1. Describe the main idea of side-channel analysis.
2. What information can be gained when successfully applying a side channel attack?
3. Explain what an invasive attack is and what a non-invasive is.
4. Explain what SPA is and what DPA is. What are the differences between them?
5. Describe what tools and equipment are required to perform power analysis attacks.
6. Describe approaches of protecting a chip against power analysis attacks.
7. What is EM emanation and how is it used to apply EM analysis attacks?
8. Describe the main idea of timing attacks and what tools are required to perform it.
9. How can side-channel attack countermeasures protect the device? And how would these countermeasures affect the performance of the system?
10. How can an attacker perform side-channel attacks on parallel based systems such as FPGAs? And how different is it compared to microcontrollers?
11. Applying EM analysis to capture critical information can be tricky, many factors can affect the quality of the signal. What measures should the attacker take to successfully perform the attack in a noisy environment? And what are the pros and cons of applying EM analysis over power analysis in this case?
12. Analyzing the delay of the output of a device can be used to gain knowledge about the design, one countermeasure used is to randomize the delays every time an operation is performed. How can this random delay be implemented? What are the challenges that the designer may face when applying this countermeasure?