Harware Dithering: A Run-Time Trojan Neutralization Method for Wireless Cryptographic ICs

Christiana Kapatsori, Angelos Antonopoulos, Yiorgos Makris

Description of research

We propose a Hardware Dithering methodology as a prevention method against hardware Trojans that seek to take advantage of the process variation margins in integrated circuits (ICs). Our Dithering approach aims to neutralize Trojans through eliminating the inherent performance margin that allows a malicious adversary, having access to the fabrication facilities, to leak sensitive information. To demonstrate this methodology we have designed a random-walk in the space of transmission performance characteristics of a wireless cryptographic IC platform[1]. In this demo the preventive nature of hardware dithering will be presented in real-time, on a hardware Trojan which is designed to leak the key of an AES cryptographic wireless transmission.

Hardware Demonstration

For the dithering method demonstration the benchmark platform comprises an advanced encryption standard (AES) core and an ultra wide-band (UWB) transmitter as shown in Fig.1(a). As presented in the following block diagram, the AES core receives and encrypts the plaintext in blocks of 128 bits. The encryption uses a 128-bit key and after the ciphertext is produced, it is stored in the output buffer in blocks of 128 bits, until it is transmitted. After the output buffer there a serialization unit and then the UWB transmitter, responsible for sending the ciphertext to the receiver, in our case an oscilloscope, Fig.2

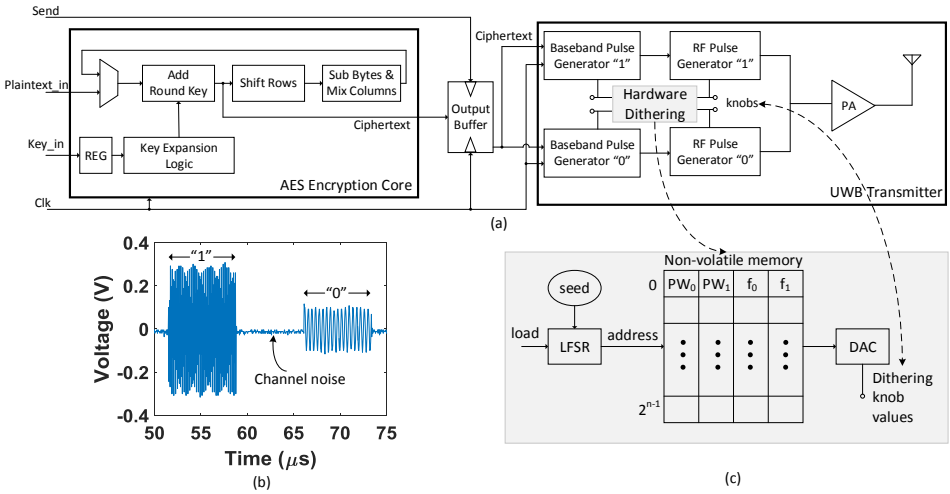

Figure 1: (a)System-level block diagram of the wireless cryptographic IC, (b)transmission voltage while sending "1" and "0", (c) dithering implementation

The implementation of the Hardware Dithering consists of four tuning knobs (PW_0, f_0, PW_1, f_1) that act on the amplitude and frequency characteristics of the transmission, Fig1(c) It also consists of a linear feedback shift register (LFSR), a finite state machine (FSM) and a non-volatile memory (NVM). The LFSR drives a random walk through the contents of NVM, which is programmed to store codes that produce the analog voltages provided from the Digital-to-Analog Converter (DAC) to the chip. The acceptable range of voltage values and by extension codes is determined by the specifications of the UWB transmitter. Depending on the knob value the transmission of a ciphertext of both 1 and 0 can either increase or decrease the amplitude and frequency of each bit of the 128-bit package. These knobs drive the cryptographic transmitter into an unpredictable, pseudo-random walk in the space of transmission performances. We must note that the dithering doesn't affect the ability of a legitimate receiver to correctly receive the package.

Hardware Setup

The setup needed for demonstration purposes is the following:

1. A custom-designed wireless cryptographic IC on top of the Opal-Kelly FPGA board
2. The oscilloscope - Tektronix MDO-4104 that acts as a wireless receiver
3. Two antennas for the wireless transmission
4. A laptop used as interface and for data demonstration

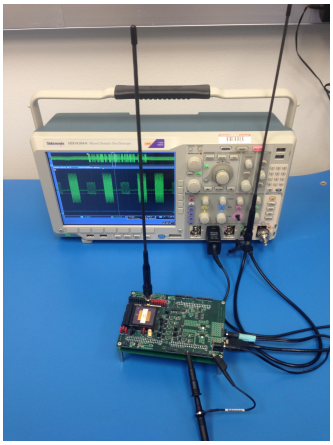

Figure 2: Wireless Cryptographic IC platform

Description of Observables

During this demonstration the audience can observe the follwoing:

- The operation of the Dithering in an non-infested transmission and the fact that the legitimate receiver remains unaffected and correctly receives/deciphers the package.
- The operation of the platform without the Dithering mechanism and how the Trojan is capable of leaking the encryption key through modulating transmission power amplitude or frequency.
- The simultaneous operation of the Dithering prevention method on an infested IC with a malicious Trojan. The adversary will loose its capability of leaking the key.

References

[1] Liu, Yu, et al. "Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 25.4 (2017): 1506-1519.