Hardware Trojan for OFDM based Wireless Cryptographic ICs

Farshad
Institute of Information and Communication Technology
Bangladesh University of Engineering and Technology
Dhaka, Bangladesh
farshad112@gmail.com

Md. Liakot Ali
Institute of Information and Communication Technology
Bangladesh University of Engineering and Technology
Dhaka, Bangladesh
liakot@iict.buet.ac.bd

***Abstract*—Hardware Trojan (HT) is now a burning issue in electronic circuit manufacturing supply chain. Over the last decade extensive research have been carried on HT detection methods for digital circuit. However the HT issue remains largely unexplored in the domain of Analog Mixed Signal (AMS)/ RF circuit where it is now an appealing target for the attackers. Now a days Orthogonal Frequency Division Multiplexing (OFDM) based wireless Cryptographic mixed signal ICs are widely used to exchange data securely over public channels. In this paper, we present a trigger based AMS HT threat model which exploits the Extended Cyclic Prefix (ECP) property of OFDM communication scheme to steal and leak the secret encryption key of 128 bit Advanced Encryption Standard (AES) encryption scheme over Additive White Gaussian Noise (AWGN) transmission channel. The possible detection mechanism for detecting such Trojan is also explored in this paper.**

***Contribution*—This paper presents a trigger based AMS HT targeting OFDM based wireless crypto ICs, which exploits the ECP property of OFDM to leak secret data in secure AWGN transmission channel and possible detection mechanism for detecting such Trojans.**

Keywords— Hardware Trojan, AES, OFDM, Wireless Crypto IC

I. INTRODUCTION

Globalization of IC supply [1] chain has resulted in a tremendous increase in vulnerabilities within the IC supply chain [2-3] that can be exploited by an adversary to insert Hardware Trojan (HT) [3] for performing malicious attacks thereby compromising security and reliability of the device. HTs are illegal modifications inside the design for malicious purposes such as theft of sensitive data, degrade performance, and cease operation once the Trojan is triggered [4-5]. Over the last decade extensive research have been carried on hardware Trojan in digital circuit. However the Trojan issue remains largely unexplored in the domain of analog circuit especially analog mixed signal (AMS)/ RF based wireless circuit [6]. It is now an appealing target for the attackers because wireless networks have become an inseparable part of everyday life and are now prevalent in most electronic systems, due to the rapid growth of telecommunications and the Internet of Things. To the best of our knowledge, recently two research works have been reported in this domain. Ref [7] shows a Trojan infested AMS/RF cryptographic IC which does not violate any digital, analog or system-level specifications, rendering traditional test methods ineffective but leaking the secret key through wireless transmission power. The presence of Trojan is possible to detect through statistical analysis of transmission power using Principle Component Analysis (PCA). Ref [8] shows a Trojan infested AMS/RF cryptographic IC where attacker leaks information exploiting Forward Error Correction (FEC) encoding of the transmitted signal and the Trojan can be detected by monitoring the noise distribution at the receiver to identify systematic inconsistencies caused by an HT. However one of the drawbacks of [7-8] was the Trojan implementation was specific to AM/FM modulation scheme which is not very widely used in higher speed wireless communication. Moreover, "always on" Trojan has been used in both cases. Now a days Orthogonal Frequency Division Multiplexing (OFDM) based wireless Cryptographic mixed signal ICs are widely used to exchange data securely over public channels. The issues related to trigger based Trojan in OFDM cryptographic AMS/RF ICs are still unexplored. In this paper we aims to introduce a Time Triggered Analog Payload based Mixed Signal HT which will steal the secret key of a secure Wireless Cryptographic IC and exploit the Extended Cyclic Prefix (ECP) property of OFDM communication scheme to embed the secret encryption key into Cyclic Prefix (CP) which acts as a guard band between successive symbols to overcome inter-symbol interference (ISI) such that it does not violate any transmission specification and the data can be extracted by a remote attacker using a predefined rare signal combination of Design for Test (DFT) scan ports in the receiver end. The scan output ports are used to extract the secret key once the rare input combination is triggered in scan input ports of the receiver.

The remainder of this paper is structured as follows. Section II explains CP property of OFDM scheme. Section III contains detailed description of Wireless Cryptographic IC which is designed and used as an experiment vehicle for demonstrating proposed HT. We focus on the Trojan Free and Trojan infested versions of an Advanced Encryption Standard

(AES-128) + OFDM scheme based Wireless Cryptographic IC. The detailed mechanism of HT implementation in the design to leak the secret key over Additive White Gaussian Noise (AWGN) transmission channel is also explained in section III. Section IV describes detection evasion mechanism of proposed HT during post-silicon testing using traditional testing methods, possible detection methods to detect the presence of HT in post-silicon manufacturing testing and a comparison table that compares our implemented HT threat model and previously implemented HT Threat models. Section V draws the conclusion.

II. CYCLIC PREFIX SCHEME IN OFDM

In OFDM communication scheme, CP is created by prepending a copy of the end of the OFDM symbol to its beginning as illustrated in Fig. 1. The CP is generally discarded and never analysed at the receiving end. Most commonly used OFDM based communication schemes like LTE, generally uses two types of CP; normal and extended [9]. In order to overcome the inter-symbol interference (ISI) problem, the length of the CP (P) must be greater than or equal to the number of the tap channels (L). In normal CP, the number of tap channels used usually equal to the length of the CP. In ECP, the number of tap channel used is greater than the length of the CP. ECP is used to transmit information over extremely noisy channel. However, if ECP is used in low noise environment then this extra P-L samples can be used to transmit valid information. Our proposed HT utilizes this extra P-L samples as a covert channel to transmit secret data over AWGN transmission channel.

III. WIRELESS CRYPTOGRAPHIC IC

The experimental vehicle chosen for this paper is an OFDM based wireless Analog/Mixed Signal cryptographic IC. The digital portion contains an AES crypto processor for encrypting plain text into secure cipher text using secure cipher keys and an output buffer for holding the cipher text and sending it to analog domain for transmission. The analog portion contains OFDM trans-receiver for transferring the secure cipher text over transmission channel using OFDM symbols. A System level block diagram of our experimental IC is shown in Fig. 2.

We have implemented two types of experimental IC model, Trojan Free and Trojan Infested. The Trojan infested IC will act like Trojan free IC when HT is dormant. But once the Trojan is triggered it will leak the secret AES encryption key over AWGN transmission channel by hiding it in the redundant bits (*P-L*) of ECP within OFDM waveform such that it does not distort the waveform. In the transmitter side the scan chain and Built-In Self-Test (BIST) circuitry is modified such that the Linear Frequency Shift Register (LFSR) circuit in BIST works as a counter that counts clock pulses in regular mode and act as a LFSR in scan mode. Once the counter reaches a predefined large value then the HT will trigger. The large value of counter required for triggering the HT is chosen such that during post-silicon testing the probability of HT activation is very low. Thus HT avoids detection during post silicon testing stage.

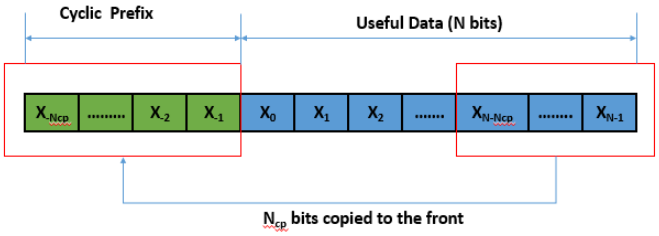

Figure 1. Cyclic Prefix

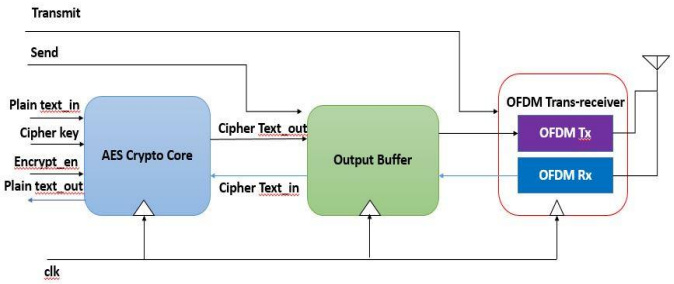

Figure 2. System Level Block diagram of experimental wireless cryptographic IC

A. *Trojan Free Version*

The AES crypto core receives a 128 bit plaintext and a 128 bit Cipher key and store them in on-chip registers. The "plain_text" and "cipher_key" input ports in the design as shown in the block diagram of Fig. 3 are used for taking the 128 bit plain text and 128 bit cipher key. The "encrypt_en" must be 1 and "scan_en" must be 0 to enable the AES encryption process. The encryption core implements AES 128 algorithm, so it requires 10 rounds to convert 128 bit plain text into 128 bit cipher text which is then stored in the output buffer. The implementation details of AES encryption and decryption algorithm is beyond the scope of this paper. The cipher text is then fed into the OFDM trans-receiver module and encrypted data is transmitted into the AWGN channel through OFDM transmitter. The detailed block diagram of the Trojan Free IC is shown in Fig. 3.

OFDM transmitter block consists of serial to parallel block (S2P), 64 point Quadrature Amplitude Modulator (64 QAM mapper), Inverse Fast Fourier Transform (IFFT) block, Cyclic Prefix Addition Block (add_cp), parallel to serial converter (P2S), Digital to Analog Converter (DAC) and IQ modulator. S2P converts the serial data stream coming from AES encryption core output buffer into parallel data stream which is fed into 64 QAM mapper for constellation mapping. The output of 64 QAM mapper is fed into IFFT block. IIFT block converts the frequency domain components of OFDM into time domain components which is fed into "add_cp" block for adding CP to the OFDM waveform. The output of "add_cp" is again converted to serial using P2S and then converted to analog signal using a DAC and IQ modulator.

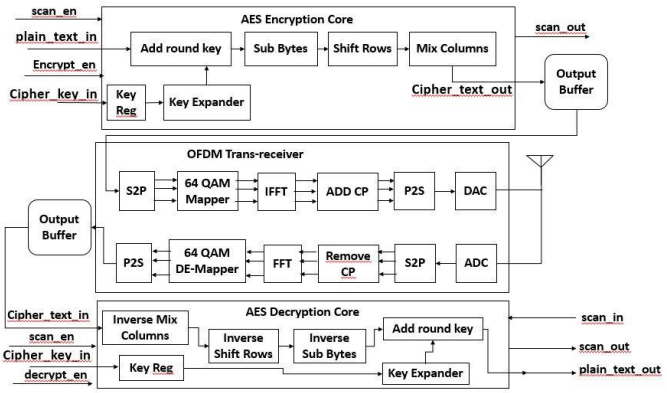

Figure 3. Detailed Block diagram of Trojan Free Cryptographic wireless IC

The receiver block consists of IQ demodulator, Analog to Digital Converter (ADC), S2P, Remove CP (rm_cp) block, Fast Fourier Transform (FFT) block, 64 point QAM de mapper (64 QAM Demod), P2S block. The received IQ modulated data is fed to the IQ demodulator and then to ADC block. Output of ADC block is fed to the "rm_cp" block which removes the CP. The output of "rm_cp" is send into the FFT block which converts the time domain components of the OFDM symbol into frequency domain component. The output of FFT is fed into the 64 QAM Demod block for constellation de-mapping. The output of 64 QAM Demod is converted into serial data stream using P2S block which is then send into output buffer. The AES decrypter core takes the encrypted data from the output buffer and cipher key from input port "cipher_key_in" and then performs decryption operation. After 10 rounds the decrypted plain text is send to the output port "plain_text_out".

B. Trojan Infested Version

Hardware Trojan is inserted into the design by modifying some circuitry in the digital and analog portion. The DFT scan chain and BIST circuitry is modified to create Trojan Trigger. In the AES Encrypter module the LFSR circuitry is modified such that it will work as LFSR when the scan mode is on and as a clock counter during normal mode. The counter value is incremented by 1 in each clock cycle. The HT is triggered when the counter reaches a predefined large value. In our design we have selected 32'hFFFF_FFFF as Trojan trigger value to ensure that Trojan remains dormant during post silicon testing. The modified LFSR schematic is shown in Fig. 4. The attacker will also add additional 64 QAM modulator and IFFT blocks to modulate the Trojan data for embedding into the ECP of OFDM symbol. The 64 QAM modulator and M point IFFT block is power gated when the Trojan is dormant and only turns on when the Trojan is activated. This mechanism helps the Trojan to avoid detection via power analysis.

Once activated on the digital portion, the Trojan will steal the secret AES encryption key from the "key_reg" register. A modified DFT scan-chain is used to store the stolen value and pass it to the Trojan 64 QAM modulator for constellation mapping. The mapped output is then fed into the Trojan IFFT block which creates Trojan OFDM symbol. The output of the IFFT block is then send into the "add_cp" block embed in the P/4 location of ECP. It is assumed that the attacker will know the fading channel tap length and the length of fading channel (L) will be less than or equal to half of CP length (P) i.e. $L \leq P/2$.

So, first P/2 samples of CP is replaced by the secret data and first P/4 locations are replaced by secret modulated symbol by performing M point IFFT on the modulated stolen key. The next P/4 location will contain the repeated version of secretly modulated symbol.

At the receiving side the HT can be enabled by using a rare combination of input ports. In our experiment we have chosen scan_in [0][0] = 1 and scan_en = 0 as Trojan trigger logic. In the receiver the attacker will also implement extra 64 QAM demodulator and M point FFT which will be power gated during Trojan dormant period to avoid detection via power analysis. Once the HT is enabled P/4 locations of CP is taken as secret data symbol which is then fed to the secret M-point FFT and 64 QAM de-modulator block and secret key is recovered. This secret key is then transmitted via scan_out ports for the attacker to extract. Block diagram of the proposed Trojan infested IC is shown in Fig. 5.

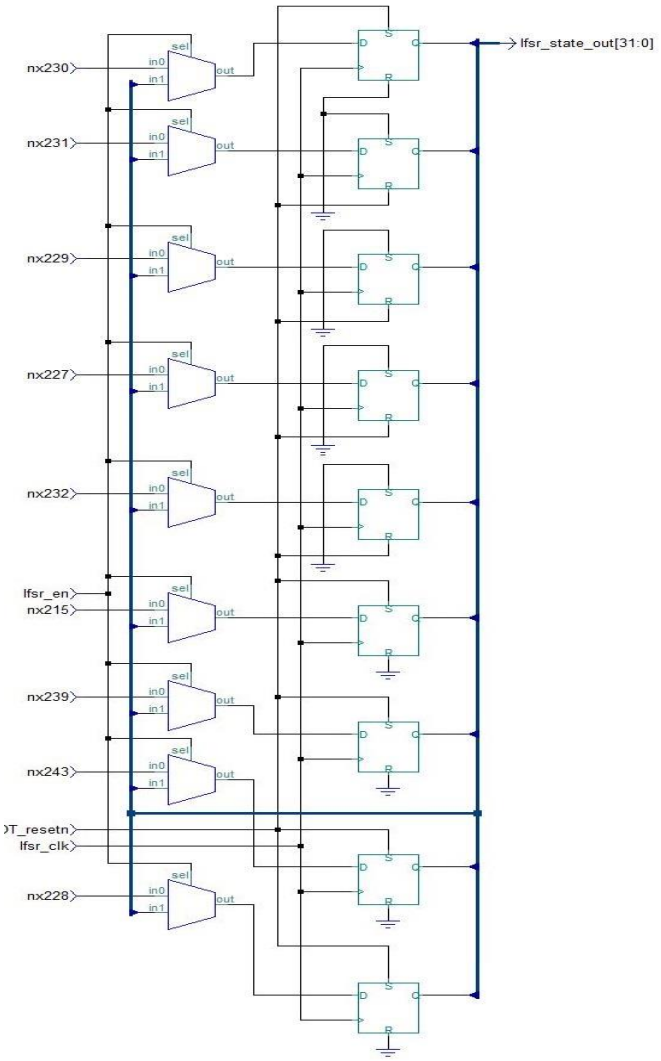

Figure 4. Schematic Diagram of Modified LFSR

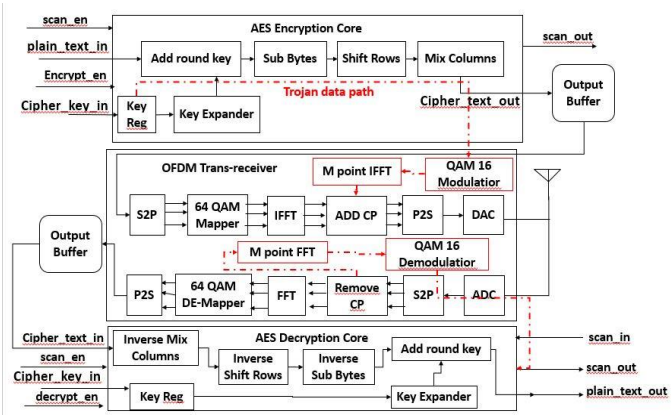

Figure 5. Detailed Block Diagram of Trojan Infested Wireless Crypto IC

IV. SIMULATION RESULTS

Both Trojan infested and Trojan free wireless crypto IC design is simulated in Cadence Incisive Unified Simulator (IUS). AWGN transmission channel is used with very high SNR value for simulating low noise environment.

A. Detection Evasion

The implemented hardware Trojan does not alter the functionality of AES crypto core nor does it distort the OFDM waveform to a visually noticeable degree once activated. Hence it is hard to detect in the transmission channel analysis during testing phase. Moreover, due the large activation value in "counter" the probability of Trojan remain dormant during testing phase is very high. The Trojan circuits are supply gated and clock gated so they do not consume any noticeable power when the HT is dormant.

We have simulated the Trojan infested design when the Trojan is dormant and Trojan free design in Cadence Incisive Unified Simulator (IUS). The output waveform for both designs are identical as shown in Fig 6 and Fig 7.

The output waveform of transmitter and receiver for Trojan Infested design when the Trojan is activated is shown in Fig. 8. In the transmitter waveform shown in Fig. 8 the cipher key is embedded in the ECP, 16 bit at a time and transmitted over AWGN transmission channel. In the receiver waveform shown in Fig. 8 the cipher key is extracted from ECP and send to the attacker via scan_out ports. In this experiment we have used scan_out[1:4] for transmitting the cipher key. scan_out[0][1] is used as output sample clock, that attacker can use as valid signal during cipher key extraction. scan_out[0][0] bit indicates that the HT is activated in the receiver end.

As shown in Fig. 6 and Fig. 8 the waveform of Trojan free and Trojan infested circuit is almost identical even when the Trojan is active, hence it is very hard to detect the leak of information without any prior knowledge.

B. Possible Detection Methods

Trojan is triggered-on type so the power profile of the IC when the Trojan is dormant and when Trojan is active will be different. From this difference it may possible to classify the ICs using machine learning based statistical analysis methods and side channel analysis.

C. Comparison between our HW Trojan threat model implementation and other known HW threat model implementations

Table I shows a comparison between our implemented Trojan threat model and previously implemented Trojan threat models for wireless crypto IC.

From Table I it is observable that all previous

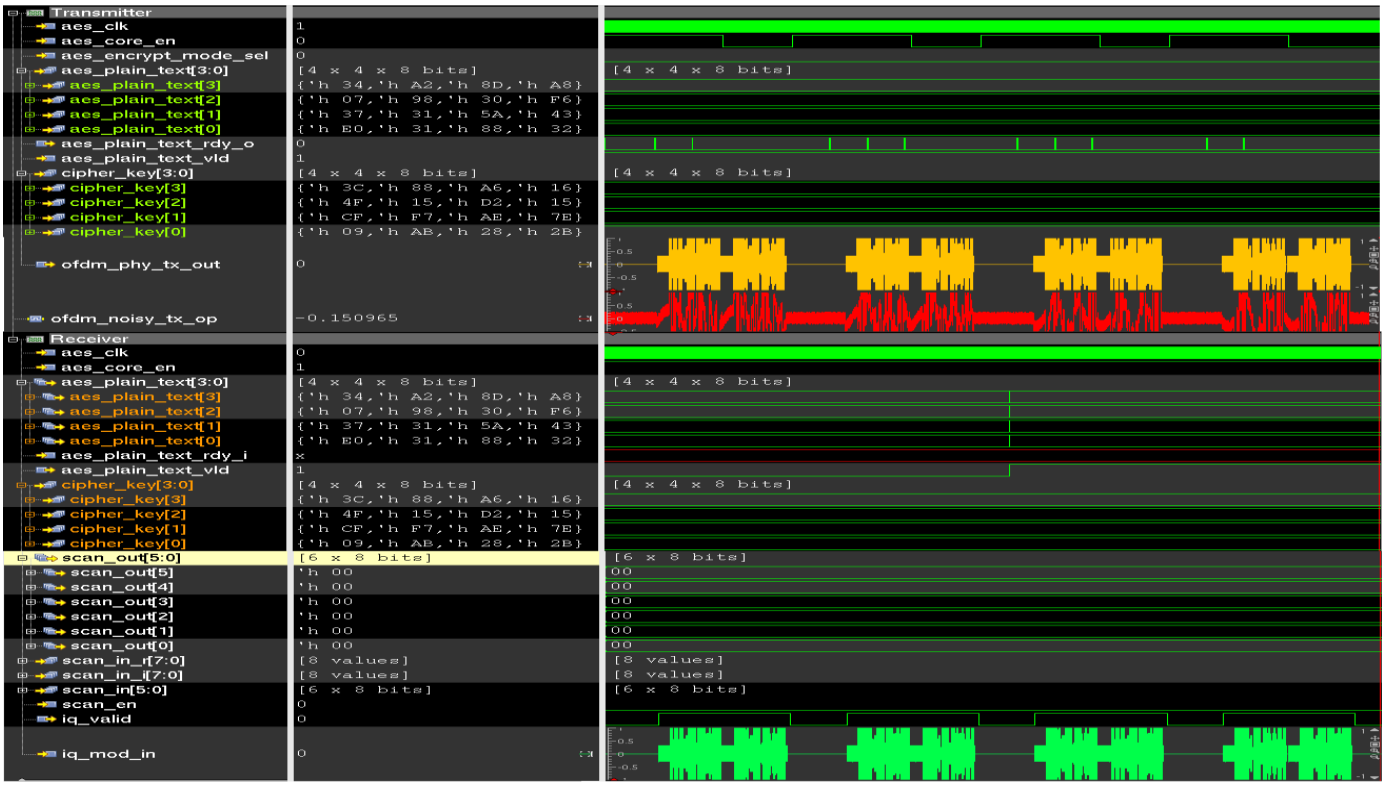

Figure 6. Waveform of Trojan Free Wireless Crypto IC

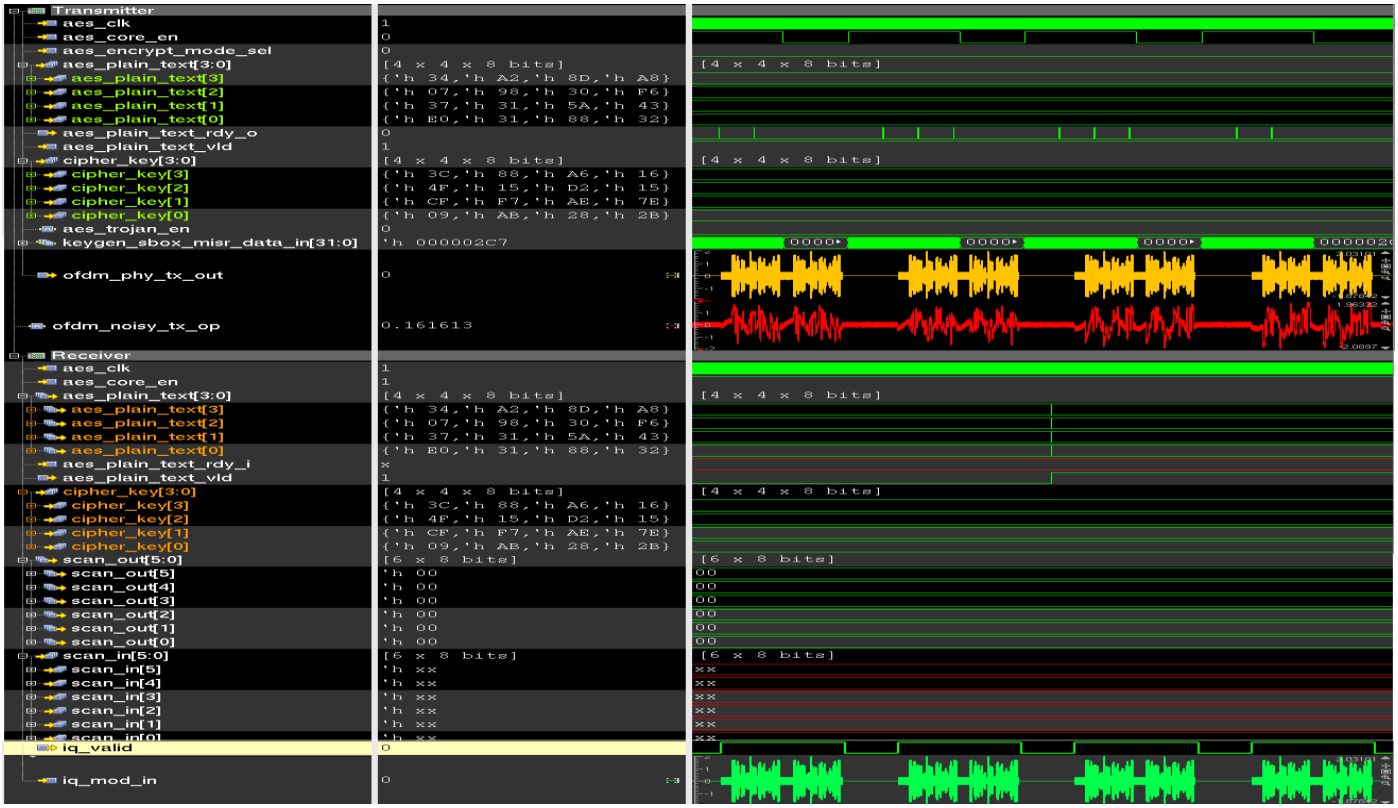

Figure 7. Waveform of Trojan Infested Wireless Crypto IC With Dormant Trojan

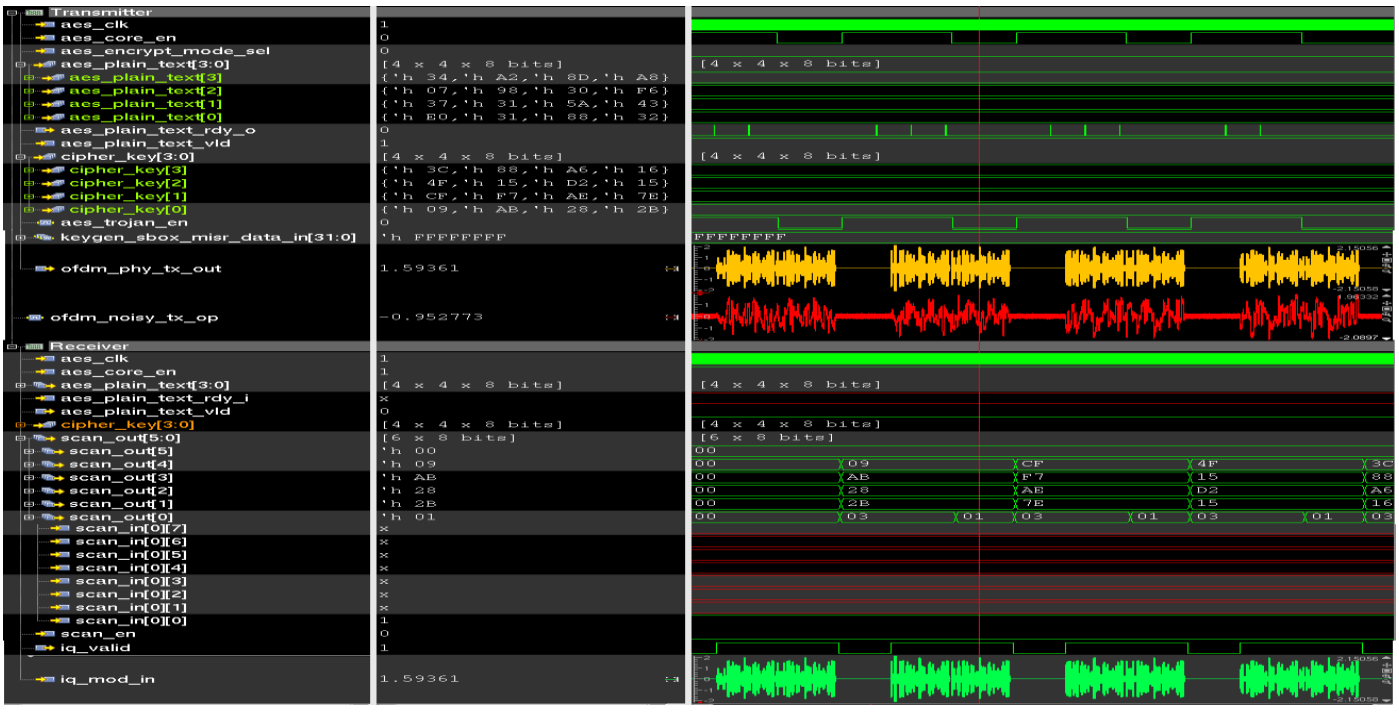

Figure 8. Waveform of Trojan Infested IC with Trojan Enabled

implementations focuses on “always on” type HT Threat model implementation and detection using various statistical analysis. Whereas we have focused on “Time Triggered” based HT implementation. As our Trojan remains dormant during traditional post-silicon manufacturing testing so, traditional golden model based side channel analysis in ineffective in detecting our Trojan.

TABLE I. COMPARISON BETWEEN PROPOSED HT THREAT MODEL AND PREVIOUS IMPLEMENTATIONS

Implementation Method Name	Trojan Type	Exploit Mechanism	Detection mechanism
Trojan Implementation On UWB Based Crypto IC [7]	Always On	Amplitude and Frequency Offset Margin	Statistical analysis of transmission power using PCA
INFECT on IEEE 802.11a/g [8]	Always On	FEC encoding of the transmitted signal	Monitoring the noise distribution at the receiver to identify systematic inconsistencies
Proposed HT Threat Model	Trigger Based	ECP Property of OFDM	Statistical analysis OF power using Side Channel Analysis

V. CONCLUSION

In this paper we have demonstrated a "time trigger" based AMS HT threat model that exploits the ECP property in OFDM communication scheme to leak sensitive information over secure AWGN transmission channel. The future work may contain the development of statistical analysis methods and verification methodologies for testing presence of such Trojans.

ACKNOWLEDGMENT

Authors are grateful to the Institute of Information and Communication Technology of Bangladesh University of Engineering and Technology for allowing us to conduct this research using its EDA design tools, resources and laboratory facilities.

REFERENCES

[1] Tehranipoor M, Guin U, Forte D (2015) Counterfeit integrated circuits: detection and avoidance. Springer International Publishing

[2] Liu B, Gang Q (2016) VLSI supply chain security risks andmitigation techniques: a survey. Integr VLSI J 55:438–448

[3] Mishra P, Bhunia S, Tehranipoor M (2017) Hardware IP securityand trust. Springer

[4] Tehranipoor M, Koushanfar F (2010) A survey of hardware Trojantaxonomy and detection. IEEE Des Test Comput 27(1):10–25

[5] Xiao K, Forte D, Jin Y, Karri R, Bhunia S, Tehranipoor M (2016)Hardware Trojans: lessons learned after one decade of research.ACM Trans Des Autom Electron Syst (TODAES) 22(1):6:1–6:23

[6] Antonopoulos A., Kapatsori C., and Makris Y., "Trusted Analog/MixedSignal/RF ICs: A Survey and a Perspective", journal of IEEE design and Test, Vol. 34 (6), Dec. 2017

[7] Liu Y., Jin Y., Nosratinia A., Makris Y., Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs. IEEE Trans. Very Large Scale Integr. Syst. PP(99), 1–14 (2016)

[8] Subrmani K.S., Antonopoulos A., Abotabl A.A., Nosratinia A., Makris Y., "INFECT: INconspicuous FEC-based Trojan: a hardware attack on an 802.11a/g wireless network," in IEEE Hardware Oriented Security and Trust Conference (HOST), 2017

[9] A. Kumar Nain, P. Rajalakshmi, "Exploring Cyclic Prefix for Secret Data Transmission over LTE Networks", in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) , 2018