Grenze International Journal of Engineering and Technology, Special Issue

Analytical Approach of Trivium FPGA Implementations against Information Security Vulnerability

Ch. Suresh[1] and M. Mahesh Babu[2]
[1-2]Electronics and Communication Engineering Dept, Methodist College of Engineering and Technology, Hyderabad 500001, India
Email: chiruvellasuresh@gmail.com, mahibabu606@gmail.com

***Abstract*—The focus of this work is addressing the issue of the information security along with to introduce faults in Trivium stream ciphers implemented on FPGA. Daily, an incredible amount of information is exchanging in many digital forms. The digital devices have become the data sources which pump out the majority of the information on the web. The evolution of the Internet of Things (IoT) has come up with innovative solutions and its demand for information security is indeed a challenging task to maintain the sensitive information integrity in an ensured way. The implementation of cryptographic algorithms in IoT provides lightweight solutions which are simpler in design. Trivium stream cipher is a cited example for IoT cryptographic lightweight initiative which is also a noted finalist of the eSTREAM project. The previous studies show that the cryptographic algorithms are regarded as vulnerable sources when it comes to hardware implementations. A simplified approach was proposed to study the vulnerability behavior field-programmable gate array (FPGA) implementations of Trivium stream ciphers against various attacks. A description of the system design alterations in the clock signal has provided. The Trivium cipher and their routing dependences are thoroughly tested with two different FPGA families to know the vulnerability and, the results show that all cases of Trivium cipher are vulnerable to fault attacks.**

***Index Terms*— Information security, FPGA, Vulnerability, Trivium cipher, IoT, Differential Power Analysis, Logic gates.**

I. INTRODUCTION

The amount of information transmitted and exchanged between the digital devices in this information era has increased drastically. The development happened in VLSI circuits in the past three decades reduce the device cost substantially and makes them more user-friendly and cost-effective [1]. The information that is exchanging in the communication networks needs the high-profile security system to protect the sensitive information from malicious sources. The cryptographic systems are designed to provide robust security to the information that is exchanging between various network channels. The progress on this subject keeps on improving with the development of the new technologies.. The primary parameters that are affected due to the second side of attack on-device hardware are power consumption, electromagnetic radiation and so on [2].

Grenze ID: 01.GIJET.4.3.36

Differential Power Analysis (DPA) and the Correlation Power Analysis (CPA) are the types of side-channel attacks are known for their ability to attack the system circuitry based on the power consumption measurements. On the other hand, the Active Fault Analysis attacks can actively attack the system circuitry through the operation conditions modifications to inject or insert the faults into the system circuitry.The proposed methodology presents an aspectual behavior and analysis of Trivium Cipher and its FPGA (Field-programmable gate array) executions in contrary to the error (fault) injections occurs in the clock signal.

II. BACKGROUND

A. FPGA

The FPGA is Field Programmable Gate Array. It is typically an integrated circuit with logic gates ranging from 10,000 to more than a million. They are called as semiconductor devices connected by programmable interconnections to accomplish the functions easily for the designers and the users. FPGA devices process reprogrammable ability even after manufacturing to desired application requirements and, this unique ability separates it from a matrix of configurable logic blocks (CLBs) [3].

III. EXISTING WORKS

Although the Trivium cipher gains the popularity of being a finalist in the project eSTREAM on the other end it failures in **many** aspects remain a concerned thing. Many works reported in the past have given the detailed explanation about the strangeness of the Trivium against DFA. In the initial stage, the majority of the papers focus on the theoretical analysis and the endangered security of the Trivium is the solo concern addressed in all works. Injecting a faulty bit in the internal state of the system by an unauthenticated source keeps the security of the system on the verge [3-5].The random fault injections in the hardware implementations by an unauthenticated source can create a tendency to break the cryptographic circuits security within a lapse of the timeline as reported by Boneh et al. [8]. Anderson and Kuhn [9] have come up with the unique concept of fault injection analysis.

Author, Contribution and the Methodology
Authors: R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. **Year:** December, 2015 **Contribution:** Challenges and the current status of the IoT networks in providing the security to the information exchanged in the online sources. **Methodology:** Internet of things has made its mark in the field of security and, it is also called trending technology in the information era. IoT offers an ocean of the opportunities to built new applications by providing the possible solutions. This paper highlights the point that a vast amount of work needs to be done to make IoT more user friendly [4].
Authors: M. Hojsík and B. Rudolf **Year:** December, 2008 **Contribution:** Analysis of the Trivium in terms of software implementation. **Methodology:** The Trivium design has come up with three different shift registers. The fast software implementation results in unresolved issues which may give scope to the unauthenticated sources to drive into the system and create the faulty bits which can affect the overall system performance [7].
Authors: F. E. Potestad-Ordóñez, C. J. Jiménez-Fernández, and M. Valencia-Barrero **Year:** November, 2016 **Contribution:** This existing work adds the significant contribution to the analysis of implementations of the FPGA against various tedious attacks. The experimental results of this paper show the sensitivity of the clock signals in the FPGA Trivium. Controlling the timing is yet another feature of this work. **Methodology:** The detection of the aspectual bits which makes the system sensitive to the various attacks is the prime motto of this work. Authors have taken the time parameter for detecting them, but this parameter is not useful. A study was done on different faulty frequencies and, it carried on till the system can find the optimum frequency. The optimum frequency, by which possible number of frequencies (faulty) can easily penetrate into the system which eventually impacts the system performance [9].
Authors: Dan Boneh, Richard A. DeMillo **Year:** 1997 **Contribution:** In the year 1997 Dan Boneh and his associates came up with a unique methodology which helps the future experiments. Every work discusses the attacks and its impact on the system performance, but this is the first work which mainly focuses on the attacks and its classification. Every VLSI and FPGA experiment must pass through two environments, one is software which deals with the design and system work and another one is the hardware where the chip design came out in physical shape. **Methodology:** The Chinese remainder theorem and its RSA based implementations have the significant place in the field of FPGA. The erroneous signatures are the new mechanism which can have the ability to breaking the RSA based implementation. The sensitivities of the FPGA integrated circuits have analyzed in this work by using Fiat-Shamir and Schnorr protocols. The Fiat-Shamir protocol is

needed less erroneous signatures compared to Schnorr protocol. But these identifier protocols are useful in finding the hardware faults. [8].

IV. Proposed Methodology

A. Contribution

The proposed methodology contribution over the existing methodologies is discussed in this section. The Trivium based FPGA implementations have gained attention due to its unique potentialities. In the year 2016 [5], a paper was published on standard Trivium and, the detailed experimental analysis has been carried out using the standard Trivium stream cipher implemented in a Spartan III Xilinx FPGA has shown the preliminary results. In the preliminary results, the fault detection has been detected by the fault injection in the variations of the clock signals. In the same year [6], another paper was published to show the time delays and valid comparisons between the static and post route approaches.

B. Aim and overview

The fault attacks are the most concerning aspect in the Trivium based FPGA implementations. The aim is to study the vulnerability behavior of the various Trivium designs to fault attacks. Applying the fault injection system to the different Trivium designs helps to detect the faulty bits in the both real and simulation experiments. The experiment to detect the faulty bits from fault injection system follows the systematic approach. The whole experiment has done on the standard Trivium with four different Trivium designs to the two different FPGA families for the implementation.. The final values are obtained by having a valid comparison of the real results with the simulation results.

C. Trivium Stream Cipher

The stream project is one of the significant works ever done in the history of the FPGA and, the main motto of the project is to design a system which has the best security system.. It is known for generating the 80 bits secret key along with 80 bits initialization vector (IV). This secret key along initialization vector (IV) is used to generate the ^{264} bits of key stream.. When an algorithm is initialized in the Trivium, it makes use of three shift registers along with one secret key. But the system needs to cycle 1152 clocks in order to generate a valid secret stream which eventually helps to generate the key stream. The inner state has a dense distribution of 288 bits in three different shift registers and, each of the shift registers has its own length to its contrary. The first shift register distributed with 93 bits, in the later shift register a total of 93 bits are distributed and, in the final shift register, a total of 111 bits are distributed uniformly. The combinational logic circuitry use XOR and the AND operations to generate the feedback in the shift registers. The depicted figure 1 shows the Trivium schematic representation.

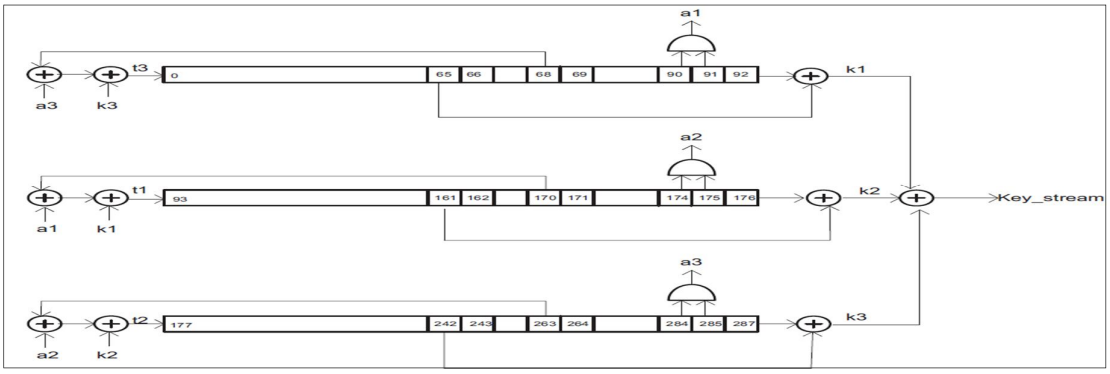

Figure 1: Schematic representation of Trivium stream cipher

The fault injection side channel attacks are thoroughly analyzed and studied for the Trivium cipher. Hojs´ık and Rudolf have proposed the initial work on this subject. In this method a method is known as differential fault analysis (DFA) is used in the encryption of the decryption process. The authors are succusesful inserting the fault bits into the inner state of the system. This approach shows that the attacker gets the tendency to change the only one bit of the inner state of the system.. Although the initial works primly focus on the fault

injection, the latter works mainly focus on generating the secret key based on the fault injection bits. The number of fault injections is kept on reducing with the development of the new algorithms.

D. Standard Multi-Radix Trivium Hardware Implementation

The FPGA integrated circuitry helps to design various applications for different fields. The internal (software) as well as external (hardware) security remains as a topic of research from over the years. The proposed approach has Trivium which is a stream cipher and, it can have the tendency to generate the 264 bits pseudorandom key stream. From these 264 bits, an 80-bit secret key along with 80-bit initialization vector created and it is initially proposed by two innovative scholars namely De Canniere and Praneel. A cyclic shift register has taken to account for internal state registers, and this cyclic shift register is 288-bit Cipher architecture. The same internal state of the Trivium cipher generated these radices and based on the requirement some bits of these radices move to the right as shown in the schematic representation of the cipher.

E. Important Considerations

Three important considerations

a) The FPGA integrated circuitry with Trivium is an excellent combinational design with internal logic. The frequencies the above the design threshold value filtered by the FPGA. These frequencies are not useful.
b) The selection of the frequency has been a challenging as the frequencies just below the designed threshold must be chosen for the system control. The fault bits insertion in the Trivium is possible by the above frequencies.

F. System Design

The main motto of the proposed algorithm is to introduce the faults in the system Cipher Trivium. The proposed system has the ability for remembering the number and location. The proposed circuitry has possessed the ability to adjust the clock signal and this ability help to control the clock signal even at the low pulses. The proposed algorithm can alter the clock signals in a defined fashion as shown in Figure 1
Although the proposed methodology can modify the short pulses of the clock signals, no algorithm can able to explain the impact of these short pulses on the inner state of the system and its perceptual performance. In the simulation results, this scenario happened vividly. In order to overcome this issue, this short pluses impact is altered in the internal state where the number of samples is sampled for operations.

V. Results and Analysis

In this experiment, The experimental analysis carried out by initializing the VHDL (VHSIC Hardware Description Language) as an apt platform to design the fault bit detection mechanism for both clock signal generation and as well as to the Trivium ciphers. Pro Analyzer. The below graphs depicts a comparison between the simulation and the experimental results.

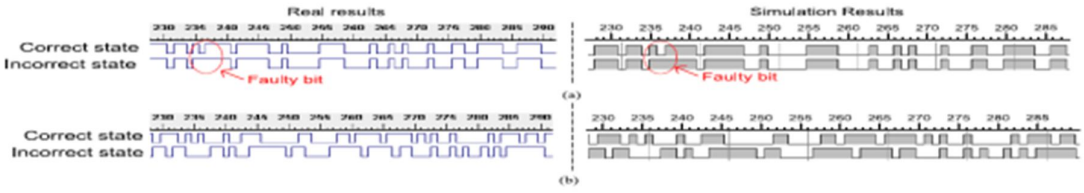

Figure 2: Comparison of experimental and from simulation between correct and faulty internal states

Table 1: Injection capacity and efficiency for Spartan family

	Spartan 3E		Spartan 6	
Trivium	Injection capacity	Injection Efficiency	Injection capacity	Injection Efficiency
Standard	59%	91%	38.44%	100%
S.I.C.	63.75%	68%	42%	92.55%
S.E.C.	56.44%	74.97%	58.66%	80.88%

TABLE II. L.P. TRIVIUM SYSTEM EFFICIENCY

FPGA	Injection capacity	Injection Efficiency
Spartan 3E	37.28%	56.33%
Spartan 6	20.99%	52.66%

V. CONCLUSION

This paper presents the optimized experimental results with elemental analysis. The three perspectives of the proposed methodology are: (a) Performing the fault injection on the proposed Trivium stream ciphers, (b) Implementation of the previous step is possible, once it embeds on the FPGA integrated circuit, and (c) performing the real-time experiments and compare it with the simulation results. The injections carried out in the Trivium ciphers are reckon on the implementation of each stream cipher at clock signal insertion. Finally, the proposed methodology shows that the system has an overall efficiency of 59% and it has the ability of 54% to introduce the faults in the inner states.

REFERENCES

[1] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in Proc. Int. Conf. Internet Technol. Secur. Trans. (ICITST), Dec. 2015, pp. 336–341.

[2] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in Proc. Int. Conf. Comput.-Aided Design (ICCAD), 2014, pp. 417–423.

[3] M. Hojsík and B. Rudolf, "Differential fault analysis of Trivium," in Fast Software Encryption—FSE. Berlin, Germany: Springer-Verlag, 2008, pp. 158–172.

[4] M. Hojsík and B. Rudolf, "Floating fault analysis of Trivium," in Proc. Int. Conf. Cryptol. India (INDOCRYPT), 2008, pp. 239–250.

[5] F. E. Potestad-Ordóñez, C. J. Jiménez-Fernández, and M. Valencia-Barrero, "Fault attack on FPGA implementations of Trivium stream cipher," in Proc. Int. Symp. Circuits Syst. (ISCAS), May 2016, pp. 562–565.

[6] F. E. Potestad-Ordóñez, C. J. Jiménez-Fernández, and M. Valencia-Barrero, "Experimental and timing analysis comparison of FPGA Trivium implementations and their vulnerability to clock fault injection," in Proc. Conf. Design Circuits Integr. Syst. (DCIS), Nov. 2016, pp. 1–6.

[7] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer-Verlag, 1997, pp. 513–525.

[8] J. J. Hoch and A. Shamir, "Fault analysis of stream ciphers," in Cryptographic Hardware and Embedded Systems—CHES. Berlin, Germany: Springer-Verlag, 2004, pp. 240–253.

[9] C. Giraud, "DFA on AES," in Advanced Encryption Standard—AES (Lecture Notes in Computer Science), vol. 3373. Berlin, Germany: Springer-Verilog, 2005, pp. 27–41.

CH.SURESH Received the Bachelor degree in Electronics and Communication Engineering (ECE) from the JNTU Hyderabad India and Master degree in VLSI from JNTU Hyderabad, India in 2012.He is working as Assistant Professor in ECE Dept at Methodist College of Engineering and Technology, India His main interests are in the fields of Very Large Scale Integration and Image Processing.

M.MAHESH BABU Received the Bachelor degree in Electronics and Communication Engineering (ECE) from Osmania University, India and Master degree in Digital Systems & Computer Electronics from JNTU hyderabad, India.He is working as Assistant Professor in ECE Dept at Methodist College of Engineering and Technology, India His major interests are in the fields of Very Large Scale Integration and Embedded systems.