ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Compact and High Speed Hardware Implementation of CLEFIA

Pankaj V. Jadhav[1], Vishnu Suryawanshi[2]

P.G. Student, Department of E&TC Engineering, GHRIET, Pune, Maharashtra, India[1]

Asst. Professor, Department of E&TC Engineering, GHRIET, Pune, Maharashtra, India[2]

ABSTRACT: We know that communication is the most important parameter in everyone's life. Generally, in the process of communication, there is one transmitter/sender and one receiver. For the purpose of security different methods have been developed by many authors. Cryptography is one of them. Basically, it is used to achieve the security in communication process. There are many methods in cryptography. Like, Advanced Encryption Standard, Clefia, RSA, DSA.Clefia is one method used in Cryptography which was developed by Sony Corporation in 2007. It is based on block cipher methodology instead of stream cipher. Different key lengths are used in Clefia like, 128 bit, 192 bit and 256 bit. This paper presents the implementation of small sized and High Speeded Hardware of Clefia.

KEYWORDS: Cryptography, Encryption, Block cipher, Clefia, Xilinx, FPGA.

I. Introduction

Communication Is Exchange Of Our Thought, Message, Information With Other People. It Can Be Through Speeches, Some Written Things, Some Signals Or Through Our Behaviors. For The Success Of Communication There Is Requirement Of Transmitter, Information And Receiver. It's Not Mandatory That The Receiver Should Be Available At The Senders End. Also, It's Not Mandatory That The Receiver Should Have Knowledge About The Information That The Sender Wants To Share.

Mobile Communication Is The Rapidly Increasing Part Of Communication. There Is Huge Growth In The Last Few Years And There Is More Than 2 Billion Users Of Mobile Communication In World. The Mobile Communication Network Is Replaced The Wired Communication Network In Almost All Fields.

II. Literature Review

In [1], the author describes compact hardware implementations of CLEFIA. He presented total three types of hardware architectures. In his implementation, the area requirements are only 2,488 GE and that are about half of the previous smallest implementation up to that point.

In [2], author did present two compact hardware structures for the computation of the CLEFIA encryption algorithm. One structure was based on the existing state of the art and a novel structure. The author achieved the throughputs above 1Gbit/s with a resource usage as low as 86 LUTs and 3 BRAMs. The LUT reduction was up to 67%.

In [3], the author introduces well-performance hardware architectures for the 128-bit CLEFIA. He evaluated their ASIC with comparing other algorithms. The author designed five types of different hardware architectures for CLEFIA, The highest hardware efficiency obtained. And it was 400.96 Kbps/gates.

In [4], the author presents a pipeline implementation of the CLEFIA. The article describes methods of developing a single encryption round. The article explains the implementation of a key scheduler. The article contains a detailed analysis of the data.

In [5], the author proposes a new 128-bit CLEFIA which supports 128, 192 and 256 bits of key lengths. He proves that CLEFIA gets a high performance both in hardware as well as software.

In [6], the main purpose is to study the basic terms used in cryptography, its aim and to compare the encryption techniques used in cryptography.

In [7], author proposes 2 kinds of developments in cryptography. They suggest ways to overcome open problems at that time. They also discussed that how the theories of communication and computation to solve old cryptographic problems.

In [8], the author proposes solution that support for multi-algorithm.

In [9], the author presents Cryptography and its Bifurcation.

In [10], the author proposes a differential fault analysis on CLEFIA. The proposed attack uses two pairs of fault-free and faulty cipher texts. It finds the secret key of 128 bit.

In [11], the author proposes a lightweight block cipher which is known as L Block. L Block can achieve good security against attacks, like differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis and related-key attacks. Also, L Block can be developed in hardware environments but also in software platforms.

In [12], the author says about meet-in-the-middle (MITM) attacks on block ciphers. They extend the MITM attack which can be applied to a wider class of block ciphers.

In 13], the author describes impossible differential cryptanalysis on the 128-bit block cipher CLEFIA. The author said that, for a 128-bit key, it is possible to apply the impossible differential attack to CLEFIA and decrease rounds to 12. Similarly, for 192 bits key lengths and 256 bits key lengths, it is possible to apply impossible differential attacks to 13-round and 14- round CLEFIA structure.

In [14], the author expresses generic complexity analysis formulas for mounting different attacks in cryptography. He develops new ideas for optimizing impossible differential cryptanalysis.

In [15], the author describes many common things related to cryptography.

In [16], the author says that CLEFIA is an efficient lightweight cipher and it gives advanced protection and authentication in computer networks.

In [17], the author explains that Efficient implementation of block ciphers is critical to get high security and high-speed.

III. Basics Of Cryptography

Cryptography mainly deals with the study of authentication, confidentiality and integrity.

Confidentiality

It is the process which protects the data from leaking to unauthorized users [15].

Authenticity

It is the process which provides assurance regarding the identity of a communicating party.

Integrity

It is the process which protects data against being modified (or at least enables modifications to be detected).

Plaintext

It is an original message not formatted text that a sender wishes to communicate with the receiver. The authentic message that has to be sent to the receiver's end in cryptography is given a unique name called plaintext [15].

cipher text

It is a text that comes as a result of encryption performed on plaintext using an algorithm called cipher. This message is a meaningless text and cannot be understood by anyone. Cipher text is also known as encrypted or encoded text as it is a non-readable form of the original text. It cannot be read by human and computer without decryption of cipher text [15].

Encryption

Encryption is a process of coding information into a form that is unreadable without a decoding key.Encryption requires two things i.e. key and encryption algorithm. It prevents our data and allows only the receiver to read the data with the help of the key.This is a process in which a plaintext is converted to a cipher text. It takes places at the sender's side.Cryptography uses encryption techniques to send confidential messages [15].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Decryption

Decryption is the exactly reverse process of encryption. It is a process of converting a cipher text back into a plaintext that the user can read.This also requires two things a key and decryption algorithm. This happens at the receiver's end so that he is able to read the original message from the encrypted message [15].

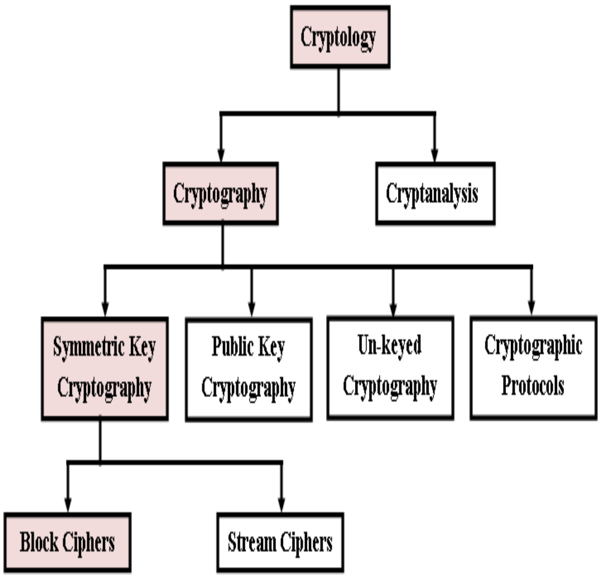

Fig. 1. Types of Cryptology

Key

A key is a value that is used to encrypt or decrypt a message. It is a numeric or alpha numeric text or may be special symbols also. In cryptography the selection of key is important as security depends on it [6].

Types of keys

a) Public key
b) Private key

Symmetric algorithm

Symmetric algorithm is one in which the encryption and decryption key are the same. It can also be a key that is easily calculated from the other. Before sending or communicating with each other the sender and the receiver must agree to the key.

Asymmetric algorithm

An asymmetric algorithm is an algorithm in which the key used in encryption is different from that of the key used decryption.

Public key cryptography

Public key cryptography is a technique in which the key used for encryption is made public but only the person who holds the corresponding private key can decrypt the message that is been encrypted and send to him.

Private key cryptography

Private keys are normally known only to the owner. Messages can be encrypted using public key and decrypted using private key.

IV. Previous Work Of Clefia

As short mentioned in literature survey, many authors have done different kinds of work on the Clefia algorithm.

A) One author has been implemented high speed Clefia. For that he implemented total three architectures.

Architecture 1:
At the start of encryption, a 128-bit original data is located to *Rij*in 16 clock cycles by giving input byte by byte from data. 144 cycles are required for total 18 rounds of the encryption, then a 128-bit cipher text is obtained. Therefore, it requires total 176 cycles for encryption. Word rotation is not necessary at the final round of encryption.For key setup, it takes 128 cycles. There are two S-boxes *S*0 and *S*1 are present in the data processing block, and one of those outputs is selected by a 2-to-1 MUX and input to the matrix multiplier.

Architecture 2:
In this architecture his main aim was the area optimization of the key scheduling block. *Double Swap*function Σ is decomposed as $\Sigma = \psi \circ \Omega$. During the encryption processing the intermediate key *L* is updated by Σ operation at the 17th cycle.At the 17th cycle, the data registers must hold the current data by clock gating.Accordingly, both 8 additional cycles for the encryption processing and 8additional cycles to recover the intermediate key *L* after outputting a cipher textare required, which results in 192 cycles for encryption. In compensation for theincrease of 16 cycle counts, a 128-bit input of MUX in the key scheduling blockcan be removed.

Architecture 3:
In Type-III architecture, by applying clock gating effectively author achieved the area optimization of the data processing block. Without using MUXes, the data stored in *R*10-*R*13 and those stored in *R*20-*R*23 are swapped by cyclically shifting these registers in 4 clock cycles, while the other data register and the key registers hold the current state by clock gating. Simultaneously, the XOR operation with a 32-bit chunk *Ki* is done by XOR gates in the matrix multiplier. It gives savings of 8 XOR gates.

B) Another author has been presented two compact hardware structures for the computation of the CLEFIA encryption algorithm.

Architecture 1:
The CLEFIA algorithm computation is divided into the Key Scheduling computation and the ciphering computation. Faster implementation of CLEFIA can be achieved by using T-boxes. The S-box operations are merged with the linear transformation layers, compressing the resulting structure into a lookup table, also resulting on a reduction of the critical path. In the CLEFIAs F-Functions operation, T-Boxes can be used to replace S0, S1, M0 and M1, by the lookup operations.

T00 = (S0, 02×S0, 04×S0, 06×S0)
T01 = (02×S1, S1, 06×S1, 04×S1)
T02 = (04×S0, 06×S0, S0, 02×S0)
T03 = (06×S1, 04×S1, 02×S1,S1)
T10 = (S1, 08×S1, 02×S1, 0A×S1)
T11 = (08×S0, S0, 0A×S0, 02×S0)
T12 = (02×S1, 0A×S1, S1, 08×S1)
T13 = (0A×S0, 02×S0, 08×S0, S0)

DOI: 10.15680/IJIRCCE.2018.0605122

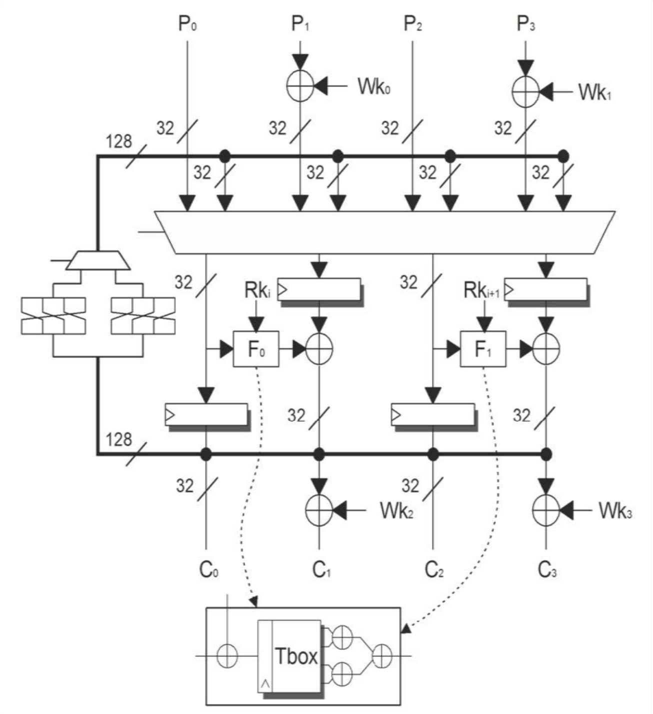

Fig. 2. Architecture 1

The block diagram of architecture 1 is shown in above figure.

Architecture 2:

With this method, approximately half of the hardware resources are required, apart from the additional selection logic. Consequently the computation of each round will require two clock cycles, which is double as much as in the architecture 1. A pipeline stage can be added to Type-II CLEFIA structure dividing the computation into two stages. In the first stage, one F-Function is computed by the T-Box structures. In the second stage, the remaining part that is data and Round Key additions are performed. For the purposed of optimizing the data path to the used FPGA technology, the pipeline stage register can be placed in different parts of the data path.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

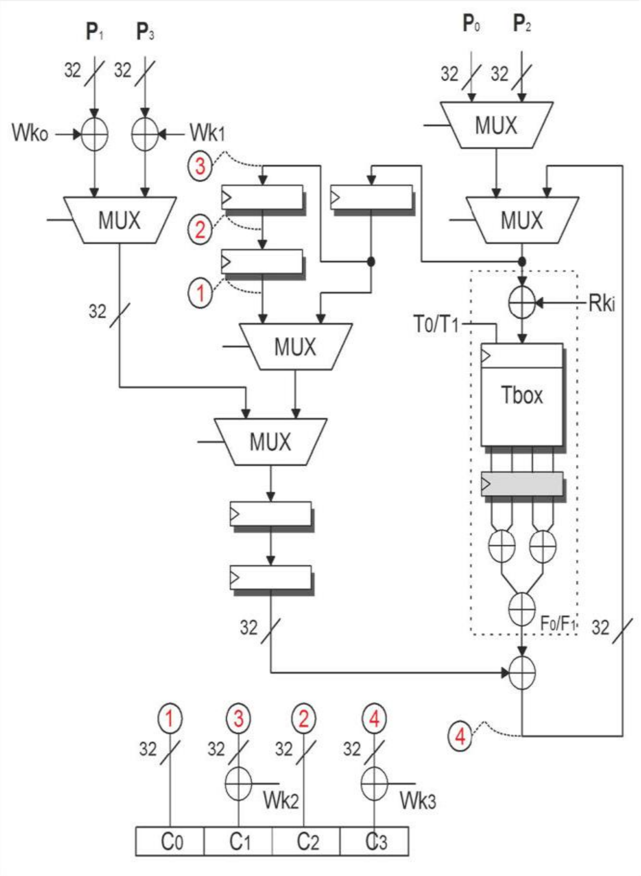

Fig. 3. Architecture 2

The block diagram of architecture 2 is shown in above figure.

C) Again another author proposed two architectures.

The Type- A architecture executes one round operation in only one clock cycle. The Type-B architecture performs one round operation in two clock cycles. Type-A architectures require 18 clock cycles and Type-B architectures require 36 clock cycles. In both architectures, he implemented two types of S-boxes, the lookup table and composite field versions. In addition to this, the T-box also applied to the Type-A architecture. In the Type-B architecture, he designed an *F*0/*F*1 component which is obtained by combining F-functions *F*0 and *F*1. For that he shared the S-boxes and the constant matrices *M*0 and *M*1. Apart from these, the circuit area is reduced by sharing XOR gates.

D) Another author has been presented a pipeline implementation of the block cipher CLEFIA. The article examines three known methods of implementing a single encryption round and proposes a new fourth method. The author described the implementation of a complete CLEFIA encryption module. Also, he analysed that the method of building a single encryption round, particularly substitution boxes (S-Boxes). Also, a new version of the F-function structure mixed is proposed. It combines the advantages of the S-Box implementation based on two different kinds of ways. Those are based on definition and the implementation using look-up table.

V. Proposed Work

In the proposed system, there would be two major functionalities. One is Key Generation or Key Scheduling. And another is Data Processing. The VHDL code is to be written for key generation process. Also, the same kind of VHDL code is to be written for Data encryption process. Then these codes are to be processed on software called as Xilinx.

As shown in below block diagram the original message is known as plain text. The plain text is to be of 16 bytes that is 128 bits. This plain text is divided into total four groups. Each contains 32 bits of original data(32 bits x 4 = 128 bits). Depending upon the size of key there requires different number of rounds. For 128 bit plain text, there requires total 18 rounds. So the 128 plain text is to be processed through the 18 rounds. Also, the 128 bit cipher key is very essential. So, it is used. So, finally the cipher text is obtained from this process and it is implemented on FPGA board.

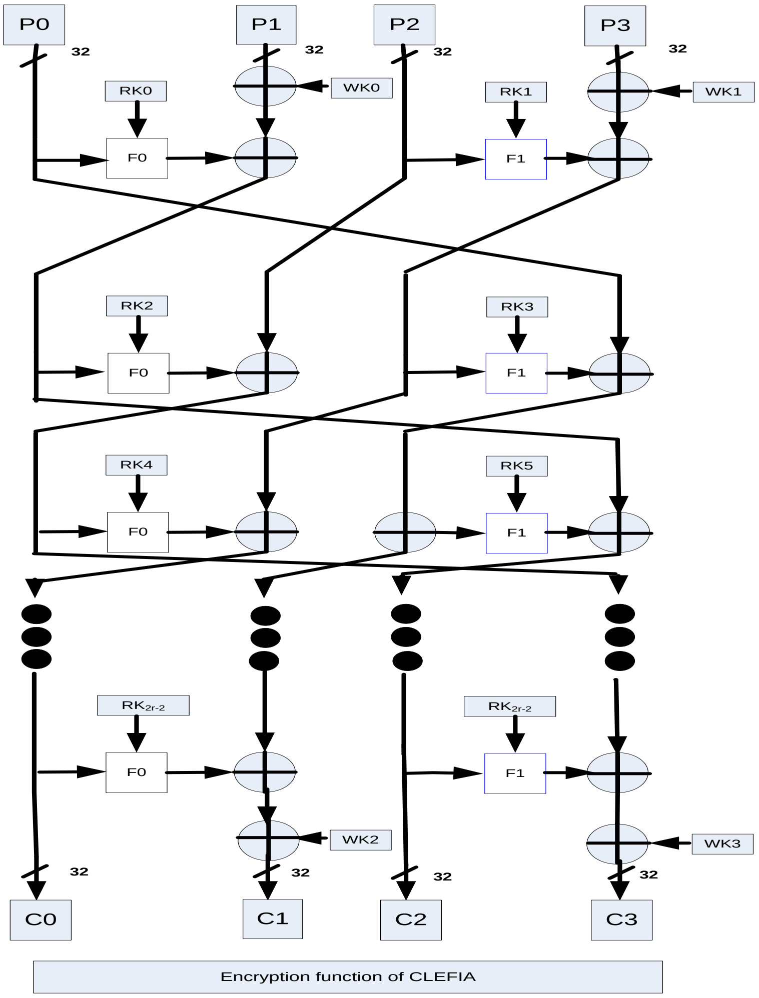

Fig. 4. Block diagram of Clefia algorithm

There are two functional blocks F0 and F1. Functional block F0 and F1 are shown in figure 5 and figure 6 respectively.

For the security purpose whitening keys are added before first round of implementation.

Only there is one difference between the F0 and F1 functions. The difference is the position of S- boxes. And the same kind of operation is done at both the functions.

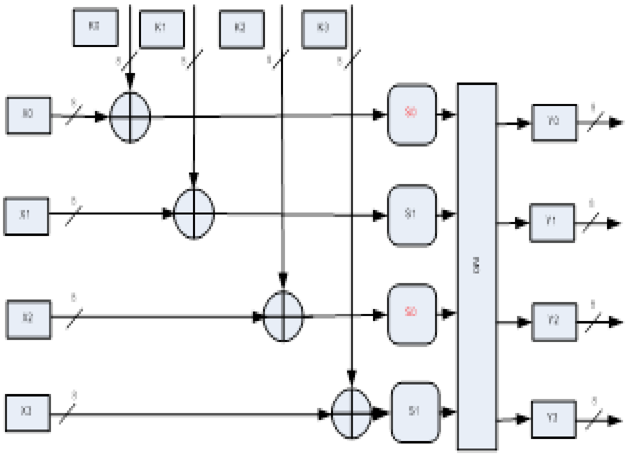

Fig. 5. F0 Function

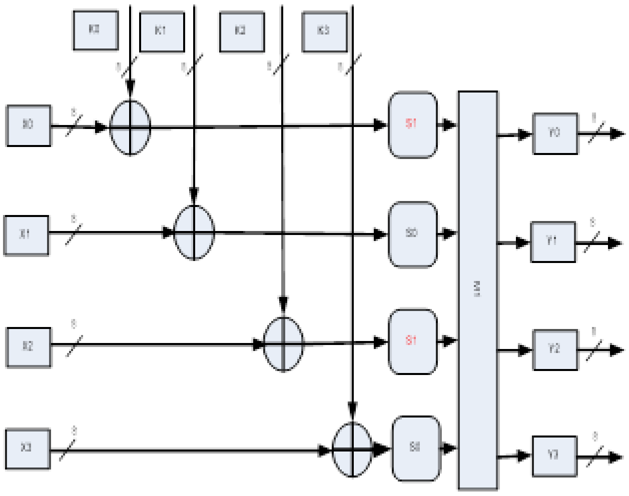

Fig. 6. F1 Function

VI. Conclusion and Future Work

The purpose of this proposed system is to implement a high speed and compact hardware structure of CLEFIA. In this paper a Clefia block cipher is presented.

References

[1] Toru Akishita and HarunagaHiwatari "Very Compact Hardware Implementations of the Block cipher CLEFIA ". *Sony Corporation*

[2] Paulo Proença and Ricardo Chaves "Compact CLEFIA Implementation On FPGAs*". 2011 21st International Conference on Field Programmable Logic and Applications.*

[3] Takeshi Sugawara, Naofumi Homma, Takafumi Aoki and Akashi Satoh.“ High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA ”.

[4] TomaszKryjak and MarekGorgoń.”Pipeline Implementation Of The 128-Bit Block Cipher CLEFIA In FPGA”. *978-1-4244-3892-1/09/$25.00 ©2009 IEEE.*

[5]TaizoShirai, KyojiShibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata.“ The 128-Bit Blockcipher CLEFIA (Extended Abstract) ”. *Sony Corporation.*

[6]K. B. PriyaIyer, R. Anusha and R. ShakthiPriya. “Comparative Study on Various Cryptographic Techniques”.*International Journal of Computer Applications(0975 – 8887) International Conference on Communication, Computing and Information Technology(ICCCMIT-2014).*

[7] WhitfieldDiffie and Martin E.Hellman “ New Directions in Cryptography ”. *IEEE Transaction on Information Theory, Vol. IT.22, No. 6, November 1970 .*

[8] NicolasSklavos, João Carlos Resende, Ricardo Chaves, Francesco Regazzoni, OsnatKeren “Efficiency of Cryptography for Multi-AlgorithmComputation on Dedicated Structures ”.

[9] RoozMunjal, PinkiTanwarandNitinGoel “ Optimized Solutions to Cryptography for Securing MANETs and Analyze Using Reputation System ”. *International Journal of Advanced Research in Computer Science and Software Engineering.*

[10]SkSubidh Ali and DebdeepMukhopadhyay “Protecting Last Four Rounds of CLEFIA is Not Enough Against Differential Fault Analysis ”.

[11]Wenling Wu and Lei Zhang “LBlock: A Lightweight Block Cipher ”.

[12] TakanoriIsobe and KyojiShibutani “All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach ”.

[13] YukiyasuTsunoo , Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki, and
Hiroyasu Kubo “Impossible Differential Cryptanalysis of CLEFIA “.

[14] Christina Boura, Maria Naya-Plasencia, ValentinSuder “Scrutinizing and Improving Impossible Di_erential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon ”.

[15] Masanobu Katagi and Shiho Moriai “Lightweight Cryptography for the Internet of Things ”.

[16] Wei Li, DawuGu, Xiaoling Xia, Ya Liu, Zhiqiang Liu “Fault Detection on the Software Implementation of CLEFIA Lightweight Cipher ”.

[17]AJ Elbirt and ChristofPaar “Efficient Implementation of Galois Field Fixed Field Constant Multiplication”.