LiCi: A new ultra-lightweight block cipher

Jagdish Patil
E&TC Department
Symbiosis Institute of Technology, Pune
PUNE, INDIA
jagdishpatil108@gmail.com

Gaurav Bansod
E&TC Department
Pune Institute of Computer Technology, Pune
PUNE, INDIA
gvbansod@pict.edu

Kumar Shashi Kant
E&TC Department
Symbiosis Institute of Technology, Pune
PUNE, INDIA
kumar.kant@sitpune.edu.in

***Abstract*— In this paper, we have presented a new lightweight, low power block cipher "LiCi". The cipher LiCi has Feistel based network which operates on 64 bits plain text and with the help of 128 bits key length it generates 64 bits cipher text. This cipher design shows good performance both on hardware as well as on software platforms. As compared to the existing cipher it requires less footprint area that consumes only 1153 GE's (Gate Equivalents) and has less memory requirements. It also consumes only 30mW which is less power as compared to the other existing ciphers. LiCi cipher needs only 1944 bytes of Flash memory which is very less memory size till date. In this paper, we proposed the security analysis as well as performance parameter of the LiCi. The LiCi cipher resists the linear and differential attack. It also shows the good resistance against the advanced attack like Biclique and Zero correlation. This cipher is well suited for application where small footprint area and low power dissipation are important design metrics.**

Keywords — Lightweight Cryptography, Feistel, IoT, WSN, Encryption, Security.

I. INTRODUCTION

The Internet of Things is the latest technology which will connect the human world with the every machine. For such an application the security is essential for protecting a sensitive and vital data. The lightweight cryptography field revolves around lightweight cipher designs for low powered and constrained devices like Wireless Sensor Nodes (WSN's) and RFID devices. The most important parameters of these devices are footprint area, power consumption and Gate Equivalents (GEs). In case of RFID devices it requires around 10000 GEs for its hardware implementation and from those, maximum 2000 GEs would be available for implementation of secure algorithms in it [3]. The standard encryption algorithms like AES and DES uses around 2400 – 3500 GEs for its hardware implementation. Recently there are many lightweight ciphers like LED [3], RECTANGLE [4], PRESENT [1], MIDORI [6], PICO [7], BORON [8], and ANU [12] which are introduced for providing security in constrained environment. All these ciphers have around 1200 - 2200 GEs. The NSA has also proposed SIMON [5] and SPECK [5] block cipher lightweight family. These ciphers are the most ultra lightweight ciphers till date because they required less GEs around 1000 and have less memory requirements, but they lacks security proofs.

In this paper, we are presenting a design of a new block cipher "LiCi", which has compact design and gives less footprint area, minimum number of GEs which are around 1153 and low power consumption. The LiCi cipher resists the linear attack as well as differential attack. And it also shows the good resistance against the advanced attack like Biclique, and Zero correlation. The data complexity of the LiCi is 2^{64} and it generates more number of active S – boxes in minimum number of rounds. All these parameters will make the LiCi relevant choice for the tightly constrained application where software and hardware parameters are the most important design metrics.

II. LICI – BLOCK CIPHER

The LiCi cipher is balanced Feistel Structure network which has 31 rounds. This design supports 128 bit key. This design contains the 4 – bit i/p and 4 – bit o/p S-box. The design criterion for S-box is given in Section 3 [12]. At the key side, from 128 bit key we have extracted 32 – bits left most LSB and applied as Rki_1 and then we have extracted subsequently left 32 – bit and applied as Rki_2. After every round key is updated with the help of key scheduling algorithm which is motivated from PRESENT key scheduling [1].

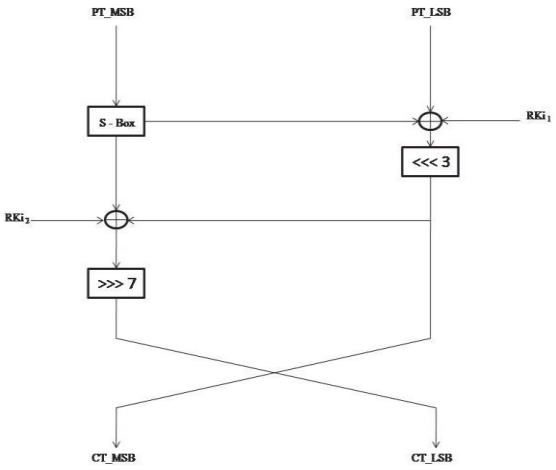

Fig. 1. The Block Cipher LiCi

The block of 64 – bit plain text is applied at the input from that PT_ MSB 32 – bit will be passed through S – box and will be substituted and will produce 32 – bit output. This output is Xor with the PT_LSB 32 bit and the left most 32 – bit LSB of Round key. The output will be passed through left circular shift block which shifts the output left circularly by 3. As shown in Fig. 1, the left circular shift output is Xor with the output of S - box and consequently LSB 32 – bit round key of

the same round. This output is fed to the right circular shift block which shifts the output right circularly by 7. These operations are repeated for 31 rounds to produce the cipher text.

A. Rationale of LiCi

Design choices of the LiCi cipher are different from existing ciphers. While designing this cipher we have focused on the hardware as well as software performance. Considering the software memory requirement, it requires only 1944 bytes of Flash memory comparatively less than other existing light weight ciphers. The hardware performance of LiCi is at par with the existing cipher as it requires only 1152 GEs for hardware implementation on ASIC platform. We have also designed lightweight S- box in the cipher design. By properly using shift operators and the design, we are able to generate maximum number of active S-boxes. When designing this cipher our main criterion is to design such an architecture that not only improves the security aspect but also make the cipher ultra lightweight.

B. Encryption Flow

The input block of 64 bits plain text is halved in two sub-block having length of 32 – bits each. It consist of 32 – bits MSB i.e. PT_MSB and 32 – bits LSB i.e. PT_LSB. The pseudo code for the cipher LiCi is given below:

```
PT = PT_MSB || PT_LSB
For i =0 to 30 do
      PT_MSB (i+1) = S[PT_MSB(i)]
      PT_LSB (i+1) = ((PT_LSB(i) ⊕ PT_MSB(i+1)⊕ Rki1 ) <<< 3)
       PT_MSB(i+1) = ((PT_MSB(i+1)⊕ PT_LSB(i+1)⊕ Rki2 ) >>> 7)
      Update Round Key ()
      CT_MSB(i) = PT_LSB(i+1)
      CT_LSB(i) =  PT_MSB(i+1)
      PT_MSB(i+1) = CT_MSB(i)
      PT_LSB(i+1) = CT_LSB(i)
End for
CT = CT_MSB ||  CT_LSB
```

C. S - Box

In LiCi cipher design, we have used 4 pin i/p and 4 pin o/p S – box. $F^4_2 \rightarrow F^4_2$ in this equation subscript 2 indicates the binary state of each i/p or o/p and the superscript 4 indicate that it has 4 bit i/p and 4 bit o/p [12][13]. Table I indicate the S – Box of LiCi cipher.

TABLE I S – BOX OF LICI

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	3	F	E	1	0	A	5	8	C	4	B	2	9	7	6	D

The 4 X 4 S – Box is described from equations which has been derived from the Karnaugh Map (K – Map). Let us consider the input $X = X_3X_2X_1X_0$ and the output $Y = Y_3Y_2Y_1Y_0$. Consider the example, X=0111 be the input of the S box, so output of the S box from Table 1 is Y=1000.

D. Key Scheduling of 128 – bit key length

Key scheduling algorithm is one of the most important parts of the any cipher this will decide the complexity of the cipher. LiCi cipher is motivated from the key scheduling algorithm of PRESENT [1] because till date there is no successful attack mounted on PRESENT key scheduling [1]. The LiCi supports user defined 128 bits key from that 64 bits are extracted and that will be used as key in the design. In the key scheduling algorithm, S – box decides the strength of the cipher [8]. K register is used to store the input 128 bit key. From that we have extracted 64 bits LSB and applied to the design [12].

$K = K_{127}\, K_{126}\, K_{125} \ldots K_2\, K_1\, K_0$

$Rki_1 = K_{31}\, K_{30}\, K_{29} \ldots K_2\, K_1\, K_0$

$Rki_2 = K_{63}\, K_{62}\, K_{61} \ldots K_{34}\, K_{33}\, K_{32}$

After extracting the 64 bits from the key register, K register will update according to following algorithm

1. K <<< 13 (K left circular shifted by 13).
2. $[K_3\, K_2\, K_1\, K_0] \leftarrow S\, [K_3\, K_2\, K_1\, K_0]$
3. $[K_7\, K_6\, K_5\, K_4] \leftarrow S\, [K_7\, K_6\, K_5\, K_4]$
4. $[K_{63}\, K_{62}\, K_{61}\, K_{60}\, K_{59}] \leftarrow [K_{63}\, K_{62}\, K_{61}\, K_{60}\, K_{59}] \oplus RC^i$

The round counter RC^i of 5 bit is Xor with 5 bit of key register i.e. from $K_{59}$to K_{63} for each respective round values [12].

III. SECURITY ANALYSIS FOR LICI

Cryptanalysis is the study of cipher and finding the plain text without knowing the key, which decides the strength of the cipher. Security analysis includes different types attacks through which we can find the resistivity of our cipher against the specific attack [8][9]. In this paper we are focusing on the basic as well as advanced attack like linear attack [11], differential attack [9], Zero correlation [12], Biclique attack [10] and Avalanche effect attack [12].

A. Design Criteria of S – Box

S-box is used to introduce non linearity in the design which plays a vital role to increase the complexity and robustness of the design. The security is the main concern of any cipher design so in order to increase the minimum number of active s – box for linear and differential cryptanalysis, S – box should be robust. In order to met all these conditions S – box should follow some important criteria which has been given in the literature [1][2][4][9][13]. Some of the essential properties for robust S – box design are as follows:

1. The S – Box is Bijective i.e. $S(p) \neq S(q)$ for all entries where $p \neq q$ [4][12].
2. The substitution should not be with the same number i.e. $S(p) \neq p$ where p is the belongs to input bits.
3. For a single bit change in input there should not be single bit change in output [12].
4. The CAR LC from the LAT defines where hamming weight of the input and hamming weight of output combination should be equal to one. i.e. HW(p) = HW(q) = 1. Where p is the input and q is the output of LAT [1][12].
5. The CAR DC value from DDT defines where hamming weight of the input and hamming weight of output combination should be equal to one. i.e. HW(p)

= HW(q) = 1 where p is the input and q is output of DDT [1][12].

B. Linear Cryptanalysis[9]

This attack is also called as plain text attack and this is also a basic attack. Every cipher should resist this attack [7]. It depends on the occurrences of high probability of linear expressions where plain text bits, cipher text bits and sub keys are accountable [12][13]. Linear approximation table values are considered while calculating the minimum number of active S – Boxes. Maximum Bias in linear approximation table can be calculated as $|P_L-1/2|$, where P_L is the linear probabilities. Bias (ε) should be calculating with considering the maximum probability in the LAT with total number of input and for LiCi cipher the maximum bias should be 2^{-2}. Matsui introduced one principle i.e. Piling-up lemma [11] for calculating the bias for 'n' rounds. Following some ways to increase the chance of resistance against linear cryptanalysis:

- By increasing the number of active S Boxes [12].
- The probability value in the LAT should be as less as possible, ideally the bias value should be 1/8 which is quite impossible practically [12].

Here in LiCi cipher, for round 4 there are 13 minimum numbers of active S – Box. Following table II shows the minimum count for active S – Boxes from linear trials.

TABLE II MINIMUM NUMBER COUNT OF ACTIVE S – BOXES FROM LINEAR TRAILS

Rounds	Minimum no. of active S – Box
1^{st}	1
2^{nd}	3
3^{rd}	7
4^{th}	13

Similarly, for 16 rounds, there are total 52 active S – Boxes. By applying the pilling up lemma for round 4,

$$\varepsilon = 2^{(\text{no. of active S Box } - 1)} \times (\text{Max. Bias})^{(\text{no. of active Sbox})}$$
$$= 2^{(13-1)} \times (2^{-2})^{13}$$
$$= 2^{-14}$$

Hence, for round 4 the maximum bias is 2^{-14}, so for round 16 the maximum bias is given by,

$$\varepsilon = 2^{(4-1)} \times (2^{-14})^4$$
$$\varepsilon = 2^{-53}$$

Hence for round 16 the maximum bias is 2^{-53}, so complexity of the known plain text can be calculated by using the formula:

$$N_L = 1/(\varepsilon)^2$$

Known plain text of LiCi cipher for round 16 is 2^{106}.So we can conclude that the total number of known plain text is 2^{106} which is greater than 2^{64}. This shows the LiCi cipher is resistible to linear attack [12].

C. Differential Cryptanalysis[8][9]

This attack is also very important and basic attack which was successfully applied on DES in 1990 [2]. In this attack, we have found out the trails using difference distribution table (DDT). The DDT has been initiated with the help of high probability input and output differences. The trails which are derived from the DDT give the minimum number of active S – boxes. The differential probability of the LiCi cipher is 2^{-2} [12]. Following are the some ways to increase the resistance of cipher against differential cryptanalysis.

- The probability value in the DDT should be as less as possible, ideally the bias value should be 1/16 [12].
- By increasing the number of active S – boxes [12].

In LiCi cipher, for round 4, there are 12 minimum number of active S – boxes. Following Table III shows the minimum count of active S – Boxes from differential trails.

TABLE III MINIMUM NUMBER OF ACTIVE S-BOXES FROM DIFFERENTIAL TRAIL

Rounds	Minimum no. of active S – Box
1^{st}	1
2^{nd}	2
3^{rd}	6
4^{th}	12

Similarly, for round 16 there are total 48 active S – boxes. Hence, the differential probability can be given by the formula:

$$Pd = (2^{-2})^{\text{Total number of active S – Boxes}} = 2^{-96}$$

Hence, the complexity of the differential attack can be calculated with the help of the chosen plain text which can be given as,

$$Nd = C/Pd$$

Where C = 1 and $Pd = 2^{-96}$ so, $Nd = 1/2^{-96} = 2^{96}$.
From the above computation we can say that the differential complexity of the LiCi cipher is 2^{96} which is greater than 2^{64} which depicts that LiCi is resistible to Differential attack with a block length of 64.

D. Zero Correlation Attack- The Advance Attack

Zero correlation [7][8][12][13] attack is the extension of linear approximation. The cipher should resist this attack. Here we have used the Matrix method to mount the zero correlation attack. In this attack, we are changing one bit of input and finding the corresponding cipher text with respect to some predefined rules. (0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 000a) (b000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000) in this correlation the values of a and b are non zero. Following table IV shows the trails for zero correlation attack and found the contradiction at round 3.

TABLE IV TRAILS OF ZERO CORRELATION FOR LICI

	P_L^i	P_R^i
0	0000 0000 0000 0000 0000 0000 0000 0000	0000 0000 0000 0000 0000 0000 0000 000a
1	0000 0000 0000 0000 0000 0000 0000 a000	0000 0000 0000 0000 0000 0000 0000 0000
2	0000 0000 0000 0000 0000 0000 0000 0000	0000 0000 0000 0000 0000 0000 0000 0000
3	000* 00*0 0000 0000 0000 0000 0000 0000	0000 0000 00*0 0*00 0000 0000 0000 0000
3	00b0 0000 000b 0000 0000 0000 000b 000*	00b0 0000 000b 0000 0000 0000 000b 0000
4	0000 00b0 0000 0000 0000 0000 0000 000b	0000 00b0 0000 0000 0000 0000 0000 000b
5	000b 0000 0000 0000 0000 0000 0000 0000	000b 0000 0000 0000 0000 0000 0000 0000
6	b000 0000 0000 0000 0000 0000 0000 0000	0000 0000 0000 0000 0000 0000 0000 0000

E. Biclique Attack

This attack is the theoretical attack, which decides the data complexity and computational complexity of the cipher. Biclique attack is the extension of meet in the middle attack (MITM) [10][12][13]. It is based on the key selection which is the important factor because it decides the complexity without interacting of two different types of keys. Here we are focusing on to the 4-Dimension key and implemented MITM for round 28, 29, 30 and 31.

The partial key position at respective rounds is stated as follows:

$$K^{28} = K_{83}, K_{82}\ldots\ldots\ldots K_{20}$$
$$K^{29} = K_{70}, K_{69}\ldots\ldots\ldots\ldots K_{7}$$
$$K^{30} = K_{57}, K_{56},\ldots K_{0}, K_{127}\ldots\ldots K_{122}$$
$$K^{31} = K_{44}, K_{43},\ldots K_{0,} K_{127}\ldots\ldots K_{109}$$

From position of above partial keys it was found that by varying (K_{42}, K_{41}, K_{40}, K_{39}) and (K_3, K_2, K_1, K_0) gives biclique on full LiCi. The biclique attack is mounted on LiCi cipher. The computational complexity is depicted through following formula [12][13],

$$C_{total} = 2^{k-2d}\,(C_{biclique} + C_{precomp} + C_{recomp} + C_{falsepos}) = 2^{127.513}$$

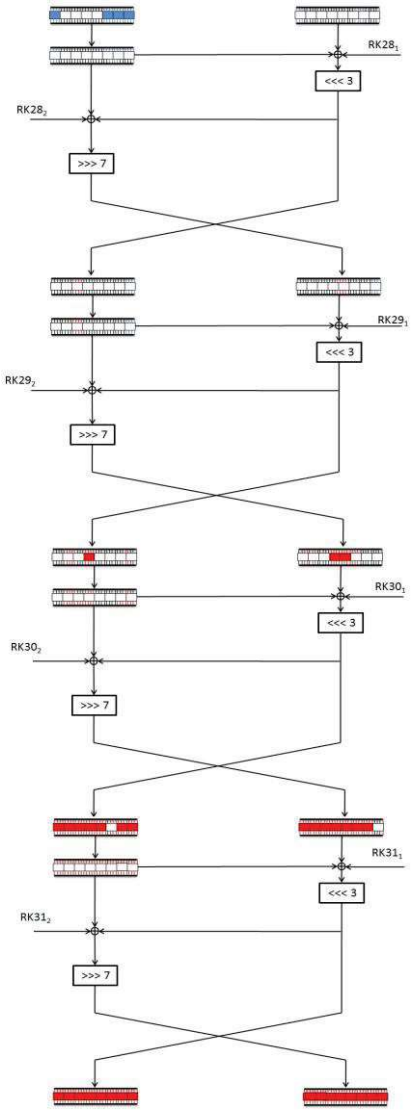

Fig. 2. Biclique Attack mounted on LiCi Cipher

F. Avalanche Effect

The avalanche effect shows the randomization nature of the cipher and strong cryptanalytic properties such that at any circumstances one cannot predict the input plain text [12]. The avalanche effect states that the single bit change in input i.e. plain text should give the 50% bits change in output i.e. cipher text with considering some +/- 1 bit tolerance[12].

The following Table V shows some sample set for LiCi cipher and gives nearly 50% output bit change.

TABLE V AVALANCHE EFFECT

Plaintext	0000 0000 0000 0000	NO. of bits changes
Key	0000 0000 0000 0000	-
	0000 0000 0000 0000	
Cipher text	7e7cea1868997560	
Key	0000 0000 0000 0000	37
	0000 0000 0000 0001	
Cipher text	b2f28489ef3c82db	
Key	0008 0000 0000 0000	30
	0000 0000 0000 0000	
Cipher text	29e07be96ffb6f31	

IV. PERFORMANCE OF LICI CIPHER

This section shows the comparison between the LiCi cipher and standard existing lightweight ciphers. This comparison is based on the security analysis, hardware performance, software performance and power consumption [12]. Following table VI shows the comparison of the linear and differential complexity.

TABLE VI LINEAR & DIFFERENTIAL ATTACK COMPARISON

Cipher Name	LiCi	PRESENT	L-Block	PICO
#Rounds	16	25	15	24
#Known Plaintext	2^{106}	2^{102}	2^{66}	2^{90}
#Chosen Plaintext	2^{96}	2^{100}	2^{64}	2^{96}
Reference	This paper	[1]	[3]	[7]

With compared to other existing ciphers the hardware performance of the LiCi cipher results in less number of GEs i.e. 1153. Fig. 3 shows the comparison of GEs with existing lightweight ciphers.

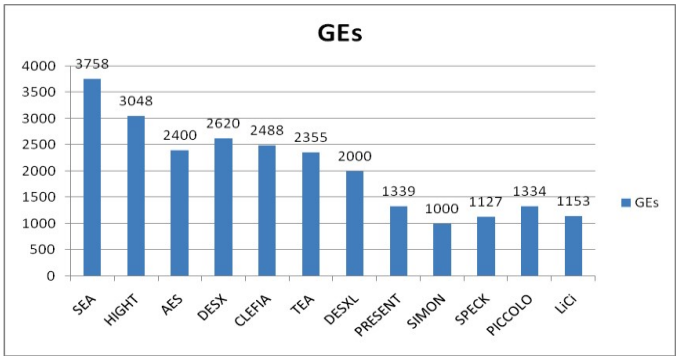

Fig. 3. Comparison of GEs of LiCi cipher with existing lightweight cipher.

All the ciphers like PRESENT, RECTANGLE, LED and SIMON are tested on the LPC 2129 platform. Following Fig. 4 shows the comparison of flash memory and RAM memory of LiCi cipher with other lightweight ciphers.

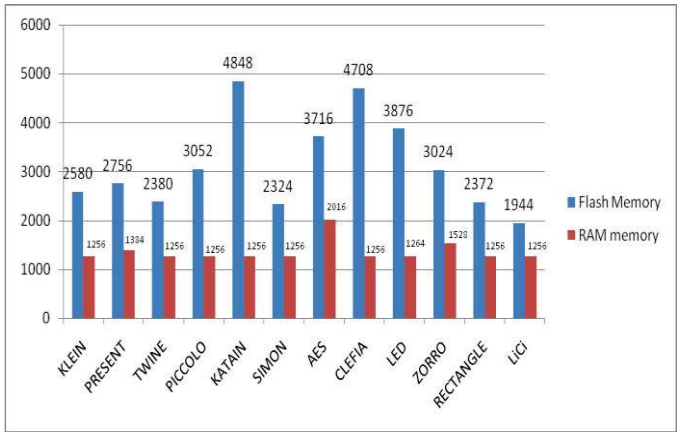

Fig. 4. Flash Memory and RAM memory comparison of LiCi cipher.

Following table VII gives the comparisons based on the Execution time, through put and number of cycles of LiCi cipher with standard existing lightweight ciphers [12].

TABLE VII COMPARISON OF EXECUTION TIME, THROUGHPUT AND NUMBER OF CYCLES

Ciphers	Block Size	Key Size	Execution Time (In uSec)	Throughput (In Kbps)	No. of Cycles
SP NETWORK					
LED	64	128	7092.86	9	425572
KLEIN	64	96	887.51	72	10650.12
HUMMINGBIRD-2	16	128	316.51	51	3798.12
PRESENT	64	128	2648.65	24.16	31783.8
FEISTEL STRUCUTRE					
SPECK	64	128	49.02	1305	588.24
SIMON	64	128	105.67	605	1268.04
PICCOLO	64	128	227.68	281	2732.16
CLEFIA	128	128	1048.01	122	12576.12
TWINE	64	128	592.87	108	7114.44
LiCi	64	128	209.87	305	2518.44

We have calculated power consumption of the LiCi cipher with the help of X power tool which is part of ISE design suit 14.2 (Xilinx) with 10MHz. We have calculated power with VERTEX VI family [12]. The following Fig. 5 show the comparison of dynamic power consumption between LiCi cipher and existing lightweight ciphers.

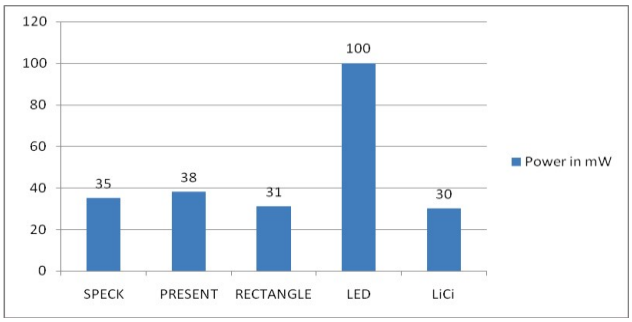

Fig. 5. Comparison of power consumption of LiCi and standard existing ciphers.

V. Conclusion

This paper presents balanced Feistel lightweight block cipher "LiCi". LiCi needs 1153 GEs for 128 bit key and have very less memory requirement which is 1944 Flash memory bytes. LiCi cipher design also results in less power dissipation around 30mW for encrypting 64 bit of plaintext with 128 bit key size. LiCi cipher not only resists basic attacks, but it also shows good resistance against advance attack. We believe the LiCi cipher design is best suited for applications where metrics like memory size and gate equivalents are the major constraints.

Test Vector of LiCi with 128 bit key

Plaintext	Key	Cipher text
00000000 00000000	00000000 00000000 00000000 00000000	7e7cea1868997560
00000000 00000000	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF	198fa9d74394a18f

References

[1] A. Bogdanov, G. Leander, L.R. Knudsen, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT - An Ultra-Lightweight Block Cipher," In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems — CHES 2007*, Vol. 4727 in *LNCS*, pp. 450-466, Springer Berlin Heidelberg, 2007.

[2] D Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks", IBM Thomas J Watson Research Center technical report RC 18613 (81421), 22 December 1992.

[3] A. Poschmann. Lightweight Cryptography - Cryptographic Engineering for a Pervasive World. Number 8 in IT Security. Europ¨aischer Universit¨atsverlag, 2009.Published: Ph.D. Thesis, Ruhr University Bochum.

[4] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, "RECTANGLE: A bit-slice ultra-lightweight block cipher suitable for multiple Platforms" *Cryptology ePrint Archive, Report 2014/084, 2014*. Available at https://eprint.iacr.org/2014/084.pdf.

[5] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. In IACR eprint archive. Available at https://eprint.iacr.org/2013/404.pdf.

[6] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni, "Midori: A Block Cipher for Low Energy (Extended Version)", In IACR eprint archive. Available at https://eprint.iacr.org/2013/404.pdf.

[7] Bansod, Gaurav, Narayan Pisharoty, and Abhijit Patil. "PICO: An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing."*Defence Science Journal* 66.3 (2016): 259-265.

[8] G BANSOD, N PISHAROTY, A PATIL, "BORON: an ultra lightweight and low power encryption design for pervasive computing", Frontiers, 2016.

[9] Howard M. Heys, "A Tutorial on Linear and Differential Cryptanalysis" http://citeseer.nj.nec.com/443539.html.

[10] Jeong, K., Kang, H., Lee, C., Sung, J., Hong, S.: "Biclique Cryptanalysis of Lightweight Block Ciphers PRESENT, Piccolo and LED", *Cryptology ePrint Archive, Report 2012/621*.

[11] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology, Proc. Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 386–397.

[12] G Bansod, A Patil, S Sutar, N Pisharoty "*An Ultra Lightweight Encryption Design for Security in Pervasive Computing*", Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016.

[13] Dr. Gaurav Bansod, "*A New Ultra Lightweight Encryption Design for Security at Node Level"*, International Journal of Security and its applications, Vol. 10, No. 12(2016) pp. 111-128.