2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security

An Ultra lightweight encryption design for security in pervasive computing

GAURAV BANSOD
ETC Department
Symbiosis Institute of Technology, Pune
PUNE, INDIA
gauravb@sitpune.edu.in

ABHIJIT PATIL
ETC Department
Symbiosis Institute of Technology, Pune
PUNE, INDIA
abhijit.patil@sitpune.edu.in

SWAPNIL SUTAR
ETC Department
Symbiosis Institute of Technology, Pune
PUNE, INDIA
swapnil.sutar@sitpune.edu.in

N. PISHAROTY
ETC Department
Symbiosis Institute of Technology, Pune
PUNE, INDIA
narayanp@sitpune.edu.in

***Abstract*— This paper proposes an ultra light weight cipher ANU. ANU is 25 round lightweight cipher which supports 80/128 bit key scheduling. It needs only 934 GEs for 128 bit key which is very less as compared to all existing cipher. ANU cipher design shows good resistance against basic and advanced attacks. This paper furnishes security analysis of the ANU cipher. ANU design not only results in small footprint area but it also consumes very less power. ANU design will be best suitable for applications like IoT, Wireless sensor nodes where memory and power consumption are the major constraints.**

Keywords—Lightweight cryptography, Feistel cipher, Block cipher, IoT, Encryption, Embedded security

I. INTRODUCTION

Lightweight cryptography is the emerging field which supports cipher design that results in small footprint area. The important parameter in lightweight cipher design is GEs (Gate Equivalents). Lightweight ciphers are specifically used in the applications where memory size, power, footprint are the major constraints. RFID used 10000 GEs for its design. In order to secure these deign cipher GEs should be less than 2000 GEs. AES and DES are the standard encryption standards which have GEs around 2400-3500. This led to the emergence of a new field called lightweight cryptography.

Lightweight cipher can be either block cipher or stream cipher. Most of the existing cipher is block cipher as it is known as workhorse in the cryptographic enviornment. Block ciphers are classified as Feistel structure and SP network. PRESENT [1], LED, mCrypton these are the existing lightweight SP network ciphers while SIMON [2], SPECK [2], and CLEFIA [3] these are the Feistel structured. Feistel structure is again divided into GFS (Generalized Feistel structure) and CFS (Classical Feistel Structure). If block size is divided into more than two parts, such structure is identified as GFS. GFS require more number of rounds to provide optimum level of security. CLEFIA developed by SONY is an example of GFS.

The cipher like PRESENT, SIMON, and SPECK have compact design and smaller number of GEs. PRESENT is designed by considering the compactness and has strong permutation layer. RECTANGLE cipher has strong cryptanalysis properties as well as strong S-box. SIMON and SPECK are considered as the most compact cipher for software and hardware performance. In this paper, we propose an ultra lightweight cipher which attains an optimal security with lesser number of GEs, minimal Flash memory and less power consumption. The design of ANU cipher results in maximum data complexity and maximum number of active S-boxes in minimum rounds. These results make an ANU cipher an obvious choice for low resourced pervasive devices.

For ANU cipher we have used the following notations

- PT	64-bit input plaintext block
- CT	64-bit output cipher text block
- RKi	128-bit Round sub key for round i
- F	Function
- ⊕	Bitwise exclusive-OR operation
- <<<n	Left cyclic shift by n bits
- >>>n	Right cyclic shift by n bits
- RC_i	Round counter i
- ||	Concatenation of two strings
- !	Bitwise NOT operation
- 64 bits	Maximum length of plain text

II. THE BLOCK CIPHER ANU

The ANU Cipher is 25 rounds Feistel based block cipher. It has 64 bit block length and 128 bit key length. Fig 1 shows the round function of the ANU cipher.

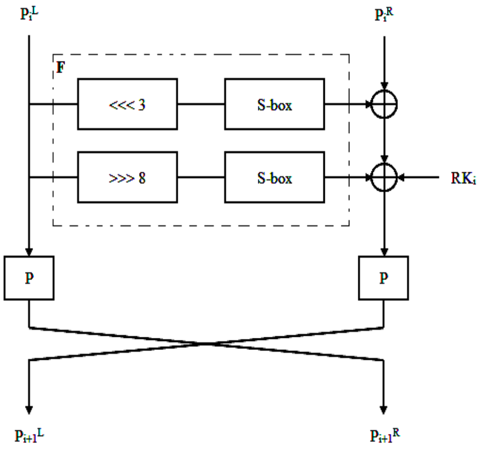

Figure 1. Block Diagram of ANU cipher

The 64 bit plaintext block divided into two parts of 32 bit block. F-function has circular shift operator and substitution box. Results from F-function is EX-ORed with the least significant 32 bit and sub key RKi. 25 different sub keys are generated using 128 bit key scheduling algorithm in the ANU cipher.

978-1-5090-2403-2/16 $31.00 © 2016 IEEE
DOI 10.1109/BigDataSecurity-HPSC-IDS.2016.29

A. Encryption algorithm

64-bit input plaintext is divided into two 32-bit plaintext, P_0^L and P_0^R. P_0^R consist of LSB 32-bits and P_0^L consist of MSB 32-bits.

$PT \leftarrow P_0^L \,||\, P_0^R$

Encryption Flow

1 Apply F function on P_i^L

$$P \leftarrow F\,(P_i^L)$$

2 XOR with $P_i^R$and RKi

$$P_t \leftarrow P \oplus P_i^R \oplus RKi$$

3 Apply bit permutation layer

$$P_{i+1}^R = BP[P_i^L]$$
$$P_{i+1}^L = BP[P_t]$$

After 25 rounds we will get the 64-bit cipher text which is concatenations of P_{25}^L and P_{25}^R.

$$CT \leftarrow P_{25}^L \,||\, P_{25}^R$$

B. F-function

F-function of the ANU cipher includes circular left shift by 3 with S-box and another branch which has circular right shifts by 8 with S-box again. P_i^L is input to F-function and P_i^R is EX-ORed with the output of F-function and sub key for a particular round. Operation of F-function depicted in Fig. 1

$$F: \{0, 1\}^{32} \leftarrow \{0, 1\}^{32}$$

C. S-BOX

S box is the only non linear element in cipher deign. It increases strength of the cipher and helps design to resist against basic attacks. The S-box used in ANU cipher design is of 4-bit to 4-bit S-box S: $F_2^4 \rightarrow F_2^4$. 4x4 S-box of ANU is compact in design and needs less footprint area in hardware implementation. TABLE I represents the hexadecimal values for the Substitution layer

TABLE I. S-BOX OF ANU CIPHER

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	2	9	7	E	1	C	A	0	4	3	8	D	F	6	5	B

D. Bit Permutation

In block cipher, bit permutation shuffles the bits in such a way that it results in a high diffusion mechanism. The combine operation of circular shifting and permutation layer will increase the count in minimum number of active S-Boxes. We have used followed the criterions for designing of P layer which are mentioned in [4].

- At round r, the output of S-box is distributed in such a way that the two of them affects the middle bits of S-box at round r+1 and other two affects the end bits.
- Four outputs from each S-box affects the four different S-boxes.

TABLE II. BIT PERMUTATION OF ANU CIPHER

i	00	01	02	03	04	05	06	07
BP[*i*]	20	16	28	24	17	21	25	29
i	08	09	10	11	12	13	14	15
BP[*i*]	22	18	30	26	19	23	27	31
i	16	17	18	19	20	21	22	23
BP[*i*]	11	15	03	07	14	10	06	02
i	24	25	26	27	28	29	30	31
BP[*i*]	09	13	01	05	12	08	04	00

Encryption Algorithm

```
Input-
Plaintext: $A_{64} \rightarrow a^{63}\,a^{62}\,a^{61}\,a^{60} \ldots a^3\,a^2\,a^1a^0$, S[16],BP[32],
Output-
Ciphertext: $C_{64}$

For i = 0 to 24 do
$P_i^L \rightarrow a^{63}\,a^{62}\,a^{61}\,a^{60} \ldots a^{35}\,a^{34}\,a^{33}a^{32}$
$P_i^R \rightarrow a^{31}\,a^{30}\,a^{29}\,a^{28} \ldots a^3\,a^2\,a^1a^0$

Pt1 $\rightarrow$ Sbox [LCS($P_i^L$,3)]
Pt2 $\rightarrow$ Sbox [RCS($P_i^L$,8)]
        Pt $\rightarrow$ Pt1$\oplus$ Pt2$\oplus$RKi
        $P_{i+1}^R \rightarrow BP[P_i^L]$
        $P_{i+1}^L \rightarrow BP[Pt]$

$A_{64} \rightarrow$   $P_{i+1}^L \,||\, P_{i+1}^R$
i = i+1
End
$C_{64} \rightarrow$   $A_{64} \rightarrow P_{25}^L \,||\, P_{25}^R$
```

E. Key Scheduling of 80 bit and 128 bit key length:

Key schedule of the ANU cipher is motivated from the PRESENT cipher key scheduling design. No attacks till date are reported on the PRESENT cipher key scheduling. In the ANU cipher, key scheduling algorithm generates total of 25 sub-keys each of size 32 bit.

128-bit key scheduling

A user defined 128-bit key is stored in the register KEY, 64-bit LSB's from KEY register is extracted as follows

$K^i = K_{31}\,K_{30} \ldots K_2\,K_1\,K_0$

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

After extracting key of 64-bits, register KEY is updated in the following manner

1. KEY <<< 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. $[K_{63}\,K_{62}\,K_{61}\,K_{60}\,K_{59}] \leftarrow [K_{63}\,K_{62}\,K_{61}\,K_{60}\,K_{59}] \oplus RC^i$

For 0 to 24 rounds, 5-bits of round counter i is XOR-ed with the 5-bits of key register KEY i.e. from $K_{59}$to $K_{63.}$

80 bit Key scheduling

A user defined 80-bit key is stored in key register KEY and LSB bits from it are used as round sub-keys.

$K^i = K_{31}\, K_{30} \ldots K_2\, K_1\, K_0$
$KEY = K_{79}\, K_{78}\, K_{77} \ldots K_2\, K_1\, K_0$
After extracting 64-bit key, register KEY is updated as follows
1. KEY<<< 13.
2. $[K_3\, K_2\, K_1\, K_0] \leftarrow S\, [K_3\, K_2\, K_1\, K_0]$.
3. $[K_{63}\, K_{62}\, K_{61}\, K_{60}\, K_{59}] \leftarrow [K_{63}\, K_{62}\, K_{61}\, K_{60}\, K_{59}] \oplus RC^i$

III. Security Analysis of ANU

Cryptanalysis is way to know useful information about the key either from cipher text or plaintext. This information served us the strength of designed lightweight cipher. In this paper, we have focused on basic attacks like linear and differential cryptanalysis as well as on advance attacks like biclique attack, zero correlation attack. S-box is the only non linear element in cipher design. We chose S- box for cipher design in such a way that it should able to resist all possible types of attacks and should result in compact implementation.

A. Design criteria of S-box

The block cipher should resist linear and differential attack where this resistivity depends mainly on the design of S-box. ANU cipher has 4x4 S-box i.e. it takes 4 bit input and generates 4 bit output. The important criterions for S- box selection mentioned previously in RECTANGLE and PRESENT cipher are used for the S- box of ANU too which are discussed below:

Complete design criteria of the ANU S-box is as follows:

- For any nonzero input and output differences $\triangle A$, $\triangle B \in F_2^4$ respectively we have

  $DC\ (\triangle A,\ \triangle B) = \#\ \{A \in F_2^4\ |S\ (x) \oplus S\ (x \oplus \triangle A) = \triangle B\} \leq 4$

- For any nonzero input and output differences $\triangle A$, $\triangle B \in F_2^4$ respectively we have such that $Hw(\triangle A) = Hw(\triangle B) = 1$, where $Hw(x)$ denotes the Hamming weight of x, we have

  $SetDC = DC\ (\triangle A,\ \triangle B) = \#\ \{A \in F_2^4\ |S\ (x) \oplus S\ (x \oplus \triangle A) = \triangle B\} = 0$

  Cardinality of SetDC can be given as CarDC, we have CarDC = 0.

- For any nonzero input sum and output sum such that $A, B \in F_2^4$ so we have

  $LC(A, B)\ LC\ (A, B) = \#\{x \in F_2^4 | A \bullet x = B \bullet S(x)\} - 8| \leq 4$

- For any nonzero input sum and output sum such that $A, B \in F_2^4$, such that $Hw(a) = Hw(b) = 1$, we have

  $SetLC = LC\ (A, B) = \#\{x \in F_2^4 | A \bullet x = B \bullet S(x)\} - 8| \neq 0$

  Cardinality of SetLC can be given as CarLC, we have CarLC = 4.

- Bijective i.e. $S\ (a) \neq S(b)$ for all values of $a \neq b$.
- No static point i.e. $S\ (a) \neq a$ for all values of $a \in F_2^4$.

B. Linear cryptanalysis

Linear cryptanalysis [5] is the most basic and significant attack. It is also known as known plaintext attack and cipher should resist such attack. It uses the high probability occurrences of linear expression containing plaintext bits, cipher text bits and sub key bits. This expression is used for mounting a linear attack on a cipher. To mount a linear attack, the attacker needs to have the knowledge about a subset of the plaintext and its corresponding cipher text. The attacker will find the correlation between them. The S-box is examined by forming the Linear Approximation TABLE (LAT). If P_L is the linear probability then its bias can be given as $|P_L\text{-}1/2|$, bias (ε) for the ANU cipher S-box is 2^{-2}. Matsui`s Piling-up lemma [6] is used to calculate probability bias for 'n' rounds.

The best way to resist against linear cryptanalysis is,

- Optimizing the bias in the LAT. For ideal S-box bias, values should be 1/8 which is practically not possible to achieve.
- Increase the number of active S-boxes in the cipher structure.

TABLE III represents minimum number of active S-boxes from linear trails

TABLE III. Minimum Number of Active S-boxes From Linear Trail

#Round	# Min. active S-boxes
1	0
2	2
3	9
4	19

Theorem1:
For 18 rounds of ANU, it has total 54 active S-boxes and the total bias for 18 rounds is 2^{-55}.
Proof:
It was found that for 3 rounds ANU has minimum 9 active S-boxes. Maximum bias for the ANU cipher S-box is 2^{-2} by using Matsui`s Pilling up Lemma for 3 rounds of ANU cipher the total bias can be given as,

$$2^8 \times (2^{-2})^9 = 2^{-10}$$

By applying the same lemma for 18 rounds the total bias (ε) can be given as,

$$\varepsilon = 2^5 \times (2^{-10})^6 = 2^{-55}$$

By calculating required number of known plaintext / cipher text, complexity of linear attack can be computed and can be given as,

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

For 18 rounds of the ANU cipher, the required number of known plaintext / ciphertext can be given as

$$N_L = 1/\ (\varepsilon)^2 = 1/\ (2^{-55})^2$$
$$N_L = 2^{110}$$

The required number of known plaintext / cipher text is 2^{110} which is greater than the available limit i.e. 2^{64}. Hence, the complete rounds of the ANU cipher show a good resistance against a Linear Attack.

C. *Differential cryptanalysis*

Differential attack [7] is also the most significant attack and cipher should resist such attack. Biham and Shamir first applied a differential attack on DES in 1990. To mount the differential attack for a specific number of rounds in an encryption system, pairs of high probability input and output occurrences are used to recover the round keys. S-box is a nonlinear component in our design and it gets examined by forming the Difference Distribution TABLE (DDT). Differential trails are formed by considering high probability input and output difference for each round, S-box that has non-zero input difference or non-zero output difference is referred to as an active S-box.

Differential probability for the ANU cipher S-box is 4/16 = 1/4 = 2^{-2}.

There are two approaches for providing security against differential cryptanalysis

- By minimizing the differential probability, for an ideal S-box, this probability is 1/16.
- It is necessary to find a structure that maximizes the minimum number of active S-boxes.

TABLE IV represents the minimum number of active S-boxes from differential trails

TABLE IV. MINIMUM NUMBER OF ACTIVE S-BOXES FROM DIFFERENTIAL TRAIL

#Round	# Min. active S-boxes
1	0
2	2
3	8
4	18

For 3 rounds of the ANU cipher, there are a minimum of 8 active S-boxes. So, for 18 rounds, there will be a minimum of 48 active S-boxes. Total differential probability P_d is given as $(2^{-2})^{48} = 2^{-96}$.

The complexity of the differential attack can be computed by calculating the required number of chosen plaintext / cipher text and can be given as,

$$N_d = C/P_d$$

Where C = 1 and $P_d = 2^{-96}$, so the required number of chosen plaintext / cipher text are

$$N_d = 1/2^{-96} = 2^{96}.$$

The required numbers of chosen plaintext / cipher text is 2^{96} which are greater than available limit i.e. 2^{64}; hence complete rounds of the ANU cipher provide resistance against a Differential Attack.

D. *Zero-correlation attack[8]*

The cipher should resist zero correlation attack; it is extension of linear approximation. Matrix method adopted here to mounting zero correlation attack. It is based on linear approximation with correlation value of zero. For (0a00000000000000) → (000000000b000000) has correlation exactly zero for which the values a and b are non-zero. Trails for zero correlation attack are shown in TABLE V and the contradiction was found at round 4 for the ANU cipher.

TABLE V. TRAILS FOR ZERO-CORRELATION FOR ANU CIPHER

	P_L^i	P_R^i
0	0000 0000 0000 0000 0000 aaaa 0000 0000	0000 0000 0000 0000 0000 0000 0000 0000
1	0000 0000 0000 0000 0000 0000 0000 0000	0a00 0a00 0a00 0a00 0000 0000 0000 0000
2	0000 0000 0000 0000 0000 0000 0a0a a0a0	0000 0000 0000 0000 0000 0000 0000 0000
3	0000 0000 0000 0000 0000 0000 0000 0000	0000 00aa 0000 00a* 0000 0000 0000 0000
4	0000 0000 0000 0000 a0a0 *0a0 0000 0000	0000 *000 **0* *00* 0**0 0*** 0**0 00*0
4	0000 **** *0** 0000 **** 0*00 0*00 *000	0*00 0000 0000 bbbb 00*0 0000 0000 0000
5	0000 00*0 0000 0000 000b 0*b0 000b 00b0	0000 0000 0000 0000 0000 0000 0000 0000
6	0000 0000 0000 0000 0000 0000 0000 0000	0b0b 0b0b 0000 0000 0000 0000 0000 0000
7	0000 0000 0000 0000 000b 00b0 000b 00b0	0000 0000 0000 0000 0000 0000 0000 0000
8	0000 0000 0000 0000 0000 0000 0000 0000	0000 0000 0000 bbbb 0000 0000 0000 0000

E. *Biclique attack*

The meet in the middle attack has extension named as biclique attack [9]. In this paper, biclique attack is mounted on ANU cipher from round 21~24 and it is a 3 dimension biclique. For these rounds, the partial keys used are (K^{21}, K^{22}, K23, and K24). The key positions for biclique attack according to key scheduling algorithm are mentioned below:

K21 = K15, K14,…K0,K127 ….. K111
K22 = K1K0,K127 ….. K98
K23 = K116, K115…….. K85
K24 = K103, K102, ….. K72

From the above equations, it was found that by varying the following sub keys (K_{14}, K13, K12) and (K_{120}, K119, K118), it gives Biclique on the full ANU. To construct the Δi-differential, sub keys (K_{14}, K13, K12) have been considered and for the ∇j-differential, sub keys (K_{120}, K119, K118) have been considered. Computational complexity obtained from biclique is,

$$C_{total} = 2^{k-2d} (C_{biclique} + C_{precomp} + C_{recomp} + C_{falsepos}) = 2^{127.75}$$

Fig. 2 represents the biclique attack mounted on ANU cipher for round 21~24.

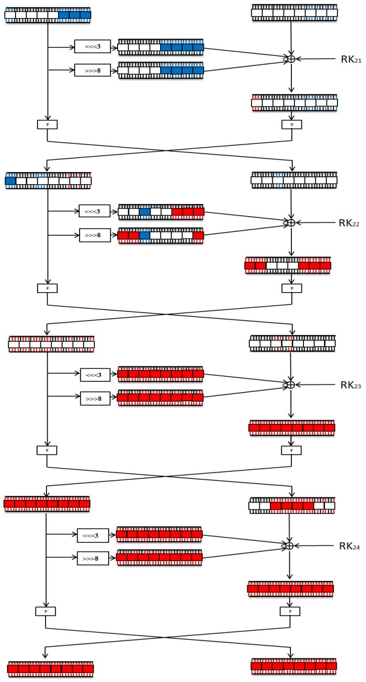

Figure 2. 3-dimensional Biclique for ANU

F. Avalanche effect

Significant change in output with change in single bit at input plaintext, this result in avalanche effect. Drastic change in output with single bit input change achieved robust cipher design. Poor randomization occurs when a block cipher does not show the avalanche effect to a significant degree.

The output obtained by applying a single bit change in the input plaintext / Key bits was observed. It was found that in the case of the ANU cipher any single bit change in key results in changes nearly half of the bits of cipher text. TABLE VI summarizes the Avalanche Effect.

TABLE VI. AVALANCHE EFFECT FOR ANU

Plaintext	0000 0000 0000 0000	NO. of bits changes
Key Cipher text	0000 0000 0000 0000 0000 0000 0000 0000 53b4 6545 6af0 3349	
Key Cipher text	0000 0000 0000 0000 0000 0200 0000 0000 96e9 6b2d d117 76b8	35
Key Cipher text	0000 1000 0000 0000 0000 0000 0000 0000 6e8f 4bcc 7b8e 246c	35

IV. SECURITY COMPARISON WITH STANDERD ALGORITHM

ANU cipher is compared with existing lightweight cipher based on security parameters, GEs, memory size and power consumption. TABLE VII compares the linear complexity and differential complexity by considering the minimum number of active S-boxes for particular rounds. TABLE VIII compares the data complexity and computational complexity of ANU with existing lightweight cipher.

TABLE VII. LINEAR AND DIFFERENTIAL ATTACK COMPARISONS

Cipher Name	ANU	PRESENT	L-Block	FEW	PICCOLO
#Rounds	18	25	15	27	30
#Known Plaintext	2^{110}	2^{102}	2^{66}	2^{90}	2^{120}
#Chosen Plaintext	2^{94}	2^{100}	2^{64}	2^{90}	2^{120}
Reference	This paper	[1]	[23]	[24]	[25]

TABLE VIII. BICLIQUE ATTACK COMPARISON

Cipher Name	Rounds	Data Complexity	Computational Complexity	Reference
ANU-128	Full(31)	2^{64}	$2^{127.75}$	This Paper
PRESENT-80	Full(31)	2^{23}	$2^{79.54}$	[9]
PRESENT-128	Full(31)	2^{19}	$2^{127.42}$	[9]
PICCOLO-80	Full(25)	2^{48}	$2^{79.13}$	[9]
PICCOLO-128	Full(31)	2^{24}	$2^{127.35}$	[9]
LED-64	Full(48)	2^{64}	$2^{63.58}$	[9]
LED-80	Full(48)	2^{64}	$2^{79.37}$	[9]
LED-96	Full(48)	2^{64}	$2^{95.37}$	[9]
LED-128	Full(48)	2^{64}	$2^{127.37}$	[9]

ANU cipher has achieved the better results as compared to other existing ciphers. Fig. 3 Shows GEs comparison of ANU with existing standard algorithms

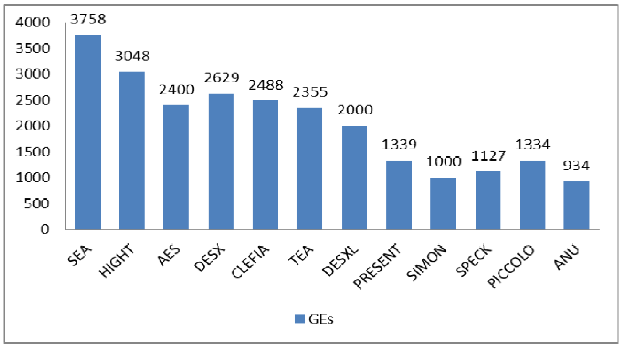

Figure 3. GEs Comparison of Standard algorithms with ANU cipher

ANU results in 934 GEs for 128 bit scheduling which is the smallest design till date. Fig. 4 shows the Flash memory and RAM memory comparison with standard lightweight algorithms.

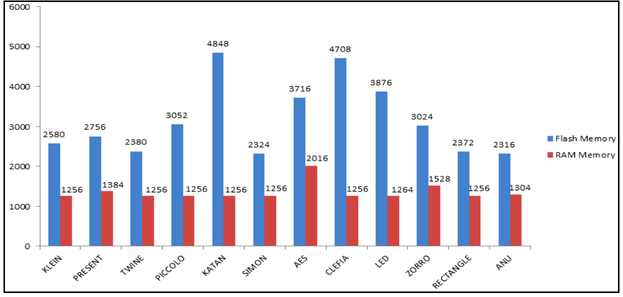

Figure 4. Flash memory and RAM memory Comparison of Standard algorithms with ANU Cipher implemented on LPC2129

TABLE IX shows the gate equivalent comparison of ANU cipher to existing cipher. From TABLE IX we can conclude that ANU achieved the best result as compared to existing lightweight ciphers. ANU GE's are 30% less than the PRESENT cipher.

TABLE IX. GEs COMPARISON OF ANU

	PRESENT	SIMON	SPECK	PICCOLO
ANU	-30.24%	-6.60%	-17.12%	-29.98%

We have calculated the power consumption by using X-power analyzer tool available in ISE design suit 14.2. Power is calculated with 10MHz frequency and on VIRTEX VI family. TABLE X represents the dynamic power consumption of standard ciphers and its comparison with ANU cipher. ANU cipher consumes only 22mw of dynamic power which is lesser than the other lightweight ciphers. PRESENT consumes nearly 38mW of power, LED consumes 100mW and RECTANGLE consumes 31mW of power. These all results are calculated on the same platform. ANU cipher results in minimal power dissipation till date.

TABLE X. POWER CONSUMPTION COMPARISON

	PRESENT	LED	RECTANGLE
ANU	-42.10%	-78%	-29.03%

V. CONCLUSION

In this paper, we have proposed a balanced Feistel based cipher "ANU", which has maximal data complexity i.e. 2^{64} and results in maximum number of active S-boxes for fewer rounds. ANU cipher needs only 934 GEs for 128 bit key length and very less power i.e. 22 mW which is very less as compared to all existing lightweight cipher till date. ANU cipher not only resists basic attacks but also it resists advance attacks like MITM, Zero correlation and Biclique. ANU cipher design will have a positive impact in the field of lightweight cryptography; specifically this kind of designs will play a vital role in making applications like IoT feasible.

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*, pages 450-466, Springer Berlin Heidelberg, 2007.

[2] F. Abed, E. List, S. Lucks, and J. Wenzel. Cryptanalysis of the speck family of block ciphers. Cryptology ePrint Archive, Report 2013/568, 2013. http://eprint.iacr.org/.

[3] "The 128 bit blockcipher" CLEFIA: Algorithm specification." On-linedocument, 2007. Sony Corporation.

[4] 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

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

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

[7] E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993

[8] Bogdanov, A., Rijmen, V.: "Zero Correlation Linear Cryptanalysis of Block Ciphers" *IACR Eprint Archive Report 2011/123 (March 2011)*

[9] 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*.