Feedback — Final_Exam

Help Center

You submitted this quiz on **Mon 23 Feb 2015 12:14 PM PST**. You got a score of **28.00** out of **30.00**.

Question 1

Which topic do you want to learn more?

Your Answer		Score	Explanation
(•) Physical attacks (invasive, side channel, etc.)	✔	0.50	
( ) Hardware Trojan design, detection, and prevention			
( ) Trust in IC (vulnerability, backdoors, etc.)			
( ) IP protection (watermarking, fingerprinting, IP metering)			
( ) Applications (FPGA, TPM, PUF, etc.)			
Total		0.50 / 0.50	

Question 2

Which topic you think is the most important for hardware security?

Your Answer		Score	Explanation
○ IP protection (watermarking, fingerprinting, IP metering)			
◉ Physical attacks (invasive, side channel, fault injection, etc.)	✔	0.50	
○ Trust in IC (vulnerability, backdoors, etc.)			
○ Applications (FPGA, TPM, PUF, etc.)			
○ Hardware Trojan design, detection, and prevention			
Total		0.50 / 0.50	

Question 3

True or false: On a sequential system, to control the accessibility of a state u, it is sufficient to check all the transitions $v \rightarrow u$ for the starting state v and the transition condition.

Your Answer		Score	Explanation
True			
False	✔	0.50	
Total		0.50 / 0.50	

Question 4

A system is supposed to output 1010 on input 00011010, but outputs 0101 after a digital watermark is embedded. Which requirement does this watermarking method violate?

Your Answer		Score	Explanation
High credibility			
Transparency			
Resilience			
Low overhead Resilience Transparency			
Correct functionality	✔	0.50	

Total	0.50 / 0.50

Question 5

Which of the followings are the goals of IP protection? Check all that apply.

Your Answer		Score	Explanation
☐ Protect IP from hardware Trojan insertion	✔	0.20	
☑ Protect IP against unauthorized use	✔	0.20	
☐ Improve the quality of the IP	✔	0.20	
☑ Enable the IP owner to detect the use of the IP	✔	0.20	
☑ Protect testing data associated with the IP	✔	0.20	
Total		1.00 / 1.00	

Question 6

When we use ICID as the tag for a device, which property does this tag have?

Your Answer		Score	Explanation
○ functional			
◉ passive	✔	1.00	
○ reproducible			
○ internal control			
Total		1.00 / 1.00	

Question 7

Convert the decimal number 2015 into binary: (write the binary number only, for example: 10101010101. No space, comma, etc.)

You entered:

11111011111

Your Answer	Score	Explanation

11111011111	✔	1.00
Total		1.00 / 1.00

Question 8

Which of the following PUFs are delay based? Check all that apply.

Your Answer		Score	Explanation
☐ SRAM PUF	✔	0.25	
☐ Butterfly PUF	✔	0.25	
☑ Ring Oscillator PUF	✔	0.25	
☑ Arbiter PUF	✔	0.25	
Total		1.00 / 1.00	

Question 9

Which of the following statements about digital watermarking and fingerprinting is correct?

Your Answer		Score	Explanation
○ Fingerprint and watermark cannot be used together.			
◉ A fingerprinting method has to guarantee that different copies of the same IP get different fingerprints.	✔	2.00	
○ It is possible to design watermarking schemes with 100% credibility.			
○ It is impossible to design watermarking schemes with guaranteed zero overhead.			
Total		2.00 / 2.00	

Question 10

Which of the following statements about don't care conditions is correct?

Your Answer		Score	Explanation
◉ When a combinational system is fabricated, the outputs will be deterministic for all the don't care conditions, but outputs may have different values on different don't care conditions.	✔	2.00	

If specific values are assigned to outputs on don't care conditions, the design will have more constraints and its quality (e.g. size, power, speed) will become worse.		
When system outputs are specified for all the input combinations, there will not be any don't care conditions in the design.		
Total	2.00 / 2.00	

Question 11

Which of the following statements about physical attacks is correct?

Your Answer		Score	Explanation
All physical attacks need to collect some measurement during system's execution.			
After being physical attacked, the system will not be able to function normally.			
All physical attacks will need the help from some tools and/or equipment.	✔	2.00	
All physical attacks need to have physical access to the target system.			
Total		2.00 / 2.00	

Question 12

Which of the followings can be used to generate fault for fault injection attacks to a system?

Your Answer		Score	Explanation
chip operating temperature			
clock glitches			
electromagnetic flux			
white light			
all of the above	✔	2.00	
Total		2.00 / 2.00	

Question 13

Which of the followings is NOT a good practice in securing a system?

Your Answer	Score	Explanation

(•) design a working system and then add the necessary protocols to secure it	✔	2.00
( ) understand the motivations of attackers		
( ) identify vulnerabilities in the system		
( ) estimate the threats to the system		
Total		2.00 / 2.00

Question 14

Which of the following statements about side channel attacks is NOT correct?

Your Answer		Score	Explanation
(•) All side channel attacks need direct access to the system to collect side channel information.	✔	2.00	
( ) The countermeasure to one type of side channel attacks may make the system more vulnerable to attacks from another side channel.			
( ) All side channel attacks are non-invasive.			

Side channel attacks can be more effective when combined with techniques such as fault injection or input control.	
Total	2.00 / 2.00

Question 15

Which of the followings can be potential sources for side channel attacks? Check all that apply.

Your Answer		Score	Explanation
system's output signals	✔	0.30	
power consumption	✔	0.20	
system's timing or delay information	✔	0.30	
acoustic side channel	✔	0.30	
electromagnetic radiation	✔	0.30	
scan chain output signals	✔	0.30	
optical side channel	✔	0.30	

Total	2.00 / 2.00

Question 16

Consider $w = x'yz + xy' + y'z$, which of the following conditions is a satisfiability don't cares?

Your Answer		Score	Explanation
○ $x = 0, y = 0, z = 0, w = 0$			
● $x = 1, y = 0, w = 0$	✔	2.00	
○ $x = 1, y = 1, w = 0$			
○ $y = 1, z = 1, w = 1$			
○ none of the above			
Total		2.00 / 2.00	

Question 17

When an FSM is implemented, which of the followings will be considered as a hardware Trojan?

Your Answer		Score	Explanation
Adding a signal that can disable the FSM for design testing and debugging.			
Tuning the design so the power consumption on each transition will be similar.			
Connecting the FSM to an antenna to send out the FSM state information.	✔	2.00	
Specifying the next state information for certain don't care transitions to embed watermark.			
Total		2.00 / 2.00	

Question 18

For an FPGA-based system developer, which of the following security vulnerabilities and attacks he will not care?

Your Answer	Score	Explanation
Reverse engineering attacks to the FPGA configuration bitstream file of his design.		
Replay attacks from the FPGA users.		

Leak of his design information from the FPGA		
Watermarks in the FPGA embedded by the FPGA vendor.	✔	2.00
Total		2.00 / 2.00

Question 19

The following 4 questions are on how to use Montgomery Reduction method to compute $67 \times 58 (mod\ 109)$. Here we have $a = 67, b = 58, N = 109$. We pick $R = 128$ and we know that $N^{-1} = 101 (mod\ 128)$.

What is $a' = aR (mod\ 109)$? Write the number only, no need to append $(mod\ 109)$.

You entered:

74

Your Answer		Score	Explanation
74	✔	0.50	
Total		0.50 / 0.50	

Question 20

Continue from the previous question, what is $b' = bR (mod\ 109)$?

You entered:

12

Your Answer		Score	Explanation
12	✔	0.50	
Total		0.50 / 0.50	

Question 21

Continue from the previous question, what is $c' = (a'b')R^{-1} (mod\ 109)$?

You entered:

41

Your Answer	Score	Explanation

41	✔	0.50
Total		0.50 / 0.50

Question 22

Continue from the previous question, what is $c = ab(mod\ 109)$?

You entered:

71

Your Answer		Score	Explanation
71	✔	0.50	
Total		0.50 / 0.50	

Question 23

What is the modular multiplicative inverse of $5(mod\ 38)$?

(hint: use Euler's Theorem, square and multiply).

You entered:

191

Your Answer		Score	Explanation
191	✖	0.00	
Total		0.00 / 2.00	