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 20-25
www.iosrjournals.org

A Study and Comparison of Lightweight Cryptographic Algorithm

[*]Vignesh Ballal[1], Kiran Kumar V.G[2], MeghaN[3], Shanta Rama Rai[4]
[1](Electronics & Communication Engineering, Sahyadri College of Engineering& Management, India)
[2](Associate professorElectronics & Communication Engineering, Sahyadri College of Engineering& Management, india)
[3](Assistant professorElectronics & Communication Engineering, Sahyadri College of Engineering& managementindia)
[4](Principal, AJ institute of technology, Mangalore, india)
Corresponding Author: Vignesh Ballal

Abstract: *As internet is in enormous demand and it acts as a repository for the data and knowledge, there is unremitting demand for real time implementation of cryptographic algorithms so that one can secure its data over this decentralized network and help in preserving the security of the system. Blowfish is a symmetric key cryptographic algorithm. It is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Xtea is extended tiny encryption algorithm which encipher the 64 bit input plain text with the help of 128 bit secret key, key is generated by using LFSR . 64 round operations is performed, it works based on fiestel network. this paper comapres XTEA and blowfish algorithms , analysis in terms of the power, delay, area, throughput, implemented on FPGA and finally concludes best algorithm among them.*

Keywords: *cryptography, Xtea, Blowfish, LFSR, FPGA*

Date of Submission: 05-07-2017 Date of acceptance: 24-07-2017

I. Introduction

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to Store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by any-one except the intended recipientSecurity attacks are increasing since data is paramount, and the main task is securing the data that will keep on increasing simultaneously maintain the resource consumption and providing the approach that will lead to optimization since utilizing number of resources undoubtedly will be a costly affair. Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and stored data.In such small devices, the fight over high performance and low power consumption, besides security are primary targets. A great deal of assistance in creating low-power and high-speed cores, comes from the simplicity of the selected algorithm for embedding as a hardware component. Different Software implementations of cryptographic algorithms are available.in this paper a novel approach for comparing the extend tiny encryption algorithm and blowfish lightweight cryptographic algorithm. Comparison is in terms of power, area, delay and throughput. Implemented on FPGA board checking corresponding test bench waveform, finally concluding that best lightweight cryptographic algorithm among these two encipher algorithm

EXTENDED TINY ENCRYPTION ALGORITHM

X-tea is a light weight cryptographic algorithm, which is specifically known for its simplicity & small code size.Since it is known for its small code size that means it can be very beneficial in designing small applications, The Extended Tiny Encryption Algorithm (XTEA) is a block cipher that uses a cryptographic key of 128 bits to encrypt or decrypt data in blocks of 64 bits. Each input block is split into two halves Ln andRnwhich are then applied to a routine similar to a Feistel network for N rounds, where N is typically 32. Most Feistel networks apply the result of a mixing function to one half of the data using XOR as a reversible function. On the other hand,XTEA uses integer addition modulo 2^{32} during encryption and subtraction modulo 2^{32}during decryption.Operations used in XTEA are just exclusive-or, additions and shifts for encryption.
Block diagram Extend tiny encryption algorithm is as shown in below

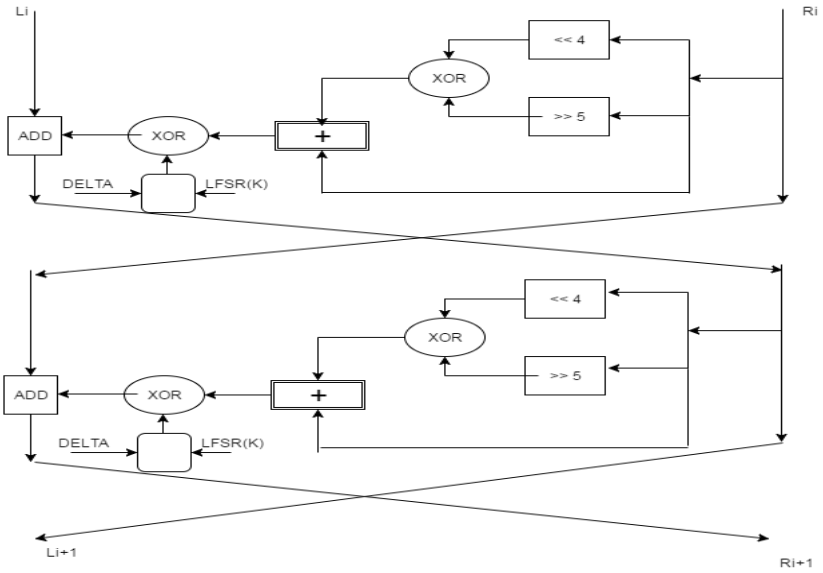

Fig.1 Block diagram of XTEA Algorithm

1.1 Methodology

- XTEA 64 bit input is divided into two 32 bits variables (Ln, Rn).
- Secret key which is 128 bit generated by Linear feedback shift register is divided into four 32 bit key, i.e. K1,K2,K3,K4
- Logical left shifts of Rn by 4 bits are denoted as Rn<< 4
- logical right shift by 5 bits as Rn>> 5.
- Bitwise XOR operation between shifted data.
- Modulo addition 2^{32} operation to maintain the the bit length.
- XORing LFSR and Delta function with shifted data.
- Perform this operation 64 round to encipher the Plain text

(Ln,Rn) are the inputsof the n-th round, for 1≤n≤64. The corresponding output of the n-th round is (Ln+1,Rn+1), where Ln+1 = Rn and Rn+1is computed using following equations:
For each i (1≤ i ≤32),
If n = 2i – 1

$$Rn{+}1{=}Ln \boxplus (((Rn \ll 4 \oplus Rn \gg 5) \boxplus Rn) \oplus ((i{-}1).\delta \boxplus (-1\ .\delta \gg 11)\&3)$$

And if n = 2i,

$$Rn{+}1{=}Ln \boxplus (((Rn \ll 4 \oplus Rn \gg 5) \boxplus Rn) \oplus (i.\delta \boxplus (i.\delta \gg 11)\&3)$$

II. BLOWFISH Lightweight Cryptographic Algorithm

Blowfish, a 64bit block cipher, is an excellent choice for encryption, since it is lightweight, public domain, and Highly secure even after extensive analysis. Blowfish algorithm works based on fiestel network. Fisetel network round has 16 round operation. key size is 32 bit size can be upto 448 bits. A graphical representation of the Blowfish algorithm appears in Figure 2. This structure is known as Fiestal network. Graphical representation of G appears in Figure 3 . The function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XORed together to produce the output. Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is cipher text

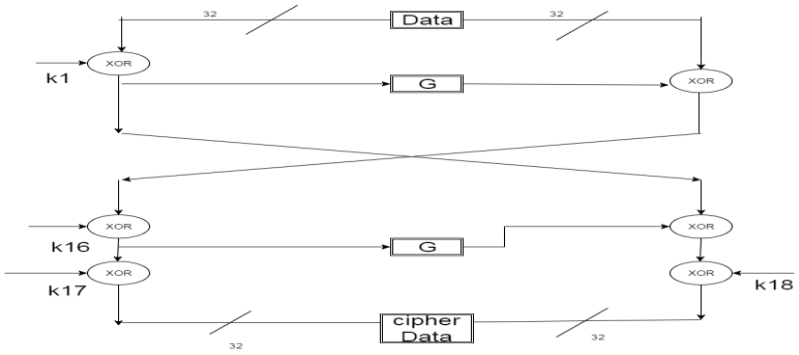

Figure 2: Block diagram of Blowfish

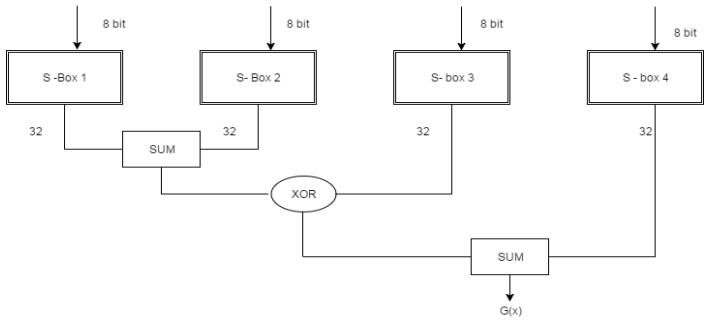

Figure 3: Function G

2.1 Methodology

2.1.1 Key generation

P is an array of eighteen 32-bit integers. S is a two-dimensional array of 32-bit integer of dimension 4x256. Both arrays are initialized with constants The P-array and S-array values used by Blowfish are pre computed based on the user's key the user's key is transformed into the P-array and S-array. This process is known as sub-key generation

1. Initialize first the P-array and then the four S boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi like the following example:
   P1 = 0x243f6a88
   P2 = 0x85a308d3
   P3 = 0x13198a2e
   P4 = 0x03707344
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key .Repeat the cycle through the key bits until the entire P-array has been XORed with key bits
3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process until the entire P valueshave been replaced.

2.1.2 Encryption

Blowfish is a Feistel network consisting of 16 rounds. The input is a 64-bit data element, x.

1. 1.For i = 1 to 16:
2. L = L XOR Ki
3. R = F(L) XOR R
4. Swap L and R
5. Swap L and R (Undo the last swap.)
6. R = R XOR K18
7. L = L XOR K17
8. Recombine L and R

III. Results And Comparisons

3.1 XTEA RTL Schematic

Fig.4 RTL Schematic

3.2XTEASimulation Results

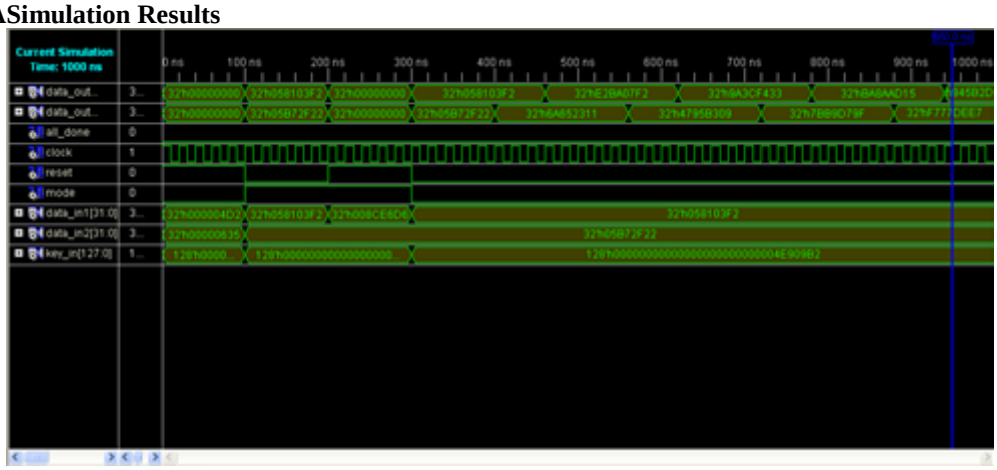

Fig.5 Simulation Result

3.3BLOWFISH RTL Schematic

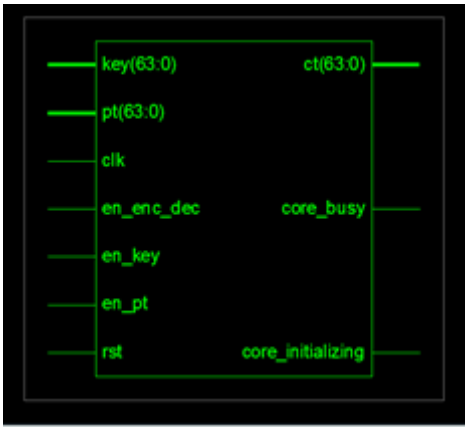

Fig 6: RTL Schematic

3.4 BLOWFISHSimulation Results

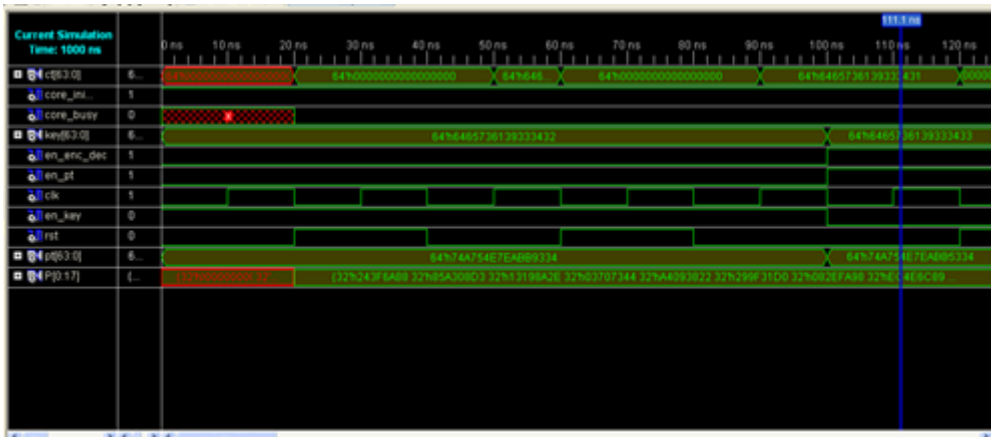

Figure 7: Simulation Results

3.5. Comparison

Extended Tiny encryption algorithm and blowfish algorithm is implemented by using XILINX CAD tools and below table is represent the comparison between the these two algorithm

Table.1 comparison table

Algorithm	Plain text(bits)	Key size(bits)	Gate	Clock period(ns)	No of LUT	Power(W)	Area(bit)
XTEA	64	128	85056	9.18	968	0.0002545	258965
BLOW FISH	64	64	183876	7.921	4477	0.0004983	372994

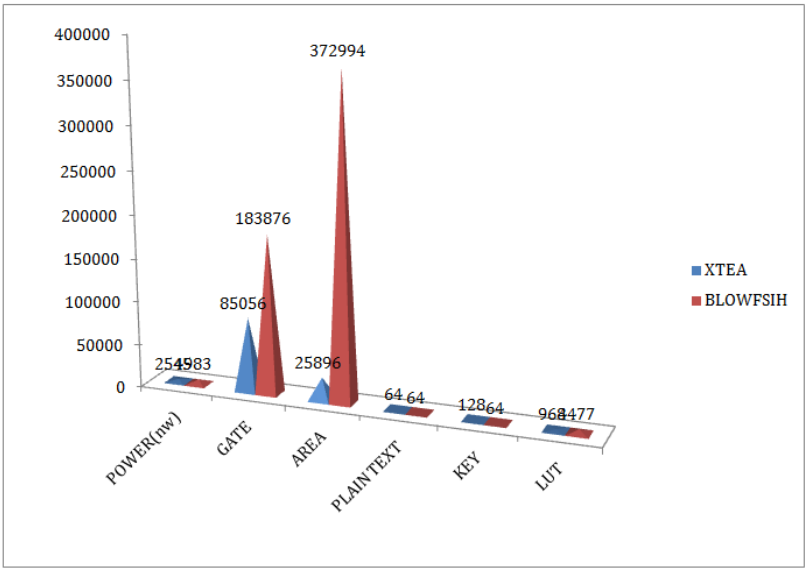

Figure 7: Graphical Representation

IV. Conclusion

Xtea and blowfish algorithm is successfully implemented by using Xinlix 10.1 software, area, power, delay are observed .by comparing these two algorithm Xea has less power consumption than blowfish, area of the blowfish larger than Xtea, gate delay of blowfish is larger than xtea. Hence Xtea is best and suitable algorithm among these two algorithm

Refernces

[1] Thomas Eisenbarth, Sandeep Kumar,ChristofPaar and Axel Poschmann and Leif Uhsadel " A Survey of Lightweight-Cryptography Implementations" IEEE Design & Test of Computers-November–December 2007.

[2] KiranKumar.V.G, SudeshJeevanMascarenhas, and Sanath Kumar published article "Design And Implementation Of Tiny Encryption Algorithm" et al. Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622,Vol. 5, Issue 6, (Part -2) June 2015, pp.94-97

[3] Rashikohili and manojkumar is presented article "FPGA Implementation of Cryptographic Algorithms using Multi-Encryption Technique" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013
[4] ManjuSuresh Neema M published an article "Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things", Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016)
[5] Niladree De, JaydebBhaumik presented article "A Modified XTEA" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012
[6] ImanZareiMoghadam, Ali ShokouhiRostami, Mohammad RasoulTanhatalab published article "Designing a random number generator with novel parallel LFSR substructure for key stream ciphers"

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

Vignesh Ballal. "A Study and Comparison of Lightweight Cryptographic Algorithm." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 12.4 (2017): 20-25.