ISSN No:-2456-2165

AES Encryption in Artix-7 by using Electromagnetic analysis in Xilinx Forums

K.Mounika
Dept of ECE, VVIT, Nambur
Guntur, India, A.P

Abstract:- In this research, the data flow from a field programmable gate array (FPGA) and the advanced encryption standard with the 256 bit key (AES-256) were used to make an electromagnetic side-channel attack. The FPGA board was a Diligent Nexys-4 with Artix-7 FPGA and partially succeeded. With only 2000-3000 electromagnetic (EM) tracks a few sub keys were successfully removed from AES-256. The remaining key assumptions were classified and shown in a chart accordingly. In addition to this, the tests conducted included an attack on an isolated hardware field in the AES algorithm by designing a single 8-bit data block, the first round and Sub Bytes.

The acquisition of data was corrupted every time someone was plugged in e.g. a cell phone charger or a laptop-charger in the nearby rooms. Longer tests are hard to perform because of random interference. In order to detect interference, the experiment was constantly supervised. For future tasks, the lateral channels attack will require more EM-trace data points, more EM-tracks, faster oscilloscope, lower-pass filters and a wider bandwidth amplifier.

Keywords:- *Electromagnetic Side-Channel Attack; AES-256; Artix-7; FPGA; Differential Analysis.*

I. INTRODUCTION

The strength of the computation to brute the password has increased greatly in the context of increasing use of advanced cryptographic algorithms to protect sensitive data. The time required is so high that when decrypted, the information becomes useless and outdated. The details are no longer valid. Two generic threats to cryptographic systems are currently present; quantum and side channel analytics. The emphasis will be the cheaper option in this project, side-channel analysis.

Side-channel analysis [1] is often called a passive non-invasive attack. This is a way to analyze an encryption scheme's metadata to achieve the actual secret key. The analysis of a side-channel is often limited to various physical aspects; electromagnetic radiation analysis, power consumption, time and audio analysis [2]. Advenica is a company that specializes in hardware applications for cyber security. Their products are used by the national military and other authorities. Advenicas products have been certified by the EU, NATO and Swedish Armed Forces to the EU SECRET, the Swedish Armed Forces TOP SECRET and NATO SECRET [3].

Security systems employ confidentiality, integrity, or authentication through mathematical algorithms. It is defined as: cryptographic devices & electronic devices which implement cryptographic algorithms and store cryptographic keys. The algorithm is installed in hardware or software and accepts two inputs; see Fig.1, message and cryptographic key.

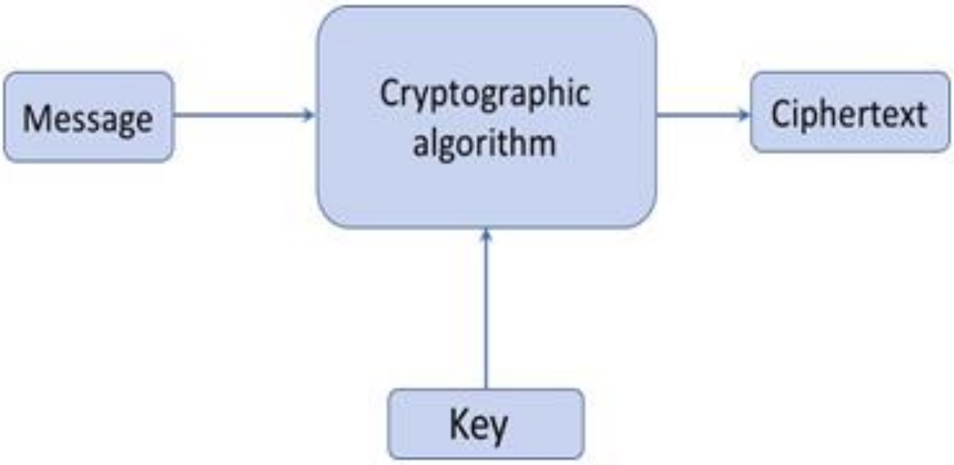

Fig 1:- Main Concept of Cryptographic Algorithm.

When we consider a larger server data storage centre, computer racks with cryptographic devices may be available. These data centres require a wide variety of maintenance. A big rotation of personnel gives the attacker the opportunity to approach the safety system and its power supply physically. Without the owner knowing it, the attacker could extract the key. The owner can also lose the encryption device and notice it days later. Fig.2 presents a fictitious threat scenario.

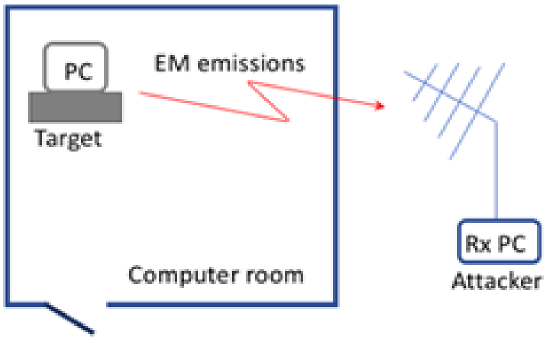

Fig 2:- Illustrative Method for Attacking a Cryptographic Device.

This thesis focuses on an FPGA's electromagnetic radiation. FPGA is a good way to speed up various cryptographic operations. This presents SASEBOGIII'S detailed architecture and features and shows the result of an electromagnetic SCA attack against the standard AES block cipher on the kintex-7 FPGA [4]. Analysis of DPA and DEMA Attacks is determined [5]. Electromagnetic Techniques and Probes for Side- Channel Analysis on Cryptographic Devices are explained[6].Side channel attacks are only a part of the physical reality but the theory of provable physical security is a long term goal in cryptography research[7]. The Advanced Encryption Standard(AES) is proved[8].This shows "A practical differential power analysis attack against an FPGA implementation of AES cryptosystem"[9].Our approach describes the first cheap and efficient way to conduct power-analysis attacks on a real implementation of a circuit in a very early stage of the design flow[10].The simulation results show that Hamming distance model based power analysis attack is efficiently used for anti-power analysis of the security chips before fabrication[11]. A classical model is used for the power consumption of cryptographic devices. The drawback of CPA regards the leakage model parameters [12]. Side Channel Attack on Low Power FPGA Platform [13]. Series FPGAs Overview (DS180)on Xilinx[14]. Spartan-6 Family Overview (DS160) on Xilinx [15].

II. PROCEDURE

Today, we know of five various side-canal attacks. Audio, electromagnetic emissions, energy consumption, temperature and timing analysis take advantage of the physical data leak in the different side channel attacks. The thesis focuses on one of them, the analysis and attack of the electromagnetic side-channel. The FPGA, the cryptographic AES algorithm and simple / differential analysis are provided in this chapter. FPGA is an integrated circuit with several logic cells, random access memory (RAM) block options and lookups. This chip can be reconfigured and produce the same hardware logic as an ASIC, but it is not equally fast when making computations and it requires more power. The benefit of a FPGA is the flexibility to create dedicated hardware. Physics creates observable physics behind an electronic device. Computing tasks create heat, power supply and noise. Electromagnetic fields. The phenomenon is measured using various devices. The FPGA is generally a low-tension semiconductor for complementary metal oxide (CMOS). The various transistors act as a current gate to open (or close) the circuit. When calculations are made by a microprocessor or an FPGA, it sends out emissions of EM. It might be an electric or magnetic field. In Fig. 3 you may view an example of a loop antenna that extracts magnetic emissions from a FPGA.

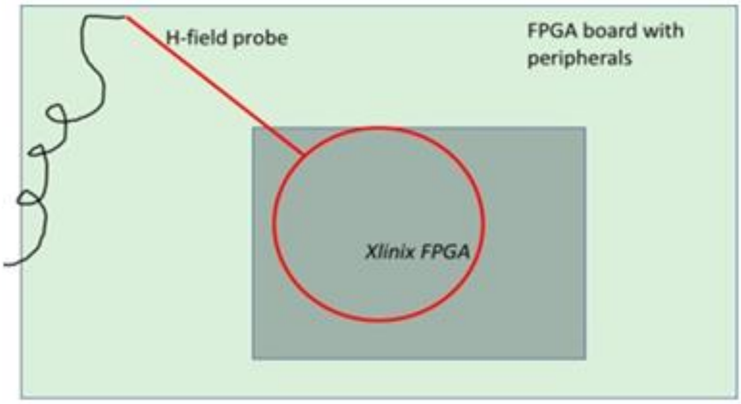

Fig 3:- An Example of Electromagnetic Measurement on FPGA with a Loop Antenna.

When the processor calculates, the attacker may observe a certain EM trace on an oscilloscope. An attacker can extract the key from the cryptographic device using a single EM trace. It is a technique that interprets directly the EM emissions collected during encryption operations. The attacker needs detailed knowledge of the encryption algorithm used to succeed in a simple electromagnetic analysis.

III. RESULTS

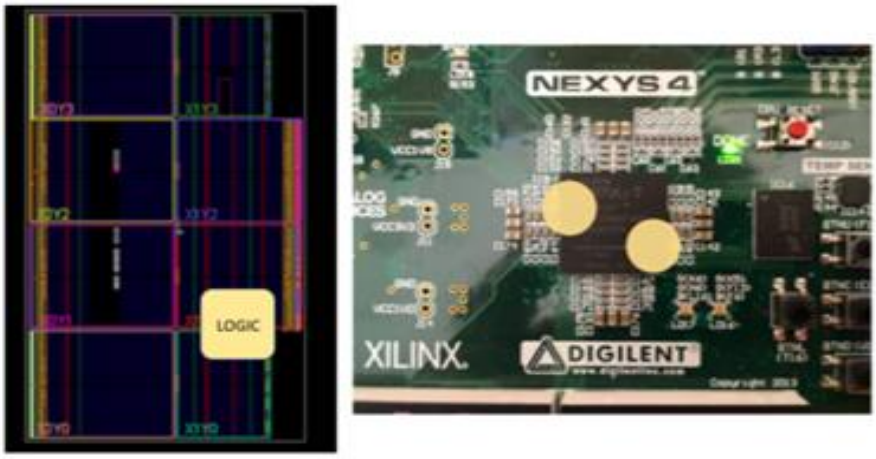

Fig. 4: Overview of the areas which are sending out electro- magnetic emissions.

Fig.4 shows the area that radiated most electromagnetic emissions. The highlight on the left is where FPGA implements the actual logic cells. The left portion of Fig.4 is an elaborate design of Xilinx Vivado. On the border of the FPGA, few cells are spread. The cells on the edge are I / O. Two highlighted electromagnetic emission areas may be observed in the right part of Fig.4. The results raise questions about the second sector of EM emissions with few logical cells. With the exception of I / O-pins no logic cells exist.

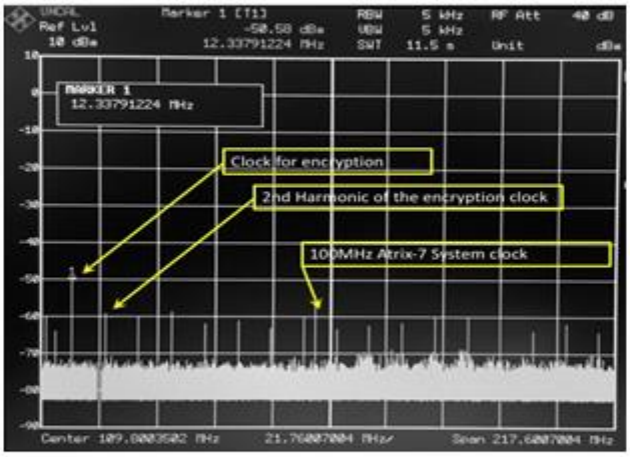

Fig 5:- The 100 MHz Internal Clock is Divided into a 12.5 MHz Clock. The Figure Presents the Frequency Spectra of the Encryption.

The spectrum analyser collected all the current frequency in the FPGA before the extraction of EM traces. The internal frequency 100 MHz and the divided frequency 12.5 MHz are shown clearly in Fig.5 It isn't 12.5 MHz precisely. For each individual harmonic there are many harmonics with+ 12,5 MHz When the 12,5 MHz clock was increased, the acquisition of data would be affected.The trigger signal with 14 rpm AES encryption plus two rpm memory storage cycles and AES wrapper is used.

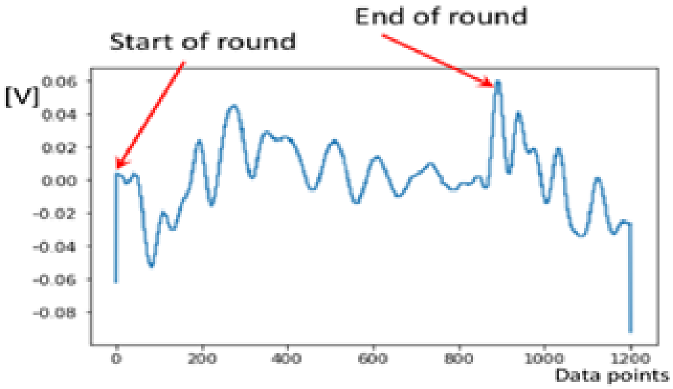

Fig 6:- Captured EM Trace at 10 cm Distance with 5 cm Loop Antenna.

Fig. 6 shows SEMA from the first round of AES at a distance of 10 cm. There is little visually similarity with this EM trace . However, the AES round, but the distance from the FPGA is different

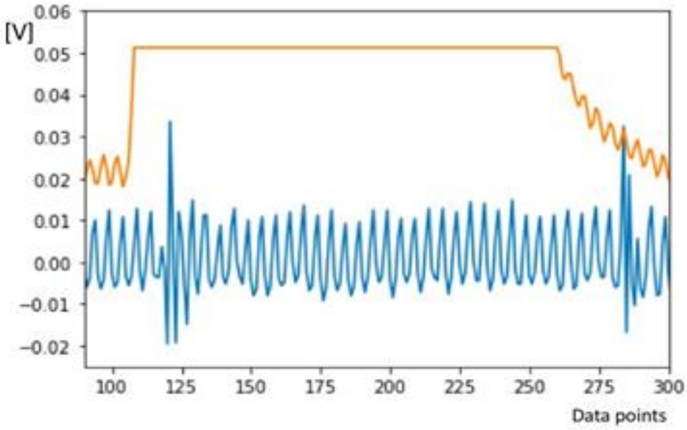

Fig 7:- Capturing EM Traces with a Frequency Over 50 MHz

Fig. 7 shows how the collection of data is affected by the collection of data at the same speed as the internal clock of 100 MHz.

The results of the DEMA simplified AES design are presented in Table 1. Due to power failure, but only with one key, various data acquisitions were made; 0x02. The top-ranking key for each 1000 EM trace is shown in Fig. 8.

Data acquisition on simplified AES, with EM traces and the ranked key.										
key	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000
0x02	215	171	54	71	110	51	41	50	37	30

Table 1:- Rank for Simplified AES

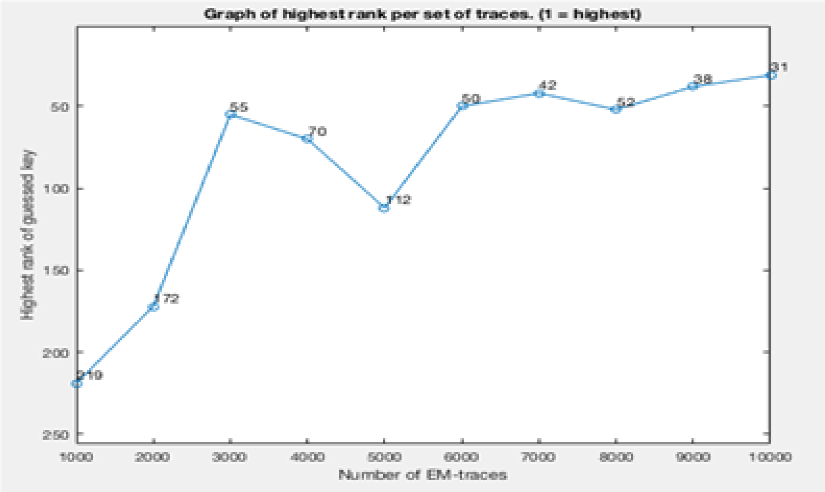

Fig 8:- The Graph Presents a Summary of Highest Rank of the Key Guesses from Table 1.

IV. CONCLUSION

One 8-bit sub key was extracted from the FPGA at a distance of 0 cm. Five sub key from 10,000 EM traces have been extracted including higher classified keys in Table 4.1. A sub key was removed at 10 cm from the FPGA. Even AES-256 is no longer safe with new technology in the form of a quantum computer and the promised calculating capacity. A complete AES-256 with present technology is considered safe after quantity. By combined with a quantum computer, the number of bits can be reduced to brute the last unextracted bits. However, all sub keys with current equipment need to be extracted longer. Three different categories of people, organizations, and nations can separate the threat sources in the cyberspace. In this thesis, the results show that a side-channel attack on a post-quantum safe encryption algorithm can be perpetrated as individual using low-cost equipment. The simplified AES has been designed to match the Hamming distance of the EM model.

REFERENCES

[1]. Elisabeth Oswald Stefan Mangard and Thomas Popp. Power Analysis Attacks. Revealing the Secrets of Smart Cards. Springer, 2007.

[2]. Defending against side-channel attacks.https://www.eetimes.com/ document.asp?doc_id=1279920. Accessed: 2018-02-14.

[3]. Advenica.https://advenica.com/en/certifications-approvals. Accessed: 2018-02-14.

[4]. 'A.Sasaki Y.Hori T.Katashita and Akashi Satoh. "Electromagnetic Side- channel Attack against 28-nm FPGA Device". In: 2012 IEEE 1st Global Conference on Consumer Electronics 32.3 (Dec. 2012), pp.657–660.issn:2378-8143.doi:10.1109/GCCE.2012.6379944.url:http://dx.doi.org/10.1109/35.267438.

[5]. Cheuk Wong. "Analysis of DPA and DEMA Attacks". MA thesis. San Jose State University, 2012.

[6]. Elke De Mulder. "Electromagnetic Techniques and Probes for Side- Channel Analysis on Cryptographic Devices". PhD thesis. Katholieke Universities Leuven - Faculty of Engineering, 2010.

[7]. Ingrid M.R. Verbauwhede (François-Xavier Standard). Secure Integrated Circuits and Systems, Chapter: Introduction to Side-Channel Attacks. Springer US, 2010.

[8]. National Institute of Standards and Technology. FIPS PUB 197: Advanced Encryption Standard(AES).2001.url:https://nvlpubs. nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[9]. Massoud Masoumi Mehdi Masoomi and Mahmoud Ahmadian. "A practical differential power analysis attack against an FPGA implementation of AES cryptosystem". In: 2010 International Conference on Information Society (i-Society) (2010), pp. 308–312.

[10]. Elisabeth Oswald Colin D. Walter Cetin K. KoçChristof Paar (Eds.) (Siddika Berna Örs and Bart Preneel). Cryptographic Hardware and Embedded Systems -CHES 2003. Chapter: Power-Analysis Attacks on an FPGA – First Experimental Results. Springer-Verlag Berlin Heidelberg, 2003.

[11]. Weiwei Shan Jie Li and Chaoxuan Tian. "Hamming Distance Model based Power Analysis for Cryptographic Algorithms". In: Applied Mechanics and Materials 121-126 (Oct. 2011), pp. 867–871. issn:1662- 7482. doi:10.4028/www.scientific.net/AMM.121-126.867.

[12]. Marc Joye, Christophe Clavier Jean-Jacques Quisquater (Eds.) (Eric Brier, and Francis Olivier). Cryptographic Hardware and Embedded Systems - CHES 2004. Chapter: Correlation Power Analysis with a Leakage Model. Springer Berlin Heidelberg New York, 2004.

[13]. Mustafa Faraj. "Side Channel Attack on Low Power FPGA Platform". MA thesis. University of Waterloo, Ontario Canada, 2016.

[14]. Series FPGAs Overview (DS180), Xilinx, Inc., 2012.

[15]. Spartan-6 Family Overview (DS160), Xilinx, Inc., 2011.