LAB ACTIVITY 1

1. Team No: 03

2. Members of the team:

Ajay Kumar
Chandra Mohan
Harshith Singh
Kushagra Chauhan
Mahendra Saini
Malavika N R
Shrishti Patil

3. Research Article Title: *"Breakthrough silicon scanning discovers backdoor in military chip"*

4. The IC architecture referred in the article is -FPGA

5. The article has an aim of the solution of:

ABSTRACT

This paper provides a concise overview of the first documented instance of discovering a backdoor in a military-grade FPGA. Through an innovative patented technique, researchers detected and thoroughly analyzed the presence of a backdoor within Actel/Microsemi ProASIC3 chips. This backdoor was integrated directly into the silicon itself, distinct from any firmware loaded onto the chip, and was embedded alongside additional JTAG functionality.Using the pioneered Pipeline Emission Analysis (PEA) technique, it is successfully extracted the secret key necessary to activate the backdoor, as well as other critical security keys such as AES and Passkey. This vulnerability enables an attacker to extract configuration data, manipulate cryptographic and access keys, alter fundamental silicon functions, access unencrypted configuration bitstreams, or permanently disable the device.The implications are profound, as the compromised devices are vulnerable to intellectual property theft, fraud, unauthorized reprogramming, and reverse engineering, potentially allowing for the insertion of new backdoors or Trojans. Compounding the issue is the inability to patch already deployed chips, forcing users of this chip family to either accept the compromised security or replace the chips physically following a redesign of the silicon.

6. The architecture/block diagram given in the article is: [Provide the diagram: you can copy paste the same]

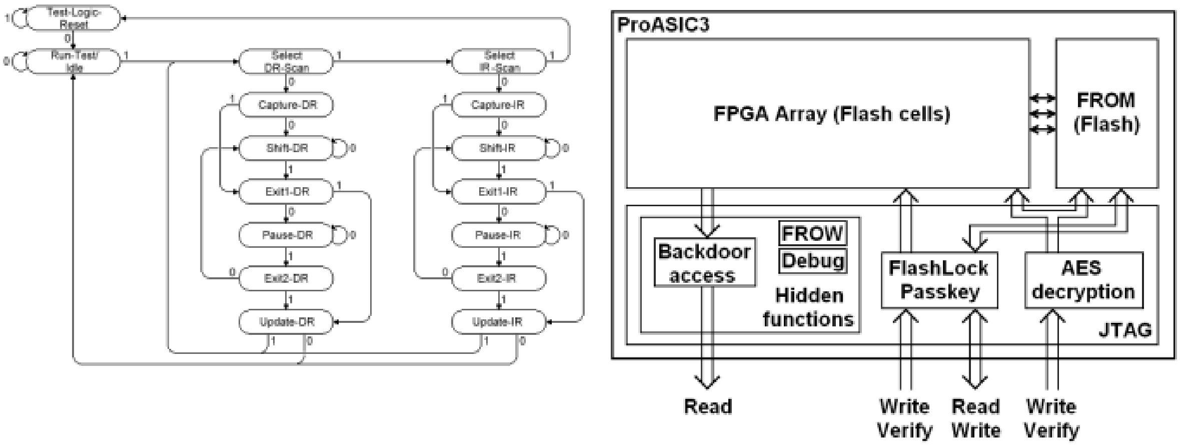

Fig 1: (a)JTAG TAP state machine, (b)Simplified ProASIC3 security

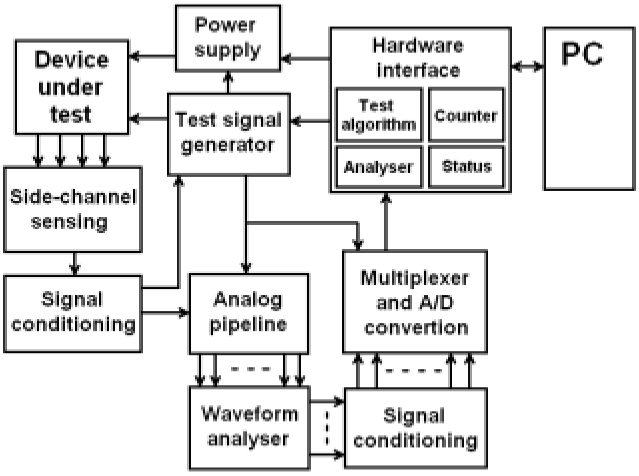

Fig 2 : Block Diagram of PEA Setup

7. The functional description of the solution provided is:

1. **Initial Analysis**: The authors began by analyzing the chip with standard design tools from Actel, such as Libero IDE and FlashPro, to understand the JTAG communication.
2. **Test Board Setup**: A special test board was constructed with a master JTAG interface and simple functions controlled by PC software via an RS-232 interface for convenience.
3. **JTAG Command Analysis**: The authors scanned the JTAG command field for unknown commands by checking the length of the associated Data Register (DR) to reveal hidden functionality.

4. **Side-Channel Analysis**: Differential Power Analysis (DPA) was initially attempted to extract security keys, but due to robust DPA countermeasures, it was not effective.
5.**PEA Technique Development**: The authors developed the PEA technique to achieve a better signal-to-noise ratio and improve the detection of side-channel emissions.
6. **Prototype Sensor Setup**: A prototype board with a sensor was built to implement the PEA technique. This setup included a control interface, a test signal generator, a programmable power supply, and a waveform analyzer.
7. **Key Extraction**: Using PEA, the authors were able to extract the secret key required to activate the backdoor and other security keys in real-time with high correlation.
8. **Backdoor Functionality Testing**: Once the backdoor feature was unlocked, the authors tested various JTAG registers and found that many became volatile and the Flash memory was reprogrammable.
9. **Implications and Further Improvements**: The authors discussed the implications of their findings and suggested improvements to their PEA technique, such as building a multi-pipeline system and more efficient hardware for probes.
10. **Conclusion**: The article concludes with a discussion on the serious questions raised about hardware assurance in the semiconductor industry and the potential for large-scale attacks exploiting the backdoor.

8. The IC Specified has the features in the proposed solution as follows:

Features of the IC

The article discusses the Actel/Microsemi ProASIC3 FPGA chip, highlighting its security features and the presence of a backdoor. Here are the features of the IC mentioned in the article:

1. **High Security Specifications**: The ProASIC3 A3P250 device is marketed with high security specifications, suitable for military and sensitive industrial applications.
2. **Low Power Flash Technology**: The chip is designed to be low-power and live on power-up, with configuration data stored securely within the device.
3. **Inherent Security**: The device is claimed to have inherent resistance to both invasive and noninvasive attacks on valuable intellectual property (IP).
4. **No Readback Feature**: According to the manufacturer, the ProASIC3 configuration files cannot be read back via JTAG or any other method, enhancing security.
5. **Multiple Security Protection Levels**: The chip offers several levels of security protection, including FlashLock with AES encryption, a Passkey for prohibiting write or verification operations, and a Permanent Lock feature for ultimate security.
6. **Remote Update Capability**: The ProASIC3 allows for secure, remote field updates over public networks, ensuring IP protection.

7. **JTAG Interface**: The chip includes a JTAG interface for testing and programming, which is standard for integrated circuit testing.
8. **Undocumented JTAG Functionality**: The article reveals hidden functionality within the JTAG controller that allows covert access to configuration data, which is part of the backdoor.
9. **Backdoor Vulnerability**: The presence of a backdoor that can be exploited to extract configuration data, reprogram the device, or even permanently damage it.
10. **Unpatchable Flaw**: The backdoor is a physical part of the silicon and cannot be patched in already deployed chips, necessitating physical replacement if compromised.

The article emphasizes the discrepancy between the manufacturer's claims of security and the actual presence of a backdoor, which undermines the device's security assurances.