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

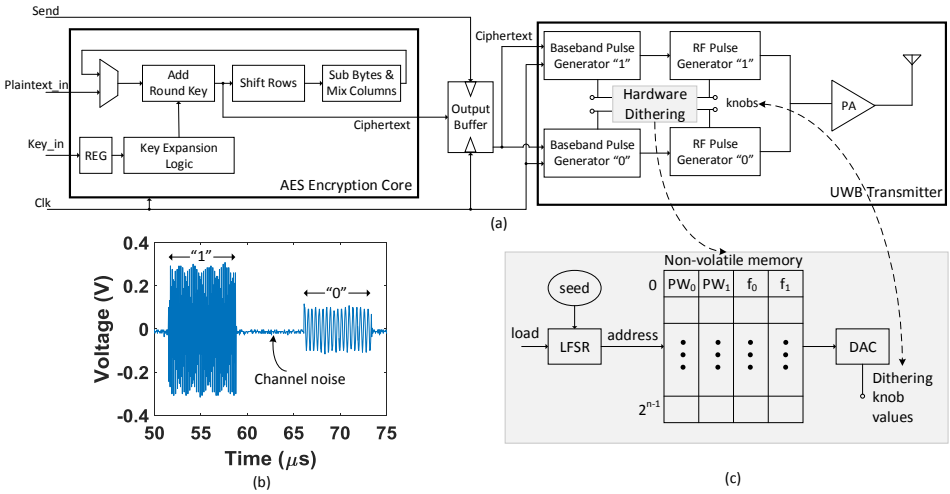

Figure 1: (a)System-level block diagram of the wireless cryptographic IC, (b)transmission voltage while sending "1" and "0", (c) dithering implementation