Compact Lightweight Cryptographic Algorithmfor Optimizationof Resources

SunithaTappari, K. Sridevi, Durga Rao Jenjeti

Abstract:*The study of Lightweight cryptography has been one of the intresting topics in symmetric cryptography in the recent years. Lightweight symmetric ciphers has gained interest due to the increasing demand for security services in constrained computing environments, such as in the Internet of Things(IoT). Though the protocols of light weight in are providingingmore security in variousapplications,resource utility is more in key generation, key scheduling, permutation layer and substitution box layer operations. More resource usage make possibletohave highutilization of power andoverhead of area. In this paper, a novel method is proposed to decrease theutility of resoures, which followsregister reutilization scheme. The resource reutilization is coordinating with the delay inSubstitutionPermutation Network (SPN).Our design is compared, using area, throughput, power, and latency as metrics.*

Keywords: *Symmetric light weight cryptography, Resource optimization, Registerreutilization, Cryptography coding.*

I. INTRODUCTION

Theworld over in the environmentcomputing can be embedded. Nowadays, the broadband Internet is generally accessible to any user and its cost of connectivity is also reduced, more sensors and gadgets are getting connected to it[1]. There are many research works focusing on complexities around the IoT[2]. For each valuable transmitting data, the sophisticated sensors are implanted in the substantialequipmentsadjacent tous.The devices itself startsthesharing process of large data which should communicate with IoT with moresecurity.

The IoT is taking the mobile network, conventional internet and sensor network to a differentlevelsare connected to the internet. IoT is furthersusceptible to serious threats of security than available network, the reason for thatis it includes resource constrained objects, assorted nature, open environment employment, lively behavior. Security in IoT environment should ensure accurate implementation of confidentiality, integrity, authentication, non-repudiation, and access control [3].

A key element of secure communication of the system is Cryptography[4]. Conventional cryptography is not suitable for resource constraint devices.The majority of these devices use limited power sources to the point where it is required to rely on energy harvesting [5], power optimization techniques [6], and novel transmission technologies [7]. Therefore it is difficult to provide cryptographic solutions for constrained environments.Lightweight Cryptography (LWCRYPT) is a new region of research that willreach the requirmentsplace by smart devices. In this, cryptography methodshave to work with minimum amount of vital resources of required objects. “Lightweight” term representsalgorithm with less consumption of energy, and less computational power requirement. LWCRYPT is a cryptography technique, customized for less resource requirement devices.

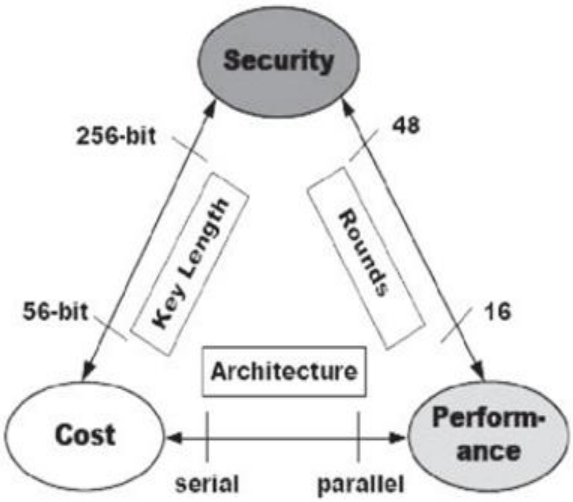

Fig.1: Scaling measures among Performance,Securityand Cost

The key length is decreasesto 56-bits from 256-bits ; the processing rounds count is reduced to 16 from 48 in the logic of encryption , the mode of architecture shifts from parallel to serialized as indicatedin Fig.1. In addition, requirement memory is decreases to Kilo bytes from Giga bytes and processing speed comes down from GHz to KHz.

One of the classification of LWCRYPT technique[8] is symmetriccryptographic algorithms Vs asymmetriccryptographic algorithms.Due to the hardware-friendly nature,Symmetric cryptography is suitable for constrained devices. Which implies minimization ofsupplementary computational cost and consumption of power.

Revised Manuscript Received on December 13, 2019.

Corresponding authors:
SunithaTappari*, Dept. of Electronics and Telematics Engineering, GNITS (for women), JNTUH, Hyderabad, India.
K. Sridevi, Dept. of ECE, GITAM (Deemed to be University), Vishakapatnam, India.
Durga Rao Jenjeti, Dept. of ECE, GITAM (Deemed to be University), Vishakapatnam, India.

II. PRESENT CIPHER

PRESENT is a symmetric light weight blockcipher.In hardware realizationsof PRESENT[9], It's circuit size is small and that enables implementation in the RFID tag, which is not possible using the standard AES encryption. PRESENT is hardware oriented block cipher algorithm of lightweight cryptography. It can serve with the input of 64bit blocks and available keys of 80/128 bits [10]. The cipher is dependent on a Substitution-Permutation Network (SPN), with a round-based processing system.As a result of its straightforwardness, it is commonly utilized in circumstances where low-control utilization and high chip proficiency are wanted.This design is derived directly from the algorithm specification and a top level description of PRESENT is shown in Fig.2.

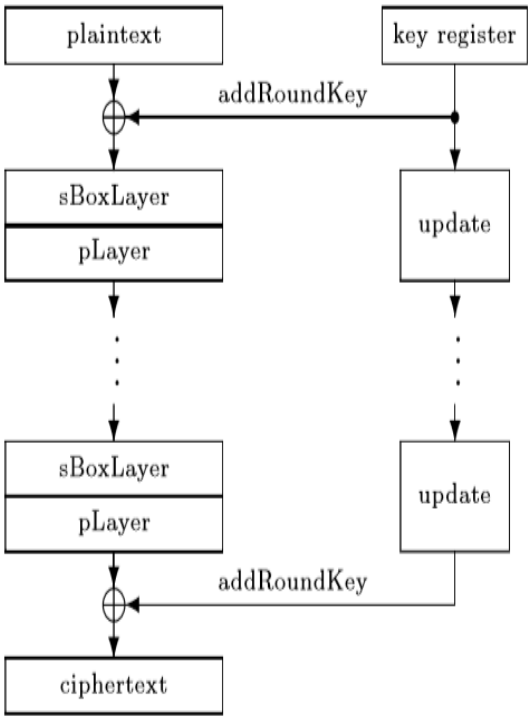

Fig.2. A top-level algorithmic description of PRESENT.

The resource overhead is generated in this approach due to recursive operation is more in key scheduling approach. This approach is proficient, but itrequires largequantity of resources.To dimnish the resource overhead, approachof resource minimizationis proposed in which delay of resource is tuned.

III. IMPROVED PRESENT CIPHER

The improved PRESENT cipher overcomes the resource overhead. The customized structure of the resource controlled light weight architecture is shown in Fig.3.

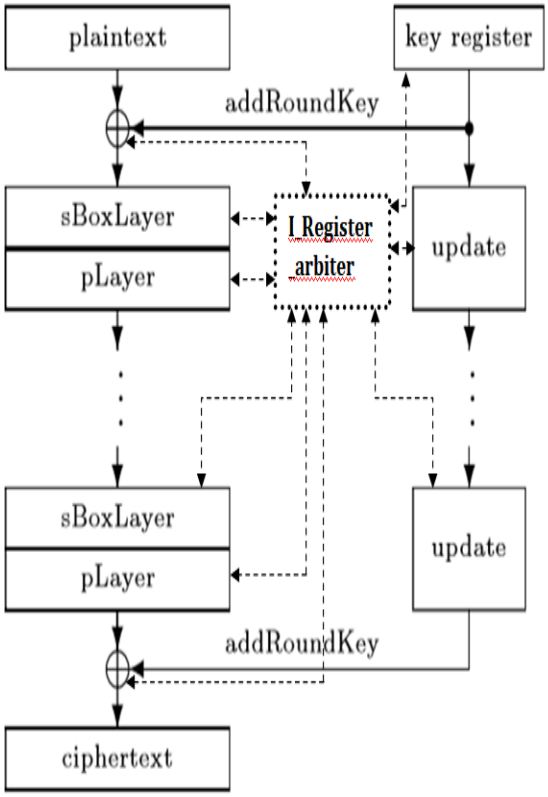

Fig.3. A top-level resource controlled light weight PRESENT.

In this approach, a 4 operational instructions set is used. The flow of data in those instruction operationsare shown in Fig.4.

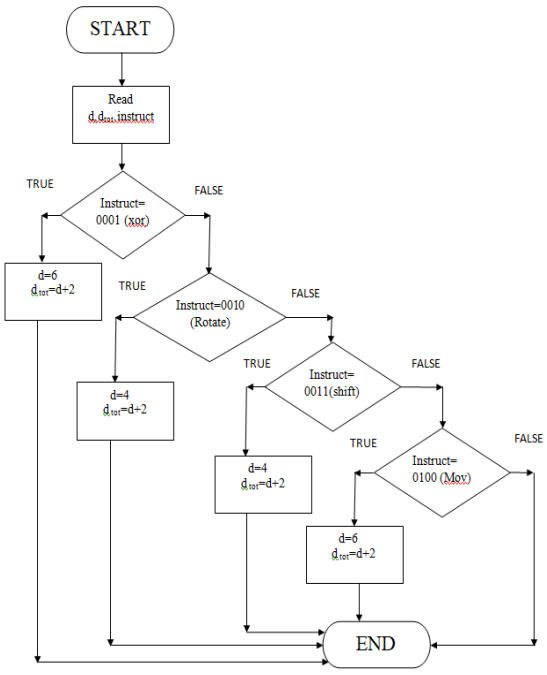

Fig.4 Data flow for instruction set.

To execute each XOR instruction, it requires, 6 delay cycles which includes 1 decode clock cycle, 2 computational clock cycles and 3 register allocation clocks. For ROTATE instruction, it requires, 4 delay cycles which includes 1 decode clock cycle, 1 computational clock cycles and 2 register allocation clocks. For SHIFT instruction, it requires, 4 delay cycles which includes 1 decode clock cycle, 1 computational clock cycles and 2 register allocation clocks. For MOV instruction, it requires, 6 delay cycles which includes 1 decode clock cycle, 2 computational clock cycles and 3 register allocation clocks. Also, each instruction to be fetch and write for operation.Resource employment in regular instruction category will reduce the overhead.

In this approach,the common clocking instructions are realignment as a set of instruction and a common delay in register allocation is defined. Single time POST codingoperation is performing by thisrealignment process, and the delay is previously mentioned as a refery array.In this case,the executed operaions do notgo off forcalculationof clockdelayand the delay buffer reference.Fig.5 represents Data flow for updatedinstruction set.

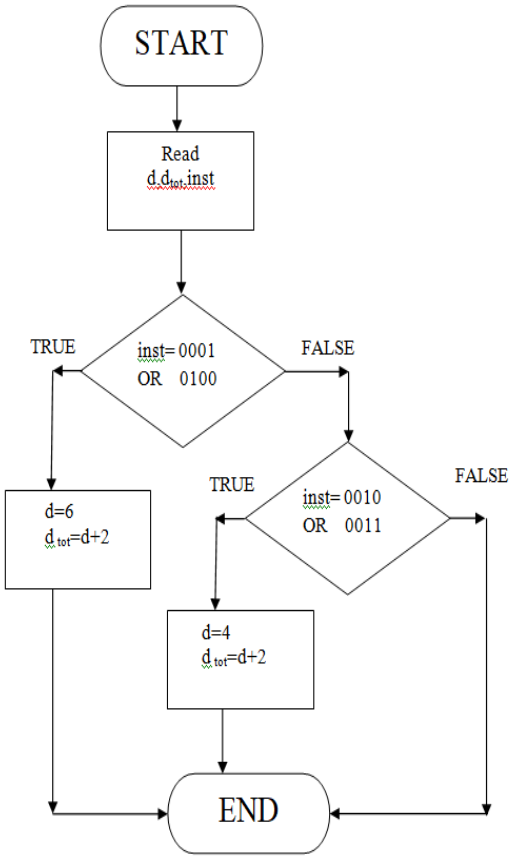

Fig.5 Data flow for Updated instruction set.

This approach reduces the latency of clock, thus the huge requirement of resource computations are eliminated.The proposed clock allocation process has an allocation of delay values for each instruction precomputed. To give best resource utility, these instructions are programmed in cryptography coding.

IV. SIMULATION RESULTS

A Hardware description language for the proposed approach is developed andsynthesizedon Xilinx ISE tool. The timing observations are simulated in same tool. FPGA designis chosen for the realization of the improvedapproach.

The latency, power,area and throughputmetrics areevaluated. For the test appraisal, 4 instruction set of operationsare performed to carry out key updating, substitution and permutation processes. The alignment of registers for a set of instruction is resulted in timing waveforms is shown in Fig.6.

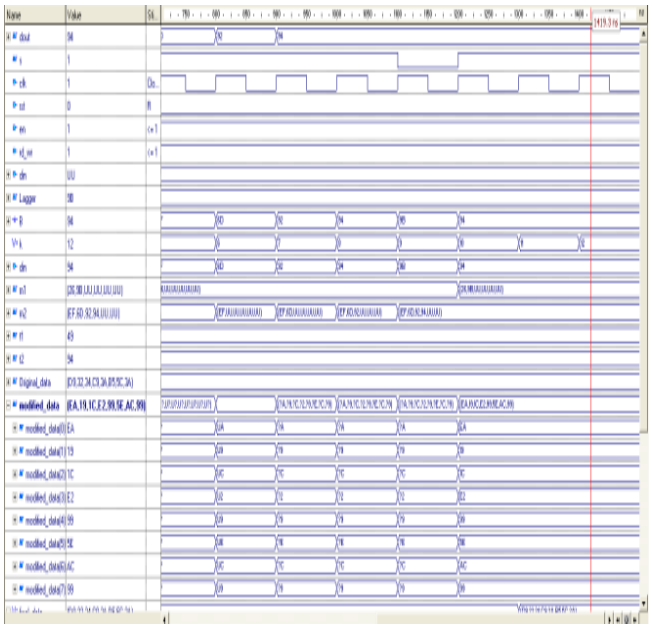

Fig.6 Alignment of registers for a set of instructions

The optimized approach in security coding is observed and as outlined below,

In designed approach, a 64-bit block of data and80-bit key is considered as

- Plain Text (PT): "123ABC467DEF8905"
- Key(K): "A111B222CD555678EEE9"
- Encrypted output(ENC_out): "52F0976087FF2314"

In encryption process, plain text is encrypt with the key, it will generate cipher text (Encrypted output). In decryption process, the cipher text is acts as a input and it is decrypt with the same key, it will generate plaintext text (original data).

The Obtained Decrypted output data is given as

- DEC_out_PT: "123ABC467DEF8905"

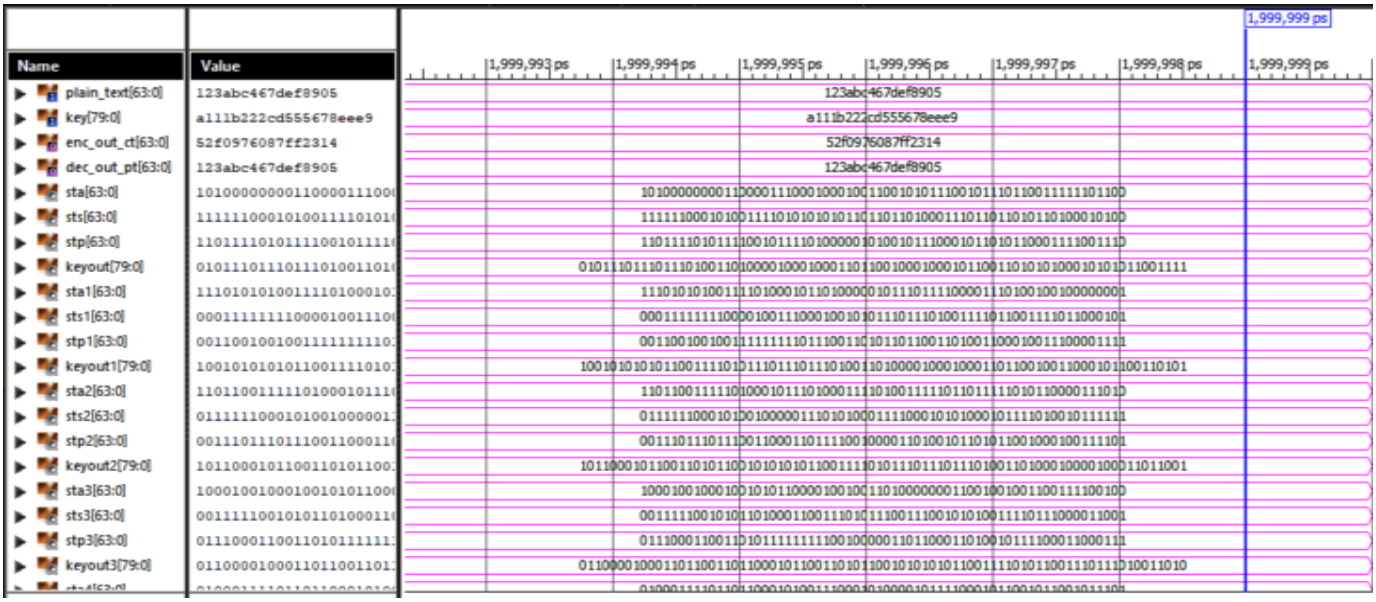

Fig.7. The Waveforms for Encryption process and Decryption process

From Fig.7, the Data is recovered same as Input data (Plaintext). The implementations ofFPGA is targeting to Xilinx FPGA device Spartan-3 (xc3s200-5ft256). The synthesis report For the targeted device , is illustrated in Table.1

Table 1:.SynthesisImplementation for targeted FPGA.

Device Utilization Summery			
Logic Utilization	**Used**	**Available**	**Utilization(%)**
• Number of Slices	99	1,920	5%
• Number of Slice Flip Flops	156	3,840	4%
• Number of slice LUTs	174	3,840	4%
• Number of occupied Slices	114	1,920	5%
• Number of Slices containing only related logic	114	114	100%
• Total Number of 4 input LUTs	174	3,840	4%
• Number used as a route thtu	128		
• Number of bonded IOBs	149	173	86%
• IOB flip flops	14		
• Number of GCLKs	1	8	12%
• Total equivalent gate count for design	1,643		
• Additional JTAG gate count for IOBs	721		

To estimate, implementation, performance, Spartan-3 is targeted are validas follows.

The power is measured by using Xilinx Xpower analyzertool.The system latency is tested for a targeted FPGA deviceand itis dimnished by resource reutilization method.The max. throughputis a function of system frequency(Fmax),a block latency cycles and the block size is computed as,

$$THR = \frac{Fmax \times Bsize}{LAT} \quad (1)$$

The area is represented intermsof no.offlipflops, no.of LUTs and no.of slices.

The matricscomparision of existing work[11]and the improved work is illustrated in Table.2.

Table:2 The comparision of different parameters.

Parameter	Existing work (PRESENT)	Improved work (IPRESENT)
• Latency (cycles)	133	129
• Power (mW)	271.5	192
• Throughput (Mbps)	102.89	188.22
• Area (FF+LUT+SC)	492	428

V. CONCLUSION

This paper presented the improvement of cryptography coding with optimal resource utilization.The new technique enhances the operation speed by usinglimitedplaying fieldcalculationmethod todiminish the calculationtime for Encryption and decryption of data using PRESENT. The surveillancesfrom the realization ofimproved PRESENT approach, the devicecan support to 64-bit data for modified with a rate of 379.4 MHz.The throughput is about 188.22 Mbps. The resource occupied on Spartan-3 targeted chip is about 543required slices. The optimized resource utility encryption is achieved and observed.

REFERENCES

1. R. Want and S. Dustdar, “Activating the internet of things [guest editors’introduction],” Computer, vol. 48, no. 9, pp. 16–20, 2015.
2. T. Macaulay, “Introduction—The Internet of Things,” in RIoT Control: Understanding and Managing Risks and the Internet of Things. Boston, MA, USA: Morgan Kaufmann, 2017, ch. 1, pp. 1–26.
3. H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: a review,” in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.
4. Muhammad Usman, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan and Usman Ali Shahy, ‘‘SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,’’ International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.
5. C. Alippi and C. Galperti, “An adaptive system for optimal solar energy harvesting in wireless sensor network nodes,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 55, no. 6, pp. 1742–1750, Jul. 2008.
6. A. A. R. Haeri, M. G. Karkani, M. Sharifkhani, M. Kamarei, and A. Fotowat-Ahmady, “Analysis and design of power harvesting circuits for ultra-low power applications,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 64, no. 2, pp. 471–479, Feb. 2017.
7. Z. Zou et al., “A low-power and flexible energy detection IR-UWB receiver for RFID and wireless sensor networks,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 58, no. 7, pp. 1470–1482, Jul. 2011.
8. Bormann, C Guidance for LightWeight Implementations of the Internet Protocol Suite; IETFInternet Draft draft-ietf-lwig-guidance-02, The Internet Engineering Task Force (IETF): Fremont,CA, USA, 2012. [9] Information Technology—Security Techniques—Lightweight Cryptography—Part 2: Block Ciphers, document ISO/IEC 29192-2, Jan. 2012.
9. A. Bogdanov et al., “PRESENT: An ultra-lightweight block cipher,” in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 4727. Berlin, Germany: Springer, 2007, pp. 450–466.
10. Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval “Lightweight Hardware Architectures for the Present Cipher in FPGA,” IEEE Transactions on Circuits and Systems–1: Regular Papers, vol. 64, no. 9, September 2017.

AUTHORS PROFILE

T.Sunitha received B.Tech in Electronics and Communication Engineering from SVITS, Mahaboobnagar, India and M.Tech in VLSI System Design from VNR VJIET, Hyderabad, Indiaand pursuingPh.D in GITAM University. She is currently working as an Assistant Professor in the Department of Electronics and Telematics Engineering, GNITS, Hyderabad, Telangana, India. Her area of interest is VLSI Design.

K. Sridevireceived her B.Tech degree in Electronics and Communication Engineering from Nagarjuna University, Andhra Pradesh and M.Tech in Digital Systems and Computer Electronics from JNTU, Hyderabad, India. She received her Ph.D from GITAM University. She is currently working as an Associate Professor in the Department of Electrical, Electronics and Communication Engineering, GITAM University, Visakhapatnam, Andhra Pradesh, India. She published more than 24 Research papers in refereed International journals, International &National Conferences. Herfields of interest includes signal processing and VLSI.

J. Durga Rao Received B.Tech. in Electronics and communication Engineering from GITAS, Bobbili, M.Tech in ‘Digital Electonics and Communication Systems’, from Chaitanya Engineering College,Visakhapatnam and pursuingPh.D in GITAM. His area of research is security improvement in Wireless Body Area Networks.