International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.85-98
http://dx.doi.org/10.14257/ijsia.2015.9.12.10

Hybrid Lightweight and Robust Encryption Design for Security in IoT

Abhijit Patil[1], Gaurav Bansod[2] and Narayan Pisharoty[3]

Electronics and Telecommunication
Symbiosis Institute of Technology, Symbiosis International University
Lavale, Pune, 412115, Maharashtra, INDIA
[1]abhijit.patil@sitpune.edu.in,[2]gauravb@sitpune.edu.in,[3]narayanp@sitpune.edu.in

Abstract

Pervasive computing is the emerging field that needs ultra lightweight secure designs. In this paper, we have proposed a robust hybrid structure by fusion of RECTANGLE, LED and SPECK. With the help of a hybrid design, we have improved the key scheduling aspect of LED and related key attacks which were neglected in the LED cipher. In this paper, we also aimed at providing robust architecture by reducing footprint area to as less as possible. By using the S-box of RECTANGLE and the bit slicing technique, clustering of linear and differential trails are avoided which also strengthens the cipher. S-box of RECTANGLE is perfectly interfaced with LED design as their combination results in a differential path probability which is has an upper bound of 2^{-50} in its first round. The use of Bit slicing technique in this hybrid design results in good differential and linear properties, which provide resistance to cache and timing attacks. LED cipher which uses S-box of PRESENT results in clustering of linear and differential trails as S-box of PRESENT is specifically designed for compact hardware implementation. Column wise substitution and robust S-box design of RECTANGLE will make LED design robust and secure and enables it to provide resistance against any type of attack. SPECK which is designed by NSA has compact key scheduling and is best suited for our hybrid design, which helps in improving key scheduling of LED. In this paper, we have introduced a novel approach for robust design by amalgam of S-box of RECTANGLE & LED structure, and key scheduling by SPECK. This hybrid cipher design is secure against linear and differential cryptanalysis.

Keywords: *Lightweight cryptography, PRESENT, LED, RECTANGLE, Embedded Security, Encryption, Pervasive Computing*

1. Introduction

Pervasive computing is the emerging field that will make the communication among devices a reality. Fields like Internet of Things (IoT) also aim at the same scenario of providing intelligence to the devices [1]. But, when implementing, many issues pop up which need to be addressed. One of the major issues that need to be addressed to make applications like IoT practical is security. Ciphers which have been known for providing optimum security have higher gate counts, which make them unsuitable for applications like IoT. There is need of lightweight ciphers for these highly constrained devices. The devices used in these applications are RFID tags, wireless sensor nodes and other tightly constrained devices. These devices have total Gate Equivalents (GEs) around 10,000. For security purpose, the GEs available would be in between 2000-2200 [2]. Ciphers like AES [3], DES [4-5], Blowfish [6], 3DES [7] have exceeded these gate counts and will not be suitable for this kind of applications. This generates the need and emergence of the field, popularly known as lightweight cryptography. Many lightweight ciphers have been

ISSN: 1738-9976 IJSIA

designed in the past that have less GEs and are best suited for pervasive computing. Ciphers like PRESENT [8], XTEA [9], KLEIN [10], TWINE [11-12], HUMMINGBIRD-2 [13], LED [14], ZORRO [15] and PICCOLO [16] are the lightweight ciphers that have less GEs and less memory requirements that can be suitable for applications like RFID tags. Recently, SIMON and SPECK designed by NSA are the popular and most discussed cipher in lightweight cryptography [17]. Apart from less gate counts, these ciphers should also provide optimum security which is needed to maintain privacy. In recent years, many attacks have been proven on some of the above mentioned ciphers which have increased the urgency of designing lightweight and secure ciphers for pervasive computing. Table 1 shows the lightweight ciphers and respective GEs.

Table 1. Lightweight Ciphers with their GEs

Ciphers	Block Size	Key Size	GEs
CLEFIA [18][19]	128	128	2488
AES [3]	128	128	2400
TEA [20]	64	128	2355
DESXL [21]	64	184	2168
KLEIN [10]	64	80	1478
RECTANGLE [22]	64	80	1467
PRESENT [8]	64	128	1339
PICCOLO [16]	64	128	1334
LED [14]	64	128	1265
SPECK [17]	64	128	1127
KATAN [23]	64	80	1054
TWINE [11] [12]	64	80	1011
SIMON [17]	64	128	1000

Lightweight cryptography has ISO standards for these lightweight ciphers which were given to PRESENT and CLEFIA in 2012. PRESENT has emerged as the most compact lightweight cipher in recent years. Ciphers like LED (Light Encryption Device) uses S-box of PRESENT in its cipher design [14]. S-box of PRESENT requires nearly 21 GEs for its implementation which makes it compact and hardware efficient [8]. S-box plays a very important role as a non linear element in cipher design. LED cipher has a structure like AES which uses modules like shift rows, mix columns, add round key and S-box [14]. LED differs from AES in its S-box design and its compact hardware structure. LED has 4 bit S-box and needs total 48 rounds to produce cipher text from plain text. LED has strong and robust design which can provide highest security compared to all other rest lightweight ciphers. Its cryptanalysis and design is strong enough to protect against all possible types of attacks. But, LED has failed in providing a robust key scheduling design and its related key attacks which has stopped the cipher being the frontrunner in this field. In this paper, we aimed at improving design of LED cipher to protect against all types of attacks including a related key attack. Section-II describes our hybrid design which aims at providing a robust architecture for LED cipher. A novel approach is used in this paper for improving key scheduling and also the overall design of the LED cipher.

2. Hybrid Cipher Design and Implementation

LED has 64 bit block size and 128 bit key size which is mostly suitable for lightweight applications. LED has structure similar to AES [14]. LED operates on 4 bit S-box instead of 8 bit or larger S-boxes. This design steps also shows the cipher is also meant for compact hardware implementation. LED has a similar structure of AES, but AES is specifically designed to do well on software, not on hardware. As AES has larger footprint area, LED was successful in compact hardware implementation. Figure 1 shows the block diagram of LED cipher.

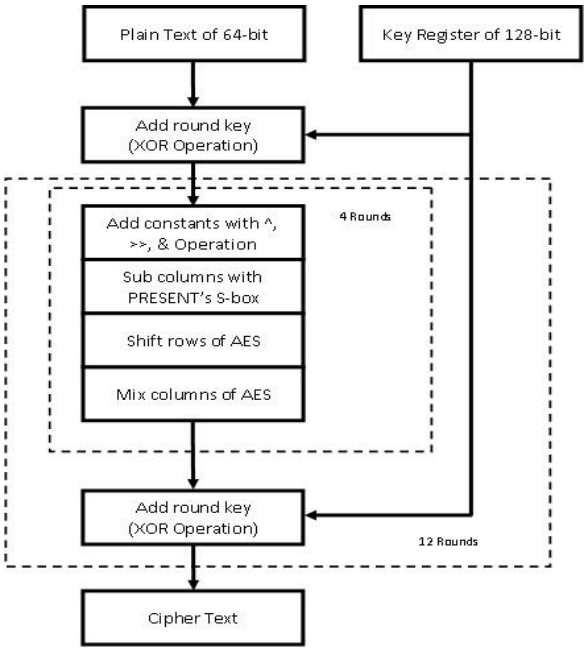

Figure 1. Block Diagram of LED

As shown in Figure 1, a plaintext is XOR-ed with the key which was randomly chosen. Then, the output is followed by "Add constants" operation which adds the XOR-ed output with fixed arrays of 8 bits. This addition helps LED to resist against slide attack. The output is given to S-box of PRESESNT cipher. S-box plays a very important role as it is the only structure which introduces non linearity. PRESENT's S-box design is the most compact S-box known so far. A single S-box of PRESENT results in around 21 to 29 GEs. The output of S-box is applied to "Shift row" and "Mixed column" operation. These operations are similar to the AES operation. This whole structure is rotated 4 times and which is called as one round. LED has 12 rounds which mean $12 \times 4 = 48$ rounds as depicted in Figure 1. The output from this round is again XOR-ed to produce cipher text.

3. Contribution and Novel design

LED cipher has neglected the key scheduling aspect which is very prominent in secure cipher designing [14]. This flaw may generate the related key attacks which can disturb the cryptanalysis of a cipher. In this paper, we aimed at providing efficient and compact key scheduling which resist against the possibility of related key attack. Various key scheduling aspects has been considered while interfacing with LED cipher. Care is taken in this work to have a proper interface which not only intact linear and differential properties of LED cipher but also improve the cipher resistance against all types of possible attacks. Recently, NSA has designed the lightweight ciphers named SIMON and SPECK which is optimized for hardware and software implementations [17]. In this work,

we have interfaced SPECK key scheduling with LED cipher to resist against related key attacks. NSA has known for interesting key scheduling. SPECK has been optimized for efficient performance on microcontroller. For 128 bit key size, SPECK key scheduling undergoes 26 rounds generating a total of 26 keys of 32 bit each. No other cipher except SPECK generates perfectly 26 keys of 32 bit each for 64 bit block size and 128 bit key size. LED cipher need overall 13 keys of 64 bit each which can be perfectly derived by SPECK. SPECK key scheduling satisfies the requirement of keys for LED cipher. We have combined keys of 32 bits each to generate 26 keys of 64 bits from SPECK key scheduling. SPECK takes a single key of 32 bit and generates the next key with the help of OR operation, Right Circular Shift, Ex-OR and Left Circular Shift [17]. The new key which is generated depends on the previous key value. The following equations represent SPECK key scheduling for LED cipher.

for i = 0 to 25

$$P[i + n-1] = (K[i] + R_{-\alpha} P[i]) \text{ ExOR } i;$$

$$K[i + 1] = R_{\beta} K[i] \textbf{ ExOR } P[i + n-1];$$

Where, n is number of keyword which is 4 for 128 bit key scheduling and 64 bit block size, R-α represent Right Circular Shift by α which is 8 and Rβ represents Left Circular Shift by β which is 3 for 64/128 cipher. K[i] represents 32 bit keys. LED demands 64 bit key where SPECK generates 32 bit key. In this paper, we have combined keys to generate 64 bit key. K[i] and K[i+1] is combined to produce 64 bit key. SPECK has the compact key scheduling and is best suited for LED cipher. SPECK generates unpredicted keys which helps in increasing resistance against slide and meet in the middle attacks [24]. It has great avalanche effect as one bit change can change the whole key structure.

LED cipher has S-box of PRESENT which adds non linear element to the cipher design. It has 4 bit S-box. Table2 represents the 4 bit S-box of PRESENT.

Table 2. 4 Bit S-Box of PRESENT

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

It is 4 bit to 4 bit S box which varies between 21 GEs to 39 GEs based on the library used. PRSENT's S-box is designed for compact hardware implementation but has poor secure design. PRESENT's S-box is among 8% worst S-boxes with respect to clustering of 1 bit linear trails [22]. In PRESENT due to the weak S-box design, there is heavy clustering of linear and differential trails because of that shortcut attack can be mounted on 26 rounds of PRESENT out of 31 [22]. This further weakens LED cipher. PRESENT cipher has large number of trails which lead to a difference propagation with higher probability value. In this paper, we aimed at improving strength of LED cipher by strengthening non linear substitution layer. In this paper, we have proposed use of S- box of RECTANGLE, a newly designed lightweight cipher which has better cryptanalysis properties than PRESENT cipher [22]. RECTANGLE also has 4 bit S-box whose design is depicted in Table3.

Table 3. 4 Bit S-Box of RECTANGLE

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

In RECTANGLE cipher due to its robust design of non linear elements, it has limited number of clustering trails while in PRESENT we find heavy clustering of differential

and linear trails. Following equations represents the designing of S-box structure where T_i is a temporary sequence and A_i indicates the i^{th} bit [22].

$T_1 = A_0 \oplus A_1$; $B_1 = T_5 \oplus T_6$;

$T_2 = A_0 \mid A_3$; $T_8 = ! B_1$;

$T_3 = A_2 \oplus T_2$; $T_9 = T_3 \mid T_8$;

$B_2 = A_1 \oplus T_3$; $B_3 = T_1 \oplus T_9$;

$T_5 = A_0 \& T_3$; $T_{11} = T_8 \mid B_3$;

$T_6 = A_3 \oplus B_2$; $B_0 = T_3 \oplus T_{11}$;

In RECTANGLE, full resistance is achieved after 25 rounds while in PRESENT we require 31 rounds to be secure. The S-box of RECTANGLE is the most preferred design due to the limited number of linear and differential trails. It has less energy per bit as compared to PRESENT [22]. Moreover, in this design along with S-box of RECTANGLE, we have added bit slice instructions also which help the design to be efficient on software platform [22]. LED is having disadvantage of high energy per bit which can be compensated by using S-box of PRESENT and bit slice instructions. The use of bit slice instructions increases the difference propagation thus provides great security levels. It also helps in providing resistance to cache and timing attacks [22]. Bit slicing technique results in efficient hardware and software implementation. Inferences from past also shows that use of bit slice techniques in ciphers like DES [4-5], SERPENT [25] increase the performance of cipher. Figure 2 shows bit slice technique which is applied for LED cipher.

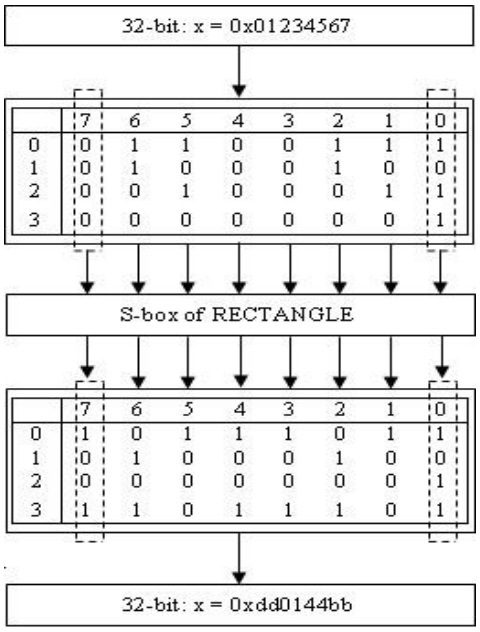

Figure 2. Bit Slice Technique with S-Box

In this paper, we aimed at improving design of LED by adding suitable key scheduling technique which can resist related key attacks and strengthening the cipher by stronger S-box and bit slice technique for efficient software implementation. SPECK key scheduling is suitable match for key scheduling operation while S-box of RECTANGLE and bit

slicing technique improves the linear and differential characteristics of a LED cipher design. This super hybrid design can be compared in terms of security at par with AES. It can also encrypt and decrypt huge amount of data with optimum security. Figure 4 shows the block diagram of hybrid design.

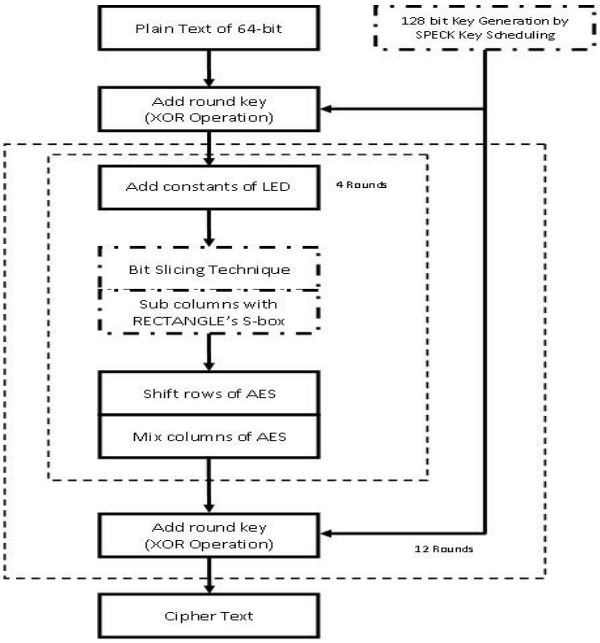

Figure 3: Block Diagram of Hybrid Design

Table 4 shows the memory requirement for hybrid design in terms of Flash and RAM memory. It also display execution time required for producing cipher text from plaintext. We have represented hybrid design as SR-LED which denotes combination of SPECK, RECTANGLE and LED. All codes are written in embedded C and implemented on 32 bit ARM7 LPC2129. This hybrid design needs small footprint area as shown in Table3. Mostly, all lightweight ciphers have FLASH memory requirement till 3900 bytes which is discussed in Section-IV.

Table 4. Memory Requirement for Hybrid Structure

Ciphers	Flash Memory	RAM Memory	Execution Time	Through Put	No. of Cycles
SR-LED	3168	1256	10434.68	6 Kbps	626081

4. Security Analysis

In cipher's security analysis, Differential [27] and Linear [28] cryptanalysis are the most important techniques. In this section, we are presenting security analysis of SR-LED design.

RECTANGLE's 4 × 4 S-box has asymmetric design with bit slicing technique which reaches to great security level [22]. From our experimentation it shows that RECTANGLE S-box is well suited for LED cipher as compared to PRESENT S-box. The one round of LED is like 4 rounds of AES. This characteristic will contain nearly 25 active S-boxes. From paper [14], the best differential characteristic contains 50 active S-boxes (PRESENT S-box has 2^{-2} differential probability; so, 4 active round of LED has $2^{-2 \cdot 25} = 2^{-50}$ differential probability) as same as linear characteristic because of duality. For

single key settings, LED-128 has 300 active S-boxes with 2^{-600} differential probability and 2^{-600} linear probability. For related key settings, LED-128 has 150 active S-boxes with 2^{-300} differential probability and 2^{-300} linear probability. We have computed number of active S-boxes from linear and differential trail.

4.1. Differential Cryptanalysis

In 1990 Biham and Shamir applied differential attack on DES cipher. Differential cryptanalysis is basic attack and need to be applied on cipher; this attack is applied by considering pairs of high probability input-output occurrences are used to recover rounds sub keys. S-box is analyzed by forming difference distribution Table (DDT).

Number of active S-boxes plays an important role while designing a structure of that gives resistance against differential cryptanalysis. The S-box that have nonzero input and output difference referred as active S-box. Maximum differential probability (p) for RECTANGLE S-box and the PRESENT S-box is $4/16 = 1/4 = 2^{-2}$.

Computer based analysis is used to compute minimum number of active S-box using RECTANGLE S-box and PRESENT S-box. Table 5 represents minimum number of Active S-boxes by using for hybrid structure LED computed from Differential Trail.

Table 5. Min. Number of Active S-Boxes for LED from Differential Trail

Num. of ROUNDS	Min. Num. Active S-boxes
1	49
2	105
3	163
4	219

Complexity of attack can be given as

$$n_d = 1/(p)^{\text{min. number of active S-boxes for n rounds}}$$

Where nd referred as required number of chosen plaintext and p is maximum differential probability, for 4 rounds there are total 219 active S-boxes so complexity can be given as

$$n_{dP} = 1/(2^{-2})^{219} = 2^{438}$$

For complete rounds of PRESENT-LED-SPECK provide resistance against differential attack. Table 6 represents minimum number of active S-box for hybrid structure SRLED.

Table 6. Min. Number of Active S-boxes for Hybrid Structure SRLED from Differential Trail

Num. of ROUNDS	Min. Num. Active S-boxes
1	52
2	113
3	164
4	222

For 4 rounds of SRLED it has 222 active S-boxes, complexity can be given as,

$$n_{dR} = (1/2^{-2})^{222} = 2^{444}$$

4.2. Linear Cryptanalysis

In linear cryptanalysis attacker having knowledge about set of plaintext and corresponding ciphertext and it finds correlation between input and output. S-box is analyzed by building linear approximation Table. Best approach to resist linear attack is finding a structure that maximizes number of active S-boxes. Linear cryptanalysis also referred as known plaintext attack. Largest bias (ε) for PRESENT and RECTANGLE S-box is 2^{-2}. Complexity of attack is given by computing required number of known plaintext.

Matsui`s Piling up Lemma:

For 'n' independent random binary variables X_1, $X_2 \ldots X_n$, the equation is,

$$\varepsilon_{(1,2,\ldots,n)} = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

Where $\varepsilon_{(1L, 2L,\ldots,nL)}$ represents the bias of $X_1 \oplus \ldots \oplus X_n = 0$. And n represents number of active S-boxes in respective rounds. Table 7 represents minimum number of active S-boxes for hybrid structure LED. Required number of known plaintext can be given as

$$n_l = (1/\varepsilon_{(1,2,\ldots,n)})^2$$

Table 7. Min. Number of Active S-boxes LED from Linear Trail

Num. of ROUNDS	Min. Num. Active S-boxes
1	49
2	107
3	165
4	221

For 4 rounds of LED there are total 221 active S-boxes, maximum bias for 4 rounds can be given as

$$\varepsilon_{P4} = 2^{220} (2^{-2})^{221} = 2^{-222}$$

Complexity for 4 rounds can be given as

$$n_{lP} = (2^{222})^2 = 2^{444}$$

Table 8 represents minimum number of active S-boxes for hybrid structure SRLED.

Table 8. Min. Number of Active S-Boxes for Hybrid Structure SRLED from Linear Trail

Num. of ROUNDS	Min. Num. Active S-boxes
1	50
2	110
3	168
4	222

SRLED has total 222 active S-boxes for 4 rounds of it; maximum bias for 4 rounds can be given as

$$\varepsilon_{R4} = 2^{221} (2^{-2})^{222} = 2^{-223}$$

Complexity for 4 rounds can be given as

$$n_{lR} = (2^{223})^2 = 2^{446}$$

4.3. Analysis and Comparison

Table 9 and 10 depicts the S-box of RECTANGLE in LED with SPECK key scheduling will provide more resistance against linear and differential attack as compared to S-box of PRESENT.

Table 9. Analysis from Differential Cryptanalysis

Hybrid Structure Name	Indication	Number of chosen plaintext
LED	n_{dP}	2^{438}
SRLED	n_{dR}	2^{444}

Table 10. Analysis from Linear Cryptanalysis

Hybrid Structure Name	Indication	Number of known plaintext
LED	n_{lP}	2^{444}
SRLED	n_{lR}	2^{446}

LED-128 consumes more footprint area and more cycles than PRESENT-128, but it gives more security than any other light weight ciphers, even more than AES-128 and AES-256. This hybrid design also consumes less GE than PRESENT-128. SR-LED, our proposed hybrid design is the step towards strengthening the LED design further to achieve optimum security against all types of possible attacks.

5. Lightweight Ciphers Comparison and Results

In this section, all lightweight ciphers are implemented on 32 bit processor to have comparison with our hybrid design. All these ciphers are implemented on 32 bit processor LPC2129 with 12 MHz clock frequency. Footprint area of lightweight cipher plays a very important role in tightly constraint applications like RFID tags and in wireless sensor nodes. Lightweight ciphers have nearly Flash memory space till 3900 bytes and RAM memory space till 1700 bytes. Figure 4 shows the comparison of hybrid design (SR-LED) with other lightweight ciphers. This hybrid structure is comfortable fit in the standard for lightweight ciphers in terms of memory requirements.

Figure 4. Lightweight Cipher Comparison with our Hybrid Design

Table 11 shows the comparison of lightweight ciphers with our hybrid design in terms of execution time. This hybrid design needs a bit more execution time as compared to other lightweight ciphers. We aimed at robust design at cost of execution time and throughput. This hybrid design has 6 Kbps as throughput.

Table 11. Execution Time Comparison

Ciphers	Block Size	Key Size	Execution Time (In uSec)
LED [14]	64	128	7092.86
PICCOLO [16]	64	128	227.68
PRESENT [8]	64	128	3609.91
TWINE [11][12]	64	128	592.87
ZORRO [15]	128	128	913.21
CLEFIA [18][19]	128	128	1048.01
AES [3]	128	128	395.25
HUMMINGBIRD-2 [13]	16	128	316.27
KLEIN [10]	64	96	887.51
SR-LED	64	128	10434.68

Figure 5 shows graphical representation for GEs needed for lightweight ciphers and comparison with our hybrid design (SR-LED). This is the most important characteristics to be evaluated as a lightweight cipher. All lightweight cipher should have maximum GEs around 2000-2200. Total GEs available in RFID tag is around 10000 [26]. This hybrid design is competitive in GEs as compared to other lightweight ciphers. SR-LED needs total 1474 GE. RECTANGLE S-box design needs 40 GEs approximately. All these GEs calculations are based on ARM CELL LIBRARY for IBM 0.13 micron ASIC process which is shown in Table 12. We have calculated number of GEs based on the values represented in Table 12. Clock frequency used for this process is 100 KHz.

Table 12. Gates Count of ARM Cell Library for IBM 8RF ASIC process

Standard Cell	Process	Library	GE
NOT	0.13µm	ARM Cell	*0.75*
AND	0.13µm	ARM Cell	*1.25*
OR	0.13µm	ARM Cell	*1.25*
MUX	0.13µm	ARM Cell	*2.25*
NAND	0.13µm	ARM Cell	*1.00*
XOR	0.13µm	ARM Cell	*2.00*
D FLIP FLOP	0.13µm	ARM Cell	*4.25*

GEs of lightweight ciphers are the most important attribute while implementing in applications like IoT. SR-LED design has 1474 GEs slightly higher than LED due to addition of S-box of RECTANGLE and bit slicing technique. SR-LED has a competitive GEs with PRESENT, RECTANGLE and PICCOLO. Figure 5 depicts SR-LED to be an ultra lightweight design as it requires less number of GEs.

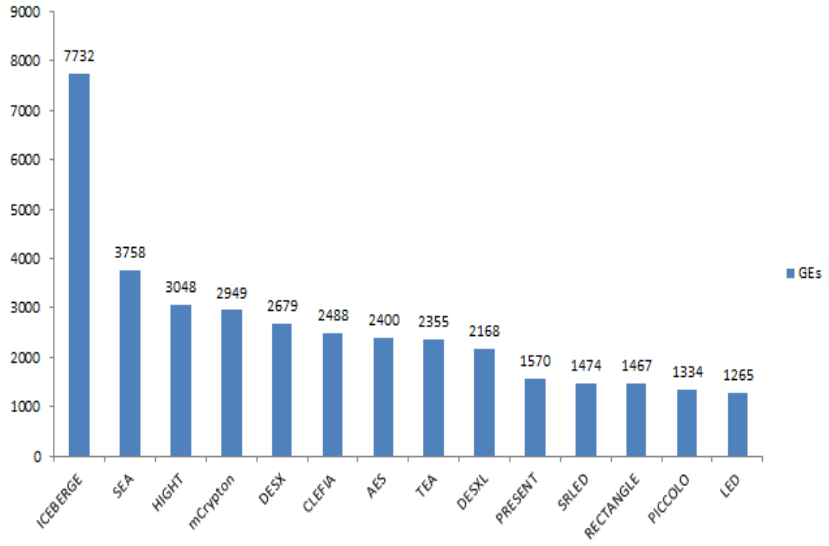

Figure 5. GEs Comparison of Lightweight Ciphers

Figure 6 shows power calculations for modified LED hybrid design. We have written code in Verilog and implemented on Vertex 6 and package as ff484 with Xilinx. For power calculation, Xpower analyzer of Xilinx is used. 1293 mWatts is the power consumption for hybrid design. We believe that power consumption can be further

reducing the number of gates required for designing the logic. SR-LED design needs 336 number of logics, 508 number of signals and 199 I/Os which is less as compared to PRESENT shown in Figure 7.

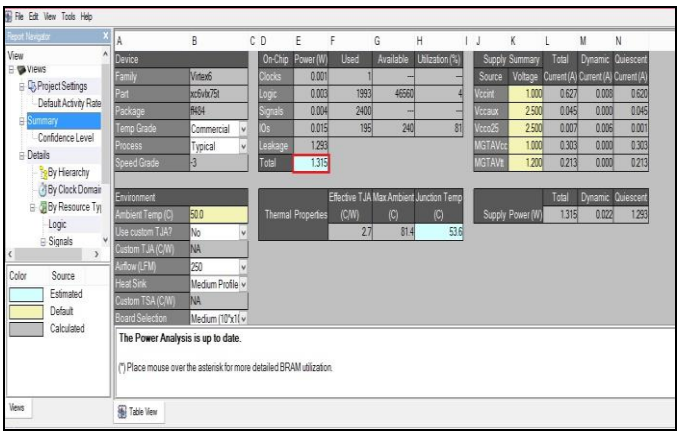

Figure 6. Power Calculation for Hybrid Design SR-LED

Power calculation mainly depends on operating frequency and technology used, in our design we kept frequency to 10MHz and technology used is of family Virtex 6.

For reference, we have also calculated power for PRESENT cipher as it is the most compact cipher known so far. PRESENT needs 1.332 Watts for its implementation on hardware.

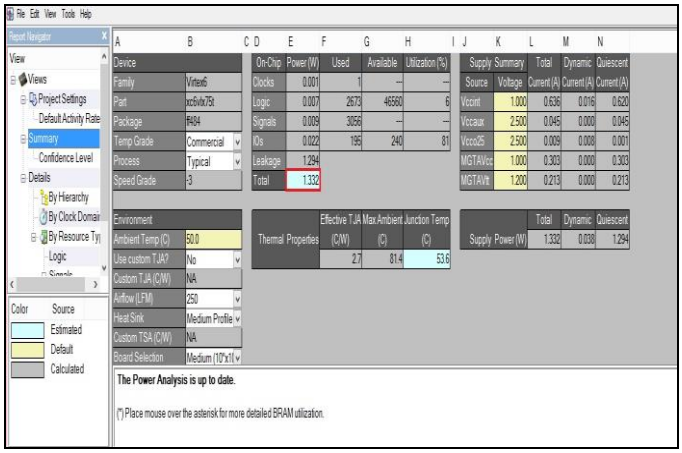

Figure 7. Power Calculations for PRESENT Cipher

SRLED consumes less power than PRESENT and LED cipher because of less footprint area requirement. LED consumes power of 1.395 watt.

6. Conclusion

In this paper, we aimed at strengthening the LED cipher by including SPECK key scheduling which was neglected during the design of LED cipher. This might expose LED to the related key attacks. SPECK key scheduling perfectly meets the requirement of LED cipher, by producing perfectly 13 keys of 64 bits each. Moreover, in this paper, we have deigned compact hybrid system for LED cipher which results in less footprint area as compared to LED cipher design. To the best of our knowledge, this is the most compact and smallest implementation of LED cipher so far. We have also replaced S-box

of PRESENT with S-box of RECTANGLE because of the serious problem of clustering of trails with PRESENT. RECTANGLE has robust S-box design and limited number of trials which make the design more robust and secure against all possible types of attacks. Further, we have also added bit slice technique which increases the software performance of LED cipher and also results in good difference propagation due to column wise substitution. This hybrid design which is a combination of SPECK, RECTANGLE and LED improves the linear and differential characteristics of LED cipher design. This hybrid design not only provides robust architecture but also results in lightweight implementation which consumes only about 1474 GEs which is competitive with the ultra lightweight cipher PRESENT. This hybrid design is robust and will provide resistance against all types of possible attacks. Further, research on this hybrid design is required to implement all types of other possible attacks which ensure robustness of design. We have achieved robust design at the cost of throughput. Further improvements can be planned to achieve higher throughput by reducing execution time. This paper provides a novel approach of hybrid design implementation of lightweight cipher which will have a positive impact in the field of lightweight cryptography

Test Vectors

Plain Text:	Key	Cipher Text
0123456789abcdef	0123456789abcdeffedcba9876543210	4d640afc4d2e8134

Acknowledgment

The authors would like to thank Symbiosis Institute of Technology, Pune, Symbiosis International University, Pune for providing resources to carry out this research successfully.

References

[1] P, Nikolaos E., Ioannis G. Askoxylakis, and Theo Tryfonas. "Life-logging in smart environments: challenges and security threats." Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012.
[2] A. Juels and S. A. Weis. Authenticating pervasive devices with human protocols. In V. Shoup, editor, Advances in Cryptology — CRYPTO 2005, Volume 3126 of Lecture Notes in Computer Science, pages 293–198. Springer-Verlag, 2005.
[3] NIST (National Institute of Standards and Technology), “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, November 2000.
[4] National Bureau of Standards (NBS), “Data Encryption Standard (DES),” Federal Information Processing Standards Publication 46-2, December 1993.
[5] National Institute of Standards and Technology. FIPS 46-3: Data Encryption Standard (DES). Available via http://csrc.nist.gov, October 1999.
[6] Schneier, B. (1994, January). Description of a new variable-length key, 64-bit block cipher (Blowfish). In Fast Software Encryption (pp. 191-204). Springer Berlin Heidelberg.
[7] B. William Curt. Recommendation for the triple data encryption algorithm (TDEA) block cipher. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2004.
[8] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In CHES, volume 4727 of LNCS, pages 450-466. Springer, 2007.
[9] D. Wheeler and R. Needham. TEA extensions. October 1997. Available via www.ftp. cl.cam.ac.uk/ftp/users/djw3/. (Also Correction to XTEA. October, 1998).
[10] Z. Gong, S. Nikova and Y.-W. Law. A New Family of Lightweight Block Ciphers. In A. Juels and C. Paar, editors, RFIDSec 2011, Springer, to appear, 2011. Available via http://www.rfidcusp.org/rfidsec/files/RFIDSec2011DraftPapers.zip.`
[11] S. Tomoyasu, *et al*. "\ textnormal {\ textsc {TWINE}}: A Lightweight Block Cipher for Multiple Platforms." Selected Areas in Cryptography. Springer Berlin Heidelberg, 2013.
[12] S. Tomoyasu, *et al*. "Twine: A lightweight, versatile block cipher." ECRYPT Workshop on Lightweight Cryptography. 2011.

[13] D. Engels,., Saarinen, M. J. O., Schweitzer, P., & Smith, E. M. (2012). The Hummingbird-2 lightweight authenticated encryption algorithm. In RFID. Security and Privacy (pp. 19-31). Springer Berlin Heidelberg.
[14] J. Guo,., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. Cryptographic Hardware and Embedded Systems CHES 2011, LNCS, Vol. 6917/2011, pp. 326-341. Springer (2011).
[15] J. Guo, Nikolic, I., Peyrin, T., & Wang, L. (2013). Cryptanalysis of Zorro. IACR Cryptology ePrint Archive, 2013, 713.
[16] S. Kyoji, *e.g.* "Piccolo: an ultra-lightweight blockcipher." Cryptographic Hardware and Embedded Systems–CHES 2011. Springer Berlin Heidelberg, 2011. 342-357.
[17] R. Beaulieu, D. Shors,, Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). The SIMON and SPECK Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive, 2013, 404.
[18] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128bit blockcipher CLEFIA." in Proceedings of Fast Software Encryption- FSE'07 (A. Biryukov, ed.), no. 4593 in LNCS, pp. 181-195, SpringerVerlag, 2007.
[19] "The 128-bit blockcipher CLEFIA: Algorithm specification." On-line document, 2007. Sony Corporation.
[20] D. Wheeler and R. Needham. TEA, a Tiny Encryption Algorithm. In B. Preneel, editor, Fast Software Encryption — FSE 1994, volume 1008 of Lecture Notes in Computer Science, pages 363–366. Springer-Verlag, 1994.
[21] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel. A Survey of Lightweight Cryptography Implementations. IEEE Design & Test of Computers – Special Issue on Secure ICs for Secure Embedded Computing, 24(6): 522-533, November/December 2007.
[22] W. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2014). RECTANGLE: A Bit-slice Ultra-Lightweight Block Cipher Suitable for Multiple Platforms. IACR Cryptology ePrint Archive, 2014, 84.
[23] C. De Canniere, , Orr Dunkelman, and Miroslav Knežević. "KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers." Cryptographic Hardware and Embedded Systems-CHES 2009. Springer Berlin Heidelberg, 2009. 272-288.
[24] F. Abed,., List, E., Lucks, S., & Wenzel, J. (2013). Cryptanalysis of the Speck Family of Block Ciphers. IACR Cryptology ePrint Archive, 2013, 568.
[25] R. Anderson, E. Biham and L. Knudsen, "Serpent: a proposal for the advanced encryption standard," NIST AES proposal 174, June 1998.available at ftp://dijkstra.urgu.org/crypto/Serpent/v1/res/serpent.pdf
[26] K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley and Sons, 2003.
[27] Biham, E., Shamir, A.: Diff erential Cryptanalysis of the Data Encryption Standard. Springer, Heidelberg (1993).
[28] M. Matsui,.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994).
[29] F. Abed, , List, E., Lucks, S., & Wenzel, J. (2013). Cryptanalysis of the Speck Family of Block Ciphers. IACR Cryptology ePrint Archive, 2013, 568.
[30] D. Itai, "Improved Differential Cryptanalysis of Round-Reduced Speck." IACR Cryptology ePrint Archive 2014 (2014): 320

