Defence Science Journal, Vol. 66, No. 3, May 2016, pp. 259-265, DOI : 10.14429/dsj.66.9276

RESEARCH PAPER

PICO : An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing

Gaurav Bansod*, Narayan Pisharoty, and Abhijit Patil

Electronics and Telecommunication, Symbiosis Institute of Technology, Pune - 412 115, India
**Correspondence e-mail: gauravb@sitpune.edu.in*

ABSTRACT

An ultra-lightweight, a very compact block cipher 'PICO' is proposed. PICO is a substitution and permutation based network, which operates on a 64 bit plain text and supports a key length of 128 bits. It has a compact structure and requires 1877 GEs. Its innovative design helps to generate a large number of active S - boxes in fewer rounds which can thwart the linear and differential attacks on the cipher. PICO shows good performance on both the hardware and the software platforms. PICO consumes only 2504 bytes of Flash memory which is less than the ultra-lightweight cipher PRESENT. PICO has a very strong substitution layer (S-box) which not only makes the design robust but also introduces a great avalanche effect. PICO has a strong and compact key scheduling which is motivated by the latest cipher SPECK designed by NSA. PICO consumes 28 mW of dynamic power which is less than the PRESENT cipher (38 mW). The security analysis of PICO and its performance as an ultra-lightweight cipher are presented.

Keywords: Lightweight cryptography, SP network, block cipher, encryption, embedded security

NOMENCLATURE

P_j	Input plaintext block of j = 64 bits
C_j	Output cipher text block of j = 64 bits
K^i	64-bit subkey for round i
$\oplus$	Bitwise exclusive-OR operation
LCS(P_j,n)	Left circular shift by n bits
RCS(P_j,n)	Right circular by n bits
$\|\|$	Concatenation of two strings
!	Bitwise NOT operation

1. INTRODUCTION

In recent years, many lightweight ciphers have been introduced which have less footprint area, low power consumption and less gate counts. Lightweight ciphers like PRESENT[1], PICCOLO[2], TWINE[3], SIMON and SPECK[4] have the robust design and needs less than 2200 gate equivalents (GEs) for implementation. National security agency (NSA) launched the SIMON and SPECK ciphers which are considered to be the most ultra-lightweight ciphers. SIMON and SPECK has robust design and interesting key scheduling. We aimed at compact design and robust S-P network cipher which not only needs less footprint area but also take care of the other factors like power consumption, throughput and the attacks. PRESENT has the bit permutations as its P- layer which only requires wires for its hardware implementation[1]. Presented a cipher called PICO which is an SP network that needs less GEs, less footprint area and has low power consumption as compared to the PRESENT cipher and the other existing lightweight ciphers. Aimed at providing a strong substitution layer that makes the design robust. PICO shows good resistance against linear and differential attacks. PICO also shows good resistance against advance attacks like biclique attacks.

Key scheduling algorithm makes a big impact on the GEs while designing the algorithm. The key scheduling of PICO cipher is motivated from SPECK cipher, which has compact key scheduling algorithm and it does not include the nonlinear layer in the design. So the GEs required to implement the PICO cipher are less as compared to the PRESENT Cipher.

PICO cipher consumes only 28 mW of power, the power consumption evaluated with X-power analyser tool available in ISE design suit 14.2. Power is calculated with 10MHz frequency and on VIRTEX VI family.

2. THE PICO BLOCK CIPHER

The design of PICO cipher is based on a substitution permutation network[5]. It has a total of 32 rounds. PICO cipher supports 64 bit plaintext and 128 bit key length. Figure 1 shows the block diagram of PICO cipher.

Plaintext bits/cipher text bits are arranged in 4 X 16 array format as shown in Fig. 2(a). Let $P = p^{63}||\cdots||p^1||p^0$ is the 64 bit plaintext, row 0 contains the first 16 bits of plaintext $p^{15}||\cdots||p^1||p^0$, row 1 contains the next 16 bits $p^{31}||\cdots||p^{17}||p^{16}$, and so on, as shown in Fig. 2(a). Figure 2(b) represents the 'Two-dimensional Representation' of 4 X 16 array. AddRoundkey, SubColumn and the Bit_Shuffle these three operations are involved to produce ciphertext. K^{32} is post whitening key.

Operations in PICO cipher are:

Received : 23 September 2015, Revised : 11 February 2016
Accepted : 22 March 2016, Online : 25 April 2016

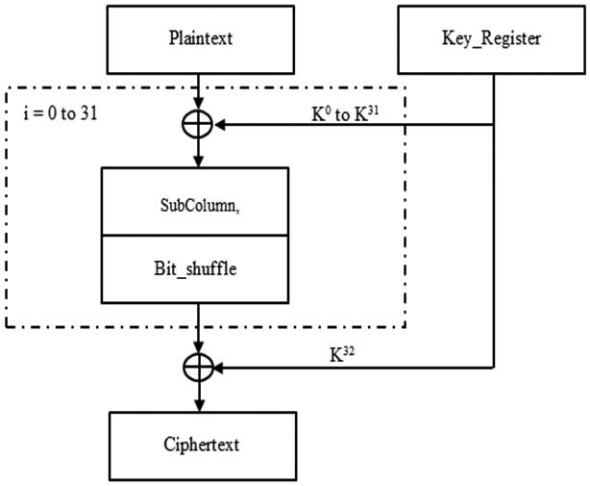

Figure 1. Block diagram of PICO cipher.

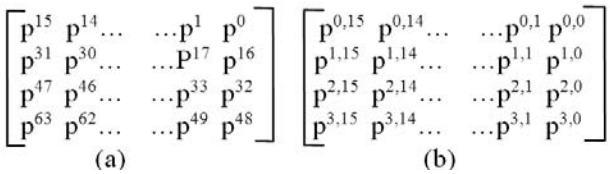

Figure 2. (a) 4 X 16 array format and (b) Two-dimensional representation of array.

2.1 Add_round_key

Add_round_key performs an XOR operation with 64 bit current state output and 64 bit sub key. Where $P \rightarrow p^{63}\ldots..p^{0}$

$P \rightarrow P \oplus K^{i}$

2.2 SubColumn

The S-box used in PICO cipher is of 4×4 and illustrated in Table 1. Substitution operation performed column wise which was previously explained in RECTANGLE cipher[6].

Table 1. S-box of PICO Cipher

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

SubColumn operation is based on the substituting S-box column wise. Operation of SubColumn is illustrated in Fig. 3. The input of a S-box is Column(i) = $p^{3,i} \| p^{2,i} \| p^{1,i} \| p^{0,i}$ where i ranges from $0 \leq i \leq 15$ and $p^{0,i}$ is LSB bit and $p^{3,i}$ is the MSB bit of the 4 bit nibble.

Let $P = p^{30}p^{20}p^{10}p^{00}$ be the input to the S-box and $Q = q^{03}q^{02}q^{01}q^{00}$ is the output. For example, if P = 0000 then Q =0001.

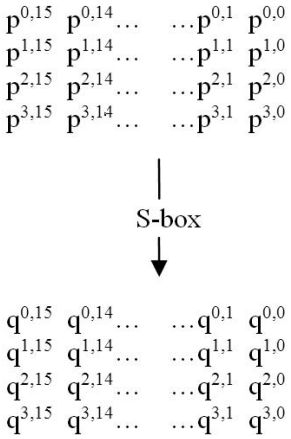

Figure 3. Subcolumn operation.

2.3 Permutation_Layer

Permutation layer of PICO cipher is based on bit permutation. The bit permutation used in PICO cipher is depicted by Table 2. The bit $p^{i,j}$ present in i^{th} row and j^{th} column is shifted to the new bit position as shown in the Table 2. Bit_ Shuffle ($p^{0,0}$) $\rightarrow p^{0,10}$. It means after permutation operation, the bit will be shifted to 0th row and 10th column. Because of the random nature of P box, it performs very well in customised hardware.

Pseudo code for PICO cipher is given as

P = P^{63} ...P^{0}
RoundKeys()
for i = 0 to 31 do
Add_round_key (P, K^{i})
SubColumn (A)
Bit_Shuffle (A)
End for
Add_round_key (A , K_{32})
C → A

2.4 Key Schedule of 128-bit Key Length

Key schedule of PICO cipher is motivated from the SPECK cipher key scheduling design[4]. SPECK key scheduling is compact in memory size requirement and no attacks till date are reported on it.

In PICO cipher total 33 subkeys are used each of size 64 bits and these 64 bits are extracted from 128 bit key scheduling algorithm which is mentioned below.

(1) *128-bit key scheduling*

User defined 128 bit key is stored in the register Key, subkey K^0 and L^1 are represented as

Key = k^{127} k^{126} k^{125}…k^{2} k^{1} k^{0}

Table 2. P-box Of PICO Cipher

j / i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0,10	1,5	1,12	2,6	2,12	3,0	3,11	0,1	3,3	0,15	2,9	0,2	3,12	2,2	1,8	1,4
1	3,8	0,6	1,1	1,15	2,4	3,5	0,12	2,14	1,14	3,4	0,11	0,4	1,7	2,3	2,8	3,15
2	0,8	2,7	0,3	2,11	3,9	3,1	1,0	1,9	2,5	2,10	3,13	3,2	0,0	0,9	1,2	1,10
3	3,10	3,7	0,7	1,3	1,13	0,14	2,15	2,0	2,1	0,5	3,14	2,13	0,13	3,6	1,6	1,11

$K^0 = k^{63}\, k^{62} \ldots k^1\, k^0$

$L^1 = k^{127}\, k^{126} \ldots k^{66}\, k^{65}\, k^{64}$

After extracting key , K^0 and L^1 each of 64 bits, the subkeys K^1 to K^{32} are generated as follows

For j = 0 to 31 do

$L^2_{64} = ((K^j_{64}) \oplus RCS(L^1_{64},3)) \oplus (L^1_{64});$

$K^{j+1}_{64} = ((L^2_{64}) \oplus LCS(K^j_{64},7)) \oplus j;$

$L^1_{64} = L^2_{64};$

End for

where LCS represents left circular shift by 7 bits and RCS represents right circular shift by 3 bits.

Subkeys are arranged in 4×16 array format as shown in Fig. 4 to perform AddRoundKey operation.

$$\begin{bmatrix} k^{0,15} & k^{0,14} \ldots & \ldots k^{0,1} & k^{0,0} \\ k^{1,15} & k^{1,14} \ldots & \ldots k^{1,1} & k^{1,0} \\ k^{2,15} & k^{2,14} \ldots & \ldots k^{2,1} & k^{2,0} \\ k^{3,15} & k^{3,14} \ldots & \ldots k^{3,1} & k^{3,0} \end{bmatrix}$$

Figure 4. 4×16, 2-D representations of subkey bits.

3. SECURITY ANALYSIS OF PICO

Various cryptanalysis techniques are applied on a cipher to find the robustness of cipher. S-box is a nonlinear layer in cipher design and it plays a very important role to provide security against well-known attacks like linear attack and differential attack.

Computer based techniques are used in this paper for selection of good S-box and to calculate the minimum number of active S-boxes.

3.1 Design Criteria of the S-box

Gate count is increased by using separate S-box in each round of cipher and similarly it does not provide sensible amount of improvement in the resistance against known attacks[7]. We have chosen 4×4 S-box in our design of PICO cipher. S-box used in the PICO cipher is robust and prevents clustering of linear and differential trails. One of the most important aspect in PICO cipher design is the nonlinear robust layer S-box.

4×4 S-box provides compactness and the selection of proper S-box provides resistance against linear and differential attack. We have considered these two parameters while designing the S-box.

PICO S-box is $S: F_2^4 \leftarrow F_2^4$, it means that it takes a 4 bit input and produces a 4 bit output. Important properties for a good S-box design are mentioned which has been considered for the S-box selection.

Complete design criteria of the S-box which we have used in designing of the PICO cipher is given as follows,

1. For any nonzero input difference $\Delta A \in F_2^4$ and output differences $\Delta B \in F_2^4$, respectively we have,
   $DC(\Delta A, \Delta B) = \#\{a \in F_2^4 \mid S(a) \oplus S(a \oplus \Delta A) = \Delta B\} \leq 4$
2. For any nonzero input differences $\Delta A \in F_2^4$ and output differences $\Delta B \in F_2^4$ such that $Hw(\Delta A) = Hw(\Delta B) = 1$, where $Hw(x)$ denote Hamming weight of x, we have,
   $Set_{DC} = DC(\Delta A, \Delta B) = \#\{a \in F_2^4 \mid S(a) \oplus S(a \oplus \Delta A) = \Delta B\} = 0$
   Cardinality of Set_{DC} can be given as Car_{DC}, we have $Car_{DC} = 2$.

   This is the most important property in designing of S-box. We have achieved Cardinality of 2 in both linear and differential table for the given S-box. This property indicates the strength and robustness of S-box.
3. For any nonzero input mask $A \in F_2^4$ and output mask such that $B \in F_2^4$ so we have $LC(A, B)$
   $LC(A, B) = \#\{a \in F_2^4 \mid A \bullet a = B \bullet S(a)\} - 8| \leq 4$
4. For any nonzero input mask $A \in F_2^4$ and output mask such that $B \in F_2^4$, such that $Hw(A) = Hw(B) = 1$, we have
   $Set_{LC} = LC(A, B) = \#\{x \in F_2^4 \mid A \bullet x = B \bullet S(x)\} - 8| \neq 0$
   Cardinality of Set_{LC} can be given as Car_{LC}, we have $Car_{LC} = 2$.
5. Bijective i.e. $S(a) \neq S(b)$ for all values of $a \neq b$.
6. No static point i.e. $S(a) \neq a$ for all values of $a \in F_2^4$.

Strength of the S-box depends on cardinality, For PICO cipher, S-box has $Car_{DC} = 2$ and $Car_{LC} = 2$.

In the case of PRESENT[6] cipher, S-box has $Car_{DC} = 0$ and $Car_{LC} = 8$, while in case of RECTANGLE[6] cipher, S-box has $Car_{DC} = 2$ and $Car_{LC} = 2$.

3.2 Linear Cryptanalysis

Liner Cryptanalysis[10] is an attack which is applicable on the symmetric-key block ciphers. This attack is the known plaintext attack. High probability occurrences of linear expression containing plaintext bits, cipher text bits and subkey bits are used for mounting the linear attack on cipher. Linear attack is mounted by having the knowledge about a subset of plaintext and its corresponding ciphertext. An attacker tries to find the correlation between them. S-box is examined by forming linear approximation table (LAT). Bias (ε) can be given as $|P_L\text{-}1/2|$ where P_L represents the linear probability. Maximum bias value for PICO cipher is 2^{-2}. Optimising the bias in LAT and increase the number of active S-boxes in cipher structure provides robustness for the linear attack.

PICO has minimum 11 active S-box for 6 rounds. By applying Matsui`s Pilling up Lemma[10] total bias for 24 rounds is 2^{-45}. The complexity of linear attack is $1/(2^{-45})^2 = 2^{90}$. Hence the complete rounds of PICO cipher shows good resistance against a linear attack.

3.3 Differential Cryptanalysis

Differential cryptanalysis[11,12] is an attack which is applicable to symmetric key block cipher. Differential cryptanalysis firstly applied on DES[11]. Pair of high probability input and output occurrences are used to mount this attack. Substitution layer is a nonlinear layer in design, which is examined by forming difference distribution table (DDT). P_D represents differential probability, P_D value for PICO S-box is $4/16 = 1/4 = 2^{-2}$. Minimize the differential probability (P_D) and build a cipher design such that it maximises the minimum number of active S-boxes provide resistance against differential attack.

There are 12 active S-boxes for 6 rounds of PICO cipher. Differential probability for 24 rounds of the cipher is $(2^{-2})^{48} = 2^{-96}$. Total number of chosen plaintext required to mount this attack are $1/2^{-96} = 2^{96}$.

3.4 Biclique Attack

Biclique attack[13,14] is an extension of meet-in-the-middle attack. We have applied 4-dimensional biclique cryptanalysis technique on PICO-128 for round 29 ~ 32.

For these rounds the partial keys used are (K^{29}, K^{30}, K^{31}, K^{32}). To construct the Δi-differential we have considered sub keys (k_{30}, k_{14}, k_{62}, k_{46}) and for the ∇j-differential we have considered sub keys (k_{15}, k_{33}, k_{44}, k_{27}).

Since the Δi-differential affects the 48 bits of the ciphertext as illustrated from Fig. 5. The data complexity does not exceed than 2^{48}. The total key recovery complexity of PICO-128 is $C_{total} = 2^{127.717}$.

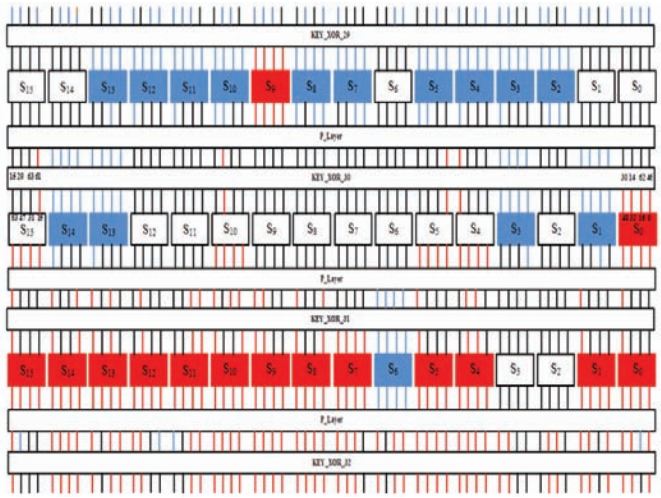

Figure 5. 4-D Biclique for PICO-128.

3.5 Algebraic Attack

Attacker applies the algebraic attack[15] more usually on stream cipher rather than applying it on block cipher. The 4 × 4 bit S-box is described by minimum 21 quadratic equations in the 8 input /output variables, Let $x = a \times 21$ are the quadratic equations and in that $y = a \times 8$ are the variables used to examine the complete cipher. Where a represents the number of S-boxes used in encryption algorithm and in key scheduling algorithm. For 32 rounds of cipher, there are a total 512 S-boxes in the encryption design. PICO cipher has the 10752 number of quadratic equations in 4096 variables, these many equations provides good resistance against the algebraic attack.

3.6 Avalanche Effect[16]

When a single bit change in the input changes the output significantly, this results in an avalanche effect. For example by flipping a single bit in the input or in a key could change the half of the bits in cipher text. Cipher with good avalanche effect has higher probability to resist all possible types of attacks. The poor randomisation occurs when a block cipher does not show the avalanche effect to a significant degree. Table 3 shows some examples of avalanche effect.

4. SECURITY COMPARISON WITH STANDARD ALGORITHM

In this section we have compared the security analysis of PICO with the other standard lightweight ciphers. The comparison is represented in Table 4 and 5. Table 4 compares the linear complexity and differential complexity by considering the number of active S-boxes for the particular rounds.

Table 3. Avalanche effect for PICO-128

Plaintext	0000 0000 0000 0000	No. of bits change
Key	00000000000000000000 000000000000	--
Ciphertext	fda7e7de58c913f4	
Key	08000000000000000 0000 000000000000	40
Ciphertext	72f4081fae46ef5d	

Table 4. Linear and differential attack comparison

Cipher name	PICO	PRESENT	L-block	FEW	PICCOLO
#Rounds	24	25	15	27	30
# Active S-box from linear trails	45	50	32	45	30
# Active S-box from differential trails	48	50	32	45	30
#Known plaintext	2^{90}	2^{102}	2^{66}	2^{90}	2^{120}
#Chosen plaintext	2^{96}	2^{100}	2^{64}	2^{90}	2^{120}
Reference	--	[1]	[9]	[19]	[3]

Table 5 compares the data complexity and computational complexity of PICO cipher with the other ciphers.

Table 5. Biclique attack comparison

Cipher name	Rounds	Data complexity	Computational complexity	Reference
PICO-128	Full(32)	2^{48}	$2^{127.717}$	This Paper
PRESENT-80	Full(31)	2^{23}	$2^{79.54}$	[13]
PRESENT-128	Full(31)	2^{19}	$2^{127.42}$	[13]
PICCOLO-80	Full(25)	2^{48}	$2^{79.13}$	[13]
PICCOLO-128	Full(31)	2^{24}	$2^{127.35}$	[13]
LED-64	Full(48)	2^{64}	$2^{63.58}$	[13]
LED-80	Full(48)	2^{64}	$2^{79.37}$	[13]
LED-96	Full(48)	2^{64}	$2^{95.37}$	[13]
LED-128	Full(48)	2^{64}	$2^{127.37}$	[13]

Table 6 compares the S-box design considerations with the lightweight ciphers. PICO S-box has CAR_{DC}=2 and CAR_{LC}=2 which illustrate that PICO cipher S-box is robust in design and provides good security than other lightweight ciphers.

5. HARDWARE AND SOFTWARE PERFORMANCE OF PICO CIPHER

Design of a PICO cipher provides optimum performance in

Table 6. S-box design consideration

Cipher name	Max. Val. in DDT	Max. Val. in LAT	CAR_{DC}	CAR_{LC}
PICO	4	4	2	2
PRESENT	4	4	0	8
RECTANGLE	4	4	2	2
TWINE	4	4	5	7

hardware as well as on software platform. We have considered the 32 bit ARM 7 LPC2129 processor for analysing software performance of PICO cipher[17].

Footprint area, i.e. GEs are computed with standard cell library based on UMCL 180 0.18 µ logic process (UMCL18G212T3)[18]. Memory size required for PICO cipher on 32 bit processor is 2504 bytes as Flash memory and 1256 as RAM memory. All other ciphers are written in embedded C and implemented on a 32 bit processor for comparison with the PICO cipher. Fig. 6 represents the memory comparison of the existing lightweight ciphers with PICO cipher. PICO needs less memory as compared to the other S-P network light weight ciphers. Datapath for the PICO cipher is shown in Fig. 7.

Area is computed with standard cell library UMCL 180 0.18 µ logic process (UMCL18G212T3)[18]. GEs calculation for PICO cipher is represented in Table 7. For 128 bit key scheduling PICO cipher needs 1877 GEs.

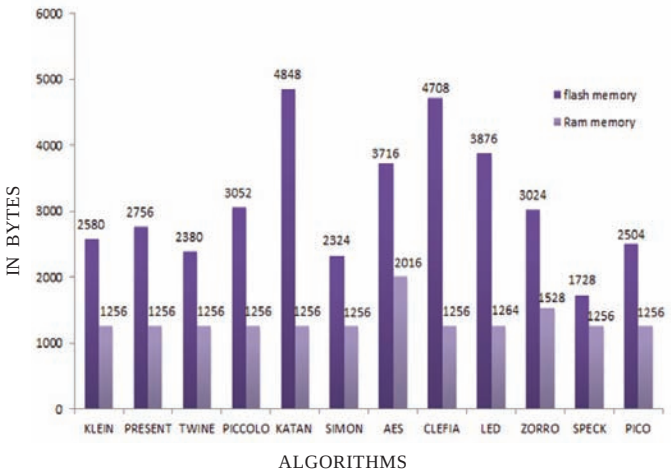

Figure 6. Comparison on the basis of memory requirement.

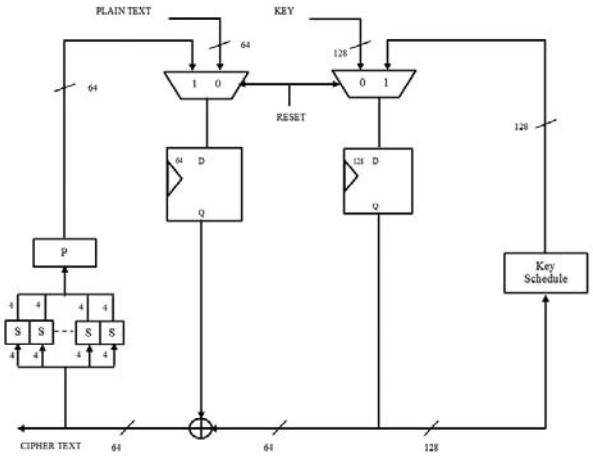

Figure 7. Data path for PICO cipher for 64-bit plaintext and 128-bit key.

Table 7. Calculation of GEs for PICO Cipher

Data layer	GEs	Key layer	GEs
D Reg.	384	K Reg.	768
S-Box	384	Shift Operator	0
P-Layer	0	S-box	0
XOR	170.88	XOR	170.88
Total	938.88	Total	938.88

Total number = 1877.76 =1878

We have calculated the power consumption by using X-power analyser tool available in ISE design suit 14.2. Power is calculated with 10 MHz frequency and on VIRTEX VI family. PICO Cipher consumes 28mW of power while PRESENT and RECTANGLE cipher consumes 38 mW and 31 mW, respectively. PICO cipher consumes 26 per cent less power as compared to the PRESENT cipher. Power consumption mentioned in Table 8.

Table 8. Power consumption of lightweight cipher

Standard cell	Dynamic power consumption in mW
PICO	28
PRESENT	38
LED	100
RECTANGLE	31

PICO results in consuming less GEs as compared to all the other existing lightweight cipher represented in Fig. 8.

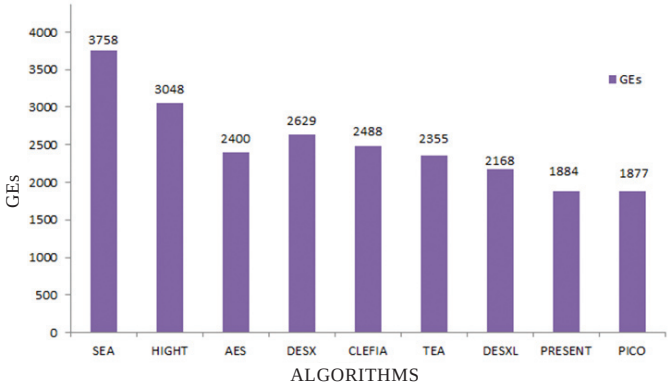

Figure 8. Comparison on the basis of area[17].

Table 9 shows the comparison of lightweight ciphers with PICO based on parameters like execution time, throughput and number of cycles required to convert plain text to cipher text. Throughput is computed on a software platform at 12 MHz.

Test Vectors

Plain text: 0000 0000 0000 0000
Key: 0000 0000 0000 0000 0000 0000 0000 0000
Cipher text: fda7e7de58c913f4
Plain text: 0123 4567 89ab cdef
Key: 0000 0000 0000 0000 0000 0000 0000 0000
Cipher text: 8ebcf6ffd7289163

Table 9. Comparison with respect to throughput, execution time and number of cycles

Ciphers	Block size	Key size	Exec. time (μs)	Throughput (Kbps)	No. of cycles
			SP Network		
LED	64	128	7092.86	9	85114.32
PICO	64	128	4134.23	15.48	49610.76
PRESENT	64	128	2648.65	24.16	31783.8

6. CONCLUSION

A PICO, an ultra-lightweight and low power cipher design is presented. PICO cipher design results in lesser foot print area and lower power consumption. PICO performs efficiently both on the hardware and the software platforms. The resistance of PICO cipher against well-known attacks as shown. PICO cipher has a very strong S-box and a robust permutation layer which prevents the cipher design from undergoing the clustering of linear and differential trails. In designing a PICO cipher, A small gate count as well as small power dissipation so that it can be implemented for security in any small scale embedded system is achieved. PICO needs less footprint area and less power consumption as compared to PRESENT, LED and other ciphers. For applications like RFID tags, Wireless sensor nodes, where small footprint area and power consumption play a crucial role, we believe the PICO cipher is one of the best suited designs.

REFERENCES

1. Bogdanov, A.; Leander, G;. Knudsen, L.R.; Paar, C.; Poschmann, A.; Robshaw, M.J.B.; Seurin, Y. & Vikkelsoe, C. PRESENT - An ultra-lightweight block cipher. *In* Cryptographic Hardware and Embedded Systems, *edited by* P. Paillier and I. Verbauwhede, Springer Berlin Heidelberg, CHES 2007, **4727** in LNCS, pp. 450-466. doi: 10.1007/978-3-540-74735-2_31
2. Shibutani, Kyoji; Isobe, Takanori; Hiwatari, Harunaga; Mitsuda, Atsushi; Akishita, Toru & Shirai, Taizo. PICCOLO: An ultra-lightweight blockcipher, *Springer* Berlin Heidelberg, 2011, **6917**, pp.342-357. doi: 10.1007/978-3-642-23951-9_23
3. Suzaki, T.; Minematsu, K.; Morioka, S. & Kobayashi, E. TWINE: A lightweight, versatile block Cipher. Cryptology ePrint Archive. *Springer,* Heidelberg, 2013, **7707**, 339-354. doi: 10.1007/978-3-642-35999-6_22
4. Beaulieu, R.; Shors, D.; Smith, J.; Clark, S.T.; Weeks, B. &Wingers, L. The SIMON and SPECK families of lightweight block Ciphers. Cryptology ePrint Archive, Report 2013/404. http://eprint.iacr.org (Accessed on 19 June 2013).
5. Menezes, A.; Oorschot, P.C. van & Vanstone, S. The handbook of applied cryptography. CRC Press, 1996.
6. Zhang, W.; Bao, Z.; Lin, D.; Rijmen, V.; Yang, B. & Verbauwhede., RECTANGLE: A bit-slice ultra-lightweight block cipher suitable for multiple platforms. *Sci. China Info. Sci.*, **58**(12), 1-15. doi: 10.1007/s11432-015-5459-7
7. Biham, E. New types of cryptanalytic attacks using related keys. *In* Proceedings of Eurocrypt 93, Springer-Verlag 1994, LNCS. **765,** pp. 398-409. doi:10.1007/3-540-48285-7_34
8. Wenling, Wu & Zhang, Lei. LBlock: a lightweight block cipher. *In* Applied Cryptography and Network Security, Springer Berlin Heidelberg, 2011, pp.327-344. doi: 10.1007/978-3-642-21554-4_19
9. National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 2000.
10. Heys, Howard M. A tutorial on linear and differential cryptanalysis. doi:10.1.1.68.4536
11. Biham, E. & Shamir, A. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 1991, **4**(1), 372. doi: 10.1007/BF00630563
12. Wang, M. Differential cryptanalysis of reduced-round PRESENT. *In* Springer Heidelberg Africacrypt 2008 LNCS, 2008, **5023**, pp.40-49. doi: 10.1007/978-3-540-68164-9_4
13. 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.
14. Bogdanov, A.; Khovratovich, D. & Rechberger, C. Biclique cryptanalysis of the full AES. Springer Berlin Heidelberg, Asiacrypt 2011, LNCS, 2011, **7073**, 344–371. doi: 10.1007/978-3-642-25385-0_19
15. Albrecht, M. & Cid, C. Algebraic techniques in differential cryptanalysis. FSE Springer, Heidelberg 2009, LNCS, 2009, **5665**, 193-208. doi : 10.1007/978-3-642-f22497-3_9.
16. Shi, Z. & Lee, R.B. Bit permutation instructions for accelerating software cryptography. *In* Proceedings of the IEEE International Conference on Application Specific Systems. Architectures and Processors (ASAP 2000), 2000, 138-148. doi: 10.1109/ASAP.2000.862385 ,
17. Bansod, Gaurav; Raval, Nishchal & Pisharoty, Narayan. Implementation of a new lightweight encryption design for embedded security. *IEEE Trans. Info. Forensics Security*, 2015, **10**(1), 142-151. doi: 10.1109/TIFS.2014.2365734
18. Poschmann, A. Lightweight cryptography: Cryptographic engineering for a pervasive world. Faculty of Electrical Engineering and Information Technology, Ruhr-University Bochum, Germany, 2009. (PhD Thesis)
19. 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.

CONTRIBUTORS

Dr Gaurav Bansod received his PhD from Symbiosis International University and MTech (Embedded Sytems) from Jawaharlal Nehru Technological University, Hyderabad, in 2008. He is currently pursing PhD from Symbiosis International University, Pune. Currently he is working as an Assistant Professor in Symbiosis Institute of Technology, Pune. His research area include: Low power cryptographic design, embedded systems, and hardware and software design.
In current study, he has contributed to the design and architecture. He has also contributed to the gate equivalent calculations

Dr Narayan Pisharoty received BTech from IIT Bombay in 1966, MTech from IIT Kanpur in 1968 and PhD from Carnegie Mellon University, Pittsburgh, USA in 1971. Currently he is the Research Mentor for Engineering at Symbiosis International University, Pune, India and a Professor in the Electronics & Telecommunication Department of Symbiosis Institute of Technology. His research area include : RFID applications, alternate energy sources and applications of microcontrollers in agriculture.
In current study, he has contributed to the basic cryptanalysis techniques and in overall flow of a paper.

Mr Abhijit S Patil perceived MTech from Symbiosis Institute of Technology, Pune in 2015. He is currently working in IBM India Pvt Ltd. His research area include : Embedded security system, lightweight cipher, embedded automotive systems and embedded real time systems.
In current study, he has contributed to the implementation of advance attacks and power calculations.