A Review on the Design of Lightweight Symmetric Block Ciphers for Cyber Physical Systems

Prathiba A, Kanchana Bhaaskaran V S

Abstract*: Selection and deployment of security hardware for Cyber Physical Systems (CPS) necessitate a smart choice. Lightweight security algorithms are viable choices for such applications. The study presented, will give an overview of lightweight symmetric block cipher algorithms and provide a summary for algorithm designers of the parameters that influence the design of a cipher algorithm and its impact on security and implementation. Comprehensive review of lightweight, symmetric, Substitution Permutation Network (SPN) type of block ciphers aids the lightweight cryptographic algorithm designer in selection of operations suitable for Cyber Physical Systems. An overall survey on existing lightweight SPN type symmetric block ciphers pertaining to design, security and hardware performance as the three corners that trade-off cipher design is made. The design composition of cipher based on security and hardware cost is the highlight of this paper.

Index Terms*: Lightweight block ciphers, security, performance and design.

I. INTRODUCTION

Cyber Physical systems (CPS) demand a compact and lightweight security deployment [1]. The way to establish security is through the deployment of lightweight cryptographic algorithms [2] – [6]. Block ciphers are of two types, namely, the Substitution Permutation Network (SPN) type and the Feistel Network (FN) type. Block ciphers of SPN type operate on a block of data of fixed size 'n', where n=32, 64 and so on. Feistel type of ciphers subdivides the data block into halves and operates separately on each block. Preferable choice is the use of block ciphers with less complexity, better throughput and reduced area occupancy in comparison against the stream ciphers. Block ciphers rely upon two principles, confusion and diffusion for establishing security. Confusion should establish complex relationship between plain and cipher texts. Diffusion is a property in which a single bit change in plain text should affect a significant number of bits of resultant cipher text . SPN block ciphers operating on fixed block size are considered for the review. Blocks of information transfer are primarily involved in the real-time applications. Parameters to evaluate a cipher are security and hardware/software performance. Structural design, chosen number of rounds, linear and non-linear operation in algorithm impacts the security properties.

Revised Manuscript Received on March 26, 2019.

A Prathiba, School of Electronics Engineering, VIT University, Chennai, India.

V S Kanchana Bhaaskaran, School of Electronics Engineering, VIT University, Chennai, India.

Every operation involved in the cipher decides its security properties as well the performance characteristics. Existing studies focus on either structural composition or involved operations in algorithms to achieve a demanded level of security. The literature lacks a study relating design, security and hardware performance of the SPN type of block ciphers [7], [8]. A comparative analysis of design, security and hardware architecture as three corners is the motive of the review presented. Overview of the tradeoff parameters is shown in Fig. 1.

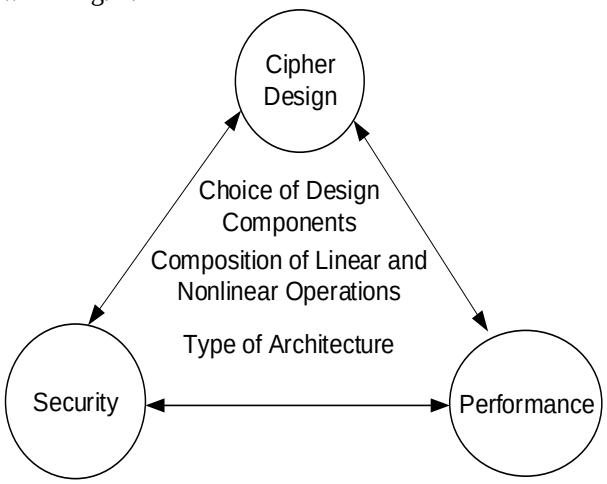

Fig.1. Survey overview

Composition of encryption schedule and key schedule are compared among the considered lightweight ciphers. Further, the bounds on the different types of attacks, namely, linear and differential cryptanalysis attacks, key related attacks, integral attacks, algebraic attacks, slide attacks, and statistical saturation attacks have also been compared. The bounds of these attacks and their resistance to the attacks provide cumulative information on dependence of every operation on the security of the cipher to the algorithm designers. Additionally, the motive of lightweight cryptography is to provide adequate security to miniature devices which are constrained in area, battery life and computation power. Hardware implementation of lightweight ciphers plays a major role in resource utilization. An overview of existing hardware architectures and its implementation for the lightweight ciphers are also presented in this paper.

II. SHORT DESCRIPTION OF CIPHERS

This section presents the specifications of the chosen iterative lightweight symmetric block ciphers of SPN type.

Type of the encryption schedule and the key schedule poses an idea of the selection of the type of hardware architecture. The non-linear operation in SPN ciphers is substitution and linear operation is permutation. The block ciphers are normally iterated ciphers where in the encryption schedule will have a set of round operations iterated for the round times specified in the algorithm. Every round operation is made key dependent on the round keys, as generated by the key scheduling algorithm. Linear operations, namely, permutation, mix columns and shift rows will have less impact on the hardware implementation since they are realized without any gates. S-box specification of the SPN ciphers under consideration are presented in Table 1 through 6. The specifications compared in Table 7 shows the collective summary of the cipher specifications.

The operations involved in encryption datapath and the key schedule for the specified ciphers are given in Table 8. Also, the type of linear and the non-linear operation in the cipher will give a better picture on the security as well as on the implementation. The structural comparison among the ciphers with the listing of the linear and the nonlinear operations involved in the chosen ciphers are presented in Table 9. The comparison concludes that the linear and the non-linear operation involved in cipher algorithm and the iterated number of rounds decide the security properties. Also the hardware performance metrics namely, speed, power and area are limited by the design composition. Ciphers compose of linear and nonlinear operations. The non-linear S-box is significant in deciding the security and cost of implementation. It is the primary non-linear operation in the security algorithms. Design of S-box quantify the critical path delay and resource occupancy of the cipher to a larger extent.

Table 1 mCRYPTON S-boxes

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S0	4	F	3	8	D	A	C	0	B	5	7	E	2	6	1	9
S1	1	C	7	A	6	D	5	3	F	B	2	0	8	4	9	E
S2	7	E	C	2	0	9	D	A	3	F	5	8	6	4	B	1
S3	B	0	A	7	D	6	4	2	C	E	3	9	1	5	F	8

Table 2 KLEIN S-box

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S	7	4	A	9	1	F	B	0	C	3	2	6	8	E	D	5

Table 3 NOEKEON S-box

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S	7	A	2	C	4	8	F	0	5	9	1	E	3	D	B	6

Table 4 PRESENT S-box

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 5 PRINCE S-box

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S	B	F	3	2	A	C	9	1	6	7	8	0	E	5	D	4

Table 6 PRINT S-box

X	0	1	2	3	4	5	6	7
S [x]	0	1	3	6	7	4	5	2

Table 7 Comparison of specifications of SPN type symmetric lightweight block ciphers

Cipher	Year	Designer	Rounds	Block size (bits)	Key size (bits)	Applications/Design aim

mCRYPTON [9]	2006	Lim and Korkishko	12	128	64,96,128	miniature CRYPTON/compact implementation in hardware and software
EPCBC [10]	2011	Huihui Yap et al.	32	48, 96	96	Electronic Product Code/generalized PRESENT, PRESENT-n
KLEIN [11]	2012	Gong et al.	12,16,24	64	64,80,96	Wireless sensors and RFID tags/software performance on legacy sensor nodes
LED [12]	2011	Guo et al.	64-bit key, s=8. 128-bit key, S=12	64	64,80,96,128	RFID tags/ ultra light key schedule, compact hardware, reasonable performance in software
NOEKEON[13]	2008	Daemen et al.	16	128	128	Smart cards/suitable for multiple platforms, resistant to implementation attacks
PRESENT [14]	2008	Rolfes et al.	31	64	80, 128	RFID tags, Low passive sensor networks
PRINCE [15]	2010	Knudsen	12	64	128	Real-time security purposes
PRINT[16]	2007	Lars Knudsen et al.	48,96	48,96	80,160	IC Printing, electronic product code.

Table 8 Comparison of operations in encryption schedule and key schedule

Cipher	Encryption schedule operations	Encryption schedule type	Key schedule operations
mCRYPTON	Add round key,Sub Nibbles, Rotate Nibbles,Mix Nibbles	SPN	Round Key,S-box layer Shifting
EPCBC	Add round-key,S-box layer P-layer	SPN	Shifting,S-box layer Round counter
KLEIN	Add round Key,Sub Nibbles Rotate Nibbles,Mix Nibbles	SPN	ith Round Key,Shifting S-box layer,Round counter
LED	Add round key,S-box layer Shift rows,Mix columns	SPN	User supply Key
NOEKEON	Add round ey,Theta,Pi1,Pi2 Gamma	SPN	User supplied Key

PRESENT	Add round-key, S-box layer P-layer	SPN	Shifting S-box layer Round counter
PRINCE	Add round key,S-box layer M/M' – layer,Round counter	SPN	User supplied Key
PRINT	Key XOR, Linear diffusion Round counter, Keyed Permutation,S-box layer	SPN	User supplied Key (Sub key1, Sub key 2)

Table 9 Comparison of cipher structures

Cipher	Key schedule	Encryption schedule	Nonlinear component	Linear component	Structural Similarity with cipher
m-CRYPTON	Counter based	Own schedule	substitution	bit permutation	CRYPTON
EPCBC (PRESENT-n)	Feistel structure	PRESENT	substitution	n bit permutation	PRESENT (S box(4 x4), Permutation)
KLEIN	Variable	Own schedule	substitution	64bit permutation	
LED	User supply Key	AES	substitution	n bit permutation	PRESENT S box (4x4)
NOEKEON	User supply Key	Own schedule	substitution (Gamma)	Theta	
PRESENT	counter based	Own schedule	substitution	64 bit permutation	-
PRINCE	User supply key	Own schedule	substitution	64-bit permutation	
PRINT	N/A	Key dependent algorithm	substitution	3-bit permutation	3-way SEA, Blowfish Two fish,GOST

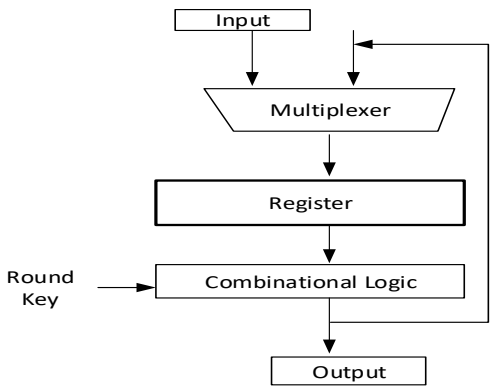

Fig. 2. Basic round architecture [17]

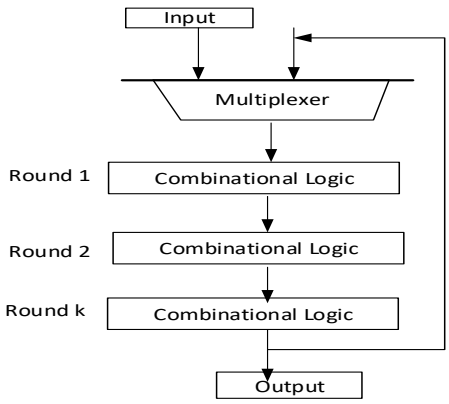

Fig.3. Partially loop unrolled architecture[17]

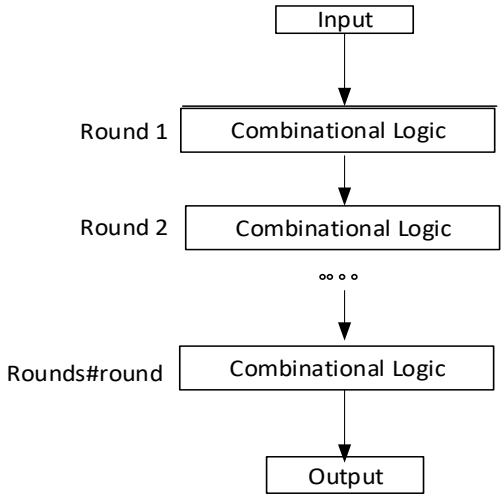

Fig. 4. Fully unrolled architecture [17]

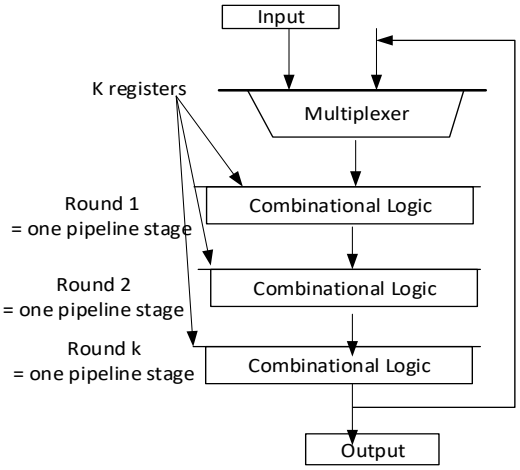

Fig. 5. Partial outer round pipelining [17]

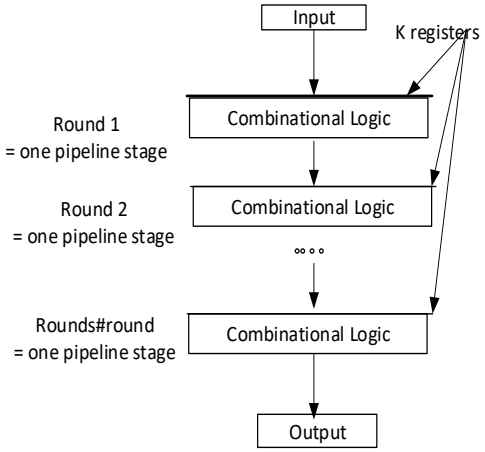

Fig. 6. Full outer round pipelining [17]

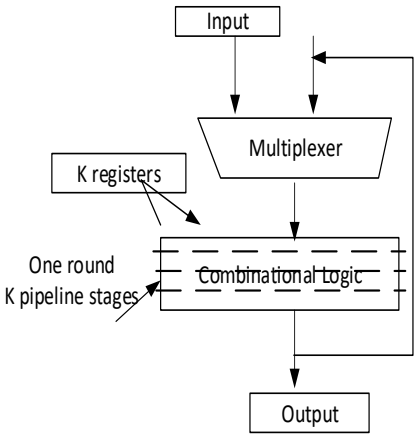

Fig. 7. Inner round pipelining [17]

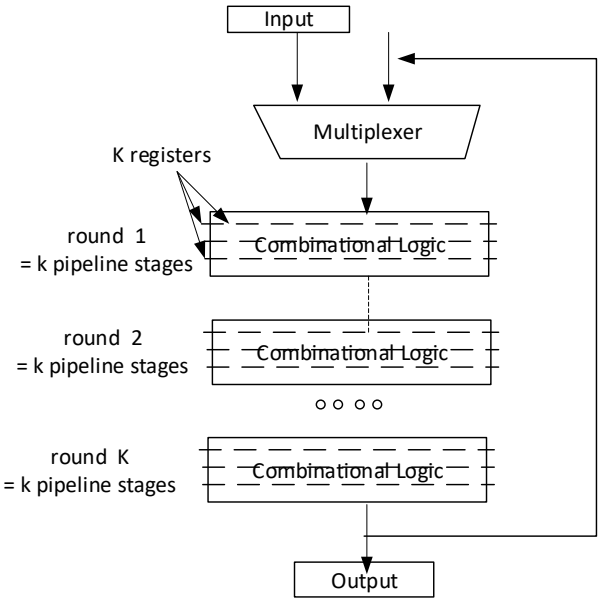

Fig. 8. Partially unrolled inner outer round pipelining [17]

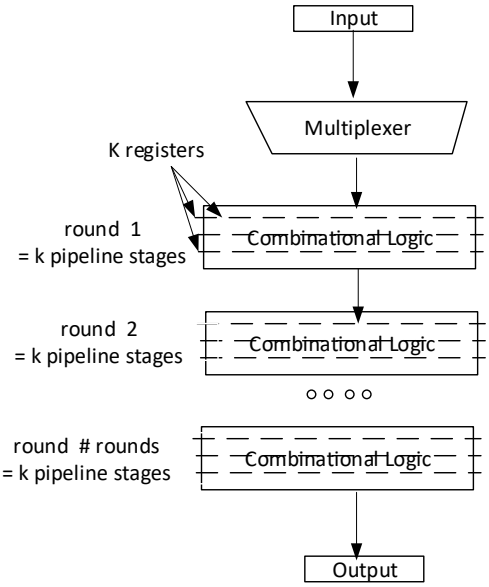

Fig. 9. Fully unrolled inner and outer round pipelining [17]

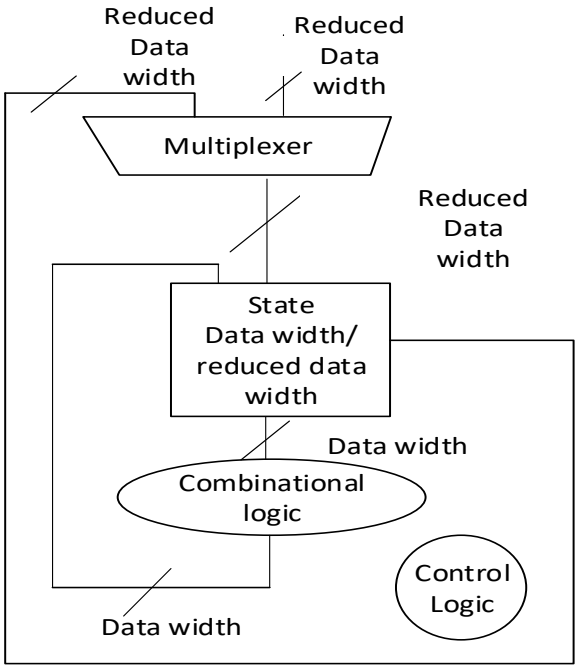

Fig. 10. Serial architecture

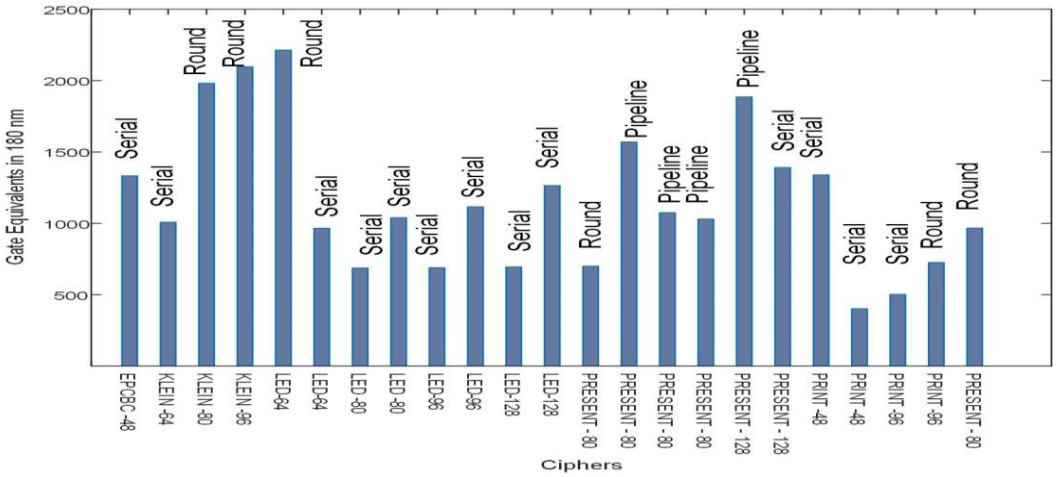

Fig. 11. Comparison of gate equivalents of existing cipher implementations

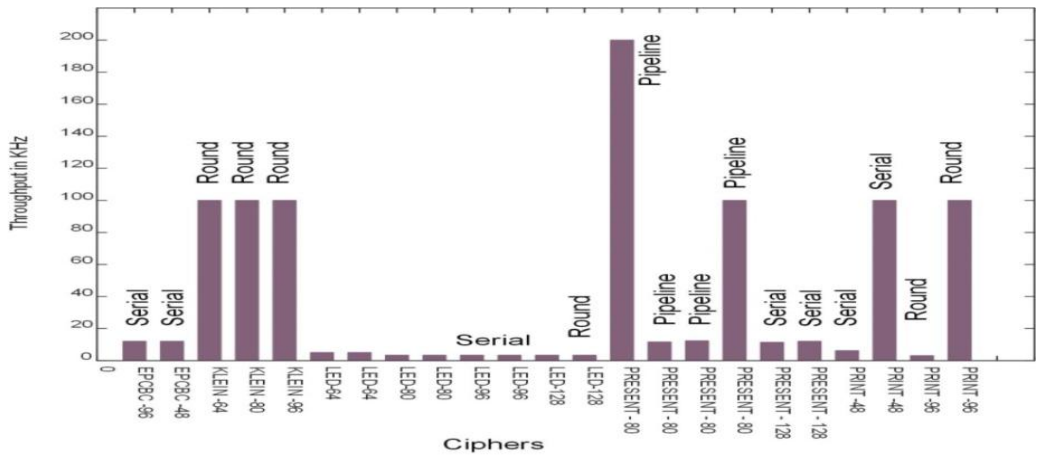

Fig. 12. Comparison of throughput of existing cipher implementations

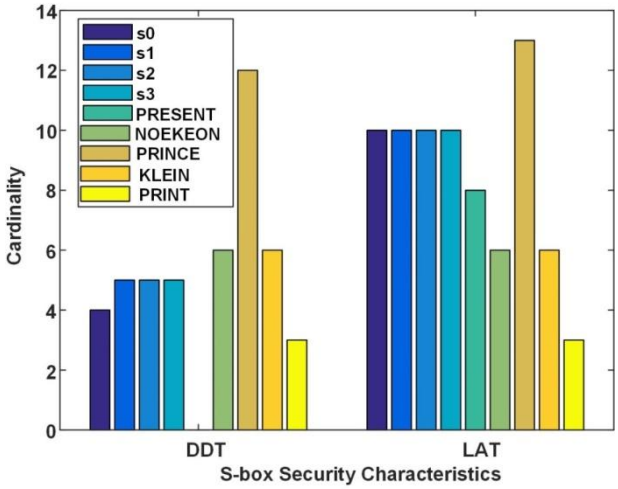

Fig. 13 Cardinality of differential uniformity and linear imbalance of the S-boxes

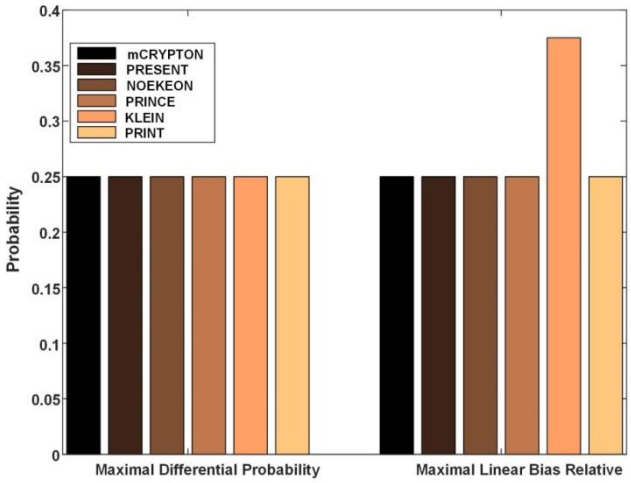

Fig. 14 Maximal differential and linear approximation probability of the S-boxes

The hardware implementations of the block ciphers are discussed in the forthcoming section.

III. VLSI ARCHITECTURES AND IMPLEMENTATIONS

Varieties of hardware architectures are possible for cryptographic algorithm and they fall under the category of serial and parallel structures. Serial architecture aims at reduced area occupancy with the penalty of increased delay. Power consumption will also be less in the case of the serial implementations since a single computation is carried out in a specified time. However the parallel architectures aim at simultaneous operations with better throughput and power consumption increases when number of operations are being carried out simultaneously. The types of hardware architectures employed in the block cipher implementation are round based single loop architecture, reduced data path serial architecture, partially unrolled loop architecture, fully unrolled architecture and parallel pipelined architectures, namely, partial outer round pipelined, full outer round pipelined, inner round pipelined, partial inner and outer round pipelined and full inner-outer round pipelined structures [17]. An outline of each of the architectures with their block diagrams is shown below. This gives a good picture of the possible choices of hardware implementation of a symmetric block cipher. Dimensions of estimation of a hardware implementation are area and throughput. Direction aiming on the area should compromise speed and that which focuses on speed should trade-off area [18] – [28]. The possible hardware implementation choices for a symmetric block cipher are explained below.

A. Round based architecture

The round based architecture aims at compact and minimum area occupancy. The round architecture comprises of a single round structure of the cipher. These single loop structural definitions have significant area saving. In this architecture speed is traded off with the area. Single loop structure will be executed the total number of round times as in the algorithm specification. Basic single round architecture is shown in Fig. 2.

B. Loop unrolled architecture

In this k rounds of the cipher are unrolled resulting in better throughput than the single round architecture with slightly more area utilization. In the fully unrolled architecture the cipher is fully unrolled. Partially unrolled and fully unrolled cipher structure is shown in Fig. 3 and 4.

C. Parallel pipelined architecture

The pipelined architectures improve the speed, performance and are applicable to the non-feedback modes of the cipher. The mechanism incorporated to improve the speed is the pipelining.

Pipelining registers can be placed in between the operations of a round and is referred to as the inner round pipelining. The pipelining registers placed after every round of the cipher are termed as the outer round pipelining. Cipher structures can be both inner and outer pipelined with partial or full unrolling. The block diagrams of the different pipelining schemes in the block cipher structures are shown in Fig. 5 - 9.

D. Serial architecture

The serial architecture is reduced data path architecture and is shown in Fig. 10. The reduced data path structure results in area reduction and increased delay and latency. This structure also has single loop structure as that of the round based architecture, but operates on reducing data width, namely 4, 8, 16 and 32 and so on. This structure has increased complexity in the control unit. Throughput of block encryption/decryption is less in this type of architecture, since it has a reduced data path. Hardware implementations of the cryptographic implementations are estimated by the following performance parameters, namely, the throughput and latency, area and cost.

- Throughput is defined as the number of blocks processed simultaneously with respect to latency for a chosen block size.
- Area utilized for a typical ASIC implementation is given in terms of number of Gate Equivalents (GEs) incurred for the typical implementation.

As concerned with area occupancy there is a limit on the maximum area occupied by an implementation. Fig. 11 and 12 depicts the hardware implementation details of the lightweight SPN type of block ciphers. The next sections focus on the security properties, security analysis bounds of the cryptanalytic attacks on these ciphers.

IV. SECURITY CHARACTERISTICS OF NON-LINEAR S-BOX OPERATION INVOLVED IN THE BLOCK CIPHERS

The typical nonlinear operation used in the block ciphers is S-box and it greatly impacts security. The number of high probability difference pairs in the S-boxes should be limited. Less number of active S-boxes with high probability difference propagation over a specified number of rounds are preferred. This results in rapid diffusion and the formation of high probable differential characteristics/linear approximation characteristics over the rounds will be eliminated. The maximal differential characteristics and the linear approximation probability for S-box are the parameters which reflect security properties. Fig. 13 and 14 shows the differential and linear approximation probability values of S-boxes for the SPN ciphers.

V. OVERVIEW OF SECURITY ATTACKS

Another significant design principle of the block ciphers is to make the cipher resistant to all attacks. The brief details of the types of attacks in block ciphers are given below [29] –[33]. This review focus on the generic algorithmic attacks and not on the implementation attacks such as the side channel attacks. Table 10 summarize the attack bounds for the chosen ciphers. Fig. 15 and 16 compares the linear bias approximation and the number of active S-boxes for the SPN ciphers.

A. Differential cryptanalysis

Differential cryptanalysis is a chosen plaintext attack which analyses on specific input differences leading to specific output differences. The differential behavior distinguishes the cipher characteristics. Differential probability characteristics and number of active rounds estimate differential characteristics. Differential characteristic of cipher with one active S-box per round with 'r' rounds is given by $|2^{-2}|^{r-1}$.

B. Linear cryptanalysis

Linear cryptanalysis a known plain text attack in which the cipher is linearly approximated and by determining high probability linear characteristics key can be exploited. Number of active S-boxes per round and their probability characteristics determines the complexity of linear cryptanalysis. The characteristics over a number of rounds give the bounds for linear characteristics. Number of active S-boxes over the rounds and the differential/linear approximation probability of the S-box define the bounds for the differential/linear cryptanalysis.

C. Key Schedule attacks

Related key attacks and slide attacks identify the relations between cipher texts encrypted using related keys. The knowledge of the key is not needed, but the relationship between the keys will reveal the secret information. Weakness in the key schedule will be exploited by the related key attacks. Round constants of the key schedule algorithm will prevent related key attacks. The linear key schedule algorithm will have less resistance to related key attacks. Slide attack exploits the self-similarity of iterative ciphers. Identical round keys with repetitiveness will lead to better attacks. These attacks are applicable to iterative ciphers.

D. Integral cryptanalysis

The integral attacks concentrate on the byte-oriented ciphers with the focus on the sum value propagation of values. The cipher will be treated as a system of propagation of certain characteristics.

E. Statistical saturation attacks

The statistical saturation attack exploits weakness of diffusion involved in the cipher. For the block ciphers, the permutation operation involved reflects the strength of the diffusion. Better the diffusion offered by the permutation operation the better is the resistance of the cipher to the statistical attacks.

F. Algebraic attacks

The algebraic types of attacks recovers secret key by considering the system as a set of polynomial equations. Some plain text cipher text pairs solve the system of equations efficiently to reveal the secret key.

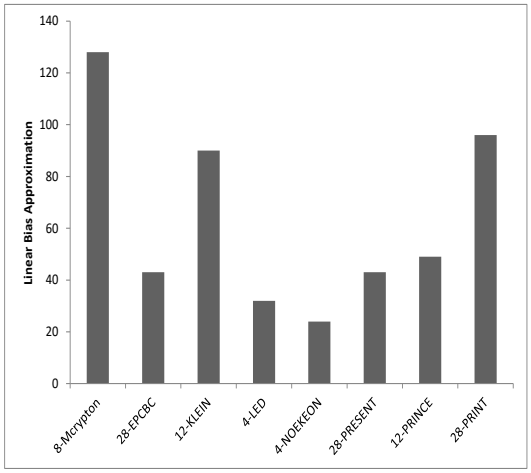

Fig. 15 Comparison of linear bias approximation of block ciphers for chosen rounds

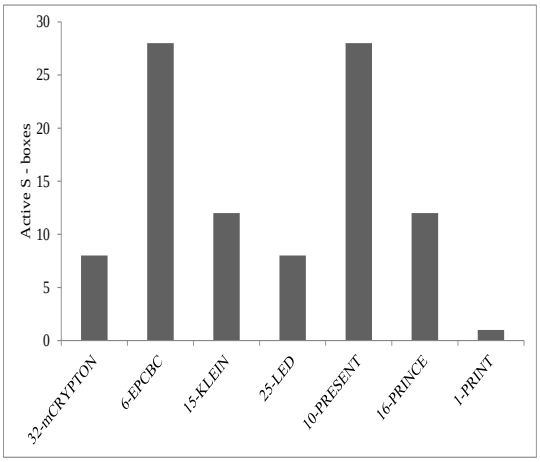

Fig. 16 Comparison of number of active S-boxes of block ciphers for chosen rounds

VI. FINDINGS AND DISCUSSION

The block ciphers operate on a block of data as a whole. The issues that trade off the block cipher design are security and performance. Summary on design, security and implementation of SPN type of lightweight block ciphers are highlighted below.

Design aspects:

- There should at least one linear and non-linear operation in the algorithm.
- The linear component employed predominantly in the SPN ciphers is the permutation operation.
- The nonlinear operation is the substitution operation which has a dominant role in deciding both the security characteristics and the performance.

Security aspects:

- Maximal differential probability and the maximal linear bias as determined by Differential Distribution Table (DDT) and Linear Approximation Table (LAT) of the S-box plays a key role in algorithm's security property.
- Architecture can be serial or parallel.
- S-boxes employed in the SPN ciphers should possess higher differential probability and higher linear bias relative.
- Further, chain of differential propagation and the linear approximation characteristics over the round should have lesser values to be less vulnerable to cryptanalytic attacks.
- It is the nonlinear substitution box and the linear permutation that decides the differential and linear characteristics of ciphers.
- Lesser the number of active S-boxes over the number of rounds, better is the resistance to linear and differential cryptanalysis.
- Larger number of rounds in the cipher algorithm better is the security.

Implementation Aspects:

- Hardware implementation of substitution box is either look up table based or non-look up table based.
- Non-look up table based S-box structure paves way to hardware optimization mechanisms through sub pipelining.

Table 10 Security related algorithm characteristics and security bound comparison

Cipher	Parameter	m CRYPTON	EPCBC	KLEIN	LED	NOEKEON	PRESENT	PRINCE	PRINT
Linear Cryptanalysis bound for r rounds 'ε_r'	linear bias approximat-ion	$\varepsilon_8 = 2^{-128}$	$\varepsilon_{28} = 2^{-43}$	$\varepsilon_{12} = 2^{-90}$	$\varepsilon_4 = 2^{-32}$	$\varepsilon_4 < 2^{-24}$	$\varepsilon_{28} = 2^{-43}$	$\varepsilon_{12} = 2^{-49}$	$\varepsilon_{48} = 2^{-96}$
	Active S-boxes/ rounds (r)	32/8	6/4	15/4	(r/8). 25	-	10/5	16/4	1/1
Differential Cryptanalysis bound	Maximum Differential Probability	2^{-2}	2^{-2}	2^{-2}	2^{-2}	-	2^{-2}	2^{-2}	2^{-2}
	Round probability	$\Delta_{8=2^{-8}}$	$\Delta_{28=2^{-84}}$	$\Delta_{12=2^{-90}}$	$\Delta_{4=2^{-25}}$	$\Delta_4 < 2^{-48}$	$\Delta_{25=2^{-100}}$	$\Delta_{12=2^{-96}}$	$\Delta_{12=2^{-24}}$
Key Schedule Attacks		round based counter, nibble substitution, nonlinear key generation and linear key updation variables	round based counter, unlikely periodicity in key schedule resists this attack		round dependent constants resists this attack		round based counter, unlikely periodicity in key schedule resists this attack		keys are uniformly random (unrealistic attack)
Integral attacks			bit based permutation resists this attack	Possible till seven rounds	seven round complexity of the attack 2^{28}		bit based permutation resists this attack		-
Statistical saturation attacks			permutation layer resists this attack		-		permutation layer resists this attack		permutation layer resists this attack
Algebraic attack			**EPCBC-48** 780 S-boxes, 6240 variables, 16380 equations **EPCBC-96** 1560 S-boxes, 12480 variables, 32760 equations	1920 variables, 5040 equations	4096 variables, 10752 equations		527 S-boxes, 4216 variables, 11067 equations		resists this attack

The review concludes the necessity of a linear and the nonlinear operation in a block cipher to provide diffusion and confusion. The predominantly employed operation for establishing them is through permutation and substitution, respectively. The linear permutation decides the vulnerability of the algorithmic attacks, namely, the integral attacks, the algebraic attacks and the statistical saturation attacks. The nonlinear operation in the cipher gives the strength against linear and differential cryptanalysis. Slide attacks and related key attacks exploit key schedule involved in the algorithm. The selection of S-box highly influences the security of the algorithm and its selection must be optimal. Maximal differential probability, maximal linear approximation probability, the cardinality of the single bit output difference for any single bit input difference, cardinality of any output selection pattern for any input selection pattern are the parameters of interest in the S-box with respect to linear and differential characteristics.

Further, the nonlinear S-box is the only possible design component for the incorporation of the implementation, optimization mechanism, since permutation in hardware has been just a rewiring. Based on the area-throughput requirements the implementation architecture of the block cipher can be serial, loop, unrolled and/or parallel. The comparison bounds on of the algorithmic attacks provide an overall idea on the margin of each of the attacks with respect to their design parameters.

The hardware design and the choice of the architectural implementation for the novel block ciphers should aim at the uniform structure architecture to avoid dynamic hazards.

The dynamic hazards will result in variable signal transition delays and hence the variable path delays. This will increase the power dissipation due to the unwanted signal transitions and also increase in the critical path delay.

VII. CONCLUSION

In this paper Substitution Permutation Network (SPN) type of block ciphers in regards to design, security and performance are comprehensively reviewed. Among the existing lightweight ciphers, the SPN type of block ciphers is identified for the study. Composition of the cipher and its structural definition determines selection of ciphers. Encryption schedule type, key schedule type, specifications, structural similarities, hardware implementations and security bounds on different types of attacks have been compared. Various types of architecture, block diagram and its implementation mechanisms are also elaborated. Literature summary of design choices, security properties and hardware implementation are presented. SPN ciphers are of type iterative ciphers and from the study it can be concluded that

- Substitution box involved in the cipher should have less differential uniformity and less linear imbalance to have better robustness against differential and linear cryptanalysis.
- Structural definition of S-box should be non-lookup table based to incorporate hardware optimization mechanisms.
- Lightweight ciphers have 4 × 4 S-box definitions to have less area resource utilization.
- Bit based permutation will be less vulnerable to integral and statistical saturation attacks against the byte based substitution. Also, the bit based permutation in hardware is a simple re-wiring without incurring any gates.
- Key schedule should have round based counters to avoid unlikely periodicity in the operations which will result in the key schedule attacks.

This paper also dealt with the diverse study of the variety of hardware architectures possible for the SPN block ciphers and their possible implementations. From the hardware implementation aspect of the ciphers it is concluded that

- Serial architecture, the reduced data path architecture is the better choice for the area constrained applications and will have less power consumption at the cost of reduced throughput.
- Parallel architectures with/ without pipelining will have a better speed performance with increased area utilization and increased power consumption.

The three corners of this study, namely the design, composition, the security and the performance of the SPN type of lightweight block ciphers serves as a reference for all the researchers interested in the novel algorithm design.

REFERENCES

1. Song, H., Fink, G. A., & Jeschke, S. (Eds.): 'Security and Privacy in Cyber-physical Systems: Foundations, Principles, and Applications', 2017, John Wiley & Sons.
2. Daemen, Joan, René Govaerts, and Joos Vandewalle. "A new approach to block cipher design." In Fast Software Encryption, pp. 18-32. Springer Berlin/Heidelberg, 1994.
3. Schneier, Bruce. "Description of a new variable-length key, 64-bit block cipher (Blowfish)." In Fast Software Encryption, pp. 191-204. Springer Berlin/Heidelberg, 1994.
4. Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, Ingrid Verbauwhede In RECTANGLE: A Bit-slice Lightweight Block Cipher Suitable for Multiple Platforms. Vol. 58: 122103 (15), Science China Information Sciences (2015).
5. Li, Lang, Botao Liu, and Hui Wang. "QTL: a new ultra-lightweight block cipher." Microprocessors and Microsystems 45 (2016): 45-55.
6. Poschmann, Axel, Gregor Leander, Kai Schramm, and Christof Paar. "New Lightweight DES Variants Suited for RFID Applications." In FSE, vol. 4593, pp. 196-210. 2007.
7. Poschmann, Axel, Gregor Leander, Kai Schramm, and Christof Paar. "New light-weight crypto algorithms for RFID." In Circuits and Systems, 2007. ISCAS 2007. IEEE International Symposium on, pp. 1843-1846. IEEE, 2007.
8. Eisenbarth, Thomas, and Sandeep Kumar. "A survey of lightweight-cryptography implementations." IEEE Design & Test of Computers 24, no. 6 (2007).
9. Lim, Chae Hoon, and Tymur Korkishko. "mCrypton-a lightweight block cipher for security of low-cost RFID tags and sensors." In WISA, vol. 3786, pp. 243-258. 2005.
10. Yap, Huihui, Khoongming Khoo, Axel Poschmann, and Matt Henricksen. "EPCBC-a block cipher suitable for electronic product code encryption." Cryptology and Network Security (2011): 76-97.
11. Gong, Zheng, Svetla Nikova, and Yee Wei Law. "KLEIN: A new family of lightweight block ciphers." RFIDSec 7055 (2011): 1-18.
12. Jian Guo, Thomas Peyrin, Axel Poschmann, Matt Robshaw In: The LED Block Cipher. LNCS 6917, pp. 326–341. Preneel, Bart, and Tsuyoshi Takagi, eds. Cryptographic Hardware and Embedded Systems--CHES 2011: 13th International Workshop, Nara, Japan, September 28--October 1, 2011, Proceedings. Vol. 6917. Springer, 2011.
13. Daemen, Joan, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. "Nessie proposal: NOEKEON." In First Open NESSIE Workshop, pp. 213-230. 2000.
14. Bogdanov, Andrey, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. "PRESENT: An ultra-lightweight block cipher." In CHES, vol. 4727, pp. 450-466. 2007.
15. 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 International Conference on the Theory and Application of Cryptology and Information Security, pp. 208-225. Springer, Berlin, Heidelberg, 2012.
16. Knudsen, Lars R., Gregor Leander, Axel Poschmann, and Matthew JB Robshaw. "PRINT cipher: A Block Cipher for IC-Printing." In CHES, vol. 6225, pp. 16-32. 2010.
17. Gaj, Kris, and Pawel Chodowiec. "FPGA and ASIC implementations of AES." In Cryptographic engineering, pp. 235-294. Springer US, 2009.
18. Hong, Eunjong, Jai-Hoon Chung, and Chae Lim. "Hardware design and performance estimation of the 128-bit block cipher CRYPTON." In Cryptographic Hardware and Embedded Systems, pp. 727-728. Springer Berlin/Heidelberg, 1999.
19. Akishita, Toru, and Harunaga Hiwatari. "Very compact hardware implementations of the blockcipher CLEFIA." In International Workshop on Selected Areas in Cryptography, pp. 278-292. Springer, Berlin, Heidelberg, 2011.
20. Rolfes, Carsten, Axel Poschmann, Gregor Leander, and Christof Paar. "Ultra-lightweight implementations for smart devices--security for 1000 gate equivalents." In CARDIS, vol. 5189, pp. 89-103. 2008.
21. Mace, Franois, Franois-Xavier Standaert, and Jean-Jacques Quisquater. "ASIC implementations of the block cipher SEA for constrained applications." In Proceedings of the Third International Conference on RFID Security-RFIDSec, vol. 2007, pp. 103-114. 2007.
22. Satoh, Akashi, Sumio Morioka, Kohji Takano, and Seiji Munetoh. "A compact Rijndael hardware architecture with S-box optimization." In Asiacrypt, vol. 2248, pp. 239-254. 2001.
23. Hamalainen, Panu, Timo Alho, Marko Hannikainen, and Timo D. Hamalainen. "Design and implementation of low-area and low-power AES encryption hardware core." In Digital System Design: Architectures, Methods and Tools, 2006. DSD 2006. 9th EUROMICRO Conference on, pp. 577-583. IEEE, 2006.
24. Yue-Chao, Hui, and Wang Yi-ming. "Secure RFID system based on lightweight block cipher algorithm of optimized S-box." In RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on, pp. 11-15. IEEE, 2010.
25. Hodjat, Alireza, Patrick Schaumont, and Ingrid Verbauwhede. "Architectural design features of a programmable high throughput AES coprocessor." In Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on, vol. 2, pp. 498-502. IEEE, 2004.

26. Rinne, Sören, Thomas Eisenbarth, and Christof Paar. "Performance analysis of contemporary light-weight block ciphers on 8-bit microcontrollers." In ECRYPT Workshop SPEED-Software Performance Enhancement for Encryption and Decryption, Amsterdam. 2007.
27. Dworkin M. "Recommendation for Block Cipher Modes of Operation NIST Special Publication 800-38A." (2001).
28. Prathiba A., and VS Kanchana Bhaaskaran. "FPGA Implementation and Analysis of the Block Cipher Mode Architectures for the PRESENT Lightweight Encryption Algorithm." Indian Journal of Science and Technology 9, no. 38 (2016).
29. Matsui, Mitsuru. "Linear cryptanalysis method for DES cipher." In Advances in Cryptology—EUROCRYPT'93, pp. 386-397. Springer Berlin/Heidelberg, 1994.
30. Biham, Eli, and Adi Shamir. "Differential cryptanalysis of DES-like cryptosystems." In Advances in Cryptology-CRYPTO, vol. 90, pp. 2-21. 1991.
31. Biham, Eli. "New types of cryptanalytic attacks using related keys." Journal of Cryptology 7, no. 4 (1994): 229-246.
32. Biryukov, Alex, and David Wagner. "Slide attacks." In International Workshop on Fast Software Encryption, pp. 245-259. Springer Berlin Heidelberg, 1999.
33. Courtois, Nicolas, and Josef Pieprzyk. "Cryptanalysis of block ciphers with over defined systems of equations." Advances in Cryptology—ASIACRYPT 2002 (2002): 267-287.

AUTHORS PROFILE

Prathiba A received her bachelor degree in Electronics and Communication in the year 2002. She obtained her Masters in Communication Systems in the year 2006. She is working as an Assistant Professor in VIT University Chennai. Currently she is pursuing her Ph.D degree and her research areas are hardware design of cryptographic architectures, vulnerability modeling of side channel attacks and lightweight cryptography.

V S Kanchana Bhaaskaran is professor at the School of Electronics Engineering and Dean of Academics at VIT Chennai, India. She obtained an undergraduate degree in electronics and communication engineering from the Institution of Engineers (India), Calcutta, India, and an MS degree in Systems and Information from Birla Institute of Technology and Sciences, Pilani, India, and a PhD from VIT Chennai. She has more than 35 years of industry, research, and teaching experience, serving with the Department of Employment and Training, the government of Tamil Nadu, IIT Madras, Salem Cooperative Sugar Mills' Polytechnic College, SSN College of Engineering, and VIT University. Her specializations include low power VLSI circuit designs, microprocessor architectures, and linear integrated circuits. She has published around 100 papers in international journals and conferences, and has three patents published. She is a reviewer for international peer-reviewed journals and conferences. She is also a Fellow at the Institution of Engineers (India), a Fellow at the Institution of Electronics and Telecommunication Engineers, a Lifetime Member of the Indian Society for Technical Education, and a Senior Member of the Institute of Electrical and Electronics Engineers Inc., USA.