1. What are the differences between reverse engineering with honest and dishonest motivations?

Those with honest motivations tend to perform RE for verification, fault analysis, research, and education of an existing product. However, when RE is used to clone, pirate, or counterfeit a design, to develop an attack, or to insert a hardware Trojan, these behaviors are considered dishonest.

2. List three categories of reverse engineering and their differences.

There are three level reverse engineering: Chip-level, PCB-level and System-level. Chip-level RE focuses on reverse engineering a silicon die including its architecture, connection and functionality. PCB-level RE is to identify the components on the board and figure out their traces and ports. System-level RE is to read out the firmware stored in the memory.

3. If KEY bits are the only asset in an encryption module and these KEY bits have been properly protected against probing attack, would it be fair to assume that this crypto hardware is probing-resistant design? Explain why.

No, it is still vulnerable to probing attack. Since if A = B xor KEY, then by controlling B and probing A, the KEY bits can still be inferred.

4. Assume that an asset wire is on Metal 2, and a shield is planned to be built on either Metal 7 or Metal 8 to prevent probing attack. In your opinion, which layer is better to use? Explain why. Also assume that a cone-shaped hole will be milled during the probing attack, and the metal on layers 7 and 8 has the same width and space. Hint: Only consider the geometric relation of asset and shield wires.

Metal 8 is better. First, metal 8 has the same direction with metal 2, which is more efficient for the shield to protect asset wire. Second, the cone shape milling hole has larger footprint on metal 8 than metal 7 since metal 8 is higher than metal 7, which means the attack will be more possible to be detected by the shield on higher layer.

5. Illustrate the basic steps to perform a front-side electrical probing attack.

Decapsulation, reverse engineering, locating target wires, reaching target wires and extracting information.

Compared to clock glitch-based fault injection attack, what are the pros and cons of a laser-based optical fault injection attack.

Pros: Laser based optical fault injection attack is more accurate, which can locally manipulate the switch of one or several transistors, while the impact of clock glitch is global and hard to focus on one transistor. Cons: The cost of laser based optical fault injection attack is high which needs more advanced equipment and corresponding trigger.

6. Can an attacker utilize modern optical or electron microscopy to reverse engineering EEPROM?

No. It is because the state of EEPROM/Flash is determined by the distribution of electrons, not by the geometric differences. Further, the SEM or TEM techniques may change the state stored in EEPROM. Hence, the attacker is not able to reverse engineer EEPROM by using optical or electron microscopy.