly. You can write the answer in pen and paper and upload the picture also.

▨	▨		
	▨		
			▨

Please upload your answer in .pdf or .jpeg file format

CamScanner 04-12-2021 17.43.14.jpg

Question 2

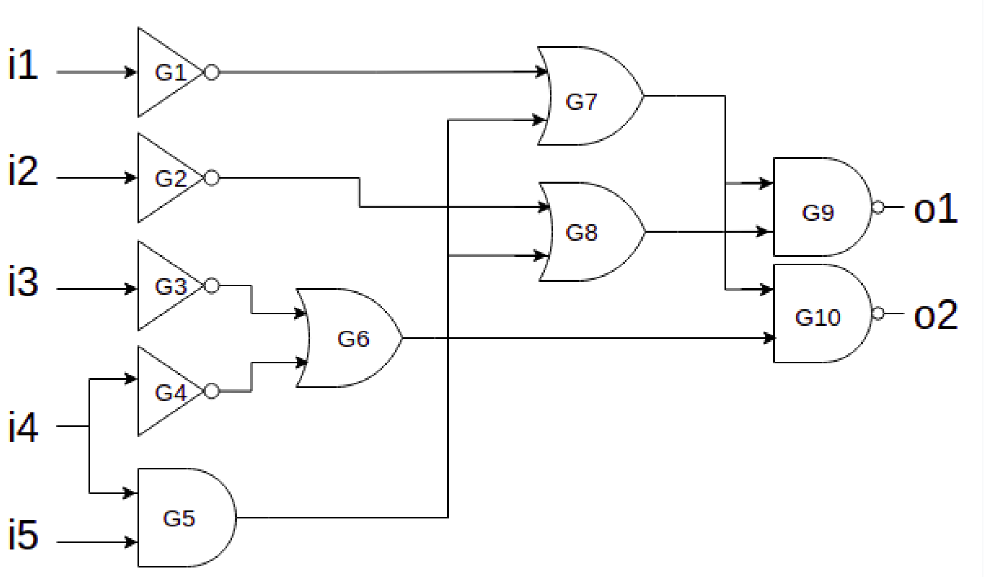
Complete

Mark 0.00 out of 5.00

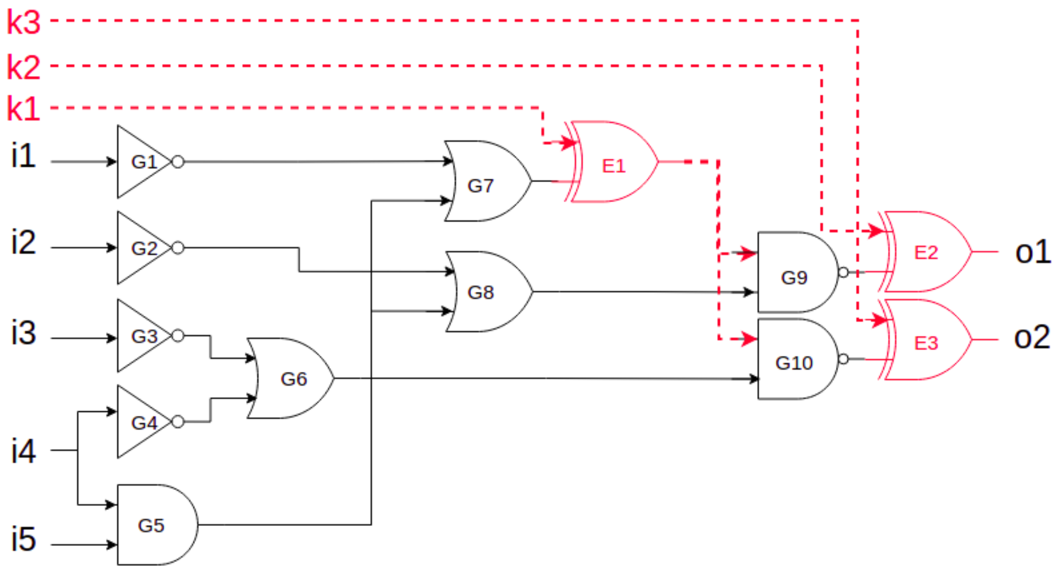
Flag question

Given the following logic locked circuit, what are the key values (k1,k2,k3) for which the wrong keys get self canceled, for the input pattern (i1, i2, i3, i4, i5) = (0,0,1,1,1)? In other words, find the keys for which the output pattern of the locked circuit is the same as the unlocked circuit.

Unlocked Circuit



Locked Circuit



Select one:

○ 010

○ 110

○ 001

● 111

Question 3

Complete

Mark 5.00 out of 5.00

Flag question

Write a probable set of output mask equations for the below function taking s_in=2 and s_out=4 so that the non-completeness property of a first-order TI is achieved.

$$A = f(X, Y, Z) = 1 \oplus X \oplus XZ \oplus YZ$$

Please upload your answer in .pdf or .jpeg file format

CamScanner 04-12-2021 17.12.31.jpg

Question **4**

Complete

Mark 5.00 out of 5.00

Flag question

Find the CNF form of the following expression [Tseytin transformation]. Here & denotes AND, | denotes or, ^ denote xor.

Y= (a | b) & c

You can upload your answer also.

CamScanner 04-12-2021 17.20.15.jpg

Question **5**

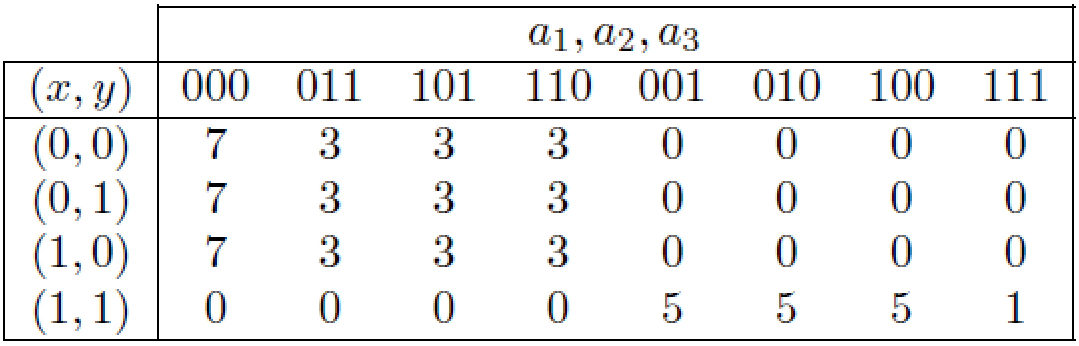
Complete

Mark 2.00 out of 2.00

Flag question

For A=f(X,Y)=XY, in order to satisfy the uniformity of masking definition where s_in=3 and s_out=3, irrespective of the output shares what should be the non zero values in the table below:

The table displays the number of times that a masking a1, a2, a3 occurs for a given input (x,y)



	a_1, a_2, a_3							
(x,y)	000	011	101	110	001	010	100	111
$(0,0)$	7	3	3	3	0	0	0	0
$(0,1)$	7	3	3	3	0	0	0	0
$(1,0)$	7	3	3	3	0	0	0	0
$(1,1)$	0	0	0	0	5	5	5	1

Select one:

○ 3

○ 2

○ 5

● 4

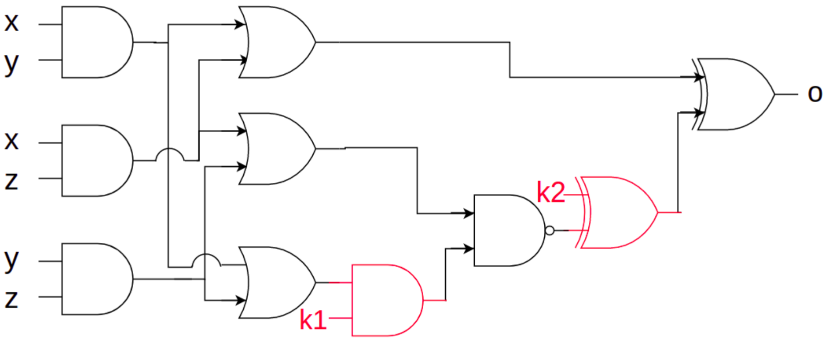
Question **6**

Complete

Mark 0.00 out of 10.00

Flag question

Use SAT attack to find the correct key used to lock the following circuit



x	y	z	f	(k1,k2)			
				(0,0)	(0,1)	(1,0)	(1,1)
0	0	0	1				
0	0	1	1				
0	1	0	1				
0	1	1	0				
1	0	0	1				
1	0	1	0				
1	1	0	0				
1	1	1	1				

f represents the unmasked output.

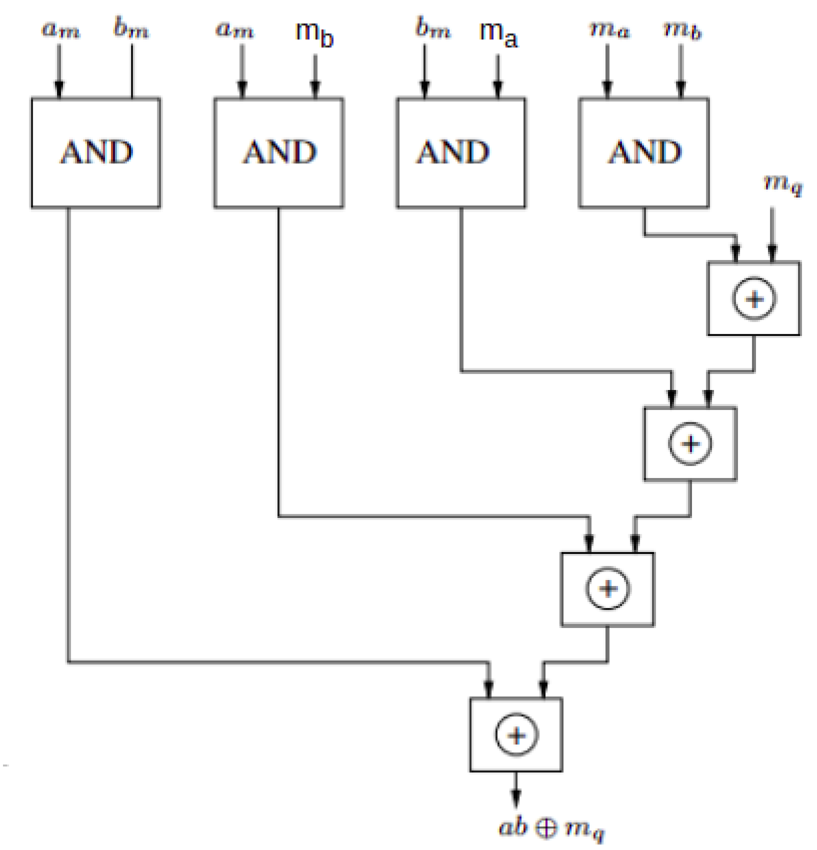
Question 7

Complete

Mark 0.00 out of 5.00

Flag question

First order masking is known to be vulnerable against glitches. In other words, the glitch power is correlated with the unmasked input. Consider the following circuit where input a_m is affected by a glitch. Show that the average glitch power for the XOR gate depends on y. You can write the answer in pen and paper and upload the picture also. Hint: Assume a 0->1 transition in a_m and consider all possible values of b_m and m_b.



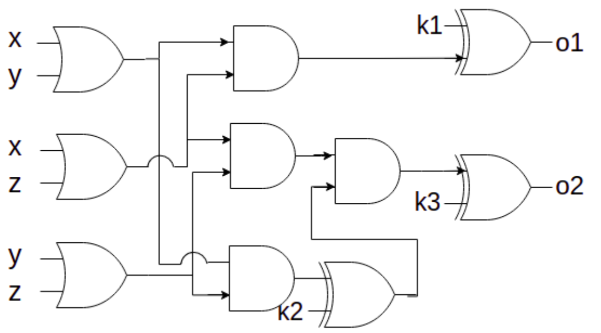
Question 8

Complete

Mark 0.00 out of 5.00

Flag question

Find the distinguishing input pattern for the following circuit where the first copy is locked with (k1, k2, k3)=(0,0,1) and the second copy is locked with (k1, k2, k3)=(0,1,1)



Question 9

Complete

Mark 0.00 out of 1.00

Flag question

The minimum number of input shares required for implementing a dth-order TI of a function with independent inputs is

Answer: 2

Finish review

QUIZ NAVIGATION

1 2 3 4 5 6 7 8 9

Show one page at a time

Finish review