Contents lists available at IdNNS
Indonesian Journal of Cybersecurity and Emerging Risks
Volume 1 ; Issue 2
journal homepage: https://journal.idnns.org/index.php/ijcyber

Ensuring High Performance During Implementation of Security Algorithms on FPGA

Neeraj Bisht[a], Sandeep Budhani[b] and Shilpi Bisht[a,i]

[a] *Birla Institute of Applied Sciences, Bhimtal, Uttarakhand 263136, India*
[b] *Graphic Era Hill University, Bhimtal, Uttarakhand 263136, India*

ARTICLE INFO

Keywords:
AES
DES
FPGA
Kintex-7 Low Voltage

ABSTRACT

Cryptography has evolved into an indispensable component of modern technology. To ensure the safety and security of critical data, which is easily accessible with a single click, it is critical to choose adequate, efficient, and viable cryptographic methods. Two widely used cryptographic algorithms are the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). In this study, the AES and DES algorithms are implemented in FPGA on the Kintex-7 Low Voltage device at three different frequencies. Comparative research is conducted using the experimental results for various critical parameters. This research aims to determine which cryptographic method consumes the least amount of power and occupies the least amount of space. The results indicate that the AES implementation for the Kintex-7 Low Voltage at 1.6 GHz was the most energy- and area-efficient algorithm, outperforming the DES implementation for the same setup.

1. Introduction

As the world progresses toward 5G communication and the Internet of Things (IoT), allowing users to control their entire home remotely, an increasing amount of data containing personal and sensitive information is being transmitted. Additionally, as technology advances to enable faster and more reliable data transportation throughout regions of the world, we must carry the weight of guaranteeing the security of data and sensitive information.

Cryptography is the most effective method of safeguarding our privacy and data. Cryptography is a centuries-old concept that stretches back to roughly 1900 BC when the Roman Empire began using hieroglyphic symbols. Additionally, Julius Caesar used substitution and transposition ciphers to safeguard the confidentiality of his forces' communications in 100 BC. These are referred to as classical cryptography approaches. Cryptography is extensively utilized and complex in today's world, and it is used by individuals, organizations, and governments equally.

[i] Corresponding author
bisneeraj@gmail.com (N. Bisht);
sandeepbudhani13@gmail.com (S. Budhani);
shilpi.bisht.lko@gmail.com (S. Bisht)
ORCID(s):

Cryptography in the modern era is split into two types: symmetric and asymmetric. In the first approach, the encryption and decryption keys are identical; in the second, they are distinct. The US government-created Data Encryption Standard (DES) is one of the most extensively used symmetric cryptographic algorithms. DES is a block iterated cipher that employs 64-bit fixed blocks at its most fundamental level. This cryptographic technique uses avalanche requirements, which are based on confusion and diffusion. The advent of numerous high-level programming languages capable of cracking DES encryption has resulted in the algorithm's popularity declining.

Advanced Encryption Standard (AES) is another frequently used form of cryptography in data transit. This cipher can be used in hardware or software. It has a block length of 128 bits and an encryption/decryption key length of 128, 192, or 256 bits. Additionally, the United States government deployed AES in 1998 to protect sensitive scientific data. Khalifa et al. Khalifa et al. (2004) assessed five cryptographic algorithms using three criteria: block or stream cipher, key size, and the algorithm's notable features. Their research establishes that AES is a secure algorithm that may be used in place of DES.

By 2025, communication technology may absorb about a fifth of all energy created on the planet, contributing to an energy crisis and substantial climatic

changes. However, current semiconductor technologies are designed to operate at high speeds while consuming very little energy, enabling the communication industry to grow. This approach will lead us along the road toward Green Computing and related endeavors.

At some point, a particular sort of semiconductor device will be capable of meeting our performance and power requirements. The Field Programmable Gate Array (FPGA) is a renowned and one-of-a-kind electrical component that offers unmatched adaptability. FPGAs are powerful electronic devices capable of performing various activities for which application-specific circuits have previously been built. Cuntan et al. Cuntan et al. (2015) conducted a study to determine the usefulness of incorporating FPGAs into students' course syllabi. They examined the benefits and drawbacks of testing circuits and signals using simulation software versus actual equipment, and discovered that simulation software provides significantly more flexibility for testing than simple circuits provide.

Unquestionably, FPGA devices are more cost-effective than application-specific integrated circuits (ASICs). Due to the versatility of FPGAs, they may be manufactured once and then reused in various applications by simply changing the programming. An FPGA is an integrated circuit that offers far greater processing freedom than a CPU. It is based on non-Von Neumann hardwired circuitry and significantly outperforms Von Neumann architectures in performance and data processing compatibility. Levin et al. Levin et al. (2016) focused their study on the FPGA's application in reconfigurable computer systems. They realized that the cooling of supercomputer systems had become a significant issue due to the massive circuits. They stated that FPGAs are critical components of reconfigurable supercomputers and that the cooling system of supercomputers has shifted to liquid cooling with the integration of Xilinx Virtex UltraScale.

This research aims to ascertain the energy efficiency of DES and AES on FPGA. The remainder of this work is organized as follows. Section 2 presents a review of relevant literature. Section 3 describes the parameters used in the comparative analysis. Section 4 presents the experimental setup and results. Section 5 discusses the comparative analysis. Finally, Section 6 summarizes the study's overall findings.

2. Literature Review

The most advantageous feature of an FPGA is that it is adaptable. Compared to conventional computer chips, FPGAs are programmable and reprogrammable to fulfill specific consumer requirements. As a result, FPGAs are capable of adapting to the bulk of our everyday and unique applications, putting them ahead of all competitors. In a review study on FPGA implementations of encryption methods, Yazdeen et al. Yazdeen et al. (2021) summarized the work of numerous academics. They asserted that data encryption and decryption methods might be implemented in FPGAs for various applications. Additionally, the authors determined that AES is a highly efficient cryptographic technique.

Most complex issues can be solved through software implementations on fast processors. Through approaches such as parallelization and flexibility, FPGAs offer a cost-effective alternative to processor-based systems while also providing much faster performance. Sakamoto et al. Sakamoto et al. (2018) conducted a research study in which they employed a NanoBridge metal atom migration type switch on FPGA devices to enhance the performance and power consumption of IoT devices. Anderson and Najm's research revealed Anderson and Najm (2004) the effect of interconnects and interconnect capacitance on power-conserving FPGA design for CAD. This work provided a model for capacitance prediction and examined noise. This design will be advantageous for low-power synthesis and layout considering power consumption.

Numerous researchers contributed to the AES and DES algorithms' FPGA implementation. Nabil et al. Nabil et al. (2020) suggested a high-performance AES implementation approach for FPGAs based on pipelining. This approach initiates a new encryption session at each clock, which improves performance, albeit it requires more resources than a standard AES implementation on an FPGA. The authors of Tonde and Dhande (2014) evaluated the AES algorithm's performance on an FPGA with a block and key size of 128. The authors conducted their experiment using all the FPGA's factory default parameters. The algorithm was implemented using Xilinx ISE software after being coded in VHDL. Das and Resmi Das and Resmi (2014) employed a Xilinx ISE 14.5 and a Vertex-5 FPGA to build the AES encryption algorithm. They chose to use ROM for key expansion rather than the register. Additionally, this design sought to eliminate shift rows. They asserted that the FPGA was more compact and efficient in terms of throughput and size. Farooq and Aslam Farooq and Aslam (2017) experimented with five different AES implementations on FPGA and performed a comparative analysis of proposed and existing work. Using seven different I/O standards and four FPGAs, Pandey et al. Pandey et al. (2021) tested the DES algorithm's energy efficiency. The SSTL 15 I/O standard and Artix-7 provided the optimal combination for energy-efficient DES implementation.

Renuka et al. Renuka et al. (2018) compared DES and AES algorithms on Virtex-6 FPGA and Microblaze Soft Core Processor on two parameters: number of slices used and maximum frequency. They concluded that a Verilog implementation consumed a lesser number of slices and produced more frequency, hence giving better area and speed options in comparison to the soft core Microblaze processor. Srilaya and Velampalli Srilaya

and Velampalli (2018) compared DES and AES based on encryption, decryption time, simulation time, and throughput for encryption and decryption time for a given plain text of 32 bytes and concluded that AES performed better than DES. Muneshwar et al. Muneshwar et al. (2022) implemented AES and DES algorithms on FPGA platform and compared both encryption algorithms.

This research aims to ascertain the energy efficiency of DES and AES on FPGA. The remainder of this work is divided into the following sections. The first section comprises an introduction; the second section contains a review of relevant literature, and the third portion contains a description of the parameters used in this comparative analysis. The fourth portion illuminates the experimental setup necessary for the work with experimental results, while the fifth section discusses the results' comparative analysis. Finally, the sixth part summarizes the study's overall findings.

3. Method and Material

This section defines the various parameters that are the basis of our experiments and comparative analysis. A summary of testing parameters is given in Figure 1.

3.1. On-Chip Power Consumption

The amount of power required internally by the FPGA is the cumulative total of Device Static plus Device Dynamic Power. Additionally, the term "thermal energy" is used for the same.

3.1.1. Static Power Consumption

The amount of power consumed by transistor leakage on all coupled voltage rails and the circuitry necessary for the FPGA to function normally following configuration. Static power is affected by a device's process, voltage, and temperature. Static power is the leakage that occurs when a device is in its steady state.

3.1.2. Device Dynamic Power

The user design consumes varying amounts of power during execution due to the given input pattern and internal design activity. This power is variable and instantaneous with each clock cycle. It is determined by the voltage levels and the logic plus routing resources used. Dynamic power consumption also comprises static current drawn by Input/Output terminations, clock controllers, and other components that require power to operate. This figure does not include power consumed by off-chip devices.

3.1.3. Junction Temperature

The junction temperature of a device indicates its operating temperature. Junction temperature equals the ambient temperature plus thermal power multiplied by the effective thermal resistance to air.

3.1.4. Ambient Temperature

This is the atmospheric air temperature during regular operation.

3.1.5. Effective Thermal Resistance to Air

TJA and Theta-JA are two alternative abbreviations for Effective Thermal Resistance to Air. This value indicates the amount of power dissipated by the FPGA circuitry into the environment. It considers everything, including the silicon chip's borders to the surrounding air, as well as any components in between, such as the packaging, the board, any heat sink, and airflow.

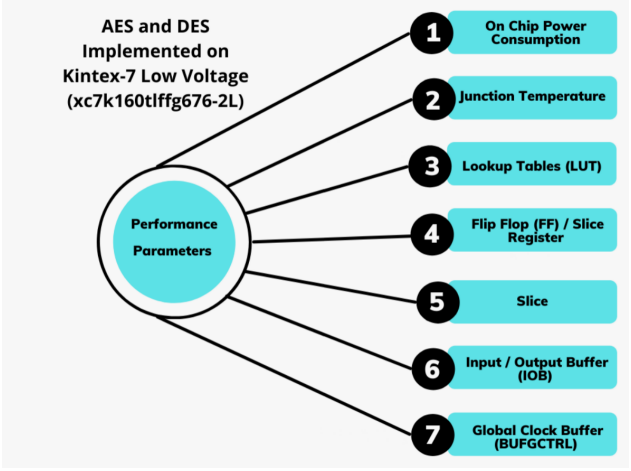

Figure 1: Performance parameters for security algorithms.

3.2. Resource Utilization

For the purposes of the comparison analysis, the following key resources are taken into consideration:

3.2.1. Lookup Tables (LUT)

When an FPGA is powered up, its LUT maintains a customized truth table. Consider the LUT as just a tiny scratchpad memory device. The LUT inputs are the address lines matching a one-bit-wide Random Access Memory cell. Whenever an FPGA is configured, individual bits of a LUT are filled with ones or zeros according to the desired truth table. Rather than wiring a series of logic gates together to construct the required truth table, a particular type of memory is utilized to simulate it.

3.2.2. Flip-Flop (FF) / Slice Register

This register entry contains the LUT result.

3.2.3. Slice

CLBs (Configurable Logic Blocks) are FPGA components used to perform logic operations. Each CLB comprises several slices, each of which can be further subdivided into look-up tables (LUTs), flip-flops (FFs), and multiplexers.

3.2.4. IOB

IOB is an abbreviation for Input/Output Buffer. In practice, this refers to the device's pin count. For example, if the design includes one reset, one clock, an 8-bit input, and an 8-bit output (all of which are single-ended), a total of $1 + 1 + 8 + 8 = 18$ pins are in use, resulting in 18 bonded IOBs.

3.2.5. Global Clock Buffers (BUFGCTRL)

The BUFGCTRL is a global clock buffer (similar to BUFG) that features two clock inputs and a sequence of control inputs for switching between the two clocks. The BUFGCTRL has the advantage of allowing the developer to switch between clocks without experiencing any glitches.

4. Experimental Setup and Results

AES and DES encryption algorithms are implemented in Verilog. Xilinx Vivado version 2020.1 simulation tool is used to obtain the results. The experiments are performed on the Kintex-7 Low Voltage (xc7k160tlffg676-2L) FPGA.

We examined the two cryptographic algorithms in terms of resource consumption and green computing performance, specifically power consumption and junction temperature.

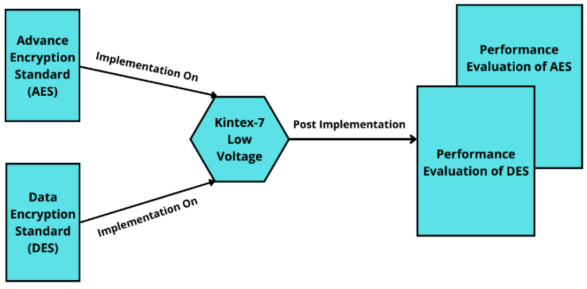

Figure 2: Schematic outline of the experiments.

Three distinct frequencies are investigated in the experiments. First, we began with a 3.4 GHz frequency and gradually decreased it to 2.4 GHz. Then finally, we conducted trials at the 1.6 GHz frequency. The reason for choosing the Kintex-7 Low Voltage (xc7k160tlffg676-2L) FPGA for our comparison analysis is that it performed the best in our prior work Bisht et al. (2022). A schematic outline of the experiments is given in Figure 2.

4.1. On-Chip Power Consumption

The dynamic, static, and total on-chip power consumption of the DES algorithm at various frequencies is shown in Table 1.

Table 2 records the AES algorithm's dynamic, static, and total on-chip power consumption for the selected frequencies.

Table 1: On-chip power consumption (in W) of DES for Kintex-7 Low Voltage.

Frequency	Dynamic	Static	Total
3.4 GHz	3.065	0.108	3.173
2.4 GHz	2.161	0.105	2.226
1.6 GHz	1.442	0.103	1.545

Table 2: On-chip power consumption (in W) of AES for Kintex-7 Low Voltage.

Frequency	Dynamic	Static	Total
3.4 GHz	0.335	0.100	0.436
2.4 GHz	0.237	0.100	0.336
1.6 GHz	0.158	0.100	0.257

Table 1 and Table 2 show that both algorithms' dynamic, static, and total on-chip power consumption are linearly related to frequency. The lowest total on-chip power usage is attained at 1.6 GHz in both cases. The minimum total power consumption on the chip for the DES algorithm is 1.545 W, whereas the minimum for the AES method is 0.257 W.

4.2. Junction Temperature

The junction temperature produced by the DES and AES algorithms for Kintex-7 Low Voltage is shown in Table 3 for the given frequencies. The junction temperature generated by DES and AES likewise decreases as the frequency is decreased. Kintex-7 Low Voltage has a minimum junction temperature of 28 C for the DES algorithm and 25.5 C for the AES algorithm. For AES, it is observed that frequency variations have a minor effect on junction temperature, but frequency variations have a significant effect on junction temperature for DES.

Table 3: Junction temperature (in C) of DES and AES for Kintex-7 Low Voltage.

Algorithm	3.4 GHz	2.4 GHz	1.6 GHz
DES	31.1	29.4	28.0
AES	25.8	25.6	25.5

4.3. Resource Utilization

To examine and compare the AES and DES algorithms' resource consumption, we recorded the total available and utilized resources (Slice LUT, slice registers, slice, Bonded IOB, and Global Clock Buffer) for all specified frequencies. This data is consistent across all frequencies: Table 4 and Table 5 detail the resource use of the DES and AES algorithms, respectively.

Table 4
Resource utilization of DES for Kintex-7 Low Voltage.

	Slice LUTs	Slice Reg.	Slice	Bonded IOB	BUFGCTRL
Total	101,400	202,800	25,350	400	32
Used	1024 (1.01%)	1024 (0.50%)	317 (1.25%)	129 (32.25%)	1 (3.13%)

Table 5
Resource utilization of AES for Kintex-7 Low Voltage.

	Slice LUTs	Slice Reg.	Slice	Bonded IOB	BUFGCTRL
Total	101,400	202,800	25,350	400	32
Used	167 (0.16%)	260 (0.13%)	67 (0.26%)	100 (25%)	1 (3.13%)

5. Comparative Analysis and Discussions

To compare the two cryptographic methods, we offered a relative value for each parameter included in our trials. A parameter's relative value is defined as:

$$\text{Relative Value} = \frac{\text{Value}_{\text{DES}} * \text{Value}_{\text{AES}}}{\text{Value}_{\text{AES}}} \quad (1)$$

This relative value provides us with efficient data for comparing the DES algorithm's consumption/production of a particular parameter to the AES algorithm.

Table 6: Relative on-chip power consumption and junction temperature by DES with respect to AES for Kintex-7 Low Voltage.

Frequency	Dynamic	Static	Total	Junction Temp.
3.4 GHz	8.14	0.08	6.27	0.20
2.4 GHz	8.11	0.05	5.62	0.148
1.6 GHz	8.12	0.03	5.01	0.098

Table 6 summarizes the calculated relative values for dynamic, static, total on-chip power consumption, and junction temperature at various frequencies. The ratio of DES's resource use to AES is computed, which is consistent across all frequencies and presented in Table 7. Figure 3–5 compare the performance of the two algorithms in terms of junction temperature, on-chip power consumption, and resource utilization.

Table 7: Relative resource utilization by DES with respect to AES for Kintex-7 Low Voltage.

Slice LUTs	Slice Reg.	Slice	Bonded IOB	BUFGCTRL
5.13	2.94	3.73	0.29	0

The relative comparative study of the DES algorithm with respect to the AES algorithm can be categorized into the following points:

- The maximum relative value of total on-chip power consumption is 6.27 for 3.4 GHz, which implies that DES has consumed 627% more power than the AES algorithm for 3.4 GHz frequency. Also, for 1.6 GHz, DES consumed 501% more total on-chip power than AES. These statistics demonstrate unequivocally that DES is a far more power-hungry algorithm than AES.
- Dynamic power consumption by the DES algorithm is 814% more than the AES algorithm in the worst case, while we observe that static power consumption by DES is just 8% more than AES in the worst case.
- The reported junction temperature for DES is approximately 20% higher than AES at 3.4 GHz but drops to 9.8% at 1.6 GHz. Increased junction temperature will cause the device to heat up, resulting in several issues.

According to Table 7, the DES implementation required 513% more Slice LUTs, 294% more Slice Registers, and 373% more Slices than the AES implementation on the same FPGA platform at the same frequency. These enormous figures strongly indicate that the DES algorithm consumes far more resources than the AES algorithm for the same architecture.

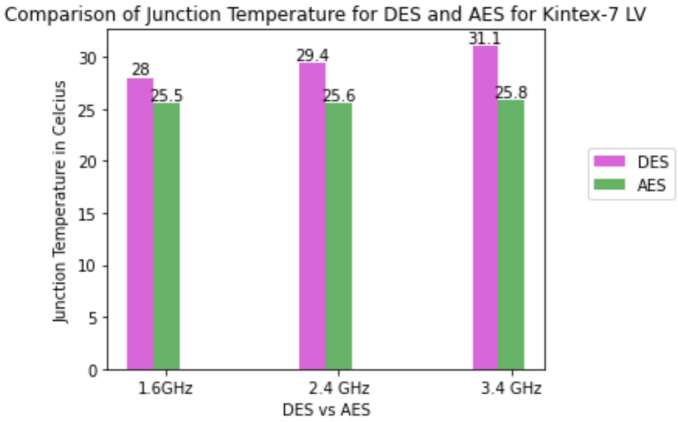

Figure 3: Comparison of junction temperature for DES and AES for Kintex-7 Low Voltage.

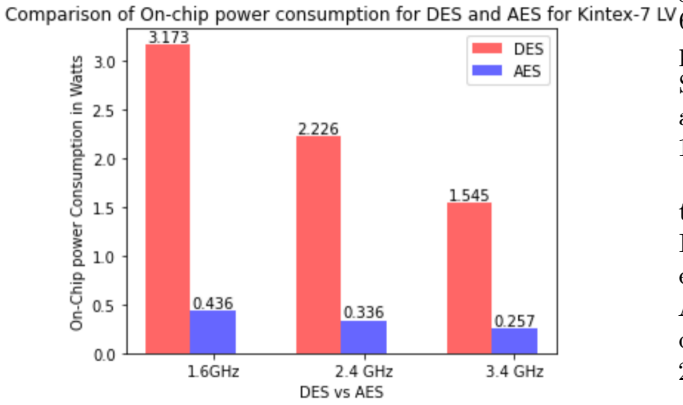

Figure 4: Comparison of on-chip power consumption for DES and AES for Kintex-7 Low Voltage.

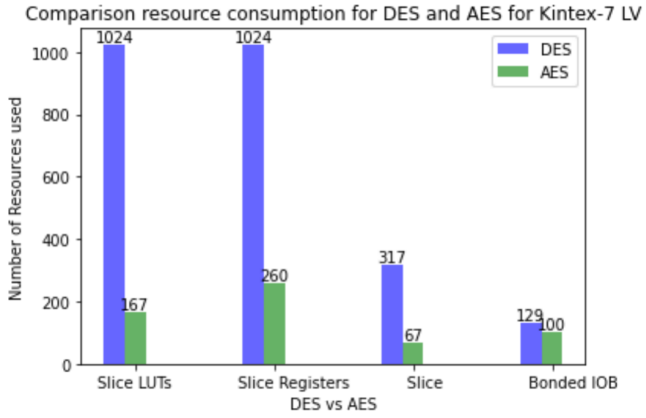

Figure 5: Comparison of resource consumption for DES and AES for Kintex-7 Low Voltage.

Additionally, we noticed that the Global Clock Buffer (BUFGCTRL) is the same for both algorithms. The Input/Output Buffer is 29% more for DES than for AES, which is a lower figure when compared to other resource utilization ratios.

These observations indicate that both AES and DES algorithms performed admirably well in power consumption on the Kintex-7 Low Voltage at 1.6 GHz. For all parameters examined in our research, we discovered that DES utilized an excessive amount of resources compared to AES and resulted in a higher junction temperature. At 1.6 GHz, AES performed admirably in terms of power usage.

Therefore, for Kintex-7 Low Voltage at 1.6 GHz, the AES implementation proves its superiority over the DES implementation for the same architecture.

6. Conclusion

This article compares two cryptographic algorithms, DES and AES, for the Kintex-7 Low Voltage. The comparison is based on experimental results. Performance analysis is conducted for various factors, including junction temperature, on-chip power consumption, and resource utilization, emphasizing the critical feature of green computing. In comparison to AES, DES required 627% more power, generated 20% more junction temperature, consumed 513% more Slice LUTs, 294% more Slice Registers, and 373% more Slices. AES performed admirably for Kintex-7 Low Voltage at a frequency of 1.6 GHz in terms of energy-efficient green computing.

In the future, it will be fascinating to investigate the performance of AES and DES on 20 nm UltraScale FPGAs and thus recommend more energy- and area-efficient cryptographic algorithm design architectures. Additionally, a performance study can be performed on additional Kintex-7 Low Voltage device features for 28 nm 7-series FPGAs.

References

Anderson, J. H. and Najm, F. N. (2004). Power estimation techniques for fpgas. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 12(10):1015–1027.

Bisht, N., Pandey, B., and Budhani, S. K. (2022). Comparative performance analysis of aes encryption algorithm for various lvcmos on different fpgas. *World J. Eng.*

Cuntan, C. D., Baciu, I., and Osaci, M. (2015). Studies on the necessity to integrate the fpga (field programmable gate array) circuits in the digital electronics lab didactic activity. *Int. J. Mod. Educ. Comput. Sci.*, 7(6):9–15.

Das, S. S. and Resmi, R. (2014). An efficient vlsi implementation of aes encryption using rom submodules and exclusion of shift rows. In *IEEE Int. Conf. Computational Systems and Communications (ICCSC)*, pages 248–251, Trivandrum, India.

Farooq, U. and Aslam, M. F. (2017). Comparative analysis of different aes implementation techniques for efficient resource usage and better performance of an fpga. *J. King Saud Univ. – Comput. Inf. Sci.*, 29(3):295–302.

Khalifa, O. O., Islam, M. R., Khan, S., and Shebani, M. S. (2004). Communications cryptography. In *IEEE 2004 RF and Microwave Conf.*, pages 220–223, Selangor, Malaysia.

Levin, I. I., Dordopulo, A. I., Fedorov, A. M., and Kalyaev, I. A. (2016). Reconfigurable computer systems: from the first fpgas towards liquid cooling systems. *Supercomput. Front. Innov.*, 3(1):22–40.

Muneshwar, A., Srinivasarao, B. K. N., and Chunduri, A. (2022). Fpga implementation and comparative analysis of des and aes encryption algorithms using verilog file i/o operations. In Ranganathan, G., Fernando, X., and Shi, F., editors, *Inventive Communication and Computational Technologies*, volume 311 of *Lect. Notes Netw. Syst.*, pages 835–848. Springer, Singapore.

Nabil, M., Khalaf, A. A., and Hassan, S. M. (2020). Design and implementation of pipelined aes encryption system using fpga. *Int. J. Recent Technol. Eng. (IJRTE)*, 8(5):2565–2571.

Pandey, B., Bisht, V., Ahmad, S., and Kotsyuba, I. (2021). Increasing cyber security by energy efficient implementation of des algorithms on fpga. *J. Green Eng.*, 11(1):72–87.

Renuka, G., Shree, V. U., and Reddy, P. C. S. (2018). Comparison of aes and des algorithms implemented on virtex-6 fpga and microblaze soft core processor. *Int. J. Electr. Comput. Eng.*, 8(5):3544.

Sakamoto, T., Miyamura, M., Bai, X., Sugibayashi, T., and Tada, M. (2018). Reducing the power consumption and increasing the performance of iot devices by using nano-bridge-fpga. *NEC Tech J.*, 13(1):93–98.

Srilaya, S. and Velampalli, S. (2018). Performance evaluation for des and aes algorithms—a comprehensive overview. In *3rd IEEE Int. Conf. Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pages 1264–1270, Bengaluru, India.

Tonde, A. R. and Dhande, A. P. (2014). Review paper on fpga based implementation of advanced encryption standard (aes) algorithm. *Int. J. Adv. Res. Comput. Sci. Eng. Inf. Technol.*, 3(1):4878–4880.

Yazdeen, A. A., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Ahmed, O. M., and Zebari, R. R. (2021). Fpga implementations for data encryption and decryption via concurrent and parallel computation: A review. *Qubahan Academic J.*, 1(2):8–16.