Compact Lightweight Cryptographic Algorithm for Optimization of Resources

Sunitha Tappari, K. Sridevi, Durga Rao Jenjeti

Abstract: The study of Lightweight cryptography has been one of the interesting 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 providing more security in various applications, resource utility is more in key generation, key scheduling, permutation layer and substitution box layer operations. More resource usage make possible to have high utilization of power and overhead of area. In this paper, a novel method is proposed to decrease the utility of resources, which follows register reutilization scheme. The resource reutilization is coordinating with the delay in Substitution Permutation Network (SPN). Our design is compared, using area, throughput, power, and latency as metrics.

Keywords: Symmetric light weight cryptography, Resource optimization, Register reutilization, Cryptography coding.

I. INTRODUCTION

The world over in the environment computing 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 substantial equipment adjacent tous. The devices itself start to the sharing process of large data which should communicate with IoT with more security.

The IoT is taking the mobile network, conventional internet and sensor network to a different level are connected to the internet. IoT is further susceptible to serious threats of security than available network, the reason for that is 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 will reach the requirements place by smart devices. In this, cryptography methods have to work with minimum amount of vital resources of required objects. “Lightweight” term represents algorithm 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, Security and Cost

The key length is decreases to 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 indicated in 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 symmetric cryptographic algorithms Vs asymmetric cryptographic algorithms. Due to the hardware-friendly nature, symmetric cryptography is suitable for constrained devices. Which implies minimization of supplementary computational cost and consumption of power.
II. PRESENT CIPHER

PRESENT is a symmetric light weight blockcipher. In hardware realizations of 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 64 bit 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](image)

The resource overhead is generated in this approach due to recursive operation is more in key scheduling approach. This approach is proficient, but it requires large quantity of resources. To diminish the resource overhead, approach of resource minimization is 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.](image)

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

![Fig.4 Data flow for instruction set.](image)
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, 2 computational clock cycles and 3 register allocation clocks. Also, each instruction to be fetched and written for operation. Resource employment in regular instruction category will reduce the overhead.

In this approach, the common clocking instructions are realigned as a set of instruction and a common delay in register allocation is defined. Single time POST coding operation is performed by this realignment process, and the delay is previously mentioned as a reference. In this case, the executed operations do not go off for calculation of clock delay and the delay buffer reference. Fig. 5 represents Data flow for updated instruction set.

**IV. SIMULATION RESULTS**

A Hardware description language for the proposed approach is developed and synthesized on Xilinx ISE tool. The timing observations are simulated in the same tool. FPGA design is chosen for the realization of the improved approach. The latency, power, area and throughput metrics are evaluated. For the test appraisal, 4 instruction set of operations are 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.5 Data flow for Updated instruction set.](image)

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.

**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 and 80-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 plain text (original data).

The Obtained Decrypted output data is given as:

- **DEC_out_PT:** "123ABC467DEF8905"
Compact Lightweight Cryptographic Algorithm for Optimization of Resources

![Waveforms for Encryption process and Decryption process](Fig.7)

From Fig.7, the Data is recovered same as Input data (Plaintext). The implementations of FPGA is targeting to Xilinx FPGA device Spartan-3 (xc3s200-5fl256). The synthesis report for the targeted device, is illustrated in Table.1

Table 1: Synthesis Implementation for targeted FPGA.

| Device Utilization Summery | 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 thru | 128 | 128 | 100% |
| 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 | 1,643 | 100% |
| Additional JTAG gate count for IOBs | 721 | 721 | 100% |

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

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

\[ THR = \frac{F_{\text{max}} \times \text{Size}}{LAT} \]  \hspace{1cm} (1)

The area is represented in terms of no. of flipflops, no. of LUTs and no. of slices.
The matrix comparison of existing work [11] and the improved work is illustrated in Table 2.

Table:2 The comparison 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 using limited playing field calculation method to diminish the calculation time for Encryption and decryption of data using PRESENT. The surveillances from the realization of improved PRESENT approach, the device can support up 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 543 required 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 Shaly, “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-Ahmad, “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; IETF Internet Draft draft-ietf-iot-ambig-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. Sunita received B.Tech in Electronics and Communication Engineering from SVITs, Mahaboobnagar, India and M.Tech in VLSI System Design from VNR VJIET, Hyderabad, India and pursuing Ph.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 VLSI Design.

K. Sridevi received 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. Her fields 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 Electronics and Communication Systems’, from Chaitanya Engineering College, Visakhapatnam and pursuing Ph.D in GITAM. His area of research is security improvement in Wireless Body Area Networks.