1. **Important points:**
   - Malicious entities within the whole supply chain can perform attacks through exploiting the scan chains.
   - Testability and security contradict to each other.
   - Scan-based Design for Testability used by test engineer have big impact on security.
   - Destruction of JTAG after use is developed to improve security but has some impact on testability
   - The TAP controller is a finite state machine driven by TCK, TMS, and TRST signals.
2. **An attacker in the supply chain may exploit the scan chain (sometimes through JTAG) to:**
   - Steal critical information from crypto IP.
   - Violate confidentiality and integrity policies.
   - Pirate IP design.
   - Illegally take control of the chip.

3. **Scan-Facilitated Differential Attack**
   - This type of attack leverages scan chains, a design-for-test (DFT) feature commonly found in integrated circuits to aid in debugging and testing. Scan chains allow easy access to internal registers during the testing phase by linking registers into chains and making them accessible from the outside.
   - An attacker can exploit scan chains by manipulating or observing the input-output patterns through these chains. By comparing (differential) outputs based on specific inputs, they can infer secrets stored in the device, like cryptographic keys. This type of attack targets the inherent vulnerability introduced by the DFT feature, which isn't meant to be accessible during regular operation.
   - This is especially dangerous in cryptographic hardware because it allows attackers to retrieve sensitive data or encryption keys without physically tampering with the chip.

4. **Resetting and Flushing Attacks:**
   - These attacks exploit the countermeasures designed to reset or flush internal states to prevent sensitive information leakage.
   - Attackers may trigger the reset or flush processes in rapid succession or under unusual conditions, causing the system to exhibit behaviors that unintentionally reveal secrets or weaken security mechanisms.
   - The system's efforts to protect itself are actually used against it, potentially exposing sensitive data or creating predictable states that attackers can exploit.

5. **Bit-Role Identification Attack:**

- In this attack, an adversary analyzes individual bits in the output to determine their role or significance in computations, particularly for cryptographic operations.
- By studying which bits influence specific functions or outputs under controlled input variations, attackers can piece together the underlying cryptographic structure or logic.

- This can lead to partial or full recovery of the internal logic or secrets, especially in cryptographic devices where certain bits hold critical importance.

6. **Combinational Function Recovery Attack**

- This attack is aimed at recovering the combinational logic or function used in a hardware circuit, often with the goal of understanding or reverse-engineering its design.
- The attacker observes the output of the device in response to various inputs and uses this information to deduce the underlying logic. This can involve brute-forcing, machine learning, or other inference techniques.
- If successful, the attacker can replicate the functionality of the hardware, bypass protections, or even introduce counterfeit components with similar functionality. This is particularly concerning for proprietary hardware designs or those implementing sensitive computations.

7. **The purpose of placing the Shadow chain into the dynamically obfuscated scan (DOS) architecture.**

- In the DOS, the Shadow chain is designed for propagating the obfuscation key at the ith scan cell along the scan chain, when the ith scan clock comes. Therefore, the Shadow chain is able to: i) protect the obfuscation key from being leaked through resetting attack; ii) prevent any unscrambled data from being scanned out, and iii) prevent adversaries from scanning in values intentionally, and at the same time, make no impact on structural and chain tests.

8. **Other countermeasures against scan-based attacks are listed below:**

- Defusing the scan-related pins: The most direct solution is to defuse the polysilicon fuses connecting the scan in or scan-enable pins.
- Test Mode Protection: By carefully designing the test controller, test mode request will reset the registers, and wrap the nonvolatile memories.

Homework questions:

1. Explain the relationship between testability and security.
2. List several countermeasures against JTAG hacks and explain in detail one of them