IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 4, Ver. II (Jul.-Aug. 2017), PP 43-47
www.iosrjournals.org

Implementation of Two Light Weight Cryptographic Algorithms

*Athmika Aravind[1], Kiran Kumar V.G[1], Shantharama Rai C[2], Nisha[2]
[1](*Electronics & Communication Engineering, Sahyadri College of Engineering& Management, India)*
[1](*Associate Professor Electronics & Communication Engineering, Sahyadri College of Engineering & Management, India)*
[2](*Principal, AJ Institute of Engineering &Technology, Mangaluru, India)*
[2](*Assistant Professor Electronics & Communication Engineering, Sahyadri College of Engineering & Management, India)*
Corresponding Author: Athmika Aravind[1]

Abstract:*In recent years, one of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in the form they can read and understand. Hence, Cryptography is one of the important features in secure communication .It makes use of key to encrypt the data so that the data sent cannot be accessed by unauthorized users. This paper focuses on Lightweight symmetric cryptography. Lightweight cryptography is used for resource-limited devices such as radio frequency identification tags,smart card etc. American National Security Agency (NSA) proposed a new block cipher family named SIMON and the aim of SIMON design is to fill the gap for secure, flexible, and analyzable and to perform exceptionally well across the full spectrum of lightweight applications. International Data Encryption Algorithm (IDEA) is a block cipher aims at providing high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key. In this project comparative study of selected lightweight symmetric block ciphers such as IDEA and SIMON are implemented using Xilinx ISE 14.2 simulator.*

Keywords: *Cryptography, IDEA, Light Weight Cryptography, SIMON, Xilinx*

Date of Submission: 15-07-2017 Date of acceptance: 24-07-2017

I. Introduction

Cryptography is the actual application and study of obscure information. Cryptography, in a communication allows verifiability of every component. It is one of the science techniques of using mathematics to encrypt and decrypt data. Data that can be read and understood without any special measures is called plaintext. The method of concealing the plaintext in such a way as to hide its contents is called encryption. Cryptography algorithm works along with a key to encrypt the plaintext. The secret knowledge or information is key, even if it contains the entire process or algorithm that is used in encryption or decryption. Encrypting plaintext results in unreadable meaningless writing called cipher text. The process of changing cipher text to its original plaintext is called decryption. International Data Encryption algorithm (IDEA) is a block cipher algorithm designed by Xuejia Lai and James L. Massey of ETH-Zurich and was first described in 1991. The original algorithm went through few modifications and finally named as International Data Encryption Algorithm (IDEA). Here the IDEA algorithm works on 64-bit plain text and cipher text block (at one time). For encryption, the 64-bit plain text and key of 128-bit is used to produce a cipher text of 64-bit. In the cryptography, IDEA is one of the ciphers which encrypt the text into an unreadable format and makes it secured in order to send it over to internet. In 2013 NSA proposed a new family of highly optimized block cipher SIMON that has flexibility and superior performance both in hardware and software environments especially on hardware devices. The SIMON algorithm has a variety of data blocks and key sizes which can be used for different implementations, thus, the users can coordinate security requirements and specific applications with algorithm. To increase the flexibility, The NSA's experts have, designed SIMON block cipher family with several, different block and key sizes. SIMON algorithm works on 128-bit plaintext and 128-bit key. For encryption process, 128-bit plaintext along with key is used to produce the cipher text.This paper briefly describes the process of IDEA algorithm and SIMON algorithm on Xilinx 14.2.Goal of this project is to achieve high security.

II. Idea Algorithm

The IDEA is a symmetric, block oriented encryption algorithm, which operates on a 64-bit plaintext and uses a128 bit length key. The substitution boxes and the associated lookup tables used in the rest block ciphers available to-date have been completely dispensed with. The required confusion in this algorithm is achieved by successively using three different and in compatible group operations on pairs of 16-bit sub-blocks and mixing them while the structure of the cipher was carefully chosen to provide the necessary diffusion requirement. The three algebraic operations are the following:

- Bit-by bit XOR
- Addition of integers modulo (2^16+1) with inputs and outputs treated as unsigned 16-bit integers
- Multiplication of integers modulo (2^16+1) with inputs and outputs treated as unsigned 16-bit integers

All these operations operate on 16-bit sub-blocks. Their use in combination provides for a complex transformation of the input making cryptanalysis much more difficult than with an algorithm such as e.g. DES, which relies solely on the XOR function. IDEA uses a 128 bit key which is double the key size of DES. Thus, making it highly immune to attacks. IDEA uses algebraic operations completely and it entirely avoids the use of any lookup tables or S-boxes. The strength of IDEA lies in its modulo multiplication operations. The working of IDEA can be visualized as—the 64-bit plain text block is divided into 4 portions of plain text (each of size 16 bits), say P1 to P4. Thus, P1 to P4 are the inputs for the first round of the algorithm. There are 8 such rounds. In each round, 6 sub-keys (each of size 16 bits) are generated from the original 128 bit key. These sub-keys are applied to the 4 input blocks P1 to P4. Thus, for the 1st round there are 6 sub-keys K1 to K6. For the 2nd round, there are keys K7 to K12. Finally, we will have keys K43 to K48. The final step consists of an Output Transformation, which uses just 4 sub-keys. The final output produced is the output produced by the Output Transformation round.

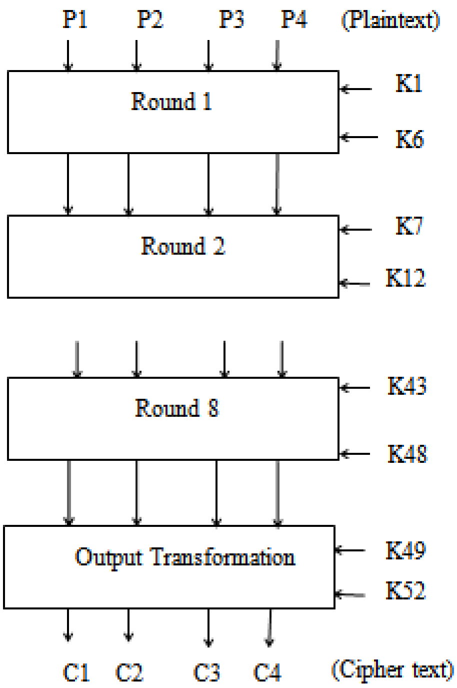

Fig.1 Architecture of IDEA

2.1Key Generation

The initial 6 sub-keys K1 to K6 are generated from the original 128 bit key. Since the sub -keys consist of 16 bits each, out of the original 128 bits, the first 96 bits are used for the first round. Thus, at the end of the first round, bits 97–128 of the original key are unused. In the second round, the unused 32 bits of the first round are used. To generate the rest of the sub -keys for the second round, 64 more bits are required. This is obtained by shifting the original key left circularly by 25 bits. Then, the modified key is now used to generate the rest of the 4 sub-keys in the same way as the first round keys were generated. The same is done for the sub-key generation for the rest of the rounds.

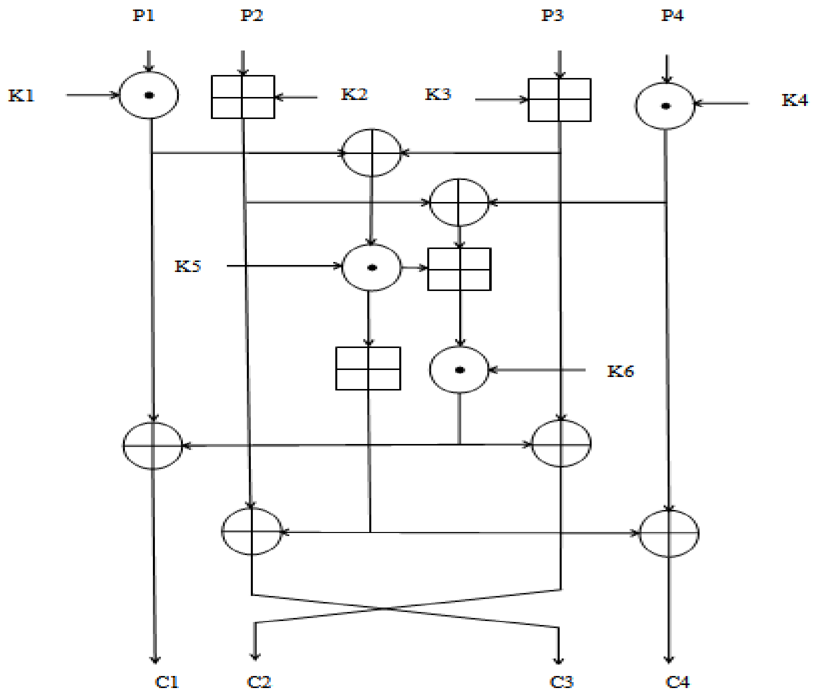

Fig.2 Round Function of IDEA

Idea encryption is simulated using Xilinx 14.2 using ISE simulator tool.

II.2 IDEA Simulation Results

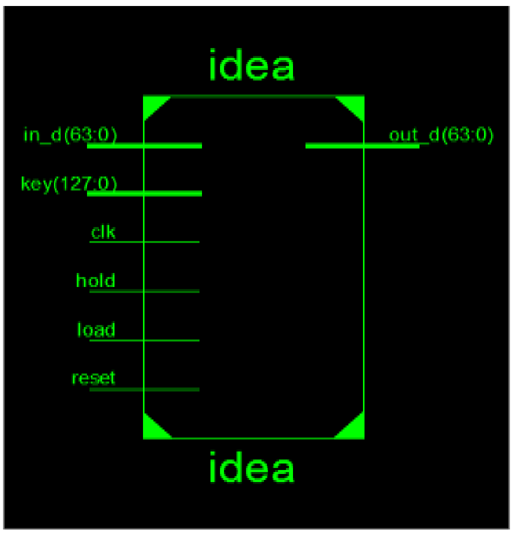

Fig.3 RTL Schematic

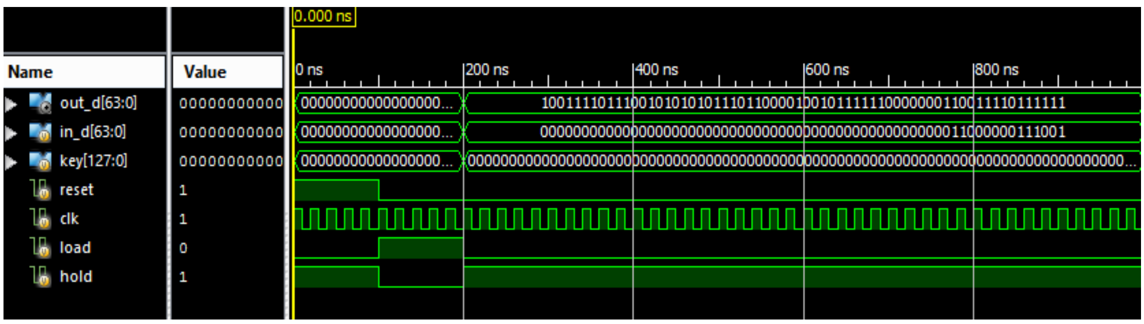

Fig.4 Simulation Result

III. Simon Algorithm

The architecture of SIMON block cipher consists of parallelism of encryptions which involves round functions and key generation blocks. For given 128 bit plain text and a 128 bit cipher key, SIMON block generates 128 bit cipher text in 68 rounds. The above block diagram describes the dimension of parallelism for the block ciphers. Depending on the parallelism choice at each dimension the hardware implementation can range from n-parallel encryptions per clock cycle to one-bit of one round encryption per clock cycle. Hence to minimize the cost, we used a bit-serialized architecture in which inputs of all operators are one bit. To implement SIMON in a bit-serialized method, we have to first bit-serialized the round function and key generation.

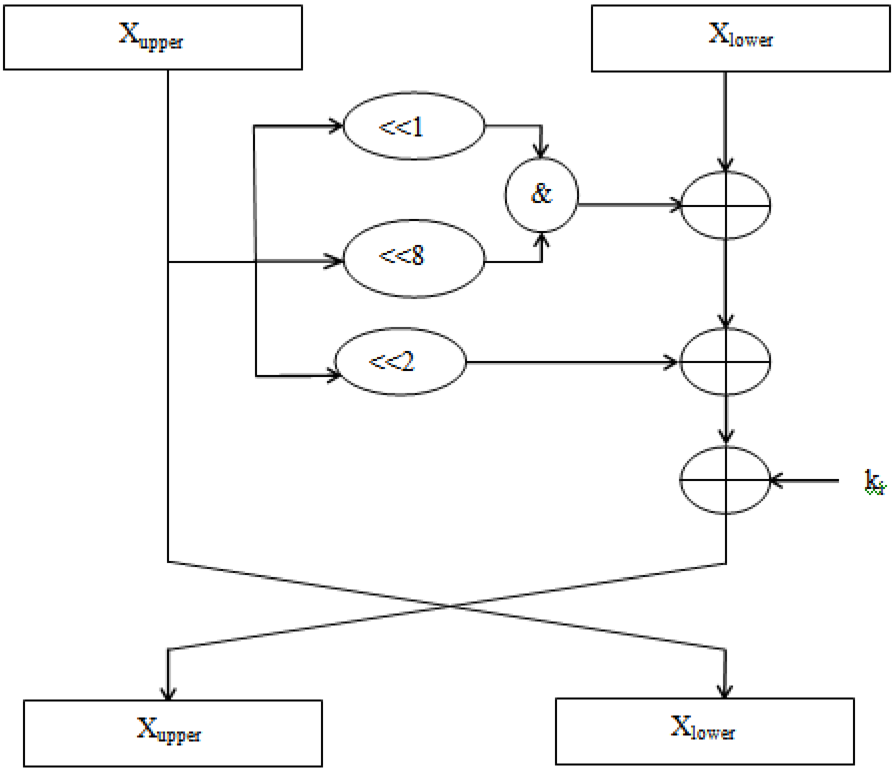

Fig.5 Round function of SIMON

This work focuses on the 128/128 configuration of SIMON with security level equivalent to AES-128. This configuration uses the inputs of 128-bit of plaintext and 128-bit key to generate 128-bit cipher text in 68 rounds [3].Fig.5 shows the round operation of SIMON. 128-bit data has been divided into two equal halves refers as upper block and lower block. The round function performs logic operations on the most significant 64-bits (the upper half block) and the result is XOR-ed with least significant 64-bits (the lower half block) and the 64-bit round key k_i. At the end of each round, the contents of the upper block is transferred to the lower block as the new generated values are written back into the upper block.

3.1 SIMON Simulation Results

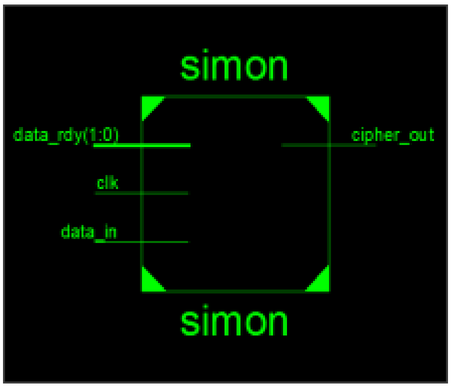

Fig.6 RTL Schematic

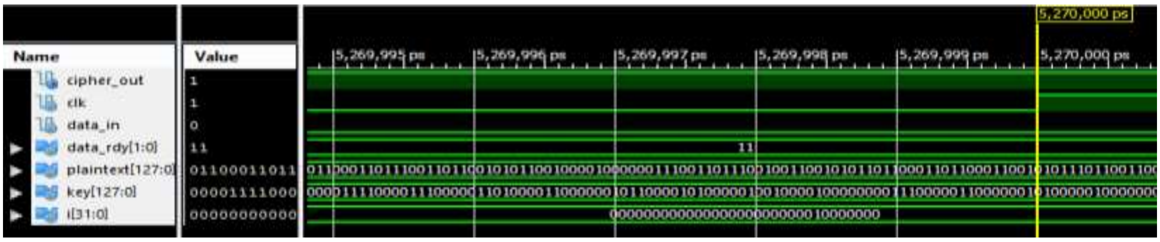

Fig.7 Simulation Result

IV. Performance Result Of The Two Algorithms

Algorithms are implemented using Xilinx 14.2 and their delay, power, area are computed using cadence tool.

Table.1 Results

Algorithms	Plain text	Key size	Rounds	Max Freq(MHz)	Time delay (ns)	LUT's	FF's	Power(W)
IDEA	64	128	8.5	69.845	8.763	357	288	0.003236
SIMON	128	128	68	114.116	14.317	92	30	0.000643

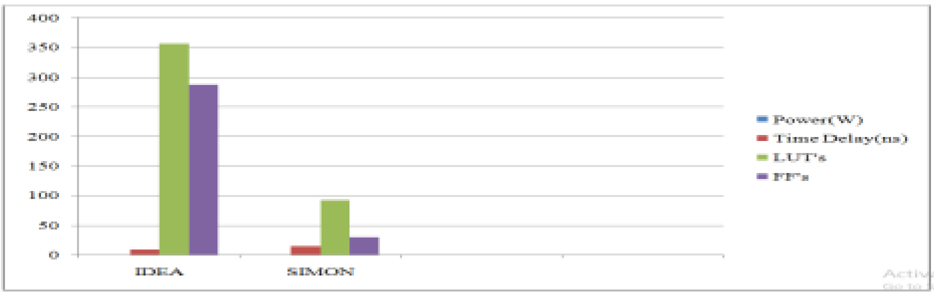

Fig.8 Comparison Graph

V. Conclusion

This paper proposes encryption of IDEA algorithm which has 128 bit key size and 64 bit block size and SIMON which has 128 bit data block and 128 bit key size. The encryptions are carried out writing programs in Verilog. From this implementation we can come to the conclusion that IDEA is indeed a strong block cipher compared to IDEA. When we compare the power SIMON is more efficient than IDEA.

References

[1] AdyinAysu,Ege, Ege Gulcan and Patrick Schaumont, "SIMONsays: Break Area Records of Block Ciphers on FPGAs", IEEE Embedded Systems Letters, Vol.6, No.2, June 2014.

[2] William Stallings fifth edition of "Cryptography and Network Security Principles and Practice".

[3] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel.A Survey of Lightweight-Cryptography Implementations.In IEEE Design & Test, Volume 24, Issue 6, pages 522–33, 2007. 21.

[4] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers, "The simon and speck of lightweight block ciphers," National Security Agency 9800 Savage Road, Fort Meade, MD 20755, USA, June 2013.

[5] Thaduri, M., Yoo, S.M. and Gaede, R., "An efficient implementation of IDEA encryption algorithm usingVHDL", 2004 Elsevier.

[6] Hamdy, Nabil, Shehata, Khaled, Elagooz, Salah and Helmy, Eng. Mohamed, "Design and Implementation of Fast Inverse Modulo (216+I) Multiplier Used in IDEA Algorithm Key Schedule on FPGA".

[7] Lai, X. and Massey, J., "A proposal for a new block encryption standard," Proceedings, Eurocrypt '90, 1990.

[8] Samir Palnitkar, Verilod HDL, A Guide to Digital Design and Synthesis, Second Edition.