Feedback — Quiz_week5

Help Center

You submitted this quiz on **Tue 17 Feb 2015 3:14 PM PST**. You got a score of **15.00** out of **15.00**.

Question 1

Which of the followings added by a system designer will be considered as hardware Trojan? Check all that apply.

Your Answer		Score	Explanation
☑ Use an additional signal to write the plain text to memory before it goes into the encryption block.	✔	0.50	
☑ Modify the system specification so when a specific input sequence is given, a critical component will be disabled.	✔	0.50	
☐ Add an extra output pin to test a particular signal on the chip.	✔	0.50	Not for malicious purpose.
☐ Assign specific values to some don't care conditions in the system specification as a proof of designer's signature.	✔	0.50	Not for malicious purpose.
Total		2.00 / 2.00	

Question 2

In the example we have showed for trusted IC and hardware Trojan, the following functions are used to implement

$F(x) = x^2$:

$Z_1 = X_1$

$Z_2 = X_2 X_3$

$Z_3 = (X_1 + X_2)X_4 + X_2 X_3'$

$Z_4 = (X_2 \oplus X_3)X_4$

$Z_5 = X_3 X_4'$

$Z_6 = 0$

$Z_7 = X_4$

what will be the output when $1110_2 = 14_{10}$ is entered as the input? Enter your answer in binary and from Z_1 to Z_7.

You entered:

1100100

Your Answer		Score	Explanation
1100100	✔	1.00	
Total		1.00 / 1.00	

Question 3

We have shown that replacing $Z_2 = X_2 X_3$ with $Z_2 = (X_1 + X_2)X_3$ will add a hardware Trojan to the circuit in question

2. Which of the following statements about hardware Trojan-free (or trusted IC) implementation are true? Check all that apply.

Your Answer		Score	Explanation
☑ We need to make sure that for any input x between 10 and 15, the circuit does not output x^2.	✔	0.50	
☑ We need to make sure that the circuit will give correct output values for input values 0-9.	✔	0.50	
☑ Replacing $Z_1 = X_1$ by $Z_1 = X_1 X_3'$ can prevent the hardware Trojan showed in this question.	✔	0.50	make sure that you check this does not mess up the output when input is between 0 and 9.
☑ Replacing $Z_6 = 0$ by $Z_6 = X_1 X_3$ can prevent the hardware Trojan showed in this question.	✔	0.50	make sure that you check this does not mess up the output when input is between 0 and 9.
Total		2.00 / 2.00	

Question 4

Hardware Trojans can be functional, which will change the system's functionality, or non-functional, which do not.

Non-functional hardware Trojans are also known as _____ Trojans.

You entered:

parametric

Your Answer		Score	Explanation
parametric	✔	0.50	
Total		0.50 / 0.50	

Question 5

Which of the following statements about hardware Trojan detection are true (assume that the Trojan detection tool is trusted)? Check all that apply.

Your Answer		Score	Explanation
☐ When a Trojan is found and fixed, the IC can be trusted.	✔	0.50	One Trojan is fixed, it does not mean that there is no other Trojans.
☐ When the hardware Trojan detection tool does not find any Trojan, the IC is trusted.	✔	0.50	This tool does not find Trojan, it does not mean that there is no Trojan.

☑ When a Trojan is reported, the IC cannot be trusted.	✔	0.50
Total		1.50 / 1.50

Question 6

Which of the following statements about physical attacks and hardware Trojan detection approaches are true? Check all that apply.

Your Answer		Score	Explanation
☑ Unlike physical attacks, hardware Trojan detection normally does not have a specific target.	✔	0.25	Attackers know what they want to attack. But we don't know what kind of Trojans might be embedded in the circuit.
☐ Physical attacks can be invasive, but hardware Trojan detection cannot.	✔	0.25	
☑ They both try to find hidden information or design details in the chip.	✔	0.25	
☑ Physical attacks can target system at	✔	0.25	This is another reason Trojan detection is harder than physical attack, for example, by side channel analysis.

normal operation, but most hardware Trojans are triggered by rare events.	
Total	1.00 / 1.00

Question 7

Which of the followings may impact the accuracy of side channel analysis based hardware Trojan detection methods? Check all that apply.

Your Answer		Score	Explanation
☑ The variations during chip's fabrication process.	✔	0.25	
☑ The errors when we collect side channel measurements.	✔	0.25	
☑ The environment in which we test the chip.	✔	0.25	Environment factors such as humidity or EM field can alter the measurements.
☑ The models we use for system's normal (Trojan-free) behavior.	✔	0.25	Incorrect or inaccurate models can be misleading.

Total	1.00 / 1.00

Question 8

A small kill switch (a 2-input AND gate and a trigger signal) is added to the chip to disable the encryption engine. Which of the following hardware Trojan detection approaches will be able to catch it? Check all that apply.

Your Answer		Score	Explanation
☑ Delay side channel analysis.	✔	0.50	When the delay of the path that include the kill switch is measured, the extra delay introduced by the Trojan will reveal the Trojan.
☑ Run time monitoring.	✔	0.50	When the Trojan is triggered, run time monitoring approach should be able to catch this. For example, the encryption engine is idle when it is supposed to do some encryption.
☐ Power side channel analysis.	✔	0.50	Because of the small size of the Trojan and the impact of noise and variations, it is unlikely for this method to catch the kill switch.
☑ Logic test at test time.	✔	0.50	When the trigger signal is set to disable the encryption engine, the Trojan will be caught. However, it might be hard to find that test vector, which should be a rare event.
Total		2.00 / 2.00	

Question 9

For two FSMs M1 and M2 and their product machine M, which of the following statements about FSM equivalence are correct?

Check all that apply.

Your Answer		Score	Explanation
☐ Let k_1, k_2 and k be the number of states in M1, M2, and M, respectively, it is possible to have $k > k_1 \times k_2$.	✔	0.50	Impossible. See the explanation for the number of starting states.
☑ If M1 and M2 give different outputs for the following input 1010101010, they cannot be equivalent.	✔	0.50	There is nothing special about this input. If M1 and M2 disagree on any input, they cannot be equivalent.
☑ The number of starting states in M will not be less than the number of starting states in M1 or M2.	✔	0.50	The starting state of M will be all the pairwise combination of starting state of M1 and M2. For example, if M1 has two starting states: A and B; and M2 has three: X,Y, and Z. Then the starting states of M will be: (A,X), (A,Y), (A,Z), (B,X), (B,Y), (B,Z).
☐ If M1 and M2 have different number of states, they cannot be equivalent.	✔	0.50	The example in the lecture shows two FSMs, one with 4 states and one with 3, are equivalent.

Total	2.00 / 2.00

Question 10

Which of the following statements about hardware Trojan prevention are true? Check all that apply.

Your Answer		Score	Explanation
☐ Rare event removal approaches remove the rare events from the chip so they will not occur and thus hardware Trojan cannot be triggered by them.	✔	0.50	The rare events are not removed, the probability of their occurrence will be increased.
☐ If you cannot trust the CAD tools, you should not use it because there is no way you can build trusted IC from the untrusted CAD tools.	✔	0.50	check the reference listed in the last slide.
☑ Digital watermarking (e.g. those based on don't care conditions) makes reverse engineering harder, so it can also be considered as one type of design obfuscation.	✔	0.50	see another advantage of adding watermark?
☑ Shadow registers can help to measure the delay of internal paths. So it can make the path	✔	0.50	

delay based hardware Trojan detection approaches more effective.	
Total	2.00 / 2.00