Educational Administration: Theory and Practice
2024, 30(5), 10302-10309
ISSN: 2148-2403
https://kuey.net/

Research Article

Enhancing DES Encryption Efficiency on 16 nm FPGA through Clock Gating for Low Power Design

Yashwant Aditya[1*], Pushpanjali Pandey[2], Leila Rzayeva[3]

[1*]University of Oxford, United Kingdom, yashwant.aditya@sbs.ox.ac.uk[1]
[2]R&D Lab, Gyancity Research Consultancy, Greater Noida, India, pushpanjali.pandey@gyancity.com
[3]Department of Intelligent System and Cyber Security, Astana IT University, Astana, Kazakhstan, l.rzayeva@astanait.edu.kz

Citation: Yashwant Aditya, et al (2024), Enhancing DES Encryption Efficiency on 16 nm FPGA through Clock Gating for Low Power Design, Educational Administration: Theory and Practice, *30*(5), 10302-10309, Doi: 10.53555/kuey.v30i5.4741

ARTICLE INFO

ABSTRACT

As advancement in the tech world is rapidly increasing, data privacy and message privacy are becoming crucial in today's generation. Securing the data with the hardware mechanism is in great demand. In this research work, a secure mechanism of hardware implementation is being highlighted. To secure the message, a Data Encryption Standard (DES) algorithm is implemented on a Field Programmable Gate Array (FPGA) device. The algorithm is implemented on a Kintex Ultrascale + 16 nm device, and the results are tested for five different ranges (1ns-25ns) of clock cycles to make the hardware design power-efficient. The encryption process utilizes low power at 25 ns clock cycle, as there is a decrement in the clock cycle speed for the encryption process the power consumption gets increased.

Keywords: FPGA, Clock Cycles, DES Algorithm, Power, Data Privacy

INTRODUCTION

In the contemporary landscape of digital communication and data storage, ensuring the privacy and security of sensitive information is paramount. The proliferation of interconnected devices and the exponential growth of data have underscored the need for robust encryption mechanisms that can safeguard data integrity and confidentiality. Among various encryption algorithms, the Data Encryption Standard (DES) has been a foundational method, widely studied and implemented due to its straightforward structure and historical significance. However, the challenge lies in optimizing these encryption algorithms to meet the dual demands of high security and low power consumption, particularly in hardware implementations [1]. The block diagram of DES algorithm is described in fig 1. The 64 bit plain-text is separated into 32 bits on right side and in 32 bits on left side after the IP. And on both side of 32 bits data process such as S-Box, P-Box along with key goes on and after FP resultant 64 bits cipher text is obtained [2].

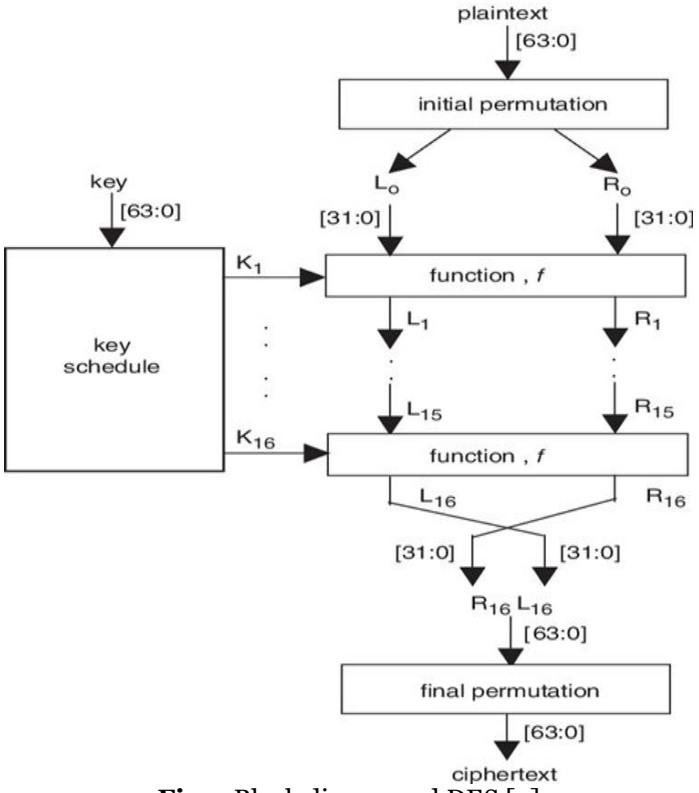

Fig 1. Block diagram od DES [3]

Field Programmable Gate Arrays (FPGAs) have emerged as a versatile and powerful platform for implementing cryptographic algorithms due to their reconfigurability, high performance, and capacity for parallel processing. The Kintex Ultrascale+ 16 nm FPGA is particularly well-suited for such tasks, offering advanced features that facilitate efficient hardware design. This research focuses on the implementation of the DES algorithm on this FPGA, leveraging clock gating techniques to achieve a low power design. The major components of FPGA is shown in fig 2. The FPGA device is basically comprising Look Up Tables (LUTs). Input Output (IOs), Memory, and Configurable Logic Blocks (CLBs) [4-5].

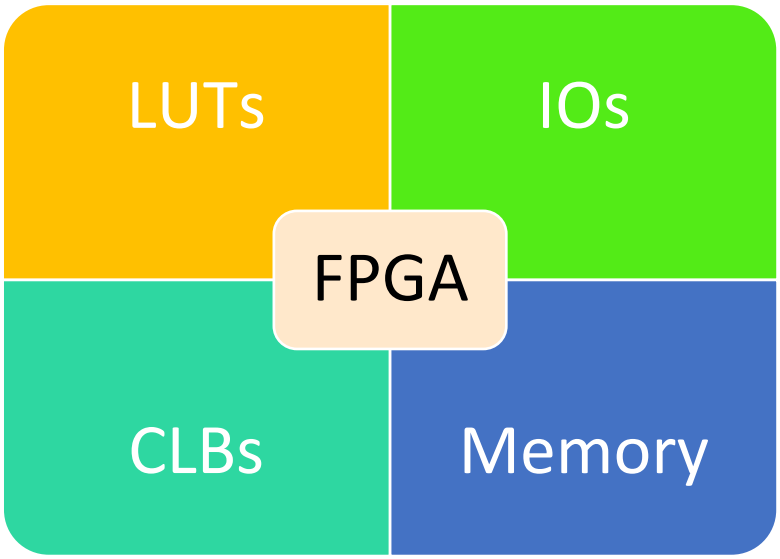

Fig 2. Major components of FPGA

Clock gating is a power-saving technique used in digital circuits to reduce dynamic power consumption by disabling the clock signal to portions of the circuitry that are not in use. By selectively enabling and disabling the clock signal, clock gating minimizes unnecessary switching activities, thereby conserving power. Integrating this technique into the DES encryption process holds the promise of significantly enhancing power efficiency without compromising the algorithm's performance. The different clock speeds used for power analysis is shown in fig 3.

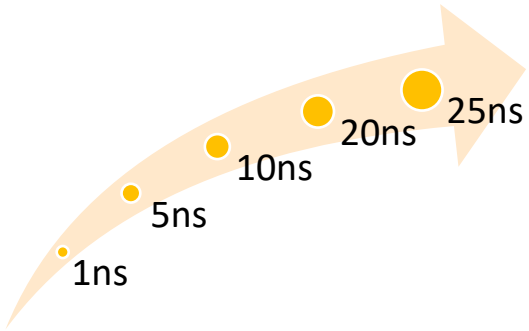

Fig 3. Various clock speed used for power analysis

The primary objective of this study is to explore the impact of clock gating on the power consumption of the DES algorithm when implemented on a 16 nm FPGA device. The DES algorithm's performance is evaluated across different clock cycle durations to identify the optimal configuration for low power consumption. The findings of this research are expected to contribute to the development of more energy-efficient cryptographic solutions, which are increasingly critical in applications ranging from mobile devices to large-scale data centers. By investigating the interplay between clock gating and power efficiency in the context of DES encryption, this research aims to provide valuable insights into designing low power cryptographic hardware. This is particularly relevant in scenarios where power resources are constrained, and energy efficiency is a critical parameter [6]. The outcomes of this study not only highlight the potential of FPGA-based implementations for secure and efficient data encryption but also pave the way for future advancements in hardware-based security mechanisms.

I. Related Work

Data privacy is a much needed topic in the current scenario of the time. For the privacy purpose lots of algorithm are available in the cryptography field. DES is one of secure algorithm of data encryption. Using the HTML method, a low power design is implemented on FPGA [1] and the security can also be increased [2]. The low power design can also be implemented applying a SSTL IO standard for DES algorithm [3]. In [4] to make the encryption process power-efficient researches implemented the DES algorithm on 28nm device. To make the implementation energy efficient on 28nm device timing analysis can also be done, therefore authors used the timing constrained parameters on high performance device to make to encryption power-efficient [5]. In [6] high performance FPGAs are in great demand for optimum power consumption for the AES algorithm. In [7] a 128-bit AES algorithm is implemented by the researchers on high performance FPGA to make the encryption power-efficient. In [8] using the high performance device authors design a low power crypto processor using the AES algorithm. In [9] researchers used a light version of AES algorithm for voice encryption process on Artix-7 device. In [10] authors used the Arix-7 device for implementing the power-efficient AES algorithm. In [11] researchers made a survey of various techniques for the implementation of various cryptography algorithms on FPGA device. In 12] researchers implemented and made a comparative analysis for the AES encryption process on the FPGA device. In [13] researchers used the 7th series of FPGA device for the implementation of AES encryption. Many research works are going on with AES and DES algorithm to for enhancing the security purpose as well as FPGA devices are used to minimize the power. As of literature and better of our knowledge no work has been done on minimizing the power with implementing the DES algorithm at various clock cycles. In this work we are making a low power design of DES algorithm using clock gating technique on 16 nm Kintex Ultrascale + FPGA device

.

II. Implementation and Synthesis

This section discuss about the implementation process of DES algorithm. The synthesis and implementation is done on Kintex Ultrascale+ 16 nm device. On the implementation of DES algorithm of 16 nm device, 1168 LUT and 184 IO resources of FPGA device is utilized [14]. The post synthesis resource consumption is represented in fig 4.

Utilization **Post-Synthesis** | Post-Implementation

Graph | **Table**

Resource	Estimation	Available	Utilization %
LUT	1168	162720	0.72
IO	184	304	60.53

Fig 4. Post Synthesis Resource Consumption

III. Results and Discussion

The power calculation of the device is the sum up of static power (SP) and dynamic power (DP) $[TP = SP + DP]$. The DP is further more calculated by adding the IO, signals, logic, and clocks power. The power is calculated for 5 distinguished clock cycles that are 1ns, 5ns, 10ns, 20ns, and 25ns respectively. As the clock cycles speed changes, the not only the power but the other parameters such as thermal margin (TM), junction temperature (JT) also varies. There is no change observed in Effective TJA (Theta Junction to Ambient). It is constant for all the clock cycles (2.6℃/W).

Tuning at 1ns clock

When the clock speed is tuned at 1ns the total power (TP) is 4.6W. at 1ns clock the DP is contributing 97% to TP while the SP is contributing 3% only. The SP and DP are 0.119W and 4.481W respectively. The on-chip power at 1ns clock is described in fig 5.

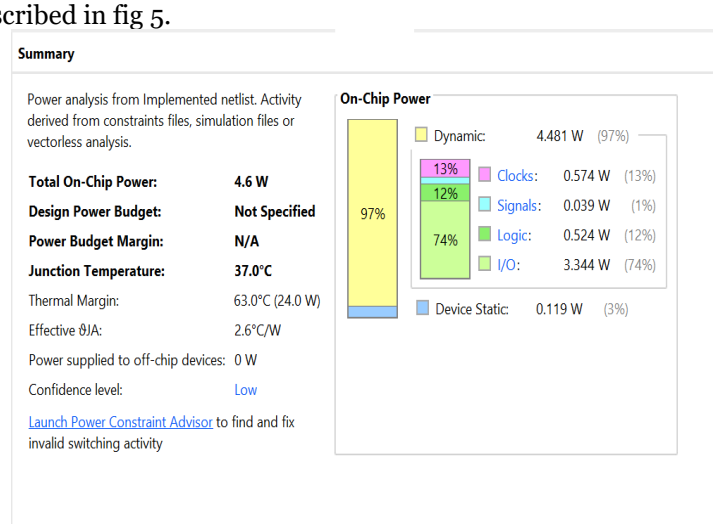

Fig 5. On-chip power at 1ns clock

Tuning at 5ns clock

When the clock speed is tuned at 1ns the total power (TP) is 1.379W. at 1ns clock the DP is contributing 92% to TP while the SP is contributing 8% only. The SP and DP are 0.114W and 1.265W respectively. The on-chip power at 1ns clock is described in fig 6.

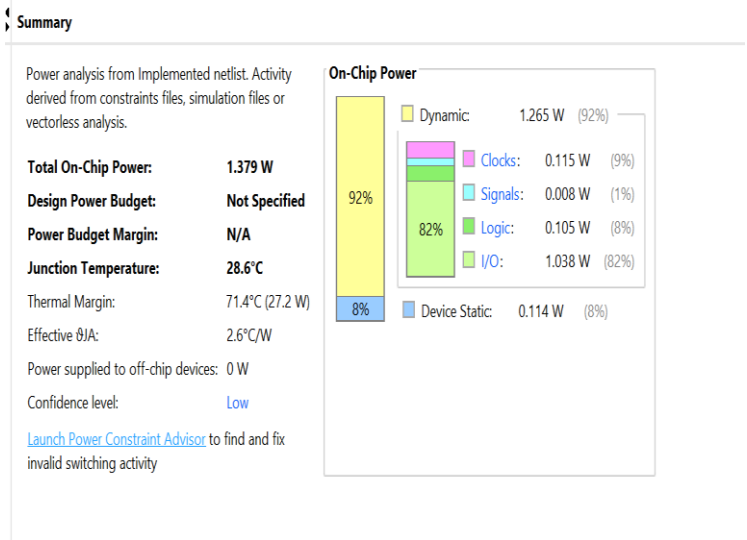

Fig 6. On-chip power at 5ns clock

Tuning at 10ns clock

When the clock speed is tuned at 1ns the total power (TP) is 0.976W. at 1ns clock the DP is contributing 88% to TP while the SP is contributing 12% only. The SP and DP are 0.114W and 0.863W respectively. The on-chip power at 1ns clock is described in fig 7.

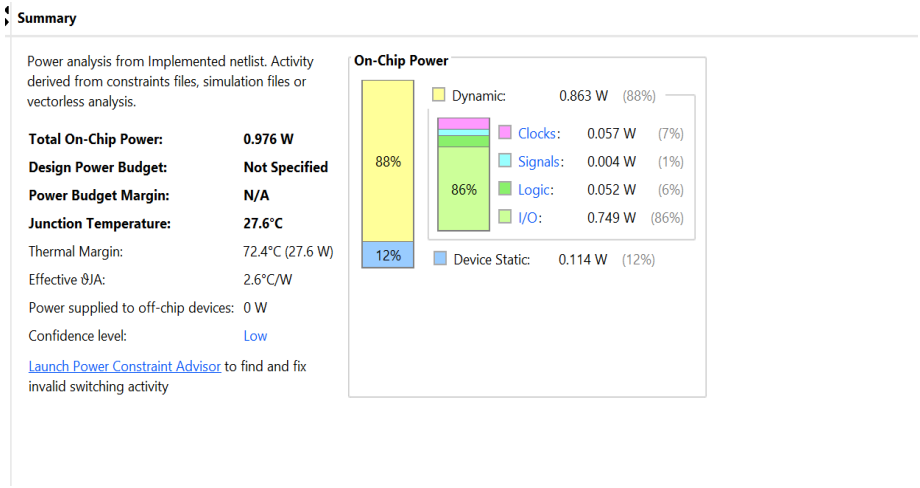

Fig 7. On-chip power at 10ns clock

Tuning at 20ns clock

When the clock speed is tuned at 1ns the total power (TP) is 0.775W. at 1ns clock the DP is contributing 85% to TP while the SP is contributing 15% only. The SP and DP are 0.113W and 0.662W respectively. The on-chip power at 1ns clock is described in fig 8.

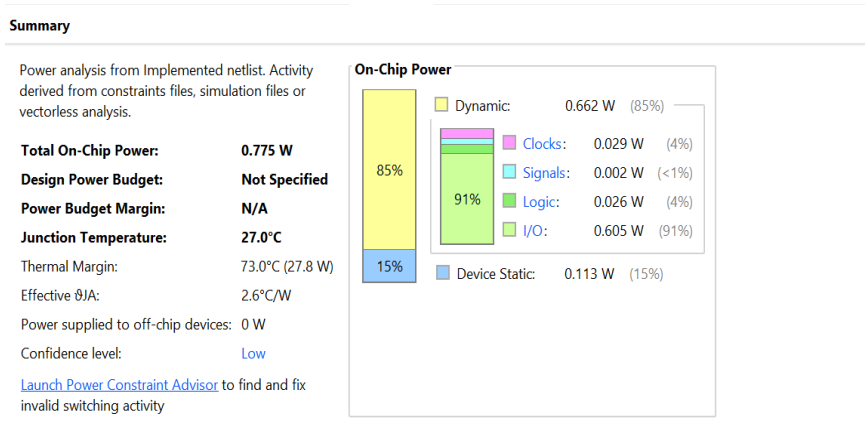

Fig 8. On-chip power at 20ns clock

Tuning at 25ns clock

When the clock speed is tuned at 1ns the total power (TP) is 0.735W. at 1ns clock the DP is contributing 85% to TP while the SP is contributing 15% only. The SP and DP are 0.113W and 0.622W respectively. The on-chip power at 1ns clock is described in fig 9.

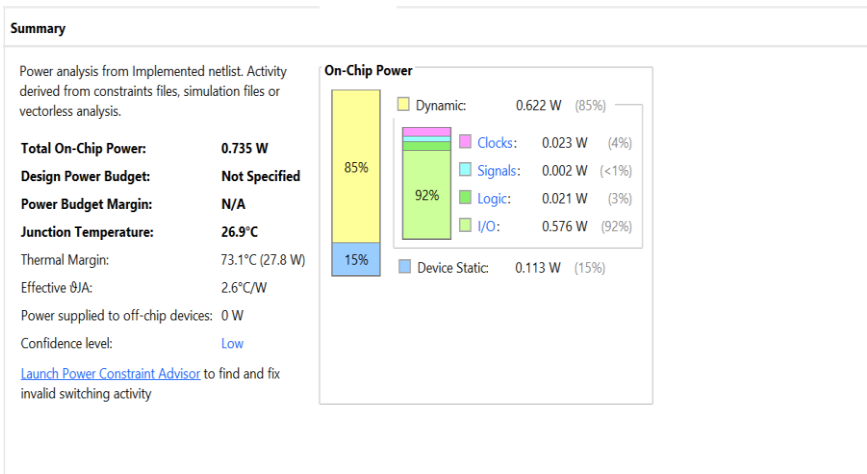

Fig 9. On-chip power at 25ns clock

Total on-chips power analysis

As the clock cycle speed increases the TP gets decreased. The contribution of DP also decreases while the contribution of SP gets increased as clock cycle gets tuned from 1ns to 25ns speed. The TP is maximum at 1ns while the minimum at 25ns speed. The total on chip power analysis is shown in table 1 and fig 10.

Table 1. Total on-chips power analysis

Clock Cycle (ns)	Total Power (W)
1	4.6
5	1.379
10	0.976
20	0.662
25	0.622

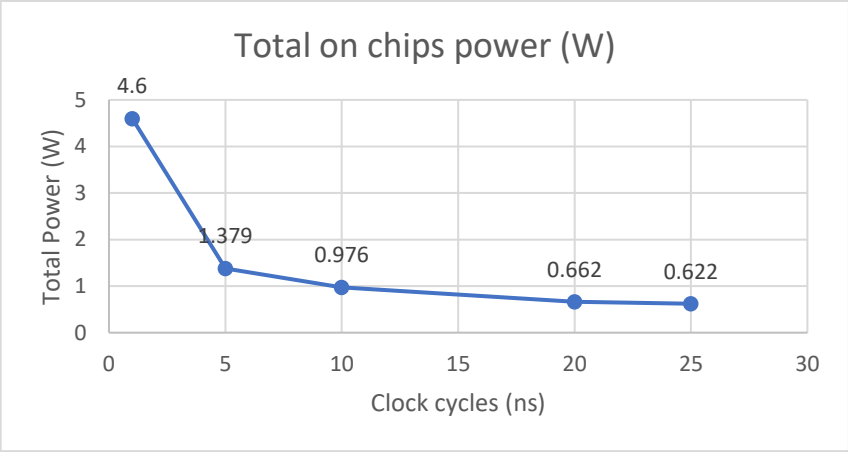

Fig 10. Total on-chips power analysis

Thermal parameters analysis

As the clock cycles speed changes, the thermal parameters such as thermal margin (TM), junction temperature (JT) also varies. There is no change observed in Effective TJA (Theta Junction to Ambient). It is constant for all the clock cycles (2.6℃/W). The analysis is shown in table 2 and fig 11.

Table 2. Thermal parameters analysis

Clock Cycle (ns)	Junction Temperature (℃)	Thermal Margin (℃)
1	37	63
5	28.6	71.4
10	27.6	72.4
20	27	73
25	26.9	73.1

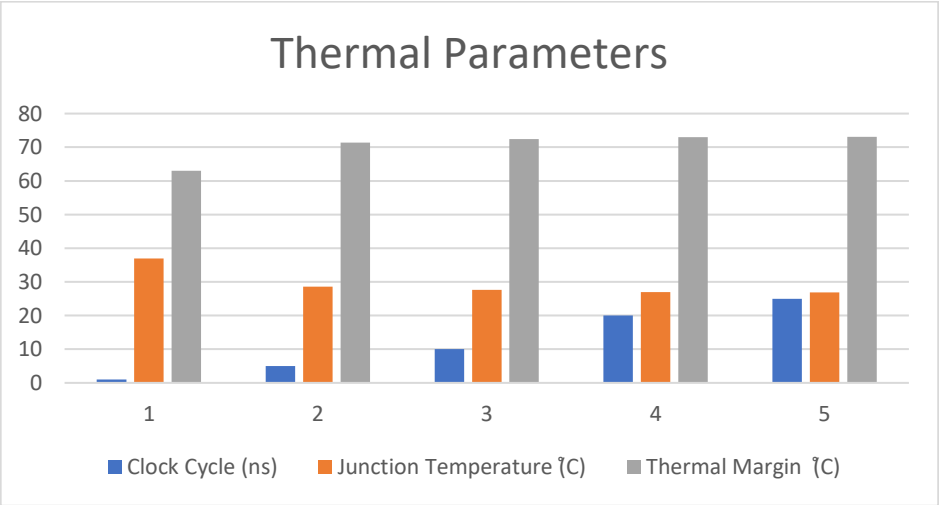

Fig 11. Thermal parameters analysis

IV. CONCLUSION

As progression in the tech world is quickly expanding, information security and message protection are becoming significant in the present age. Protecting the information with the equipment system is extremely popular. In this exploration work, a solid system of equipment execution is being featured. To get the message, an Data Encryption Standard (DES) calculation is carried out on a Field Programmable Gate Arrays (FPGA) gadget. In order to make the hardware design power-efficient, the results of the algorithm's implementation on a Kintex Ultrascale + 16 nm device are evaluated across five distinct clock cycle ranges, ranging from 1ns to 25ns. The encryption cycle uses low power at 25 ns clock cycle, as there is a decrement in the clock cycle speed for the encryption cycle the power utilization gets expanded.

V. FUTURE SCOPE

In this work, we are using clock gating technique for optimizing the power for DES implementation on 16nm FPGA. Moreover, there are several other power-efficient methodologies such as voltage scaling, frequency scaling, IO standards etc., can also be used to make the implementation power-efficient so that that it may promote the ethics of green communication. Also, with the advancement in machine learning and artificial intelligence (AI) techniques we can also design an AI enabled power efficient encryption standard with FPGA devices.

REFERENCES

1. Thind, V., Pandey, B., Kalia, K., Hussain, D.A., Das, T. and Kumar, T., 2016. FPGA based low power DES algorithm design and implementation using HTML technology. International Journal of Software Engineering and Its Applications, 10(6), pp.81-92.
2. Pandey, B., Bisht, V., Ahmad, S. and Kotsyuba, I., 2021. Increasing cyber security by energy efficient implementation of DES algorithms on FPGA. Journal of Green Engineering, 11(10), pp.72-82.
3. Pandey, B., Thind, V., Sandhu, S.K., Walia, T. and Sharma, S., 2015. SSTL based power efficient implementation of DES security algorithm on 28nm FPGA. International Journal of Security and Its Application, 9(7), pp.267-274.
4. Thind, V., Pandey, B. and Hussain, D.A., 2016, August. Power analysis of energy efficient DES algorithm and implementation on 28nm FPGA. In 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES) (pp. 600-603). IEEE.
5. Thind, V., Pandey, S., Akbar Hussain, D.M., Das, B., Abdullah, M.F.L. and Pandey, B., 2018. Timing constraints-based high-performance DES design and implementation on 28-nm FPGA. In System and Architecture: Proceedings of CSI 2015 (pp. 123-137). Springer Singapore.
6. Kumar, K., Singh, V., Mishra, G., Babu, B.R., Tripathi, N. and Kumar, P., 2022, December. Power-Efficient Secured Hardware Design of AES Algorithm on High Performance FPGA. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (pp. 1634-1637). IEEE.
7. Aditya, Y. and Kumar, K., 2022. Implementation of Novel Power Efficient AES Design on High Performance FPGA. NeuroQuantology, 20(10), p.5815.
8. Aditya, Y. and Kumar, K., 2022. Implementation of High-Performance AES Crypto Processor for Green Communication. Telematique, pp.6808-6816.
9. Kumar, K., Ramkumar, K.R. and Kaur, A., 2022. A lightweight AES algorithm implementation for encrypting voice messages using field programmable gate arrays. Journal of King Saud University-Computer and Information Sciences, 34(6), pp.3878-3885.
10. Kumar, K., Kaur, A., Ramkumar, K.R., Shrivastava, A., Moyal, V. and Kumar, Y., 2021, November. A design of power-efficient AES algorithm on Artix-7 FPGA for green communication. In 2021 International Conference on Technological Advancements and Innovations (ICTAI) (pp. 561-564). IEEE.
11. Kumar, K., Ramkumar, K.R., Kaur, A. and Choudhary, S., 2020, April. A survey on hardware implementation of cryptographic algorithms using field programmable gate array. In 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 189-194). IEEE.
12. Kumar, K., Ramkumar, K.R. and Kaur, A., 2020, June. A design implementation and comparative analysis of advanced encryption standard (AES) algorithm on FPGA. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 182-185). IEEE.
13. Jindal, P., Kaushik, A. and Kumar, K., 2020, July. Design and implementation of advanced encryption standard algorithm on 7th series field programmable gate array. In 2020 7th international conference on smart structures and systems (ICSSS) (pp. 1-3). IEEE.

14. Kumar, K., Kaur, A., Pandey, B. and Panda, S.N., 2018, November. Low power UART design using different nanometer technology based FPGA. In 2018 8th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 1-3). IEEE