Modified SIMON and SPECK: Lightweight Hybrid Design for Embedded Security

GAURAV BANSOD, NISHCHAL RAVAL, NARAYAN PISHAROTY, ABHIJIT PATIL
Electronics and Telecommunication
Symbiosis Institute of Technology, Symbiosis International University
Lavale, Pune, 412115, Maharashtra
INDIA
gauravb@sitpune.edu.in, nishchal.raval@sitpune.edu.in, narayanp@sitpune.edu.in, abhijit.patil@sitpune.edu.in

***Abstract*— Lightweight cryptography is an emerging field that will play a critical role in areas like pervasive computing and Internet of Things (IoT). In recent years, many lightweight ciphers have been designed that are better suited for small scale embedded security. Lightweight ciphers like PRESENT, KLEIN, Hummingbird 2, XTEA, CLEFIA etc. are the ciphers known for compact hardware implementations. Recently SIMON and SPECK ciphers have been introduced which are Feistel based designs. SIMON and SPECK are flexible and are having very less memory requirements and better performance in both hardware and software. There is always a tradeoff between security and performance. Strengthening the design of these ciphers will increase their acceptability for all embedded applications. In this paper, we have proposed a novel approach which increases the strength and performance of SIMON and SPECK. Further a confusion layer is added in the design of the newly designed cipher RECTANGLE. RECTANGLE has a robust S-box as compared to other lightweight ciphers which makes the design fast and efficient. We have added the substitution property to the SIMON and SPECK cipher after analyzing the cryptanalysis properties of both the ciphers. S-box of RECTANGLE is best suited for SIMON and SPECK because the SIMON and SPECK designs have an asymmetric permutation which is the basic requirement for RECTANGLE. Combination of S-box and asymmetric permutation together achieves a robust design. The hybrid design proposed in this paper needs less memory space as compared to the existing ciphers. This approach makes SIMON and SPECK design more robust and resistive against all possible attacks due to the addition of the non-linear substitution layer. This robust design will have a positive impact in the field of lightweight cryptosystems.**

***Index Terms*— Lightweight cryptography, RECTANGLE, SIMON, SPECK, Embedded Security, Encryption, Bit slice instructions, pervasive computing.**

I. INTRODUCTION

Pervasive computing is an emerging field that needs devices which have less power consumption and less memory requirements specifically devices like RFID tags and wireless sensor nodes. Privacy is of a great concern in applications like internet of things (IoT) where each device has intelligence and has the ability to communicate with other devices. The total Gate Equivalents (GEs) required to build an RFID tag circuit is approximately 10000. In that design for providing security, the GEs should not be more than 2000-2200 [1][2]. For such applications, the ciphers like AES [3], DES [4][5] are not suitable for deploying security, as they need 2400-3500 GEs. This has led to the emergence of the field of lightweight cryptography. In this field, new ciphers are needed which have less GEs and have less RAM and Flash requirements. In recent years, many lightweight ciphers have been designed.

These lightweight ciphers are either block ciphers or stream ciphers. In block ciphers, the ciphers are divided either as Feistel structures or as SP-networks. Stream ciphers are compact in nature, which results in smaller hardware implementation and faster throughput. However, the stream ciphers are also known to be vulnerable to serious attacks. Specially, by using reused key attacks, stream ciphers can be broken while block ciphers are versatile structures and they have made their mark in the cryptographic environment as structures that are difficult to break. KLEIN [6], PRESENT [7], LED [8], mCrypton [9] and ZORRO [10] are SP-network block ciphers, while CLEFIA [11][12], PICCOLO [13], TWINE [14][15], TEA [16], XTEA [17], SIMON [18] and SPECK [18] are Feistel networks. These Feistel networks have classifications as Generalized Feistel structures (GFS) and classical Feistel structures. In GFS, a block size is divided into more than or equal to 3 sub blocks. CLEFIA is the example of GFS developed by SONY. But, the GFS has the disadvantage of requiring more number of rounds to provide optimum security. KATAN and KTANTAN are based on stream ciphers [19].

Table 1 shows the comparison of lightweight ciphers and their classifications. All these ciphers have GEs ranging from 1000 to 3000. Among these PRESENT and SIMON are considered to be ultra lightweight designs and have compact hardware implementations. All these ciphers have been implemented on a processor and the results are compared with our hybrid design in this paper. Our main focus in this paper is on block ciphers as they are the versatile structures for

providing security in embedded applications.

TABLE 1
COMPARISON OF LIGHTWEIGHT CIPHERS

Ciphers	Block Size	Key Size	Structure	No. of Rounds
AES [3]	128	128	SP	10
CLEFIA [11][12]	128	128	Feistel	18
DESXL [20]	64	184	Feistel	16
HIGHT [21]	64	128	Feistel	32
KATAN & KTANTAN [19]	32 /48 /64	80	Stream	254
KLEIN [6]	64	64 /80 /96	SP	12/16/ 20
LBLOCK [22]	64	80	Feistel	32
LED [8]	64	64 /128	SP	32/48
ZORRO [10]	128	128	SP	24
mCRYPTON [9]	64	64 /96 /128	SP	12
PICCOLO [13]	64	80 /128	Feistel	25/31
PRESENT [7]	64	80 /128	SP	31
TEA [16] & XTEA [17]	64	128	Feistel	64
TWINE [14][15]	64	80 /128	Feistel	36
SIMON [18]	64 /128	128 /256	Feistel	68
SPECK [18]	64 /128	128 /256	Feistel	68
PUFFIN-2 [23]	64	128	SP	34
RECTANGLE [24]	64	80	SP	25
FEW [25]	64	80	Feistel	32
I-PRESENT [26]	64	80	SP	30

PRESENT is considered to be the most compact lightweight block cipher and which is also designated under ISO/IEC as the standard for lightweight cryptography. PRESENT has shown resistance against structural, algebraic and key schedule attacks [7]. It has good linear and differential cryptanalysis which makes the design robust. Hummingbird-2 is a hybrid lightweight cipher which is a combination of block and steam ciphers which was considered to be robust [27]. However, in 2013, Hummingbird-2 was broken by using a related key model. RECTANGLE [24] is the latest cipher based on SP-network and reported in literature. RECTANGLE has a robust S-box and the use of bit slice instructions makes the design faster and efficient on the software platform. Recently, SIMON and SPECK have emerged as the new ultra lightweight designs for embedded security [18]. These ciphers are at par in performance as compared to PRESENT. SIMON and SPECK are based on Feistel structure and have around 1000 GEs which is considered to be the best suited for small scale embedded systems. Some of the papers have reported differential cryptanalysis of SIMON and SPECK cipher [28][29][30]. SIMON has shown resistance against differential attacks and has good avalanche effect which makes the cipher design more robust.

In our research, we made an attempt to increase the strength of SIMON and SPECK by using S-box of the cipher RECTANGLE. S-box of RECTANGLE is chosen because of its robust design criteria. S-box of PRESENT is very compact but has various security issues [24]. S-box of RECTANGLE has an edge over the S-boxes of other lightweight ciphers due to its robust design. S-box of RECTANGLE is best suited design to be interfaced with SIMON and SPECK to achieve higher strength and resistance against all possible attacks. The inferences drawn by us from the past work also show that the addition of the confusion property in Feistel structure always benefits the design by increasing the resistance against attacks on the cipher. DES [4][5] and BLOWFISH [31] have used the confusion property to make their designs robust.

Section II shows SIMON and SPECK implementation on a 32 bit processor for variable block and key sizes. Section III shows the novel approach of designing robust lightweight design by using S-box of RECTANGLE cipher and the use of bit slice instructions. Section IV is devoted to various lightweight ciphers, comparison and implementation on 32 bit processor LPC2129. Section V depicts the security issues related to the new hybrid design. All above implementations reported in this paper are carried on the processor LPC2129 of the ARM family. LPC2129 is well suited for small scale embedded systems. It has 128/256 kB on-chip Flash Program Memory.128-bit wide interface/accelerator enables high speed 60 MHz operation. It also has Embedded ICE-RT interface enables breakpoints and watch points. Interrupt service routines can continue to execute while the foreground task is debugged with the on-chip 'RealMonitor' software. LPC2129 has the feature of individual enable/disable of peripheral functions for power optimization. All of the above characteristics make this processor an obvious choice for implementation. All the implementations and the designs presented in this paper are carried out on the same platform.

II. SIMON AND SPECK DESIGN

SIMON and SPECK are the recent lightweight block ciphers which are highly optimized to perform efficiently on hardware and software. Generally, the function which runs efficiently on hardware will have slower performance on hardware and vice versa. SIMON is specifically meant to perform efficiently on hardware and SPECK is for the software [18]. These designs are flexible and highly optimized to meet the future requirements for lightweight cryptography and fields like IoT [32]. SIMON and SPECK are versatile block ciphers which are designed to operate on various block sizes and key sizes. Block size of SIMON and SPECK vary from 32 to 128 bits and key size also from 64 to 256 bits. The design that is best suited for pervasive computing is 64 bit block size and 128 bit key size. In this section, we have implemented SIMON and SPECK cipher on 32 bit processor

with 80, 96 and 128 bit key sizes and 64 and 128 block sizes. These specifications are common and popular among many lightweight ciphers. Various lightweight ciphers like PRESENT, CLEFIA, KLEIN, TWINE and PICCOLO are implemented with the same key and block sizes.

SIMON block cipher [18] is having block size of 2b, where b is the word size and key size of n × b, where n is number of keywords. R is number of rounds required for specific length of block and key size. SIMON and SPECK cipher have two parts, one is key expansion and other is encryption. Key expansion accepts word size of 'n' and accordingly makes 'm' key words. These 'm' keywords of 'n' word size are applied to key expansion. In the key expansion, numbers of keywords are generated by 'Ex-oring' the n keyword with 'C', which is a constant sequence of 62 bits. 'C' varies from 0 to 4, where each constant consisting of 62 bits. More keys are generated in this scheduling section based on number of rounds R. Table 2 shows key expansion components.

TABLE 2
KEY EXPANSION COMPONENTS OF SIMON CIPHER

BLOCK SIZE 2b	WORD SIZE b	KEY WORDS n	KEY SIZE b × n	CONSTANT SEQUENCE	ROUNDS R
32	16	4	64	C_0	32
48	24	3 4	72 96	C_0 C_1	36 36
64	32	3 4	96 128	C_2 C_3	42 44
96	48	2 3	96 144	C_2 C_3	52 54
128	64	2 3 4	128 192 256	C_2 C_3 C_4	68 69 72

Encryption of SIMON cipher consists of bitwise 'XOR', bitwise 'AND' and left circular shift by 'j' bits. A total key size based on the number of rounds is used during encryption. Fig. 1 shows the block diagram of SIMON block cipher for 64 block size and 128 bit key size.

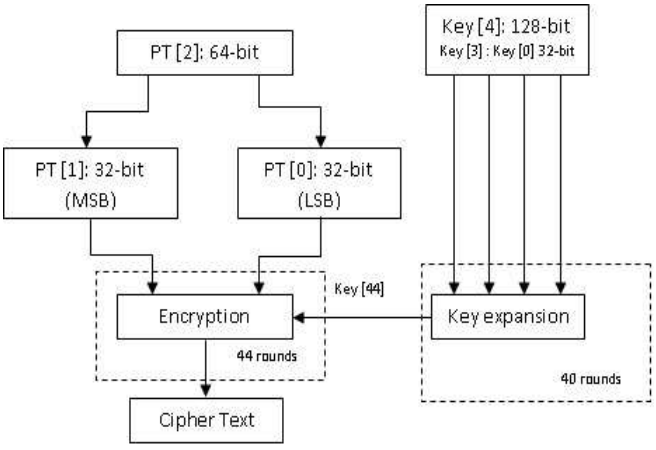

Fig. 1: SIMON Block Diagram for 64/128

SPECK [18] is lightweight block cipher with block size of 2b, where b is word size. Key size of n × b, where n is number of keywords. R is number of rounds for specific block and key size. In SPECK key scheduling, the constant 'C' is not used. Instead of that two variables, α and β are the constants used for key expansion. More keys are produced in this scheduling section by 'OR-ing', 'Ex-ORing', left and right circular shift by α and β. –α represents right circular shift while +β represents left circular shift. Table 3 shows SPECK key scheduling components.

TABLE 3
KEY EXPANSION COMPONENTS OF SPECK CIPHER

BLOCK SIZE 2b	WORD SIZE b	KEY WORDS n	KEY SIZE b × n	Rot α	Rot β	ROUNDS R
32	16	4	64	7	2	22
48	24	3 4	72 96	8	3	22 23
64	32	3 4	96 128	8	3	26 27
96	48	2 3	96 144	8	3	28 29
128	64	2 3 4	128 192 256	8	3	32 33 34

SPECK cipher consisting bitwise 'XOR', addition modulo 2b and left and right circular shifts by α and β. Fig. 2 shows block diagram for SPECK 64 bit block size and 128 bit key size.

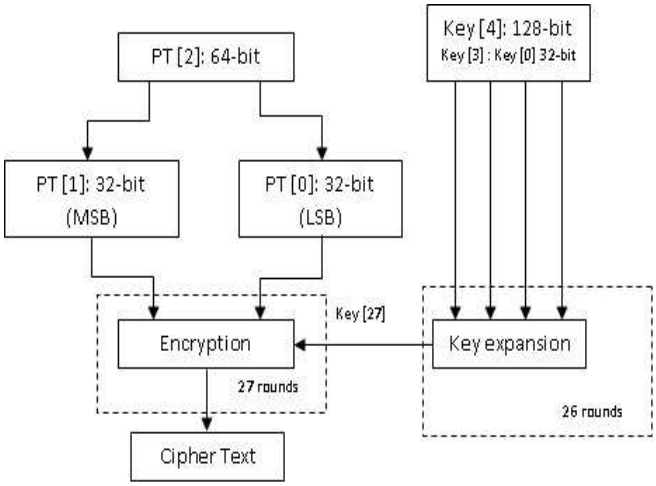

Fig. 2: SPECK Block Diagram for 64/128

SIMON and SPECK ciphers are implemented on 32 bit processor for variants 64/128, 64/96 and 128/128. Flash memory and RAM memory size is calculated and displayed in Table 4. SPECK results in compact memory implementation because of tightly constrained key scheduling as compared to SIMON. We have chosen only few variants of SIMON and SPECK as these key sizes and block sizes are popular among other light weight ciphers.

TABLE 4
RAM AND FLASH MEMORY REQUIREMENTS OF SIMON AND SPECK ON 32 BIT PROCESSOR

Ciphers	Block Size	Key Size	Flash Memory (Bytes)	RAM Memory (Bytes)
SIMON	64	96	2308	1256
	64	128	2324	1256
	128	128	2744	1256
SPECK	64	96	1720	1256
	64	128	1728	1256
	128	128	2164	1256

Fig. 3 represents SIMON and SPECK execution time on 32 bit processor which is necessary for calculating overall throughput of encryption as well as decryption. SPECK results in least execution time because of compact structure. Execution time denotes amount of time required for converting plain text to cipher text.

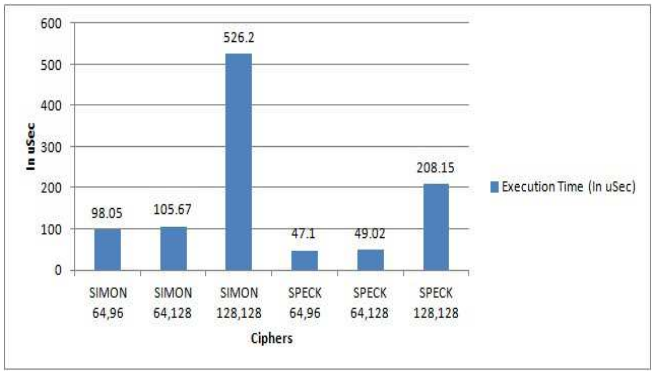

Fig. 3: Execution Time for SIMON and SPECK

One of the important parameters in the comparison of ciphers is throughput. Higher throughput will result in faster execution. Fig. 4 represents throughput for SIMON and SPECK on LPC2129. There is always tradeoff between throughput and security which is addressed in Section III. SPECK results in higher throughput due to its less execution time. As we increase the size of block length, throughput of the cipher decreases accordingly and vice versa [18].

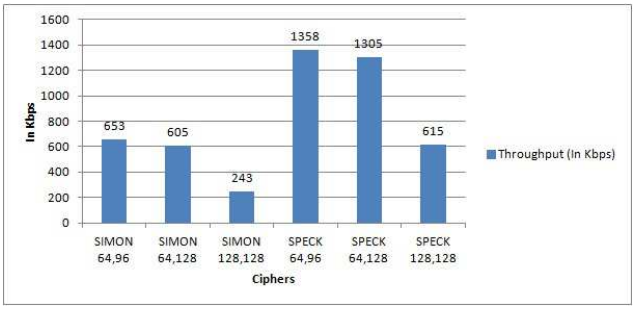

Fig. 4: Throughputs for SIMON and SPECK

III. MODIFIED SIMON AND SPECK DESIGN: NEW HYBRID LIGHTWEIGHT DESIGN

SIMON and SPECK are based on Feistel structure. SIMON and SPECK are designed to perform efficiently both on hardware and software platforms. The advantages of these ciphers are their ultra lightweight design that results in approximately 1000 GEs. As it is a Feistel structure, it executes at a faster rate and at a given time only one bit gets updated, and not the blocks. Serialized architecture has been followed in designing these ciphers. These architectures can be optimized easily to achieve compact design but at a lesser throughput. Literature review suggests that lesser throughput is not the constraint of lightweight applications. Instead of a single bit to get updated, if block is updated, it results in higher throughput. DES, AES are examples of higher throughputs.

SIMON and SPECK are designs consisting of simple round functions, which may be susceptible to attacks like open key model attacks. Open key models are categorized as chosen key models and known key models. These attacks are well known and can be avoided by adding strong non-linear properties and increasing the number of rounds and the key size. If these are achieved in SIMON and SPECK, then design could be even helpful while implementing hash functions.

While studying cryptanalysis of SIMON and SPECK, we felt the need of the non-linear element in the design which could further improve the design of the cipher and it could then be resistant all possible key based attacks. In this paper, we have proposed a novel approach for strengthening the existing design of SIMON and SPECK. Non-linearity plays a very important role in deciding the strength of a cipher. Inferences from our past work also shows that Feistel based structures in which a non-linear element is incorporated has better resistance against all possible attacks as compared to the rest of Feistel structure based ciphers which lack substitution property. BLOWFISH [31], DES [4][5], TRIPLE DES [33] all use a nonlinear element known as S-box. DES was prone to attacks because of shorter key size length. Later, TRIPLE DES has been proposed which uses sufficient key size that provides resistance against key schedule attacks. BLOWFISH is the best example of Feistel cipher that uses S-box and gives efficient encryption rate and optimum security.

In lightweight cryptography, various S-boxes have been designed and have been implemented to produce a robust cipher [34]. In this paper, we have carefully analyzed various S-boxes of lightweight ciphers to be suited of SIMON and SPECK design. Analysis includes their non-linearity property, differential and linear cryptanalysis, robust and compact design. We took care of not disturbing the basic differential cryptanalysis and properties of SIMON and SPECK while introducing this concept in design.

PRESENT [7], the most engineered cipher, has the most efficient and compact S-box among other lightweight ciphers. It has better linear [35] and differential [36] cryptanalysis properties and has shown resistance against structural and algebraic attacks. But, the PRESENT S-box is designed to provide compact structure, not for a robust design. Security

analysis of S-box shows its vulnerability against attacks [7][24]. PRESENT S-box undergoes clustering of trails which results in poor linear cryptanalysis. Recently, RECTANGLE, the new cipher is introduced based on SP-network which has the robust design as compared to PRESENT. RECTANGLE due to its robust and compact design also achieves good speed both in hardware and also at software platforms [24].

RECTANGLE is the only ultra lightweight cipher which achieves optimum and competitive speed as compared to SIMON and SPECK which results in higher throughput. RECTANGLE has 4 bit S-box. It needs 25 rounds to be in resistive mode against all possible attacks. Due to the robust design of S-box, it has lesser number of trails which results in difference propagations with lower probabilities. This makes the design achieve good results when differential cryptanalysis is done [24]. Clustering of linear trails in RECTANGLE is limited and 25 rounds are good enough to resist linear cryptanalysis attacks. For construction of 4 bit S-box, we need approximately 40 GEs according to ARM CELL LIBRARY for IBM 0.13 micron process. Table 5 shows 4 bit S-box of RECTANGLE.

TABLE 5
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

The aim of interfacing of S-box of RECTANGLE with SIMON and SPECK design is to make the design robust against all possible attacks. S-box of RECTANGLE is suited only for those applications where permutation is asymmetric [24]. Together, these two characteristics help to achieve the desired strength and make the cipher resistant to attacks. SIMON and SPECK design have asymmetric permutation layer and stronger cryptanalysis properties. Addition of substitution property which is best suited for asymmetric permutation is of the cipher RECTANGLE. This hybrid design achieves a very high security and performance tradeoff. Addition of confusion layer in current SIMON and SPECK design will make this design versatile for its use as a secure cipher in most applications.

Fig. 5 represents the comparison of the S-boxes of other lightweight ciphers on the basis of memory requirements. Most of the ciphers in the Fig. 5 represent 1296 as flash memory and 1256 as RAM memory. All these ciphers are having 4 bit S-boxes. SEA (Scalable Encryption Algorithm) results in small size as compared to others due to the use of 3 bit S-box. But, SEA requires more number of rounds to secure its structure against attacks.

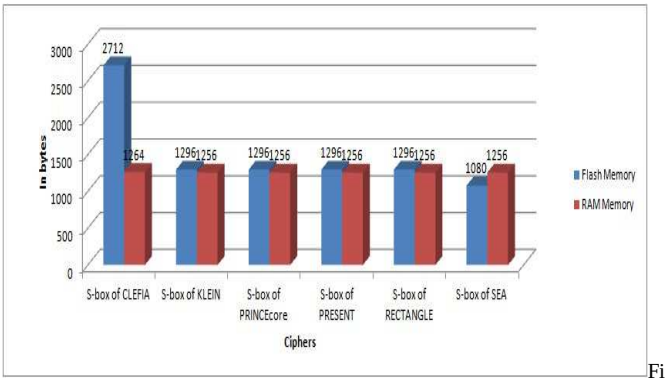

Fig. 5: S-Box comparison of lightweight ciphers

S-box is interfaced with the design of SIMON both in the key expansion and also in the encryption mode. 4 bit to 4 bit S-box is interfaced with the given block size and key size. Each key is passed through the S-box and the updated key will generate new keys. In SIMON block cipher, number of rounds are 44 which are used to generate 44 different keys. S-box is also used 44 times in the modified SIMON design. Every time the key is updated through the S-box. Each round adds strength to the cipher and makes the design more robust. Similarly, in encryption, plain text is passed through the S-box and after each round the value gets updated. Fig. 6 shows the block diagram for the updated SIMON design.

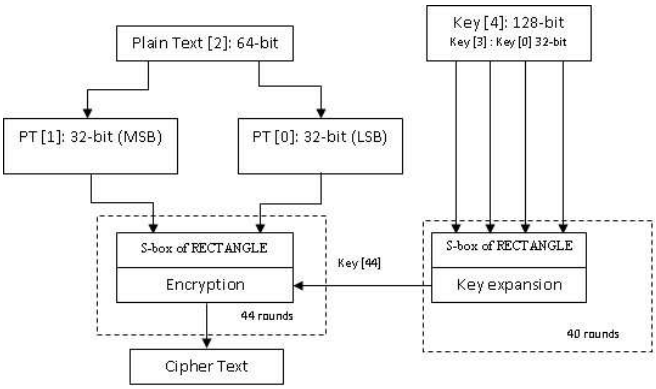

Fig. 6: Block Diagram of modified SIMON design

Fig. 7 shows memory requirements of modified SIMON design for various block and key sizes. Modified SIMON design of 64/96 results in 2492 bytes of Flash memory space which is acceptable and desirable for all lightweight applications like IoT and Wireless sensor nodes. Comparison with other light weighted ciphers is discussed in Section IV.

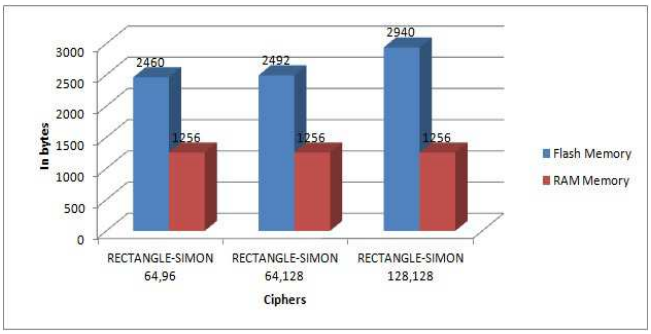

Fig. 7: Memory requirements for modified SIMON

Table 6 shows number of cycles required for this hybrid model. It also shows execution time and throughput of modified SIMON cipher. Cipher having less execution time and less number of bytes of plain text results in higher throughput.

TABLE 6
THROUGHPUT, EXECUTION TIME AND NUMBER OF CYCLES FOR MODIFIED SIMON

Ciphers	Execution Time (In µSec)	Throughput (In Kbps)	No. of Cycles
RECTANGLE-SIMON 64,96	318.1	201	19086
RECTANGLE-SIMON 64,128	333.87	192	20032
RECTANGLE-SIMON 128,128	1838.33	70	110300

Fig. 8 shows modified SPECK interface for 64 bit block size and 128 bit key size. S-box is used at key expansion and also in encryption. In SPECK, each key is derived from its previous key. Modified SPECK design updates the first key through S-box which generates second key and so on. S-box rotates in 27 rounds in key expansion of SPECK.

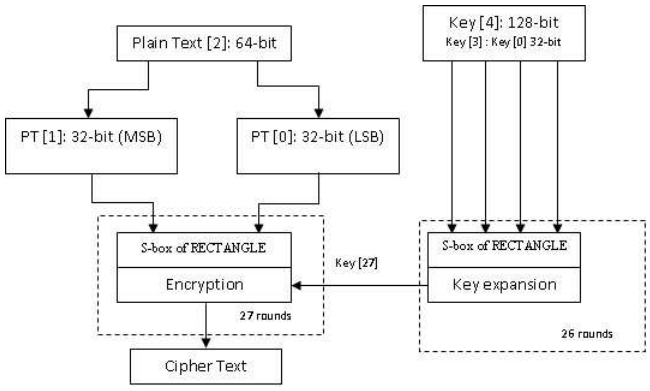

Fig. 8: Block diagram for modified SPECK

Fig. 9 shows RAM and Flash memory requirements for this hybrid model on 32 bit processor LPC2129. Modified SPECK needs less memory space as compared to modified SIMON due to its compact key scheduling and tight encryption design.

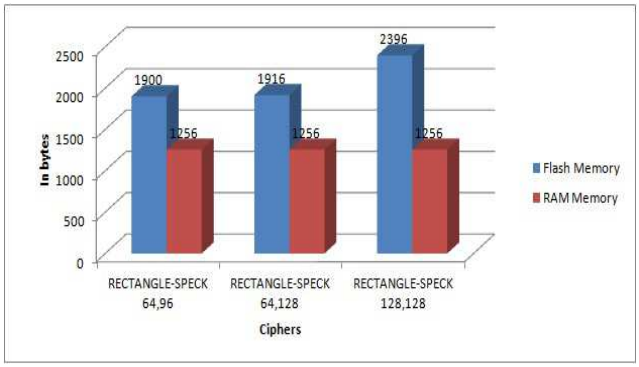

Fig. 9: Memory requirements for modified SPECK

Table 7 shows number of cycles needed for this hybrid design along with execution time and throughput. RECTANGLE-SPECK have higher throughput than RECTANGLE-SIMON and works efficiently on software based platforms. Modified SPECK of 64/96 results in higher throughput due to less number of cycles required for execution.

TABLE 7
THROUGHPUT, EXECUTION TIME AND NUMBER OF CYCLES FOR MODIFIED SPECK

Ciphers	Execution Time (In µSec)	Throughput (In Kbps)	No. of Cycles
RECTANGLE-SPECK 64,96	257.53	249	15452
RECTANGLE-SPECK 64,128	267.65	239	16059
RECTANGLE-SPECK 128,128	1134.94	113	68096

Throughput is calculated as total plain text in bytes encrypted by execution time required to convert plain text to cipher text. All codes of lightweight ciphers reported in this paper are having user defined block size, key size and plain text. 8 bit UART module acts as a demonstrator to see the output on UART window. Simulator used for executing codes is KEIL uVision version 4. All codes are written in embedded C. All codes are operated on hexadecimal inputs and produce hexadecimal outputs. The platform operates at 60 MHz clock frequency. This hybrid design adds strength to existing SIMON and SPECK cipher in terms of resistance to all types of possible attacks. Addition of compact S-box in Feistel network based on the suitability of given design always results in making the design more suitable for cryptographic environment. 8 bit S-box results in higher memory requirement while 4 bit S-box results in compact hardware implementation.

IV. Lightweight Ciphers, Implementation and Comparison

Many lightweight ciphers in recent years are designed and implemented for applications like ubiquitous computing. Lightweight ciphers are having less memory requirements, compact hardware implementations, less GEs and less power consumption. In this paper, the proposed hybrid design of SIMON and SPECK is compared with the other existing lightweight ciphers. All these lightweight ciphers are implemented on the same platform (LPC2129) on which SIMON and SPECK hybrid design is also implemented. Ciphers like PRESENT [7], CLEFIA [11][12], AES [3], KLEIN [6], LED [8], ZORRO [10], PICCOLO [13], TWINE [14][15] and KATAN [19] are implemented on the 32 bit processor. Comparison is made based on Flash and RAM size, throughput, execution time, number of cycles and GEs. Table 8 shows the RECTANGLE-SIMON and RECTANGLE-SPECK comparison with other light weight ciphers based on RAM and Flash memory requirement. Modified SIMON and SPECK memory requirements are very less as compared to all other lightweight ciphers except KLEIN. KLEIN also has similar memory requirement as our hybrid design. In this paper, we have not put any efforts for reducing bytes for our hybrid design as it results in decreasing throughput too. Table 8 clearly depicts modified SIMON and SPECK to be the ultra lightweight compact design in terms of memory requirements.

TABLE 8
Comparison with respect to Memory Size

Ciphers	Block Size	Key Size	Flash Memory	RAM Memory
LED	64	128	3876	1264
PICCOLO	64	128	3052	1256
PRESENT	64	128	3200	1320
TWINE	64	128	2380	1256
RECTANGLE-SIMON	64	128	2492	1256
RECTANGLE-SPECK	64	128	1916	1256
ZORRO	128	128	3024	1528
CLEFIA	128	128	4708	1256
AES	128	128	3716	2016
RECTANGLE-SIMON	128	128	2940	1256
RECTANGLE-SPECK	128	128	2396	1256
HUMMING BIRD-2	16	128	3852	1320
KATAN	64	80	4848	1256
KLEIN	64	96	2580	1256
RECTANGLE-SIMON	64	96	2460	1256
RECTANGLE-SPECK	64	96	1900	1256

Table 9 shows comparison with hybrid design based on parameters like execution time, throughput and number of cycles required to convert plain text to cipher text.

TABLE 9
Comparison with respect to Throughput, Execution Time and Number of Cycles

Ciphers	Block Size	Key Size	Execution Time (In uSec)	Throughput (In Kbps)	No. of Cycles
LED	64	128	7092.86	9	425572
PICCOLO	64	128	227.68	281	13661
PRESENT	64	128	3609.91	18	216595
TWINE	64	128	592.87	108	35572
RECTANGLE-SIMON	64	128	333.87	192	20032
RECTANGLE-SPECK	64	128	267.65	239	16059
ZORRO	128	128	913.21	140	54793
CLEFIA	128	128	1048.01	122	62881
AES	128	128	395.25	324	23715
RECTANGLE-SIMON	128	128	1838.33	70	110300
RECTANGLE-SPECK	128	128	1134.94	113	68096
HUMMING BIRD-2	16	128	316.27	51	18976
KLEIN	64	96	887.51	72	53251
RECTANGLE-SIMON	64	96	318.1	201	19086
RECTANGLE-SPECK	64	96	257.53	249	15452

From Table 9, it is clear that modified SIMON and SPECK have higher throughput in 64/96 and 64/128 ciphers. In 64 block size and 96 key size, modified SIMON and SPECK gives very high throughput compared to others. While in 64/128 modified SPECK design achieves higher throughput of 239 Kbps.

Fig. 10 shows GEs comparison of lightweight ciphers with our hybrid design. These results are based on ASIC implementation. In this paper, we have referred ARM CELL LIBRARY for IBM 0.13 micron ASIC process. For RECTANGLE S-box, the average gate equivalent consumption is approximately 40 GEs [7]. The bar-graph, in Fig. 10, suggests modified SIMON and SPECK to be the most compact hardware implementation in terms of GEs in all variants of block and key sizes. In Fig. 10, comparison is based on key and block sizes. First classification indicates 64 bit block size and 128 bit keys while second classification indicates 128 bit block size and 128 bit keys and third one indicates 64 bit block size and 96 bit keys for KLEIN; while KATAN has 64 bit block size and 80 bit key size. For 64/128 block ciphers, RECTANGLE-SIMON needs less GEs 1316 as

compared to other lightweight ciphers. In second classification of 128/128 cipher RECTANGLE-SIMON and RECTANGLE-SPECK both have less GEs as compared to AES. In the third classification, RECTANGLE-SIMON needs only 1154 GEs with 96 bit key size and 64 bit block size which is less compared to the KLEIN cipher.

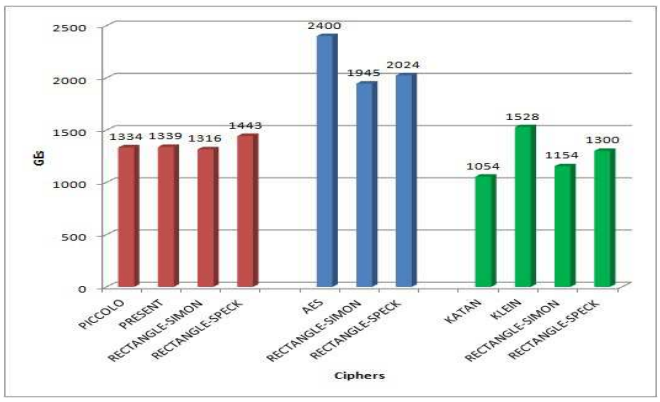

Fig. 10: GEs comparison of lightweight ciphers with modified SIMON and SPECK

V. Security Analysis

Differential [36] and Linear [35] cryptanalysis are the most important techniques for the cryptanalysis of ciphers. In this section we are reporting security analysis of modified SIMON and SPECK design. This hybrid model is a combination of cipher RECTANGLE and SIMON, similarly RECTANGLE and SPECK.

RECTANGLE's 4x4 S-boxes has asymmetric design with the permutation layer which reaches to strong security-level. For N-bit plain text, the probability must be larger than 2^{1-N} to achieve desire differential cryptanalysis with specific rounds. In RECTANGLE cipher, the probability must be larger than 2^{-63}. From paper [24], the differential probabilities are mentioned with no. of rounds in Table 10.

TABLE 10
Differential Probability of RECTANGLE

No. of Rounds	Probability	No. of Rounds	Probability
1	2^{-2}	9	2^{-36}
2	2^{-4}	10	2^{-41}
3	2^{-7}	11	2^{-46}
4	2^{-10}	12	2^{-51}
5	2^{-14}	13	2^{-56}
6	2^{-18}	14	2^{-61}
7	2^{-25}	15	2^{-66}
8	2^{-31}		

From Table 10, RECATANGLE achieve desire security in 15 rounds while in modified design of SIMON and SPECK it undergoes 44 and 27 rounds respectively.As it is kind of branch and bound cipher, the probability lies between 2^{-66} to 2^{-76} for differential trails for 15 rounds of RECTANGLE. Mostly, for 15 rounds of RECTANGLE, the probabilities are $2^{-65.66}$ and $2^{-67.87}$ for the best 32 differential propagations and for the maximum number of trails, respectively while the probabilities are $2^{-62.175}$ and $2^{-62.133}$ for 31996 trails and 83270 differential trails of 16 rounds of PRESENT.

Linear cryptanalysis for RECTANGLE 4 bit S-box, if the probability of linear trails is P, then the correlation of coefficient will be 2(P-1/2). For N-bit plain text, the amplitude of linear propagation must be higher than $2^{-N/2}$. So, in RECTANGLE cipher, the amplitude must be larger than 2^{-32}. From paper [24], the linear correlation coefficients are mentioned with no. of rounds in Table 11.

TABLE 11
Linear Correlation Coefficient of RECTANGLE

No. of Rounds	Correlation Coefficient	No. of Rounds	Correlation Coefficient
1	$\pm 2^{-1}$	9	$\pm 2^{-19}$
2	$\pm 2^{-2}$	10	$\pm 2^{-22}$
3	$\pm 2^{-4}$	11	$\pm 2^{-25}$
4	$\pm 2^{-6}$	12	$\pm 2^{-28}$
5	$\pm 2^{-8}$	13	$\pm 2^{-31}$
6	$\pm 2^{-10}$	14	$\pm 2^{-34}$
7	$\pm 2^{-13}$	15	$\pm 2^{-37}$
8	$\pm 2^{-16}$		

From paper [24], the amplitude of correlation coefficients is $2^{-34.58}$ for 883 linear trails for the 15 rounds of RECTANGLE while the amplitude of correlation coefficients is $2^{-22.63}$ for 435600 linear trails for the 16 rounds of PRESENT. From these results, RECTANGLE can resist against differential and linear cryptanalysis attacks by considering only 25 rounds. Modified SIMON and SPECK design has 44 and 27 rounds respectively will further strengthen the differential and linear properties of SIMON and SPECK.

Regarding S-box of RECTANGLE, assume ($D_i \rightarrow D_o$) where D_i indicates input difference and D_o indicates output difference. From paper [24], the probability will be 1 for (0100 → *1**), where * indicates don't care bit. Similarly, for inverse S-box of RECTANGLE, the probability will be 1 for (1100 → ***0). Hence, 4 rounds of RECTANGLE will achieve great dependency, from which full rounds of RECTANGLE-SIMON and RECTANGLE-SPECK may provide full resistance against impossible differential cryptanalysis.

We have also studied security analysis of SIMON and SPECK as they are base designs of our hybrid ciphers RECTANGLE-SIMON and RECTANGLE-SPECK.

SIMON is designed by the NSA with the aim of providing a cipher with an optimal hardware performance [28]. The SIMON has Feistel structure which is operating on two n-bit halves in each round, thus the general round block size is 2n bits. Because of these two n-bit halves in each round of SIMON, it gives better non-linearity which means it has also

non-invertible function A [28]:

$$A(y) = ((y \ll 8) \wedge (y \ll 1)) \oplus (y \ll 2)$$

In the paper [28], one of two properties of A are used to perform differential cryptanalysis. In type 1 characteristic with 6 rounds, the pairs of n-bit differences (x,y) are assumed for the combined probability $P(x \rightarrow y) \times P(x \rightarrow y)$ which is maximized. $P(x \rightarrow y)$ indicates the probability of x difference y over the function A which is taken over all inputs, where, x and y are the same input / output difference. In the type 2 characteristic for 3 rounds, a single difference x is used, for $P(x \rightarrow x)$ which is maximized [28].

In SP-network structure, N-bit S-box plays the key role for obtaining non-linearity and the output difference and the input difference on N consecutive bits. For the function A used in SIMON, there is no S-Box, and in general a single bit of the output difference ΔM depends on 2 bits of the input L and 3 bits of the input difference ΔL, which is shown below:

$$\Delta M_i = L_{i-1} \times \Delta L_{i-8} \oplus \Delta L_{i-1} \times L_{i-8} \oplus \Delta L_{i-1} \times \Delta L_{i-8} \oplus \Delta L_{i-2}$$

Where, all indices are computed as modulo n. For n = 16, for the type 1 characteristic, the best pairs (x,y) yield a probability [28]:

$$P(x \rightarrow y) \times P(x \rightarrow y) = 2^{-13}$$

Similarly, for the 6 rounds, 2^{-26} is the probability of type 1 characteristic. From the paper [28], for n = 16 and n = 24, the diagonal differential probabilities are mentioned in Table 12.

TABLE 12
DIAGONAL DIFFERENTIAL PROPERTIES

n	Prob.	Differences					
16	2^{-8}	5555	aaaa	ac0e	1d58	ab03	581d
		3ab0	6075	5607	0eac	b03a	7560
		c0ea	03ab	eac0	81d5	0756	d581
24	2^{-12}	555555	aaaaaa	0e22ac	1c4558	388ab0	711560
		c45581	e22ac0	88ab03	115607	22ac0e	45581c
		ab0388	b0388a	560711	8ab038		

From the Table 12, for n=16, the differences are very low, but it is also shown that the best probability for a diagonal entry is $2^{-n/2}$. So, the probability would be too low for such characteristic, even for two iterations of the type 2 characteristic, as the number of plain text pairs needed for the attack would exceed the possible number of plain text pairs, 2^{2n}. Hence, all these differences are calculated from the Feistel structure of SIMON without any N-bit S-box. So, after adding RECTANGLE's 4-bit S-box in SIMON, this S-box will result in strong and high differences in differential characteristics. In addition to interfacing a non-linear S-box in SIMON, we have tried to improve robustness of cipher SIMON which is one more step forward towards the improvement of security of this cipher.

SPECK family is straightforward ARX-based Feistel network (And,Or,Xor), that processes the input as 2 words. Two attacks are explained about the cryptanalysis of SPECK. One is Differential and other is Rectangle [29].

From paper [29], Differential characteristics are created for SPECK by employing a branch-and-bound algorithm. It is started from differences with one active bit within the middle, and generates all doable output differences when first round is completed.

In Differentials characteristic of SPECK, the key recovery attack is explained on SPECK-32/64 [29]. For SPECK-32/64, the differences from round 2 to round 9 are following:

$$D^2 = (D_{5,6,9,11}, D_{0,2,9,14}) \longleftrightarrow (D_{1,3,5,15}, D_{3,5,7,10,12,14,15}) = D^9$$

For above equation, the probability is 2^{-24} at round 9 which is also given in Table 13. D^2 indicates the differences for round 2 and D^9 indicates the differences for round 9. These differences are taken from the paper [29] which is indicated in Table 13.

TABLE 13
DIFFERENTIAL CHARACTERISTIC FOR SPECK-32/64

Rounds	D_m^i	D_n^i	Probability
0	$D_{5,6,9,11}$	$D_{0,2,9,14}$	
1	$D_{0,4,9}$	$D_{2,9,11}$	2^{-5}
2	$D_{11,13}$	D_4	2^{-9}
3	D_6	0	2^{-11}
4	D_{15}	D_{15}	2^{-11}
5	$D_{8,15}$	$D_{1,8,15}$	2^{-12}
6	D_{15}	$D_{1,3,10,15}$	2^{-15}
7	$D_{1,3,8,10,15}$	$D_{5,8,10,12,15}$	2^{-18}
8	$D_{1,3,5,15}$	$D_{3,5,7,10,12,14,15}$	2^{-24}

Key Recovery Attack process is conducted in three phases; a collection, a key guessing and a brute attack which are explained below [29]:

1. Collection Phase

- To choose 2^{28} plain text pairs (X_i, X_i'). After the 1st round, their difference is $X_i \oplus X_i' = D^2$.
- To collect cipher text pairs (Y_i, Y_i') after 1st round of decryption, where $Y_i = Z(X_i)$ and $Y_i' = Z(X_i')$.
- To calculate $D_m{}^9{}_{0\text{-}3}$, $D_n{}^9$ and store all cipher text pairs (Y_i, Y_i') with $D_m{}^9{}_{0\text{-}3} = D_3$ and $D_n{}^9 = D_{3,5,7,10,12,14,15}$ which are in a list У.

2. Key Guessing Phase

- To initialize 2^{12} counters list.
- For the 12 key bits $Ke^{9}_{4\text{-}15}$, and for all cipher text pairs $(Y_i,Y_i') \in Y$; Partially decrypted cipher text (Y_i,Y_i') to the state after completion of round 9, and calculate D_m^{9}. If $D_m^{9} = D_{1,3,5,15}$, then increment the counter of the current key.
- Output all keys must have a counter of at least four associated to them to be potentially correct.
- To Mark all pairs which are corrected D^9 for correct keys pairs.

3. Brute-force Phase

- Round by round all sub key bits $Ke^{9}_{0\text{-}3}$, Ke^{8}, Ke^{7}, and Ke^{6} are partially decrypted from all correct pairs.

From Table 13 and by considering above procedures, the probability of differential characteristic is nearly 2^{-24}. Hence, from the paper [29], error probability will be nearly 0 which satisfy D^9 for at least 4 pairs. Similarly, for 64 bit state size, the differences are calculated up to round 13 which are shown in Table 14 [29].

TABLE 14
DIFFERENTIAL CHARACTERISTIC FOR SPECK-64/K

Rounds	D_m^i	D_n^i	Probability
0	$D_{6,17,22,28}$	$D_{14,17,30}$	
1	$D_{9,17,20}$	$D_{1,9}$	2^{-5}
2	D_{12}	D_4	2^{-8}
3	0	D_7	2^{-9}
4	D_{30}	D_{30}	2^{-10}
5	$D_{22,30}$	$D_{1,22,30}$	2^{-12}
6	$D_{1,14,30}$	$D_{4,14,25,30}$	2^{-16}
7	$D_{4,6,7,14,22,30}$	$D_{1,4,6,14,17,22,28,30}$	$2^{-22.93}$
8	$D_{1,4,7,17,31}$	$D_{9,20,25}$	$2^{-31.82}$
9	$D_{20,23,28,31}$	$D_{12,20,31}$	$2^{-36.9}$
10	$D_{15,23,31}$	D2,31	$2^{-40.9}$
11	$D_{2,7,15,23,31}$	$D_{5,7,15,23,31}$	$2^{-44.9}$
12	$D_{5,26}$	$D_{2,5,8,10,18}$	$2^{-49.9}$
13	$D_{2,5,8,10,29}$	$D_{2,10,11,13,21,29}$	$2^{-55.9}$

One of the positive points of the NSA construction is the round-wise key addition which is a powerful key schedule. NSA is known for its interesting and robust key schedule. This feature protects the cipher from the slide and the meet-in-the-middle attacks with required number of rounds. Further, research is still going for security analysis of SPECK. In paper [30], the attacks have been reported for differential cryptanalysis based on framework. This type of attacks is sufficiently capable to break a cipher text with more rounds than the numbers of rounds are covered in differential cryptanalysis. Specifically, if it is used at applications where cipher text/plain text uses more number of secret keys than their own block size/state size. So, whenever designer proposes new cryptosystem, the sub-cipher attacks must be considered.

By addition of S-box of RECTANGLE in SIMON and SPECK Feistel structure, results in a cipher with more strength against attacks and makes this design more robust and suitable for deploying security in embedded systems. S-box of RECTANGLE in SIMON and SPECK structure has lesser number of trails which will results in difference propagations with very less probabilities. Due to the S-box of RECTANGLE in this hybrid design, clustering of linear trails are limited which results in robust design. Most of the ultra lightweight cipher has a problem of clustering of linear trail which make the design susceptible to attacks and results in very weak S-box. PRESENT S-box also has clustering problems, both in linear as well as in differential trails. Combination of S-box of RECTANGLE with SIMON and SPECK works because of asymmetric permutation. Further, cryptanalysis and attacks for this hybrid structure should be carried out in the future before implementing this design for any real time application.

VI. CONCLUSION

Pervasive devices and IoT are the fields that need compact and robust ciphers to address security issues in them. Research in Lightweight cryptography in recent years, has given rise to many lightweight ciphers that can be applied and implemented in applications like RFID sensors or wireless sensor nodes. SIMON and SPECK block ciphers have been designed recently and they have better properties as an ultra lightweight cipher as compared to the rest of the existing ciphers. In this work, we aimed at increasing the strength of these block ciphers so that it can be suitable for any embedded application. By interfacing nonlinear property in the existing architecture we have made the design more robust and more resistive against attacks like open key model and others. This paper proposes a novel approach by adding the S-box of ultra lightweight cipher RECTANGLE in the existing Feistel based structure of SIMON and SPECK. Inferences from the past work also suggest that the introduction of S-box in Feistel structure can drastically improve the security of the cipher.

A perfect S-box makes computational attacks infeasible and this makes the cipher design resistive against all types of structural and algebraic attacks. RECTANGLE S-box is best suited for the permutations which are asymmetric. SIMON and SPECK has asymmetric permutation. Adding a confusion property will improve its linear cryptanalysis and resistance to

known attacks. This hybrid design of SIMON and SPECK has added strength in the existing design and will make this structure more robust. Results also show its compactness over other ciphers in terms of memory size, execution time and throughput. This hybrid design can be tested for different possible attacks by cryptographic society and we hope this design will have a positive impact in the field of embedded security.

ACKNOWLEDGMENT

The authors would like to thank Symbiosis Institute of Technology, Pune, Symbiosis International University, Pune Prof Ayan Mahalanobis from IISER,Pune and eminent industrialists from automotive embedded domain, Pune for providing suggestions and valuable inputs to carry out this research successfully. Special thanks to Dr. Markku-Juhani O. Saarinen one of the coauthors of Hummingbird 2 cipher and whose guidance and suggestions helped us to pursue this line of research. Thanks to Axel York Poschmann and Ray Beaulieu whose thesis and work motivated this research and also prompted our ideas to carry on the work in the future.

REFERENCES

[1] K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley and Sons, 2003.

[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] 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. rfid-cusp.org/rfidsec/files/RFIDSec2011DraftPapers.zip.

[7] 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.

[8] Guo, J., 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).

[9] L. Brown, J. Pieprzyk, and J. Seberry. LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications. In J. Pieprzyk and J. Seberry, editors, Advances in Cryptology — AUSCRYPT 1990, volume 453 of Lecture Notes in Computer Science, pages 229–236. Springer-Verlag, 1990.

[10] Guo, J., Nikolic, I., Peyrin, T., & Wang, L. (2013). Cryptanalysis of Zorro. IACR Cryptology ePrint Archive, 2013, 713.

[11] 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.

[12] “The 128-bit blockcipher CLEFIA: Algorithm specification." On-line document, 2007. Sony Corporation.

[13] Shibutani, Kyoji, et al. "Piccolo: an ultra-lightweight blockcipher." *Cryptographic Hardware and Embedded Systems–CHES 2011*. Springer Berlin Heidelberg, 2011. 342-357.

[14] Suzaki, Tomoyasu, et al. "\ textnormal {\ textsc {TWINE}}: A Lightweight Block Cipher for Multiple Platforms." *Selected Areas in Cryptography*. Springer Berlin Heidelberg, 2013.

[15] Suzaki, Tomoyasu, et al. "Twine: A lightweight, versatile block cipher." *ECRYPT Workshop on Lightweight Cryptography*. 2011.

[16] 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.

[17] 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).

[18] Beaulieu, R., Shors, D., 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.

[19] De Canniere, Christophe, 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.

[20] 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.

[21] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee. HIGHT: A New Block Cipher Suitable for Low-Resource Device. In L. Goubin and M. Matsui, editors, Cryptographic Hardware and Embedded Systems — CHES 2006, number 4249 in Lecture Notes in Computer Science, pages 46–59. Springer-Verlag, 2006.

[22] Wu, Wenling, and Lei Zhang. "LBlock: a lightweight block cipher." *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, 2011.

[23] Wang, C., Heys, H. M.: An Ultra Compact Block Cipher for Serialized Architecture Implementations. In: Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2009), St. John’s, Newfoundland, May 2009. (2009)

[24] 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.

[25] Kumar, M., Pal, S. K., & Panigrahi, A. (2014). FeW: A Lightweight Block Cipher. *IACR Cryptology ePrint Archive*, *2014*, 326.

[26] Z’aba, M. R., Jamil, N., Rusli, M. E., Jamaludin, M. Z., & Yasir, A. A. M. (2014). I-PRESENT TM: An Involutive Lightweight Block Cipher. *Journal of Information Security*, *2014*.

[27] Engels, D., 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.

[28] AlKhzaimi, Hoda, and Martin M. Lauridsen. "Cryptanalysis of the SIMON Family of Block Ciphers." *IACR Cryptology ePrint Archive* 2013 (2013): 543.

[29] Abed, F., List, E., Lucks, S., & Wenzel, J. (2013). Cryptanalysis of the Speck Family of Block Ciphers. *IACR Cryptology ePrint Archive*, *2013*, 568.

[30] Dinur, Itai. "Improved Differential Cryptanalysis of Round-Reduced Speck." *IACR Cryptology ePrint Archive* 2014 (2014): 320.

[31] 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.

[32] Petroulakis, 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.

[33] Barker, 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.

[34] Poschmann, A. Y. (2009). Lightweight cryptography: cryptographic engineering for a pervasive world. In *Ph. D. Thesis*.

[35] Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994).

[36] Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer, Heidelberg (1993).

[37] F.X. Standaert, G. Piret, N. Gershenfeld, and J.-J. Quisquater. SEA: A Scalable Encryption Algorithm for Small Embedded Applications. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, Smart Card Research and Applications, Proceedings of CARDIS 2006, volume 3928 of Lecture Notes in Computer Science, pages 222–236. Springer-Verlag, 2006.

[38] Borghoff, Julia, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander et al. "Prince–a low-latency block cipher for pervasive computing applications." In Advances in Cryptology–ASIACRYPT 2012, pp. 208-225. Springer Berlin Heidelberg, 2012.

Gaurav Bansod received the M.Tech. Degree in Embedded Sytems from Jawaharlal Nehru Technological University, Hyderabad, India in 2008. He is currently pursing Ph.D from Symbiosis International University, Pune, He has publications in IEEE international conference , IEEE transactions on Information forensics and security and also in WSEAS transactions. His research area includes low power cryptographic design, embedded system and hardware and software design.

.

Nishchal Raval received the B.E. Degree in Electronics and Communication from Babaria Institute of Technology, Varnama, Vadodara, in 2011. He is currently studying towards the M.Tech. degree in Electronics and Telecommunication in Symbiosis Institute of Technology, Pune. His research interests are in the embedded security system, biometric system, cryptographic design, lightweight ciphers and embedded automotive systems.

Narayan Pisharoty received B.E. degree from IIT Bombay in 1966, M.Tech. degree from IIT Kanpur in 1968 and Ph.D from Carnegie Mellon University, Pittsburgh, USA in 1971. He held the post of Managing Director in Systech Ltd from 1972 to 2004 and Business Development Consultant in Persistent Systems Ltd from 2008 to 2010. Currently he is the Research Mentor for Engineering at Symbiosis International University, Pune, India and a Professor in the Electronics & Telecom. Department of SIT. He has published many papers in reputed journals including IEEE transactions on Biomedical Engineering. He is guiding 7 Ph.D students on different topics like matrix topology for multimode converters, UBW microwave antenna, and performance enhancement using dynamic partial reconfiguration. His research area includes RFID Applications, Alternate energy sources and Applications of microcontrollers in Agriculture.

Abhijit S Patil received the B.E. Degree in Electronics from Shivaji University, Kolhapur in 2012. He is currently pursuing the M.Tech Degree in Electronics and Telecommunication from Symbiosis Institute of Technology, Pune. He had work experience in Quality Analyst Field from year 2012 to 2013 in “EMERSON NETWORK POWER”. His research interests are in the embedded system security, lightweight cipher, embedded automotive systems and embedded real time system.