International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.5 (Sep-2020)
http://dx.doi.org/10.12785/ijcds/090512

ACT: An Ultra-Light Weight Block Cipher For Internet of Things

Jithendra.K.B[1]and ShahanaT.Kassim[2]

[1] *Department of Electronics and Communication, College of Engineering, Thalassery, Kerala, India*
[2]*Division of Electronics, School of Engineering, CUSAT, Kerala, India*

Received 1 Nov.2019, Revised 31 Jan. 2020, Accepted 25 Jul. 2020, Published 1 Sep. 2020

Abstract: In this paper an ultra-light weight block cipher named ACT is proposed. This cipher is exclusively designed to operate in resource constrained environments. ACT is a 64-bitsubstitution permutation network (SPN) with a key length of 80 bits. The construction of ACT requires only 1481 Gate Equivalents (GE). The new 4-bit substitution box (sbox) introduced in this design achieves minimal differential and linear cardinalities. The Permutation layer proposed in this design, combined with sbox properties offers excellent security performance which is indicated by large numbers of both linear and differential active sboxes in a fewer number of rounds. The minimum number of rounds required for a full diffusion of data is just 3. Key schedule and permutation layer together provide excellent resistance against biclique attacks. The dynamic power consumption of ACT is just 30 mW which is lesser compared to other block ciphers like PRESENT, LED etc. The details of differential, linear, biclique and algebraic cryptanalyses are given in this paper. Comparison of parameters with other block ciphers is also given.

Keywords: Light Weight Cryptography, Block Cipher, Security, Cryptanalysis, Complexity

1. INTRODUCTION

Block ciphers play a major role in providing data security. Data Encryption Standard (DES) was proposed by the US Government in 1977 but became obsolete soon because of its security weakness. In 2001 Daemon and Rijmen proposed Rijndael algorithm which later adopted as Advance Encryption Standard (AES)[1]. AES survived almost all types of cryptanalyses [2-8] carried out by different cryptologists so far and became a very popular and trustable block cipher. The first successful attack on full round AES was proposed by Bogdanov et al. in 2011 [9]. Based on this, a modified attack proposed in 2015 [10] but the time complexity required for the attack is at a level which is comparable to that of brute force attack.

So there are no practical issues in using AES algorithm till now. But the complexity of the system is much high so that it can't be used for any resource constrained environment. Different versions of AES implementations are available in the literature [11- 13] but even the most efficient implementation consumes 2400 GE for the implementation of AES.

Internet of Things (IoT) has become an emerging technology nowadays and there is a growing demand for the applications like RFID systems and wireless sensor networks, which are the significant exponents of IoT. Main constrains for these systems are area, memory, and power consumption. These systems also require certain level of security since they exchange information. Light weight block cipher design has become a hot research topic nowadays since it offers sufficient security to resource constrained applications.

Many light weight block ciphers are introduced in recent years to perform in resource constrained platforms. PRESENT [14], LED [15], LBlock [16], GIFT [17], RECTANGLE[18] etc. are some of the popular light weight block ciphers. All of these block ciphers have robust designs and can be implemented using less than 2200 gate equivalents(GE).

PRESENT was introduced in CHES 2007 and widely attracted the attention of crypto world because of its simple structure and security. The sbox of PRESENT was selected primarily because of its small area and not based on highest security. Later the weakness of PRESENT sbox was revealed through many cryptanalyses. Properties of permutation layer, though itis highly symmetric, combined with the weakness of sbox together leads to increased clustering of linear and differential trails in

E-mail address: jithendrakb@gmail.com, shahanatk@cusat.ac.in

higher rounds. Since linear cardinality of PRESNT sbox is 8, the cipher is much vulnerable to linear cryptanalysis.

Later Banik.S et al. modified PRESENT to GIFT, which optimizes PRESENT to a great extent. The differential and linear cardinalities of GIFT are 1 and 3 respectively, which indicates that vulnerability towards linear cryptanalysis is not minimal. To reduce the area and power consumption, key addition of GIFT is done only to half the number of data bits by exploiting the advantage of permutation layer, which reduces the security strength.

RECTANGLE also is an SPN based design, which performs 25 rounds of operation for a full encryption. 4-bitsbox is used to substitute data in a column wise fashion. LED is an Advance Encryption Standard (AES) based design, but performs nibble wise operations. It performs excellently in software platform. LBlock is a Feistel network-based design which achieves both hardware and software efficiency. Piccolo [19], KLEIN [20], PRIDE [21], PRINCE [22], Simon and Speck [23], FeW [24], PICO [25] etc. are other block ciphers introduced recently

In this paper we present a new block cipher named ACT, which is exclusively designed for highly constraint hardware platforms. So, we focus on least area and power consumption but without any reduction in security. This design is based on the concept of Substitution Permutation Network. Both linear and differential cardinalities of ACT sbox is 2, which is the least optimum values possible. Effort to reduce either cardinality number from the value 2 will end up in increased cardinality number of the other. We use a permutation layer, which is different from that of PRESENT, yet the whole data gets diffused completely in 3 rounds. The key length is 80 bits.

The paper is organized as follows. Section 2 describes the construction of ACT. A detailed explanation of different operations performed during each round is also given in this section. In section 3 different types of cryptanalyses are applied on the cipher to evaluate the security strength. The comparisons of security strengths of different block ciphers are also given. Section 4explain about the hardware details such as gate count, power consumption etc. Conclusion with future scope is given in section 5.

2. CONSTRUCTION OF ACT

ACT is a bitwise block cipher based on Substitution Permutation Network (SPN) concept. It has 64 data bits and a single key variant, which is of 80 bits. A complete encryption process consists of 31 rounds. Each round is completed by performing 3 operations. These are AddRoundKey, SubNibble and BitPermute. The block diagram of ACT is given in Figure 1

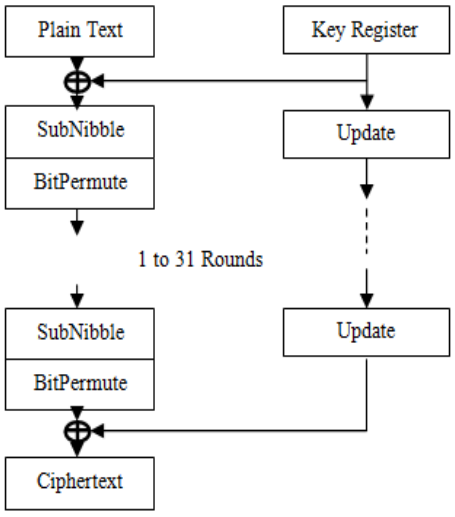

Figure 1. Block diagram of ACT

A. AddRoundKey

This operation is performed by Exclusively ORing 64 key bits with the 64 data bits. Method of selection of 64 key bits is given in the key schedule process. If the data bits are denoted by $d = d_{63}d_{62}....d_1d_0$andkey bits used in a particular round are denoted by $K= K_{63}K_{62}....K_1K_0$ then AddRoundKey operation is mathematically denoted as

$$d_i = d_i \oplus K_i$$

B. SubNibble

Even though ACT is a bitwise block cipher, the substitution process is done nibble wise. In substitution process, the original data in each round is substituted with another data so that after a number of rounds, the original data becomes really hidden. This nonlinear operation is effective for bringing security to systems, if properly designed. ACT uses a bijective 4×4 sbox, which is given in Table I. Four-bit sbox reduce the hardware complexity to a considerable extent comparing to an eight-bit sbox as in the case of AES. Sixteen nibbles of sbox accommodate 64 data bits as shown below

$N_i = d_{4i+3}||d_{4i+2}||d_{4i+1}||d_{4i}$, where $0 \le i \le 15$

TABLE I. SBOX OF ACT

input	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
output	4	B	D	8	1	6	2	F
input	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
output	A	5	E	3	9	C	7	0

The most crucial element in the design of any block cipher is sbox. It's primarily because of its nonlinear nature which resists different types of cryptanalytic attacks effectively. In ACT, 16 parallel sboxes are used to

substitute 64 data bits simultaneously. Cluttering of linear and differential trails is prevented effectively with the sbox designed for ACT. The compactness of the sbox makes it suitable for using in resource constraint devices. The important criteria considered for designing the sbox is listed and explained below.

- If both the input difference $\Delta X \in F_2^4$ and output difference $\Delta Y \in F_2^4$ are non-zero, then $DC(\Delta X, \Delta Y) = \#\{x \in F_2^4 | S(x) \oplus S(x \oplus \Delta X) = \Delta Y\} \leq 4$
- Let $Hw(\Delta X)$ and $Hw(\Delta Y)$ be the hamming weight of any non-zero input difference $\Delta X \in F_2^4$ and output difference $\Delta Y \in F_2^4$ respectively, then $Set_{DC} = DC(\Delta X, \Delta Y) = \#\{x \in F_2^4 | S(x) \oplus S(x \oplus \Delta X) = \Delta Y\} = 0$
- $LC(X,Y) = \#\{ x \in F_2^4 | X.x = Y.s(x) - 8\} \leq 4$ for $X \in F_2^4$ and $Y \in F_2^4$, where $X \in F_2^4$ represents any nonzero input masks and $Y \in F_2^4$ represents any nonzero output masks
- Let $Hw(X)$ and $Hw(Y)$ be the hamming weight of any nonzero input masks $X \in F_2^4$ and output difference $Y \in F_2^4$ respectively, then $Set_{lC} = LC(X,Y) = \#\{ x \in F_2^4 | X.x = Y.s(x) - 8\} \neq 0$
- The sbox possess bijective property i.e., $S(x) \neq S(y)$, where x and y represent any input and output values respectively.
- The sbox doesn't possess any static points i.e., For any value x, $S(x) \neq x$

TABLE II. COMPARISON OF SBOX PROPERTIES

Cipher	Max value in DDT	Max value in LAT	Car_{LC}	Car_{DC}
ACT	4	4	2	2
PRESENT	4	4	0	8
GIFT	4	4	1	3
PICO	4	4	2	2

The cryptographic strength of a sbox is mainly determined by the cardinalities. We have achieved $Car_{DC} = 2$ and $Car_{LC} = 2$. For the block cipher PRESENT, $Car_{DC} = 0$ and $Car_{LC} = 8$. It is proved that the higher linear cardinality of PRESENT lead to vulnerability towards linear cryptanalysis [26][27]. Comparison of sbox properties is given in Table II

The differential distribution table (DDT) and Linear Activation Table (LAT) is given in Table IV and Table V respectively.

C. BitPermute

The data bits are permuted in the following fashion which gives complete diffusion with just 3 rounds. BitPermute operation doesn't need any hardware and thus consumes no power. The input and output positions of BitPermute function is given in Table III

TABLE III. BIT PERMUTATION OF ACT

input	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
output	1	17	33	49	0	16	32	48
input	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
output	3	19	35	51	2	18	34	50
input	16	17	18	19	20	21	22	23
output	5	21	37	53	4	20	36	52
input	24	25	26	27	28	29	30	31
output	7	23	39	55	6	22	38	54
input	32	33	34	35	36	37	38	39
output	9	25	41	57	8	24	40	56
input	40	41	42	43	44	45	46	47
output	11	27	43	59	10	26	42	58
input	48	49	50	51	52	53	54	55
output	13	29	45	61	12	28	44	60
input	56	57	58	59	60	61	62	63
output	15	31	47	63	14	30	46	62

D. Key Scheduling

Let the key be $K = k_{79}k_{78}k_{77}....k_2k_1k_0$,

Now the following operation is performed

- Bit replacement
  $k^{i+1}_{63} = k^i_{63} \oplus k^i_{62}$
  $k^{i+1}_{62} = k^i_{62} \oplus k^i_{61}$
  $k^{i+1}_{61} = k^i_{61} \oplus k^i_{60}$
  $k^{i+1}_{60} = k^i_{60} \oplus k^{i+1}_{63}$

The above given operation is equivalent to a 4-round operation of a 4-bit Linear Feedback Shift Register with polynomial $x^4 + x^3 = 1$. The function is achieved with just 4 xor gates. The operation is reversible too.

- A 5-bit pseudo random sequence is generated and xored to key bits k_{31} to k_{27}. The random sequence is generated using the primitive polynomial $x^5 + x^3 = 1$.

TABLE IV. DIFFERENTIAL DISTRIBUTION TABLE OF ACT SBOX

Input Difference \ Output Difference	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4
2	0	0	4	2	0	2	0	0	4	0	0	2	0	2	0
3	0	0	0	2	0	2	0	0	4	0	4	2	0	2	0
4	0	0	4	0	2	0	2	0	4	0	0	0	2	0	2
5	0	4	0	2	0	2	0	0	0	4	0	2	0	2	0
6	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
7	0	4	0	0	0	0	0	0	4	4	4	0	0	0	0
8	0	0	2	0	2	0	0	2	0	2	2	0	0	4	2
9	4	2	0	0	0	2	0	2	0	0	0	0	2	2	2
a	0	0	2	0	0	4	2	2	0	2	2	0	2	0	0
b	4	2	0	0	2	2	2	2	0	0	0	0	0	2	0
c	0	0	2	0	0	0	2	2	0	2	2	4	2	0	0
d	4	2	0	2	0	0	0	2	0	0	0	2	2	0	2
e	0	0	2	4	2	0	0	2	0	2	2	0	0	0	2
f	4	2	0	2	2	0	2	2	0	0	0	2	0	0	0

TABLE V. LINEAR ACTIVATION TABLE OF ACT SBOX

OPD \ IPD(Input Probability Deviation)	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	0	0	0	0	4	0	4	0	0	0	0	0	-4	0	4
2	0	2	2	0	0	-2	-2	0	4	-2	2	4	0	-2	2
3	-4	-2	2	0	0	2	2	0	0	2	2	4	0	2	-2
4	0	0	4	0	-4	0	0	0	0	0	-4	0	-4	0	0
5	0	-4	0	0	0	4	0	0	0	-4	0	0	0	-4	0
6	0	-2	2	-4	0	-2	-2	0	-4	2	2	0	0	-2	2
7	-4	-2	-2	4	0	-2	-2	0	0	2	-2	0	0	-2	2
8	0	0	0	-2	-2	2	2	0	4	4	0	-2	2	-2	2
9	0	0	0	-2	2	2	-2	4	0	0	-4	2	2	2	2
a	0	2	2	2	2	4	-4	0	0	2	2	-2	-2	0	0
b	4	-2	2	2	2	0	0	-4	0	2	-2	2	2	0	0
c	0	-4	0	-2	2	-2	-2	0	4	0	0	-2	-2	2	-2
d	0	0	-4	-2	-2	2	-2	-4	0	0	0	2	-2	2	2
e	0	2	-2	-2	2	0	0	0	0	2	-2	2	-2	-4	-4
f	-4	2	2	-2	2	0	0	-4	0	-2	-2	-2	2	0	0

- Now the key bits are shifted 18 position towards right ie.$k_{79}k_{78}k_{77}...k_2k_1k_0$ = $k_{17}k_{16}..k_1k_0k_{79}k_{78}...k_{19}k_{18}$
- Now the key bits used in each round is given by $K_{63}K_{62}K_{61}.....K_2K_1K_0$ = $k_{79}k_{78}k_{77}....k_{18}k_{17}k_{16}$

3. CRYPTANALYSIS

The strength of the cipher is evaluated using different cryptanalysis methods. The most popular and efficient methods of evaluations are linear cryptanalysis, differential cryptanalysis and algebraic cryptanalysis. Also, we applied biclique cryptanalysis which is one of the recent techniques for cryptanalysis to measure the strength of any block cipher. The results of different methods are given below which proves the robustness of ACT against various types of attacks.

A. Differential Cryptanalysis

Differential cryptanalysis [28, 29] is one of the strongest methods used for key recovery of block ciphers. Measuring the cryptographic strength against differential and linear cryptanalysis is an essential and fundamental requirement in security analysis. Calculation of lower bound for the number of active sboxes is one of the methods used to check the resistance of a cipher against attacks. The differential probability and characteristics are calculated from the differential distribution table (DDT).

We have achieved differential cardinality of 2 which is a good measure of security against differential

cryptanalysis. The maximum value in the DDT is 4, which means the maximum probability is $4/16 = 2^{-2}$. For the first 15 rounds ACT achieves 30 active sboxes. We used mixed integer linear programming (MILP) for the calculation of minimum number of active sboxes. For 15 rounds we achieved a differential probability of 2^{-33}. So, the chosen plain text complexity = $1/(2^{-33})^2 = 2^{66}$. This shows that ACT is well secured against differential attacks.

B. *Linear cryptanalysis*

Linear cryptanalysis[30] is another powerful method to gauge the resistance of a block cipher. Key retrieval is done by finding out the linear relations between plain texts, cipher texts and subkeys. If *p* is the probability of a linear trail, then the probability bias ε is given by *p*-1/2. An *n* bit block cipher can be attacked using linear cryptanalysis only if the amplitude of linear propagation is significantly larger than $2^{-n/2}$.

TABLE VI. COMPARISON OF RESISTANCE AGAINST LINEAR AND DIFFERENTIAL CRYPTANALYSES

	ACT	Piccolo	LBlock	PRESENT	FEW
No.of Rounds	15	30	15	25	27
Chosen Plain Text	2^{66}	2^{120}	2^{64}	2^{100}	2^{90}
Known Plain Text	2^{68}	2^{120}	2^{66}	2^{102}	2^{90}
No.of Active sbox from differential trails	30	30	32	50	45
No. of active sbox from linear trails	32	30	32	25	45
Reference	This paper	[19]	[16]	[14]	[24]

A set of linear trails forms a linear propagation. From the input/output mask patterns, the correlation coefficients of linear trails are calculated and summed up to get the amplitude of linear propagation. Linear activation table (LAT) is used for the calculation. The magnitude of maximum probability deviation in the table is 2^{-2}. The linear cardinality of ACT sbox Car_{LC} is 2. At the same time *CarLC* of PRSENT ad GIFT is 8 and 3 respectively. Lower values of cardinality, probability bias and higher values of active sboxes indicate higher security.

ACT SPN structure achieved a minimum number of 32 active sboxes in first 15 rounds. Using Matsui's Piling up Lemma [31], total bias is calculated as 2^{-34} for first 15 rounds. So, the data complexity required for 15 round attack is $1/(2^{-34})^2 = 2^{68}$, which indicates excellent resistance against Linear cryptanalysis. The comparison of resistance of ACT towards linear and differential cryptanalysis with that of other ciphers are given in Table VI

C. *Biclique Cryptanalysis*

ACT shows good resistance against Biclique cryptanalysis also. Biclique cryptanalysis is a recently developed cryptanalysis method [32, 33], which is a kind of meet-in-the-middle attack with improved efficiency. The efficiency of computations is enhanced by constructing bicliques on target cipher. We created a 4-dimensionalbiclique to attack ACT, based on the concept of independent bicliques and matching with precomputation. Subkey bits $\{k_{26}, k_{27}, k_{28}, k_{29}\}$ and $\{k_{11}, k_{12}, k_{13}, k_{14}\}$ are selected to construct forward differential $\Delta_i$and reverse differential ∇_j respectively. The 4-dimensional biclique for the last 3 rounds of ACT is shown in Figure 2

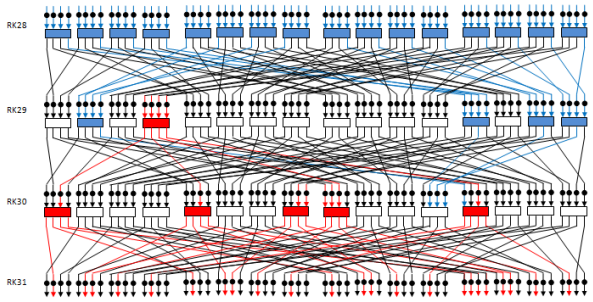

Figure 2. 4 Dimensinal Biclique of ACT (3 Rounds)

The time complexity is calculated as $2^{79.71}$ full round encryption. From Fig 2, it can be seen that only 23 bits are affected by the forward differential, so that the data complexity will not exceed 2^{23}chosen plain text. This shows ACT has sufficient resistance towards biclique cryptanalysis. Comparison of resistance of different ciphers towards biclique cryptanalysis is given in Table VII

TABLE VII. COMPARISON OF RESISTANCE TOWARDS BICLIQUE CRYPTANALYSIS

Cipher	No. of Rounds	Time complexity	Data complexity	Reference
PRESENT 80	31	$2^{79.54}$	2^{23}	[33]
PICCOLO 80	25	$2^{79.13}$	2^{48}	[33]
LED 80	48	$2^{79.37}$	2^{64}	[33]
ACT 80	31	$2^{79.71}$	2^{23}	This paper

D. Algebraic Cryptanalysis

Algebraic equations can be developed by finding the mathematical relations between different bits of sbox. Solving the algebraic equations will lead to key recovery. Using the tool SAGEMATH, we found that the ACT sbox is represented by a total of 267 inequalities which are given below

```
1.  An inequality (-1, 0, 0, 0, 0, 0, 0, 0)
    x + 1 >= 0,
2.  An inequality (0, -1, 0, 0, 0, 0, 0, 0)
    x + 1 >= 0,
3.  An inequality (0, 0, -1, 0, 0, 0, 0, 0)
    x + 1 >= 0,
                    ……….
                    ……….
                    ……….
 265.  An inequality (0, -1, -1, -1, -1, -1, -
1, 0) x + 5 >= 0,
 266.  An inequality (-1, -2, -1, -1, -1, -1,
-2, 1) x + 7 >= 0,
 267.  An inequality (-1, 1, -2, -2, -2, -1,
1, -1) x + 7 >= 0
```

Using Mixed Integer Linear Program [34, 35] we found that the differential distribution table (DDT) of sbox can be represented with just 21 inequalities. Increasing number of equations indicates weakness in security. The sbox proposed for ACT has 21 equations with 8 variables. For 31 rounds, ACT has 10416 quadratic equations with 3968 variables. This number of equations guarantees excellent resistance against algebraic cryptanalysis. The 21 inequalities which represent the differential distribution table of ACT sbox are given below. Here 'x' indicates input bits and 'y' indicates output bits.

-1 x3 + 0 x2 - 1 x1 - 1 x0 - 1 y3 + 0 y2 + 0 y1 - 1 y0 + 4 >= 0
-1 x3 - 1 x2 + 0 x1 - 1 x0 - 1 y3 + 0 y2 - 1 y1 + 1 y0 + 4 >= 0
-1 x3 + 1 x2 + 0 x1 + 0 x0 - 1 y3 + 0 y2 - 1 y1 + 1 y0 + 1 >= 0
-1 x3 - 1 x2 - 1 x1 + 1 x0 - 1 y3 - 1 y2 + 0 y1 + 1 y0 + 3 >= 0
-1 x3 + 0 x2 - 1 x1 - 1 x0 - 1 y3 + 1 y2 + 2 y1 - 2 y0 + 4 >= 0
1 x3 -2 x2 +0 x1 +0 x0 + 1 y3 + 2 y2 + 2 y1 + 1 y0 + 0>= 0
1 x3 + 0 x2 +3 x1 - 2 x0 - 1 y3 + 3 y2 - 1 y1 - 3 y0 + 4 >= 0
2 x3 -1 x2 - 1 x1 - 2 x0 - 0 y3 -2 y2 + 0 y1 - 1 y0 + 5>= 0
2 x3 + 1 x2 +2 x1 + 1 x0 +0 y3 -2 y2 + 0 y1 + 1 y0 + 0>= 0
1 x3 + 2 x2 +2 x1 +2 x0 + 1 y3 -1 y2 -1 y1 +0 y0 + 0>= 0
-2 x3 + 0 x2 +0 x1 + 1 x0 +2 y3 + 2 y2 + 1 y1 + 1 y0 + 0>= 0
1 x3 + 2 x2 - 1 x1 + 1 x0 - 1 y3 - 1 y2 - 1 y1 - 2 y0 + 4 >= 0
-2 x3 -2 x2 - 1 x1 + 1 x0 + 1 y3 -1 y2 -2 y1 + 1 y0 + 6>= 0
2 x3 -1 x2 - 1 x1 +2 x0 +0 y3 + 2 y2 + 0 y1 + 1 y0 + 0>= 0
1 x3 + 2 x2 - 1 x1 + 1 x0 +2 y3 + 0 y2 + 2 y1 - 2 y0 + 1>= 0
2 x3 + 3 x2 +0 x1 - 1 x0 - 1 y3 + 3 y2 -1 y1 +3 y0 + 0>= 0
-1 x3 -2 x2 + 1 x1 + 1 x0 - 1 y3 -2 y2 -2 y1 +1 y0 + 6>= 0
-1 x3 -1 x2 +3 x1 +3 x0 +3 y3 - 1y2 -1 y1 + 4 y0 + 0>= 0
-1 x3 + 0 x2 + 1 x1 - 3 x0 + 1 y3 + 2 y2 -3 y1 - 3 y0 + 7>= 0
1 x3 + 2 x2 +2 x1 +2 x0 - 1 y3 + 0 y2 + 1 y1 - 1 y0 + 0>= 0
-1 x3 -1 x2 +2 x1 - 1 x0 +2 y3 -2 y2 + 1 y1 - 2 y0 + 5>= 0

4. GATE COUNT AND POWER CONSUMPTION

As discussed in the introduction, the power consumption and gate count are very significant parameters for constrained devices. The power consumption is measured using Cadence RTL Compiler v11.10 and found that it is less than that of available block ciphers. Comparison of power consumption of different block ciphers is given in Table VIII. The total gate equivalents is calculated and given in Table IX. The comparison of gate equivalents of different light weight block ciphers is given in Figure 3. Data path for ACT is given Figure 4

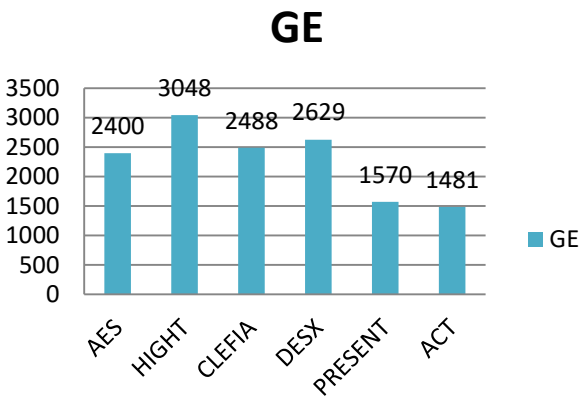

Figure 3. Comparison of Gate Equivalents

TABLE VIII. COMPARISON OF POWER CONSUMPTION OF DIFFERENT BLOCK CIPHERS

Cipher	Power consumed(mW)
ACT	30
LED	100
PRESENT	38
RECTANGLE	31

TABLE IX. CALCULATION OF GATE EQUIVALANTS OF ACT

Data layer	Number	GE for single element	Total GE
D flipflop (data)	64	6	384
sbox (data)	64	6	392
D flipflop (key)	80	6	480
D flipflop (round constant	5	6	30
Xorgate (key addition)	64	2.67	170.88
Xorgate (replacement – key)	4	2.67	10.68
Xorgate (round constant)	5	2.67	13.35
Total GE			1480.91

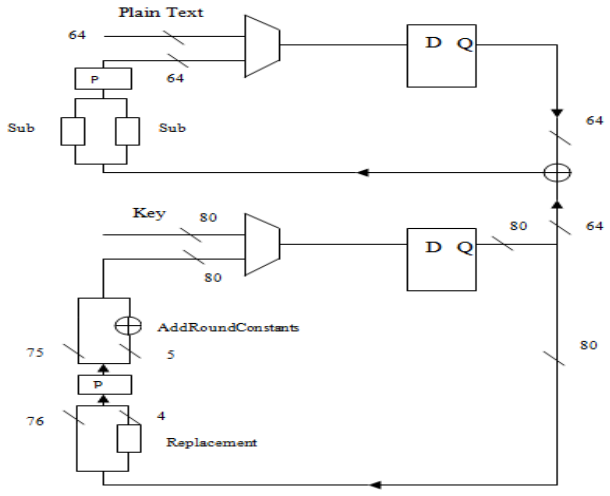

Figure 4. Data path for ACT (Plain text of 64 bits and key of 80 bits)

5. CONCLUSION

A lightweight block cipher ACT is designed for resource constrained environments. The cipher is constructed with 1481 GEs and consumes 30 mW. The proposed sbox and permutation layer provides excellent resistance towards different types of attacks. Linear, differential, biclique and algebraic attacks are carried out in this paper, results of which prove the robustness of the cipher. For 15 rounds ACT achieves 30 differentially active sbox and 32 linearly active sboxes. The time complexity and data complexity required for a full round biclique attack on ACT is $2^{79.71}$and 2^{23} respectively. Comparisons of different parameters with those of existing block ciphers are also given. We believe that the cipher proposed in this paper will be best suited for IoT kind of applications.

Researchers can try for further reduction in GEs and power consumption without reduction in security levels. In order to increase the security of ACT, one can experiment the implementation of 96 or 128 bit keys. In this case a new key schedule will have to be designed and the improved security will be at the cost of increased GEs. We encourage any security analysis on the cipher proposed here.

REFERENCES

[1] J. Daemen and V. Rijmen. The Design of Rijndael: AES – The Advanced Encryption Standard. Springer Verlag, 2002

[2] Zhang W., Wu W., Feng D. (2007) "New Results on Impossible Differential Cryptanalysis of Reduced AES". In: Nam KH., Rhee G. (eds) Information Security and Cryptology - ICISC 2007. ICISC 2007. Lecture Notes in Computer Science, vol 4817. Springer, Berlin, Heidelberg. pp 239-250

[3] Jakimoski G., Desmedt Y. (2004) "Related-Key Differential Cryptanalysis of 192-bit Key AES Variants". In: Matsui M., Zuccherato R.J. (eds) Selected Areas in Cryptography. SAC 2003. Lecture Notes in Computer Science, vol 3006. Springer, Berlin, Heidelberg pp 208-221

[4] Keliher L. (2005) "Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES". In: Dobbertin H., Rijmen V., Sowa A. (eds) Advanced Encryption Standard – AES. AES 2004. Lecture Notes in Computer Science, vol 3373. Springer, Berlin, Heidelberg pp 42-57

[5] Park S., Sung S.H., Lee S., Lim J. (2003) "Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES". In: Johansson T. (eds) Fast Software Encryption. FSE 2003. Lecture Notes in Computer Science, vol 2887. Springer, Berlin, Heidelberg pp 247-260

[6] Schramm K., Leander G., Felke P., Paar C. (2004) "A Collision-Attack on AES". In: Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004. CHES 2004. Lecture Notes in Computer Science, vol 3156. Springer, Berlin, Heidelberg pp 163-175

[7] Renauld M., Standaert FX., Veyrat-Charvillon N. (2009) "Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA". In: Clavier C., Gaj K. (eds) Cryptographic Hardware and Embedded Systems - CHES 2009. CHES 2009. Lecture Notes in Computer Science, vol 5747. Springer, Berlin, Heidelberg pp 97-111

[8] Jithendra.K.B, Shahana.T.K, "New Results in Related Key Impossible Differential Cryptanalysis on Reduced Round AES-192", International Conference On Advances in Communication and Computing Technology (ICACCT), Sangamner, India, IEEE Xplore -2018 February pp 291-295

[9] Bogdanov A., Khovratovich D., Rechberger C. (2011) "Biclique Cryptanalysis of the Full AES". In: Lee D.H., Wang X. (eds) Advances in Cryptology – ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science, vol 7073. Springer, Berlin, Heidelberg pp. 344-371

[10] Tao B., Wu H. (2015) "Improving the Biclique Cryptanalysis of AES". In: Foo E., Stebila D. (eds) Information Security and Privacy. ACISP 2015. Lecture Notes in Computer Science, vol 9144. Springer, Cham pp 39-56

[11] Standaert FX., Rouvroy G., Quisquater JJ., Legat JD. (2003) "Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs". In: Walter C.D., Koç Ç.K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2003. CHES 2003. Lecture Notes in Computer Science, vol 2779. Springer, Berlin, Heidelberg pp 334-350

[12] Tillich S., Großschädl J. (2006) "Instruction Set Extensions for Efficient AES Implementation on 32-bit Processors". In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg pp 270-284

[13] Rebeiro C., Selvakumar D., Devi A.S.L. (2006) "Bitslice Implementation of AES". In: Pointcheval D., Mu Y., Chen K. (eds) Cryptology and Network Security. CANS 2006. Lecture Notes in Computer Science, vol 4301. Springer, Berlin, Heidelberg pp 203-212

[14] Bogdanov A., Knudsen L.R, Leander G, et al. (2007) "PRESENT: An Ultra-Lightweight Block Cipher". In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg pp 450-466

[15] J. Guo, T. Peyrin, A. Poschmann, and M. J. Robshaw. "The LED block cipher". In Cryptographic Hardware and Embedded Systems — CHES 2011, volume 6917 of Lecture Notes in Computer Science, pages 326–341. Springer Verlag, 2011

[16] W. Wu and L. Zhang. "LBlock: A lightweight block cipher". In J. López and G. Tsudik, editors, Applied Cryptography and Network Security — ACNS 2011, volume 6715 of Lecture Notes in Computer Science, pages 327–344. Springer Verlag, 2011.

[17] Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: "A small present - towards reaching the limit of lightweight encryption". In: Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. pp. 321–345 (2017)

[18] Zhang, W., Bao, Z., Lin, D. et al. "RECTANGLE : a bit-slice block cipher suitable for multiple platforms". Sci. China Inf. Sci. (2015) pp 1–15.

[19] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai. "Piccolo: An ultra-lightweight blockcipher". In B. Preneel and T. Takagi, editors, Cryptographic Hardware and Embedded Systems — CHES 2011, volume 6917 of Lecture Notes in Computer Science, pages 342–357. Springer Verlag, 2011

[20] Gong Z., Nikova S., Law Y.W. (2012) "KLEIN: A New Family of Lightweight Block Ciphers". In: Juels A., Paar C. (eds) RFID. Security and Privacy. RFIDSec 2011. Lecture Notes in Computer Science, vol 7055. Springer, Berlin, Heidelberg pp 1-18

[21] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, and T. Yalçin. "Block ciphers – Focus on the linear layer" (feat. PRIDE). In J. A. Garay and R. Gennaro, editors, Advances in Cryptology — CRYPTO 2014, volume 8616 of Lecture Notes in Computer Science, pages 57–76. Springer Verlag, 2014.

[22] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçin. "PRINCE – A low-latency block cipher for pervasive computing applications". In X. Wang and K. Sako, editors, Advances in Cryptology — ASIACRYPT 2012, volume 7658 of Lecture Notes in Computer Science, pages 208–225. Springer Verlag, 2012

[23] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. "The SIMON and SPECK families of lightweight block ciphers". Cryptology ePrint Archive, Report 2013/404, 2013.

[24] Kumar, M. Pal, S.K. & Panigrahi, A. "FeW: A lightweight block Cipher". In SAG (DRDO), Department of Mathematics, University of Delhi, India, 2014. http://eprint.iacr.org/2014:326, Vers.: 20140512:054453

[25] Bansod, G., Pisharoty, N. and Patil, A., 2016. "PICO: An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing".Defence Science Journal,66(3)

[26] Ohkuma K. (2009) "Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis". In: Jacobson M.J., Rijmen V., Safavi-Naini R. (eds) Selected Areas in Cryptography. SAC 2009. Lecture Notes in Computer Science, vol 5867. Springer, Berlin, Heidelberg pp 249-265

[27] Cho J.Y. (2010) "Linear Cryptanalysis of Reduced-Round PRESENT". In: Pieprzyk J. (eds) Topics in Cryptology - CT-RSA 2010. CT-RSA 2010. Lecture Notes in Computer Science, vol 5985. Springer, Berlin, Heidelbergpp. 302-317

[28] Biham E., Shamir A. (1992) "Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer". In: Feigenbaum J. (eds) Advances in Cryptology — CRYPTO '91. CRYPTO 1991. Lecture Notes in Computer Science, vol 576. Springer, Berlin, Heidelberg , pp 156-171

[29] Jithendra.K.B, Shahana.T.K, "A Novel Approach in Substitution for Reduced Complexity and Better Cryptographic Strength of AES. " Journal of Advanced Research in Dynamical and Control Systems, vol.10, no.15, pp. 183 - 191, Nov. 2018.

[30] Hermelin M., Cho J.Y., Nyberg K. (2008) "Multidimensional Linear Cryptanalysis of Reduced Round Serpent". In: Mu Y., Susilo W., Seberry J. (eds) Information Security and Privacy. ACISP 2008. Lecture Notes in Computer Science, vol 5107. Springer, Berlin, Heidelberg pp 203-215

[31] Matsui M. (1994) "Linear Cryptanalysis Method for DES Cipher". In: Helleseth T. (eds) Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. Springer, pp 386-397

[32] F. Abed, C. Forler, E. List, S. Lucks and J. Wenzel, "Biclique Cryptanalysis of the PRESENT and LED Lightweight Ciphers", Cryptology ePrint Archive, Report 2012/591, 2012.

[33] Jeong, K., Kang, H., Lee, C., Sung, J., Hong, S.: "Biclique cryptanalysis of lightweight block ciphers present, piccolo and led". IACR Cryptol. ePrint Arch. p. 621 (2012)

[34] Mouha N., Wang Q., Gu D., Preneel B. (2012) "Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming". In: Wu CK., Yung M., Lin D. (eds) Information Security and Cryptology. Inscrypt 2011. Lecture Notes in Computer Science, vol 7537. Springer, Berlin, Heidelbergpp 57-76

[35] Zhu B., Dong X., Yu H. (2019) "MILP-Based Differential Attack on Round-Reduced GIFT". In: Matsui M. (eds) Topics in Cryptology – CT-RSA 2019. CT-RSA 2019. Lecture Notes in Computer Science, vol 11405. Springer, Cham pp. 372-390

Jithendra.K.B : Completed B.Tech in Electronics and Communication from Rajiv Gandhi Institute of Technology, Kottayam, INDIA and M.Tech in Embedded Systems from National Institute of Electronics and Information Technology, Kozhikode, INDIA. Presently Working as Asst. Professor in College of Engineering, Thalassery, India and doing research from Cochin University of Science and Technology, Cochin. Areas of interests includes VLSI Design, Analog Circuits Design and Cryptography.

Shahana.T.Kassim: Professor at Cochin University of Science and Technology (CUSAT), Kerala, India. She received her Ph. D. in VLSI Design from CUSAT in 2009, M.Tech in Digital Electronics from CUSAT in 1999 and B.Tech in Electronics and Communication Engineering from Mahatma Gandhi University in 1997. Her research interests include VLSI implementation of digital systems, Digital Filters, Multi-standard wireless transceivers, RNS-based arithmetic circuits, Low-power design, Cryptography etc.