IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 3, Ver. II (May - June 2017), PP 66-71
www.iosrjournals.org

Comparative Study of Cryptographic Encryption Algorithms

Chaitra B[1], Kiran Kumar V.G.[1], Shantharama Rai C[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)*

Abstract: *Protection of the network to enhance the safety of the information is great challenge in cryptography. With the developments in the cryptography lightweight cryptography has large space towards security by its simplicity in the implementations. For majority of applications PRESENT and TEA are excellent and preferred choices. However PRESENT is suitable for low constrained devices like RFID tags and sensor network. In this paper we describe ultra-lightweight cryptographic algorithms in detail. Both efficiency and security of information are important while designing and implementation considering security, cost and performance. The efficiency of PRESENT and TEA are higher as they have ability to resist cryptographic attacks and also due to their adequate security. In this paper the performance analysis of PRESENT and Tea are described.*

I. Introduction

In digital era secrecy of the information plays important role in cryptography. Cryptography is the integral part of communication organization. PRESENT is newly introduced lightweight cryptographic algorithm. It is mainly designed for devices which have extremely low constrained resources in terms of area power and time. If we relate the performance analysis with other PRESENT is better block ciphers. PRESENT has substitution permutation structure. Confusion and diffusion makes algorithm to become resistant to most cryptographic attacks. In the highly developed world RFID, WSN plays main role in people's work and life. Less area and power consumption also very important factors while designing. TEA is simple algorithm to implement and describe. The implementation of block cipher is little better compared with the stream cipher. The design of algorithm considering power and area is major criteria. The fact is stream ciphers are more compact than the block ciphers.

This paper briefly describes the process of PRESENT algorithm and Tea algorithm on Xilinx 14.2. PRESENT is new hardware optimized algorithm developed from the scratch of the cryptography. Considering low resource constrained devices in mind easily achieved maximum speed and throughput. Tea is simple and tiny algorithm. Goal of this project is achieving simplicity with security. I have put my true effort to show the algorithms description and results.

II. PRESENT algorithm

The PRESENT algorithm uses 64 bit plain text and 80 or 128 bit key length. I have taken key size of length 80 bits. PRESENT has SPN structure which is mainly substitution and permutation network. It consists of 31 rounds and final round. One regular round involves key mixing, substitution and permutation layer. We can divide the algorithm into two divisions one is iteration operation and the other one is key updating. Iteration consists of three operations Add round key, S box substitution and permutation layer. Updated key will be used in the add round key operation each time in the encryption. Key updating is used to generate round key each time for add round key operation. Transformations operate on intermediate results are named as state. There are 31 iteration rounds and in the final round intermediate result is XORed with round key to get cipher text. Add round key is also called as key mixing step fig.1 shows the block diagram of PRESENT encryption process.

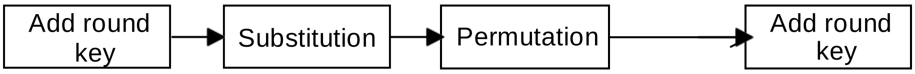


Fig 1. PRESENT encryption block diagram

Fig. 2 shows the flowchart of the PRESENT encryption algorithm. The steps are as follows

1. Generate the round keys (Key updating)
2. Round key will be XOR ed with the state
3. For 31 rounds substitute s box on the state
4. For 31 rounds apply permutation layer on the state
5. For 32nd round only Add round key operates.

2.1. Key updating

It involves 61 bit left rotation with substitution box and 5 bit round counter. Leftmost 4 bits are passed through s box. Least significant rightmost values of round counter are XOR ed with bits of K (K_{19} K_{18} K_{17} K_{16} K_{15}). PRESENT-80 uses single s-box and PRESENT-128 uses two s boxes.

2.2 S box substitution

Substitution layer consists of 16 s boxes with 4 bit inputs and 4 bit outputs. 8 bit s boxes require more area than 4 bit s box. Even though 4 bit s boxes are weaker than 8 bit s boxes we can achieve more security in 4 bit s box. Each S box has 4 bit input.

2.3 Permutation layer or P layer

It is simple and regular transformation of bit transposition. Every bit is moved to corresponding bit position as in the permutation layer table. The bit i is moved to the position P(i). For example bit 0 is moved to 0th position and every 4th bits position increases by one. As bits on left increases bit position will be sum of the previous bit and 16 and it starts for every 4, 8, 12, 16 and so on.

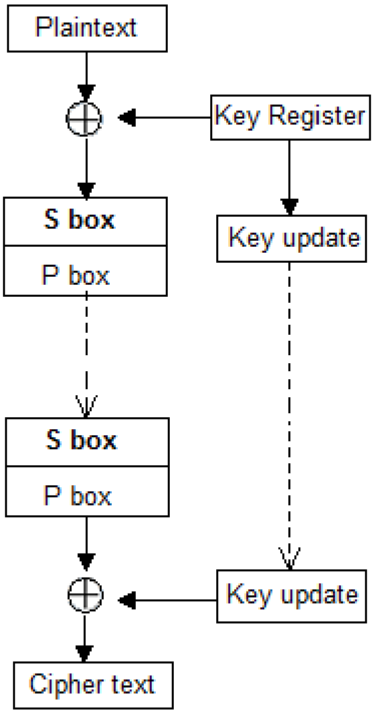
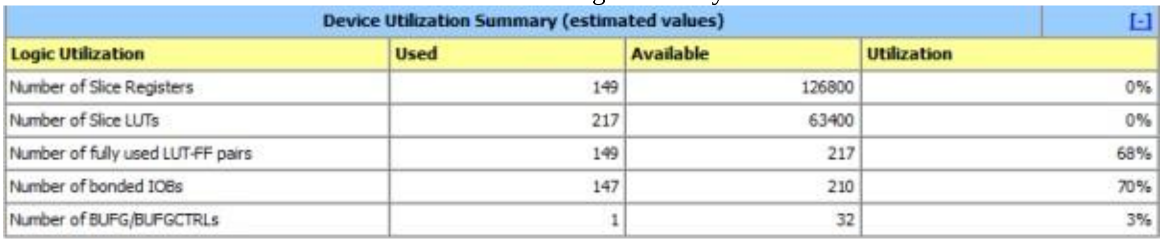


Fig 2. PRESENT encryption algorithm

PRESENT encryption is simulates using Xilinx 14.2 using ISE simulator tool.

2.4 PRESENT simulation results

Table 1. Design summary



Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	149	126800	0%
Number of Slice LUTs	217	63400	0%
Number of fully used LUT-FF pairs	149	217	68%
Number of bonded IOBs	147	210	70%
Number of BUFG/BUFGCTRLs	1	32	3%

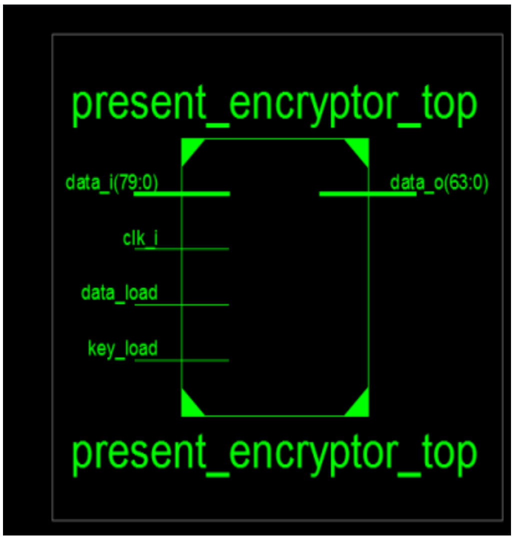
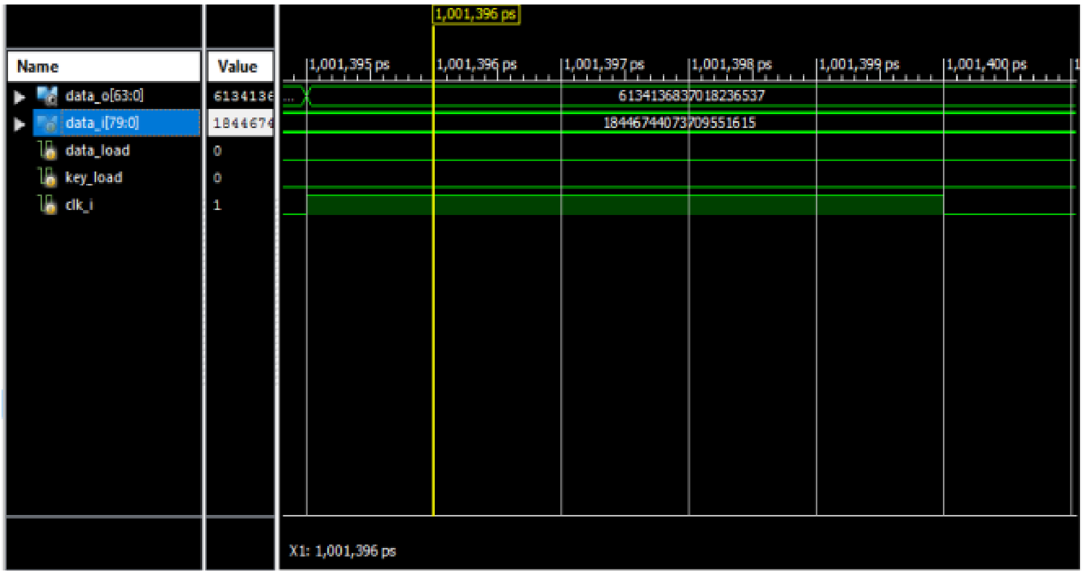


Fig 3. RTL schematic



Name	Value
data_o[63:0]	6134136
data_i[79:0]	1844674
data_load	0
key_load	0
clk_i	1

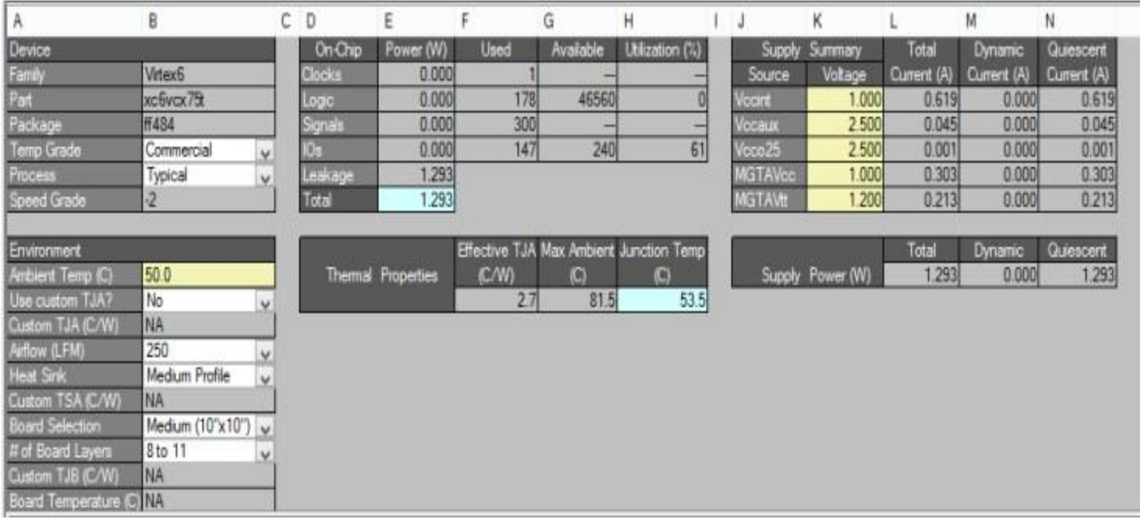
6134136837018236537

18446744073709551615

Fig 4. Simulation results

When we implement and translate the power report is obtained.

Table 2. Power analysis table


A
B
C
D
E
F
G
H
I
J
K
L
M
N

Device	
Family	Virtex6
Part	xc6vcx75t
Package	ff484
Temp Grade	Commercial
Process	Typical
Speed Grade	-2

Environment	
Ambient Temp (C)	50.0
Use custom TJA?	No
Custom TJA (C/W)	NA
Airflow (LFM)	250
Heat Sink	Medium Profile
Custom TSA (C/W)	NA
Board Selection	Medium (10"x10")
# of Board Layers	8 to 11
Custom TJB (C/W)	NA
Board Temperature (C)	NA

On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.000	1	–	–
Logic	0.000	178	46560	0
Signals	0.000	300	–	–
IOs	0.000	147	240	61
Leakage	1.293			
Total	1.293			

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	2.7	81.5	53.5

Supply Summary		Total	Dynamic	Quiescent
Source	Voltage	Current (A)	Current (A)	Current (A)
Vccint	1.000	0.619	0.000	0.619
Vccaux	2.500	0.045	0.000	0.045
Vcco25	2.500	0.001	0.000	0.001
MGTAVcc	1.000	0.303	0.000	0.303
MGTAVtt	1.200	0.213	0.000	0.213

	Total	Dynamic	Quiescent
Supply Power (W)	1.293	0.000	1.293

III. TEA algorithm

Both safety of information and ease of implementation is equally important and hence TEA is an outstanding choice in cryptography. The Tiny Encryption Algorithm is block cipher and it is simpler as a few lines of the code. It is fast, safe and simple in explanation and operation than IDEA nevertheless it uses same algebraic mixed group's method as the privacy of the data is more significant. TEA is protected and needs least storage space. Tea is highly strong to differential cryptanalysis and attains complete diffusion. The TEA takes 64 bit (block size) data bits using 128 bit keys with 32 rounds. This cipher starts with a 64 bit data block that is divided up into two 32 bit blocks in which the block on the left side is called as L and the block on the right side is called as R. These blocks are exchanged per Round.

3.1 Key schedule : 128 bit key is splitting into four 32 bit sub key Ki where i= 0 to 3 and it uses a constant named as delta, 2^{32}/ (golden ratio), which is 2654435769 is an integer. Here 128 bit key is given as input as seed. Multiples of delta are used in each iteration (mod 2^{32}) and addition operations are mod 2^32. The first half R goes through a left shift of 4 and then is added to K [0]. R is added to Delta. R goes through a right shift of 5 and then it is added to K [1]. An XOR operation is then applied to the result of those three operations and finally, the result of The XOR operation is added to L (i-1). It creates the half of the block cipher for the next iteration. Similar operations are performed for the next half round L [i-1] function.

TEA encryption algorithm diagram is shown in fig. 5.

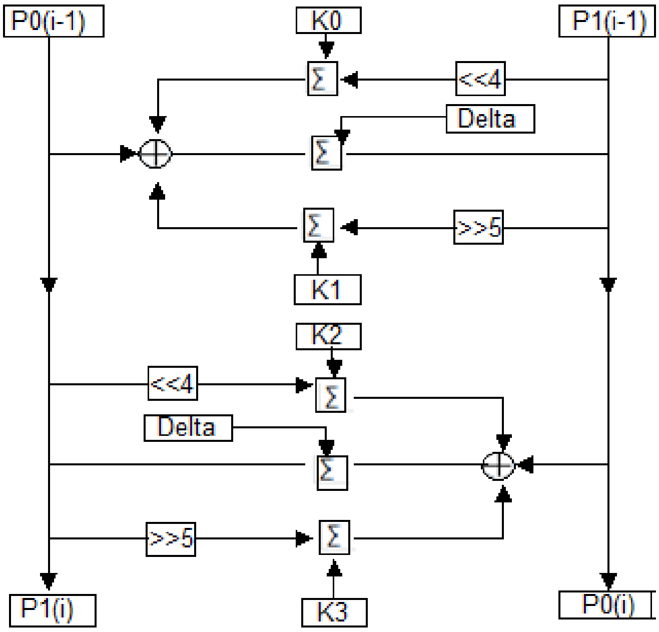
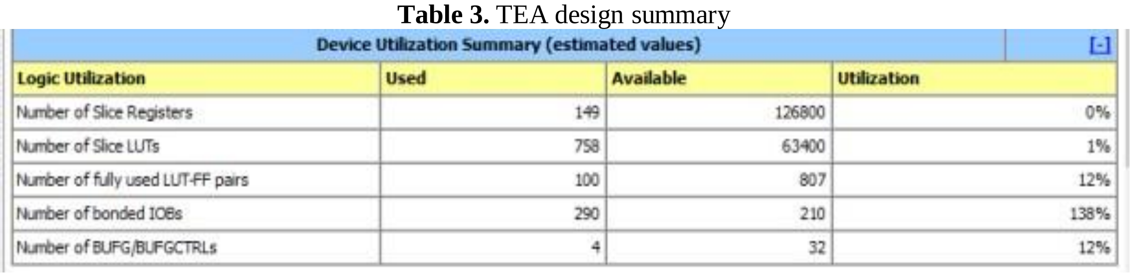


Fig 5. TEA encryption algorithm

3.1TEA synthesis results

Table 3. TEA design summary



Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	149	126800	0%
Number of Slice LUTs	758	63400	1%
Number of fully used LUT-FF pairs	100	807	12%
Number of bonded IOBs	290	210	138%
Number of BUFG/BUFGCTRLs	4	32	12%

Table 3 shows the Logic utilization of TEA encryption algorithm.

RTL schematic of TEA encryption is shown in fig.6. Fig 7 shows the Simulation results.

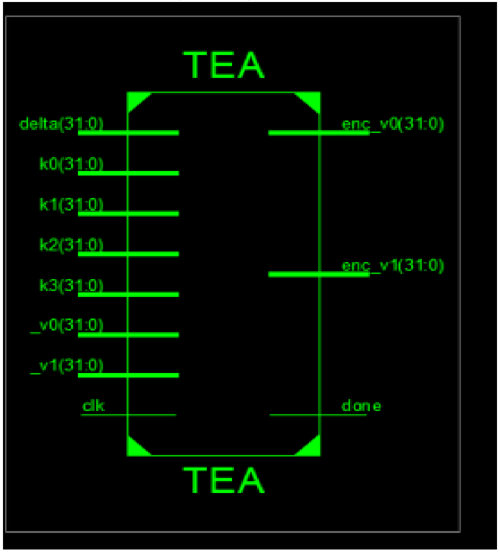
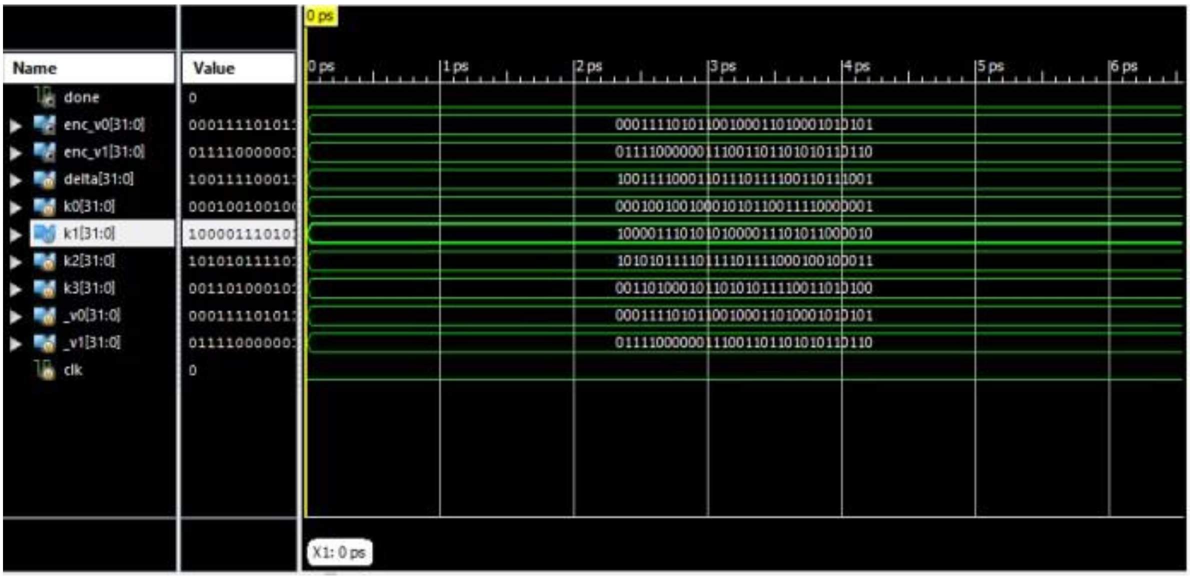


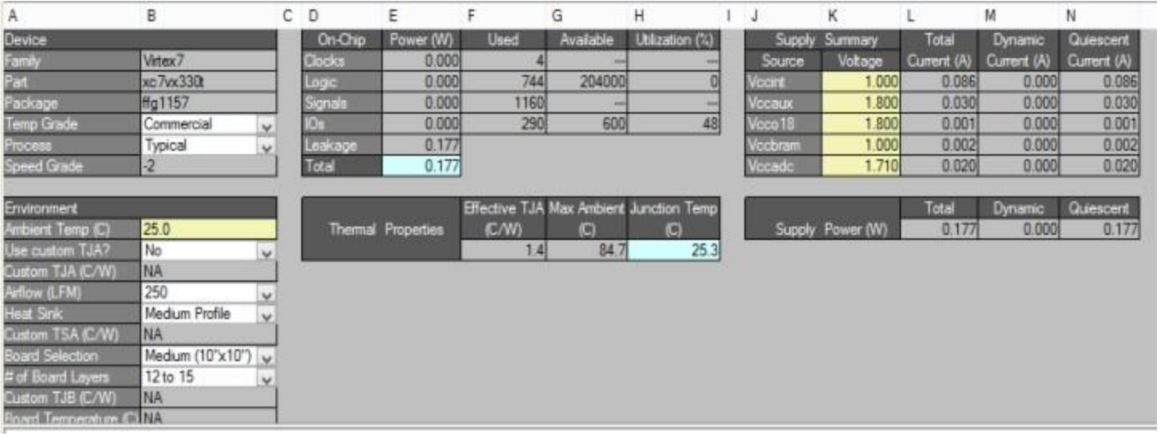
Fig 6. TEA RTL schematic



Name	Value	
done	0	
enc_v0[31:0]	000111101011	00011110101100100011010001010101
enc_v1[31:0]	011110000001	01111000000111001101101010110110
delta[31:0]	100111100011	10011110001101110111100110111001
k0[31:0]	000100100100	00010010010001010110011110000001
k1[31:0]	100001110101	10000111010101000011101011000010
k2[31:0]	101010111101	10101011110111101111000100100011
k3[31:0]	001101000101	00110100010110101011110011010100
_v0[31:0]	000111101011	00011110101100100011010001010101
_v1[31:0]	011110000001	01111000000111001101101010110110
clk	0	

Fig 7. TEA simulation results

Table 4. Power analysis



Device	
Family	Virtex7
Part	xc7vx330t
Package	ffg1157
Temp Grade	Commercial
Process	Typical
Speed Grade	-2

Environment	
Ambient Temp (C)	25.0
Use custom TJA?	No
Custom TJA (C/W)	NA
Airflow (LFM)	250
Heat Sink	Medium Profile
Custom TSA (C/W)	NA
Board Selection	Medium (10"x10")
# of Board Layers	12 to 15
Custom TJB (C/W)	NA
Board Temperature (C)	NA

On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.000	4	---	---
Logic	0.000	744	204000	0
Signals	0.000	1160	---	---
IOs	0.000	290	600	48
Leakage	0.177			
Total	0.177			

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	1.4	84.7	25.3

Supply Summary		Total	Dynamic	Quiescent
Source	Voltage	Current (A)	Current (A)	Current (A)
Vccint	1.000	0.086	0.000	0.086
Vccaux	1.800	0.030	0.000	0.030
Vcco18	1.800	0.001	0.000	0.001
Vccbram	1.000	0.002	0.000	0.002
Vccadc	1.710	0.020	0.000	0.020

	Total	Dynamic	Quiescent
Supply Power (W)	0.177	0.000	0.177

IV. The Performance Results of Encryption

We have implemented the algorithm on Verilog Xilinx 14.2 these results are obtained. Table 4 shows the power analysis of the proposed algorithm. Table 5 shows performance result of the proposed algorithm and Fig. 8 the comparison graph. Note that the PRESENT which we have taken is of key length 80 bit and key of 128 bit is given as input to TEA.

Table 5. Xilinx results

Algorithm	Key size	Plain text Block size	Rounds	Max frequency in MHz	Time delay	LUT's	FF's	Power consumption in watts	Logic process-no used as logic
PRESENT	80	64	32	607.4	1.646ns	217	149	1.293	217
TEA	128	64	32	147.29	6.789ns	758	149	0.177	758

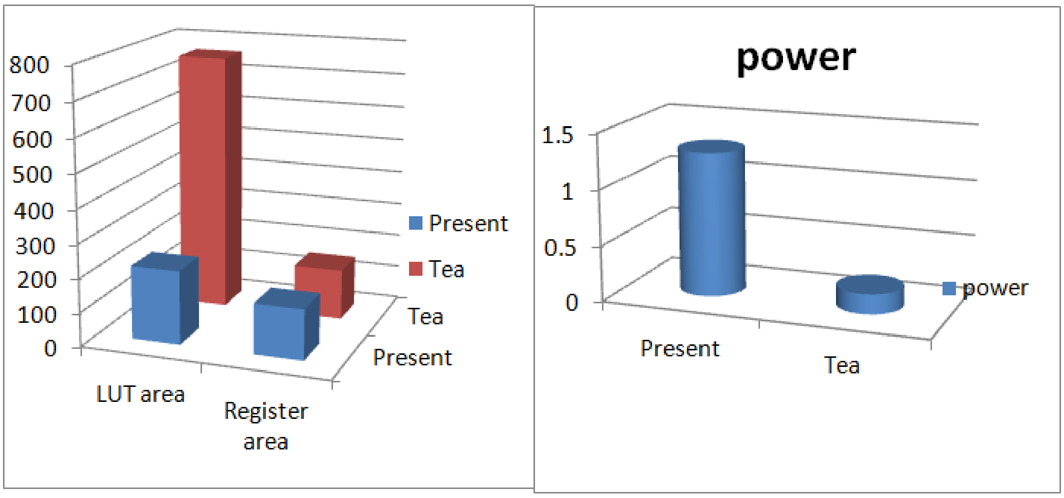


Fig 8. Comparison graph

V. Conclusion

This paper proposes encryption of, PRESENT algorithm which has 80 bit key size and 64 bit block size and TEA which has 64 bit data block and 128 bit key. PRESENT Algorithm is well proved to have the ability to resist differential and linear attacks. It is not only proved from the theory it has certain value from the implementation. The encryptions are carried out writing programs in Verilog. From this implementation we can come to the conclusion that PRESENT is indeed a strong block cipher compared to TEA. When we compare the power consumption Tea is slightly less than PRESENT but area is more for Tea compared to PRESENT. Overall by considering power, area and time shows that PRESENT is a better cipher in terms of area security and performance.

References

[1]. ”A Random PRESENT encryption algorithm based on dynamic s box”, Ziyingi Tang, Jie cie, Hong Zhong, Mingyong yu, International journal of security and its applications, Volume 10 no.3, 2016

[2]. ”A Survey of lightweight cryptographic implementations”, Thomas eisenbarth, Sandeep Kumar, Christoff paar and Axel poschmann, Leif Uhsadel, Design and test IC’s for secure embedded computing, 4/10/2017.

[3]. ” A Secure encryption technique based on advanced hill cipher for a public key cryptosystem”, Suman chandrashekhar, Akash H.p., Adarsh K., Mrs. Smitha sasi, Volume 11, issue 2, May-june 2013.

[4]. ”Design space exploration of PRESENT implementations for FPGA’s”, Mohamad sbeiti, Michael silbermann, Axel poschmann, christof paar, Hortz gortz institute for IT security.

[5]. ” PRESENT: an ultralightweight block cipher”, A. bogdanov1 , L.R. Knudsen2, G. Leander1, C.Paar1, A. Poschmann1, MJ.B. Robshaw3, Y. Securin3, C. Vikkelsoe2, Hortz gortz institute for IT security.

[6]. ” PRESENT cipher encryption IP core”, Reza ameli, Digital system lab, Iran.

[7]. ” A Survey on Various Lightweight Cryptographic Algorithms on FPGA”, Chaitra B1, Kiran Kumar.V.1, Shatharama Rai C2, IOSR journal of Electronics and communication engineering, Volume 12, issue 1, 2017

[8]. ” Design and implementation of Tiny encryption algorithm”, Kiran Kumar.V.1, Sudesh Jeevan Mascarenhas2, Sanath Kumar3, Viven Rakesh J. Pais4 Kiran Kumar.V.G et al. Int. Journal of Engineering Research and Applications, Volume 5, issue 6, June 2015.