A Black Box Attack Using Side Channel Analysis and Hardware Trojans”

RajaAdhithan Radhakrishnan
r.rajaadhithan@gmail.com
Society For Electronic Transactions and Security(SETS)

Abstract. The emergence of hardware trojans as significant threats in various aspects of hardware design, including Firmware, open-source IP, and PCB design, has raised serious concerns. Simultaneously, AI technologies have been employed to simplify the complexity of Side Channel Analysis (SCA) attacks. Due to the increasing risk posed by these threats, it becomes essential to test hardware by considering all possible attack vectors. This paper aims to propose a black box attack using side channel analysis with the aid of hardware trojan insertion. The objective is to emphasize the necessity of side channel-based testing to defend against such attacks. The proposed attack can be executed in FPGA, ASIC, and microcontroller designs. The paper is primarily focused on Verilog design based hardware trojan insertion, and a small example demonstration is provided to illustrate this attack.

Keywords: Side-channel attacks · Hardware trojan· Black box attack

1 Introduction

In recent years, the field of hardware design has encountered a pressing and formidable challenge in the form of hardware trojans. These insidious threats have surfaced in various aspects of hardware development, spanning Firmware, open-source IP, and PCB design, triggering serious apprehensions among researchers and industry experts alike. Concurrently, the integration of AI technologies has revolutionized the landscape of Side Channel Analysis (SCA) attacks, offering streamlined approaches to deciphering vulnerabilities.

As the risk posed by hardware trojans and side channel attacks escalates, the imperative to rigorously test hardware systems has never been more pronounced. It is crucial to explore and address all potential attack vectors, leaving no stone unturned in the quest to bolster security measures. In light of this pressing need, this paper sets out on a novel endeavor - to present a black box attack that harnesses the power of side channel analysis in conjunction with hardware trojan insertion.

The central goal of this research is to underscore the criticality of side channel-based testing as an effective defense mechanism against such insidious attacks. By simulating and investigating the proposed attack in the context of FPGA, ASIC, and microcontroller designs, this paper elucidates its applicability across a broad spectrum of hardware architectures.

Throughout this study, I will delve into the intricacies of Verilog design, delving deep into the underlying principles that make the proposed black box attack viable. To provide concrete insights, a small example demonstration is included to illustrate the mechanics and potential ramifications of this combined attack strategy. In doing so, I hope to raise awareness about the importance of proactive security measures and contribute to the collective effort in fortifying hardware systems against emerging threats.So our objective in this paper is:

- Explain the need of additional information required for side channel attack and hardware trojan insertion.
- Hardware trojan insrtion to become side channel as black attack
- Small example demonstration.

The rest of the paper is organized as follows: Section 2 Back ground. Section 3 Hardware trojan insertion based side channel attack. Section 4 Explanation of Proposed attack in AES . I conclude the paper in Section 5.

2 Background

Side-channel attacks are a class of security threats that exploit unintended information leakage from a system during its normal operation. Instead of directly targeting the cryptographic algorithms or security mechanisms themselves, side-channel attacks focus on exploiting the physical implementation or the system's behavior to extract sensitive information. These attacks take advantage of observable side-channel signals, such as power consumption, electromagnetic radiation, or timing variations, to infer secret data like encryption keys or other confidential information.On Other hand Hardware Trojan insertion involves maliciously adding additional components or modifying existing ones in integrated circuits (ICs) or other hardware devices during the manufacturing process. The purpose of inserting hardware Trojans is usually to compromise the functionality or security of the target device covertly. These Trojans remain dormant during regular operation and only get activated under specific conditions or trigger events, which can be as subtle as a specific input signal or a time-based event.so in this paper my objective is to combine this two attack to reduce attack complexity and shown that, there is need of side channel testing for this attack and approach.

3 Hardware trojan insertion based side channel attack.

Before delving into the proposed attack, I am interested in discussing side-channel-based attacks and hardware trojan insertion. Side-channel attacks are typically classified into two categories: white-box attacks and black-box attacks.

3.1 White box attack

A white-box attack implies that the attacker possesses complete knowledge about the target device and its executing algorithm. For instance, the attacker is aware of the device where the algorithm is running, the clock frequency in use, input and output accessibility, and the detailed implementation. With this information, the attacker can create a hypothetical model and correlate it with the original traces to retrieve the encryption key [1].

3.2 Black box attack

In a black-box attack, the attacker only has access to the input, output, and side-channel information of the device. Other internal details remain hidden. Despite this limited information, the attacker is still capable of extracting secret data, thereby classifying the attack as a black-box attack [2].

3.3 Hardware trojan insertion

A hardware Trojan insertion attack involves the introduction of a malicious piece of hardware into a device. This malicious hardware is used to either retrieve confidential information through an output port or disrupt the device’s functionality [3]. For example, in AES encryption, a hardware Trojan can be inserted to extract the encryption key through the ciphertext output port.

3.4 Proposed hardware trojan insertion to enhance the black box attack

This subsection focuses on discussing a proposed attack that combines hardware Trojan and side-channel techniques to enhance black-box attacks. In this attack, a set of software code or a portion of the hardware is integrated into the hardware design, enabling the extraction of confidential information from the device through side channels as depicted in Fig 1. This approach represents a fusion of hardware Trojan insertion and side-channel attacks.

In the next section, I will delve into a detailed discussion of this attack concerning its application to the AES (Advanced Encryption Standard) design.

4 Explanation of Proposed attack in AES

In this section, I will delve into the proposed attack’s to AES (Advanced Encryption Standard) with two distinct attack strategies: 1) Attack with an additional S (sub-byte) box, and 2) Attack with no additional S box.

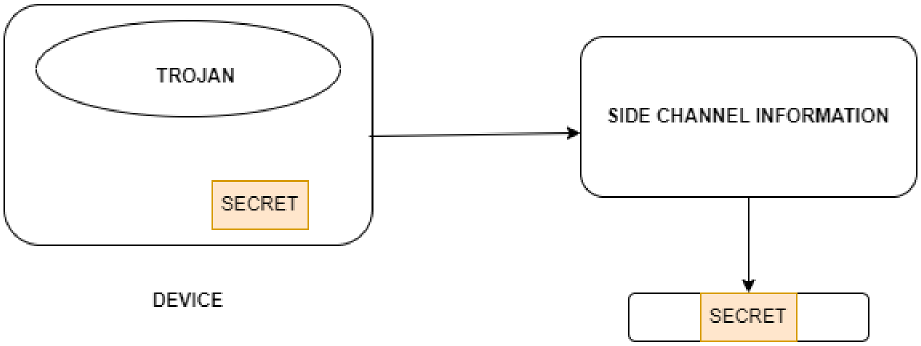

Fig. 1. Side channel to retrieve secret information by inserting hardware Trojan

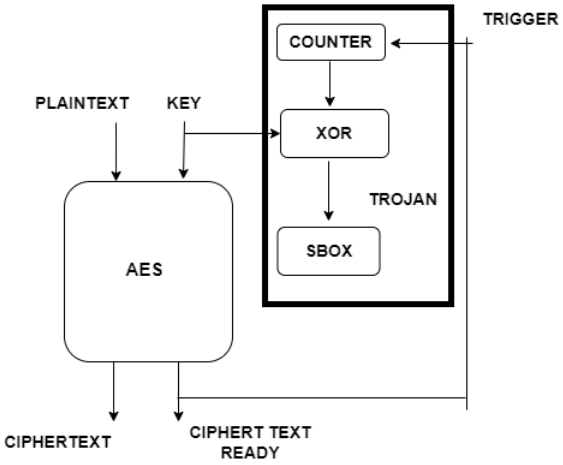

Fig. 2. Attack with additional S box

4.1 Attack with additional S box

To illustrate this attack strategy, I have chosen an AES implementation. In this implementation, we introduce a piece of hardware designed to facilitate the retrieval of the secret key of AES-128 solely through side-channel information. This hardware module incorporates a key XOR operation followed by an S-box operation, as depicted in Fig 2. As the counter value is sequential, the attacker can efficiently compute a hypothetical model and correlate it with the original power traces to extract the key. This technique allows the extraction of secret information from the device using only side-channel information, without the need for any other details. This attack is applicable to various designs and implementations, including FPGA, ASIC, and embedded platforms. It is particularly potent on embedded platforms, as identifying the hardware Trojan may be challenging,

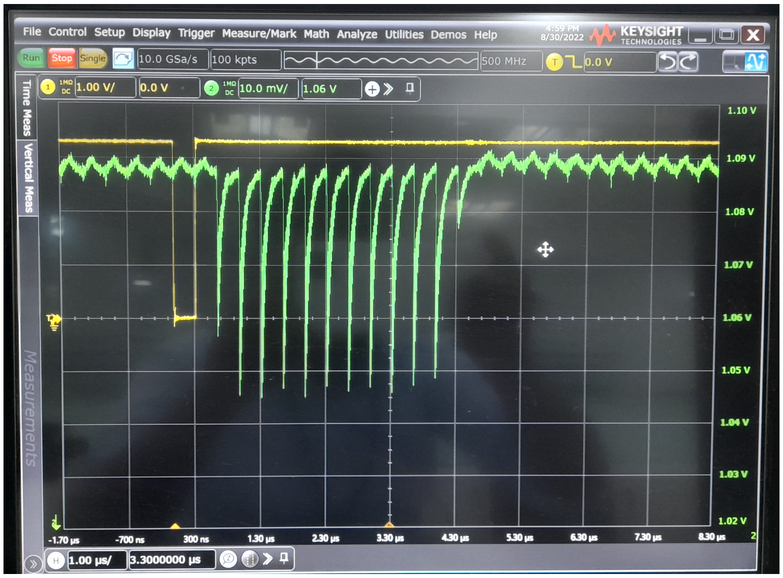

Fig. 3. Trojan is triggered after each encryption

unlike in FPGA and ASIC devices. To demonstrate this, I activate the Trojan at the end of each encryption cycle, as shown in Figure 3.

4.2 Attack with no additional S box

For the second type of attack strategy, I again employ the AES algorithm. However, in this implementation, I refrain from adding an extra S-box due to its space requirements. Instead, I leverage a portion of the AES circuit itself to serve as the Trojan without the need for additional hardware insertion. In this approach, the extra hardware manipulates the AES algorithm’s timing by feeding the counter input as plaintext, as demonstrated in the figure. This method makes it challenging to detect the Trojan within the device and is suitable for various platforms, although it may be more effective for specific designs.

5 Conclusion

In this paper, I have introduced and discussed a novel attack that enables the retrieval of secret information solely through side-channel data by inserting hardware Trojans into the design. My objective is to emphasize the need for establishing proper test setups to detect and mitigate this type of attack.

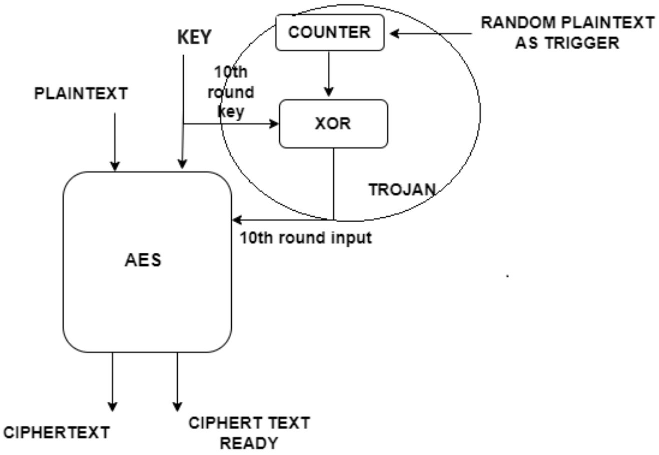

Fig. 4. Attack with no additional S box

References

1. A. Amaar, I. Ashour, and M. Shiple, "Efficient implementation of aes algorithm immune to dpa attack," in 2012 UKSim 14th International Conference on Computer Modelling and Simulation, 2012, pp. 396–401.
2. https://www.rambus.com/blogs/side-channel-attacks/
3. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7570641/