M2 CyberSecurity 2019-2020

Physical Security (WMM9SY05)

Hardware and Embedded Systems

Paolo MAISTRI, Ioana VATAJELU

No documents allowed

About 50 minutes

LAST NAME / NOM :

FIRST NAME / PRENOM :

1. Read the following statements, and tick the corresponding column if they are true or false. If you need to articulate your answer, you can write additional text below the table.

#	Statement	TRUE	FALSE
1	Right-to-left or Left-to-right exponentiation algorithms are equivalent with respect to side channel analysis		
2	Ring Oscillators, used in Random Number Generators, can be biased by electromagnetic pulses		
3	Projective representation systems can be a countermeasure to side channel analysis		
4	Electromagnetic pulses induce delay faults		
5	SAT solvers can be used to help side channel attacks		
6	The order of the operands in a finite field operation is important		
7	Hardware Trojans can be detected through side channel analysis		
8	Masking is always effective against side channel attacks, independently of the implementation choices		
9	Hardware Trojans can be detected only at the end of the design flow, once we have the physical circuit		
10	Voltage glitches can be used to inject faults		
11	Side channel attacks must analyze the dynamic behavior of the circuit		
12	Pipelined designs can be exploited to protect against passive and active attacks		
13	Physical Unclonable Functions have no practical use		
14	Advanced laser attacks can be used to circumvent protections based on redundancy		
15	AI (Artificial Intelligence) can be used to circumvent protections against side channel analysis		

2. Describe a countermeasure against side channel attacks that can be applied at architectural level

3. Discuss the motivations, requirements, advantages, and disadvantages of Double-Data-Rate as a countermeasure against fault attacks.

4. Discuss the motivations, requirements, advantages, and disadvantages of scrambling the scan chain from a security point of view.

5. Which are the main counterfeiting techniques, where can they occur in the untrusted chain, and how they can be prevented?

6. Explain the principle of operation of an SRAM PUF.