A Hardware Trojan Detection Framework

Georgina Kalogeridou
Computer Laboratory
University of Cambridge,
UK

Nicolas Sklavos
KNOSSOSnet Research
Group, TEI of Western
Greece, Hellas

Andrew W. Moore
Computer Laboratory
University of Cambridge,
UK

***Abstract* - In the recent years, hardware trojans have become a serious issue in the field of integrated circuits. Our work presents a framework for hardware trojan detection in wireless cryptographic integrated circuits. It deals with the leaking of secret information through a wireless communication, using a mixed-signal integrated circuit technique. A trojan is inserted in the introduced system, which does not change the functionality of it. It is presented that it is efficient to expose the trojan successfully through statistics regarding the transmission frequency, amplitude and power of the system.**

I. INTRODUCTION

The increasing use of system-on-chip in our days has a similar effect on the hardware trojan intrusions on them. From the wireless communications to governmental and industrial tasks, people need more and more reliable systems and safe communications [1]. There are many different kinds of hardware Trojans, based on their main characteristics, which are: type, trigger and payload [2].

Type describes the kind of the attack, it either aims to the logic or the parametric functionality of the chip. Trigger is related to the way the Trojan will be activated, based for example on an input signal or after a specific time. Payload refers to the malicious functionality that is going to be included to the chip.

Interestingly, the majority of manufacturing tests remain unable to expose such hardware alterations. Recent attempts, like enhanced functional testing [3] or side-channel fingerprint generation and checking [4], aim to detect hardware trojans. In this paper, we focus on wireless cryptographic integrated circuits [5, 6] and present a hardware trojan detection framework using a mixed-signal integrated circuit [7].

II. IMPLEMENTATION

The mixed-signal integrated circuit which is selected to be implemented includes: the PRESENT lightweight block cipher [8], with an output buffer for the digital part of the system and an Ultra-Wide-Band (UWB) transmitter for the analog part, which are shown in Figure 1. The PRESENT encryption algorithm is used mostly in applications which require low power consumption and high chip efficiency. It needs at about two and a half times less resources than AES, while it supports a block length of 64-bit and the key length can be either 80- or 128- bit. It makes use of an SP-Network (Substitution-Permutation Network), where it is executed in 31 rounds. Every round introduces the next key bit by XORing it with the data. The 32nd key bit acts as key whitening before the first round and after the last round, presenting a linear permutation and a non-linear substitution layer. In our work, PRESENT encryption algorithm is applied, with 80-bit key length.

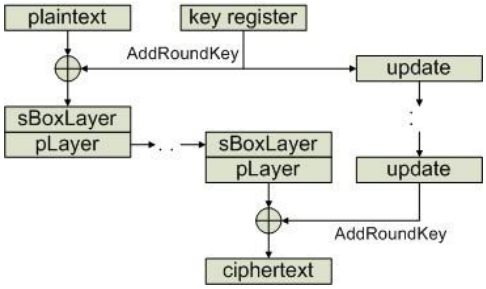

Figure 1: Top Level of PRESENT Block Cipher

The output buffer of the digital part is a First-In-First-Out (FIFO) queue, implemented as an enhanced scan-chain flip flop structure.

There are two alternative hardware trojans designs, which only affect the digital part of the system. These trojans are divided in two parts. The first part is a modification of the system's original scan-chain, as it is highlighted in Figure 3. Some digital logic gates (AND, OR, XOR and NOT gates), have also been added. They do not affect the function behavior of the system, but they allow the intruder to steal sensitive information. These extra gates will increase the system's area, but this increment is not enough as to be recognized as a harmful intrusion to the system.

The second part deals with the differences in the transmission frequency and amplitude between the original and the modified system.

In the first alternative (Figure 2), related to frequency, when the stolen key bit is "1", the transmission signal is delayed by a buffer, which at last increases the transmission frequency.

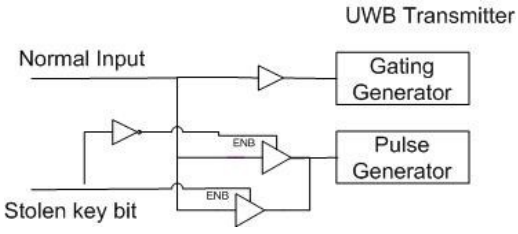

Figure 2: First Trojan - Measuring Frequency

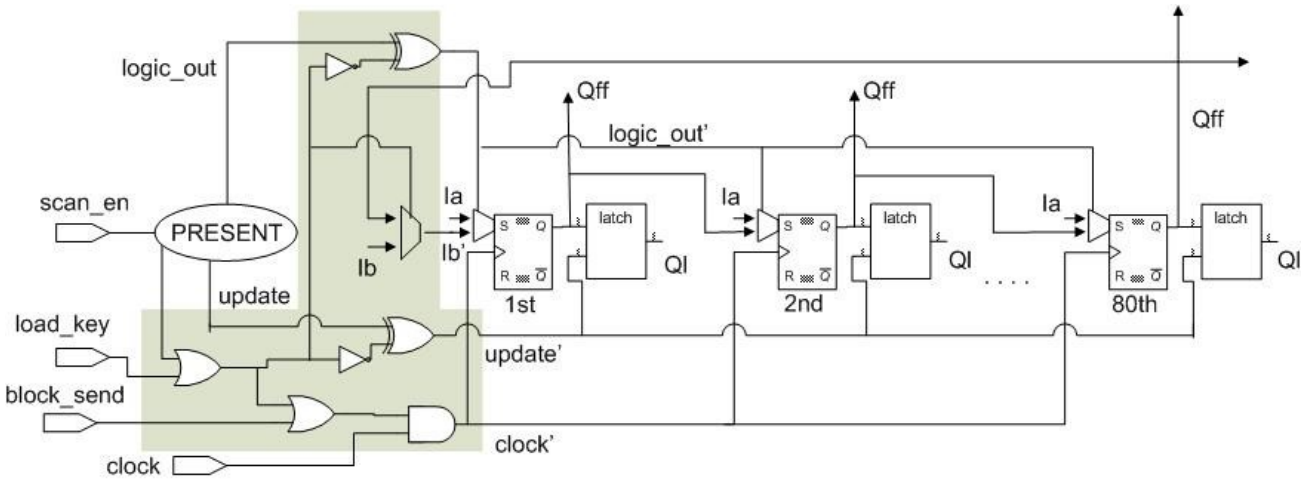

Figure 3: Modified Scan Chain

In the second alternative (Figure 4), related to the amplitude, when the stolen key bit is equal to "1", the transmission signal is strengthened by a driver, concluding to an increased transmission amplitude.

These hardware trojans leak the algorithm's encryption key thought the wireless transmission. When 80-bit are completely transmitted, the encryption key is at last known to the intruder.

Regarding the trojans characteristics, the type is referred to the area required from the modified system because of the inserted trojan, which does not change the design's specifications. The payload is referred to the technique of making the secret key well know to the attacker, through the public wireless channel. Based on that, it is needed to be assumed that the inputs of the system is always active, so there is no trigger point that can be defined.

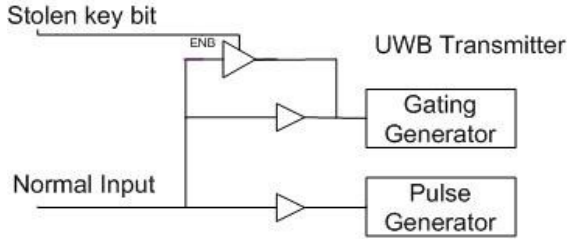

Figure 4: Second Trojan - Measuring Amplitude

III. CONCLUSIONS

In this work, a hardware Trojan detection framework is introduced. It is explained how an intruder can add trojans in a system, which affect only the digital part of it and without changing the functionality and the specifications. We try to answer to the question of how someone can steal the encryption key through the wireless transmission. This technique affects the transmission frequency and amplitude of the system. The trojan is efficient to be detected successfully, through these changes and other kind of statistics, like the outputs' transmission power.

ACKNOWLEDGEMENT

This work was partially supported by COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE).

REFERENCES

[1] N. Sklavos, “Securing Communication Devices via Physical Unclonable Functions (PUFs)”, Information Security Solutions Europe (isse’13), Brussels, 22-23 October, Belgium, 2013.

[2] R. M. Rad, X.Wang, M. Tehranipoor, and J. Plusquellic, “Power supply signal calibration techniques for improving detection resolution to hardware Trojans,” in IEEE/ACM International Conference on Computer-Aided Design, 2008.

[3] H. Salmani, M. Tehranipoor, and J. Plusquellic, “New design strategy for improving hardware Trojan detection and reducing Trojan activation time,” in IEEE International Workshop on Hardware-Oriented Security and Trust, 2009.

[4] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, “Trojan detection using IC fingerprinting,” in IEEE Symposium on Security and Privacy, 2007.

[5] G. Kalogeridou, N. Sklavos, P. Kitsos, "System Design and FPGA Implementation for a Cognitive Radio Wireless Device", Chapter in the Book: *Cognitive Radio and its Technological Impact on Wireless Cellular and Vehicular Networks*, editors V. Hrishikesh, M. Gabriel-Miro, Series Lectures Notes in Electrical Engineering, Vol. 116, *Springer*, 2012.

[6] L. Lin, M. Kasper, T. Guneysu, C. Paar, and W. Burleson, “Trojan side-channels: Lightweight hardware Trojans through side-channel engineering,” in Cryptographic Hardware and Embedded Systems, vol. 5747 of LNCS, Springer-Verlag, 2009.

[7] Yier Jin, Yiorgos Makris, "Hardware Trojans in Wireless Cryptographic ICs," IEEE Design & Test of Computers, vol. 27, no. 1, Jan.-Feb. 2010.

[8] A. Bogdanov, G. Leander, L. R. Knudsen, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT - An Ultra-Lightweight Block Cipher,” in Proceedings of CHES 2007, ser. LNCS, no. 4727. Springer-Verlag, 2007.