International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 09 | Sep 2024 www.irjet.net p-ISSN: 2395-0072

A Comprehensive Analogy of Latest FPGA Implementation of Data Encryption Techniques in Wireless Communication

Vijay Santosh Tawar[1], Dr. Nafees Ahmed M. Kazi[2]

[1] *Assistant Professor, Electronics & Telecommunication Engineering, SSVPS' B. S. Deore COE, Dhule, MS, India*
[2] *Associate Professor, Electronics & Telecommunication Engineering, SSBT' COET, Bambhori, Jalgaon, MS, India*

ABSTRACT

Given the fast pace of the development of wireless communication technologies and corresponding demands for secure data transmission due to the sensitivity of information being transmitted, FPGAs have garnered much interest as a gateway for implementing encryption techniques because of their flexibility and high-speed processing with energy efficiency compared to other conventional hardware technologies. In this regard, the paper would like to present a comprehensive review of the latest FPGA implementations of various data encryption techniques used in wireless communication systems [4, 5]. In this discussion, various traditional encryption algorithms, namely AES, RSA, and DES, along with their FPGA implementations will be explored. Later, recent trends of elliptic curve cryptography, quantum-resistant cryptosystem, and related performance metrics like throughput, latency, resource utilization, and power efficiency for these implementations will also be discussed, giving insights into their applicability in real-time wireless communication systems.

Keywords: FPGA, data encryption, wireless communication, AES, RSA, DES, elliptic curve cryptography, quantum cryptography

1. INTRODUCTION

The proliferation of wireless communication systems in various domains, such as cellular networks military applications and IoT, has only raised concerns over the security of the transmitted data [1].

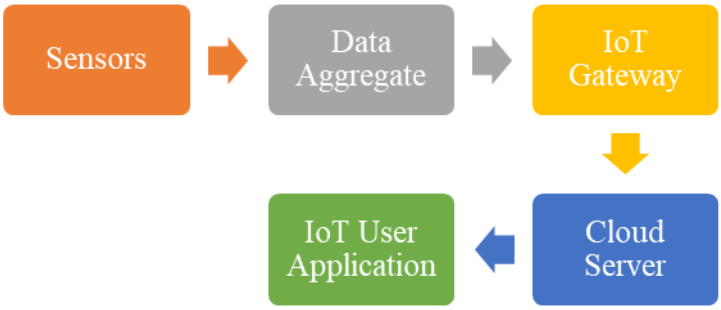

Fig. 1 Block Diagram IoT System

The need for secure and efficient encryption techniques has never been more critical, especially as the wireless communication system continues to expand into sensitive fields like finance and healthcare, defense, etc. [2] Figure 1 shows general purpose illustration of flow in normal IoT system.

FPGAs will provide a concrete platform in the design of cryptography techniques due to their intrinsic capability in parallel processing, re-configurability, and high performance. On the contrary, conventional microprocessors and the supported conventional software-based encryption schemes are flexible but not capable to present solutions to modern wireless communication systems with their high demanding real-time processing requirements [2]. FPGAs can be reprogrammed for intended applications, hence ensuring that they outperform in speed, power consumption, and better use of resources [1]. In figure 2 implementation of FPGA system with block level working is indicated.

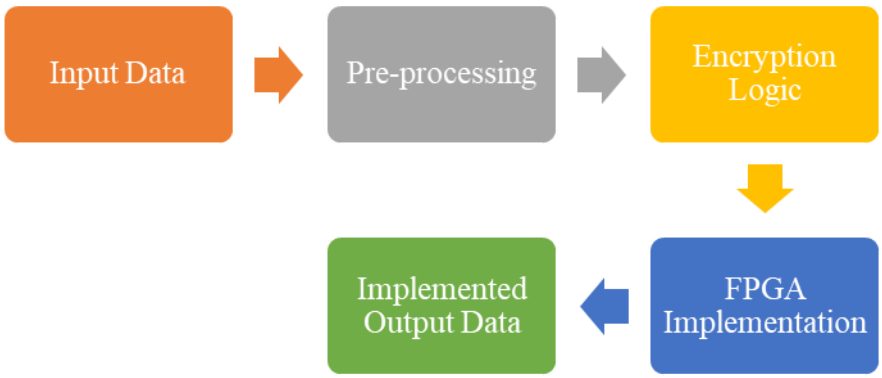

Fig. 2 FPGA Implementation System

The aim of this work is to review recent FPGA implementations of data encryption techniques in wireless communication. The paper will study traditional algorithms like AES, RSA, and DES, along with newer techniques of encryption like elliptic curve cryptography and quantum-resistant cryptography. The challenges and future trends in implementing encryption using FPGA in the field of wireless communication systems are also proposed in this work. In figure 3, the flow of encryption algorithm for general purpose system is shown.

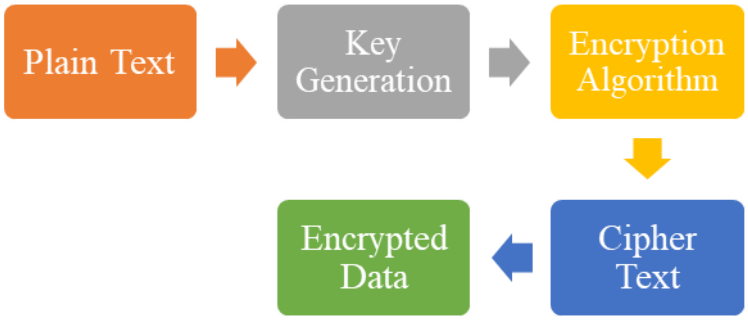

Fig. 3 Encryption Algorithm Generalized System

2. FPGA ARCHITECTURE FOR DATA ENCRYPTION

2.1 Overview of FPGA Technology

FPGAs are semiconductor devices whose configurations by the user can be done post-manufacturing for implementing a wide range of functions. An immediate and overwhelming advantage of this ability to program FPGAs for certain tasks is over the ASICs and any form of software processing.

Xilinx and Intel-seven, formerly Altera-dominant families of FPGAs are widely used for the realization of various encryption algorithms. Logic blocks, interconnections, and memory elements form programmable FPGA devices that are capable of carrying out most cryptographic functions in parallel with high throughput/low latency [10].

2.2 Why FPGA for Encryption?

Some of the advantages of implementing FPGAs for various encryption techniques include the following:

- **Parallel Processing:** FPGAs can process different cryptographic operations simultaneously, making them better suited for high-speed encryption.
- **Flexibility:** FPGAs can be reprogrammed in case of the introduction of new encryption algorithms or updates that might be carried out in a wireless communication system when the protocols change [15].
- **Energy Efficiency:** FPGAs feature low power use compared to general-purpose processors, hence they would be very suitable for mobile and IoT applications [1].

3. DATA ENCRYPTION TECHNIQUES ON FPGA

3.1 Traditional Encryption Algorithms

3.1.1 Advanced Encryption Standard (AES)

One of the most deployed encryption standards for secure communication is AES. The FPGA implementation has shown prominent improvement in speed and efficiency compared to a software-based solution. Inherent parallelism of AES rounds allows execution of rounds simultaneously on FPGAs, hence enhancing the throughput to a great extent. Generalized flow diagram for AES algorithm is as shown in figure 4. Several architectures concerning AES encryption on FPGA have been proposed by various researchers. Most of them work towards the reduction of the number of logic elements used and, at the same time, reduce power consumption [7]. For example, a fully pipelined AES implementation is capable of producing several Gbps throughput with very minimal latency [5].

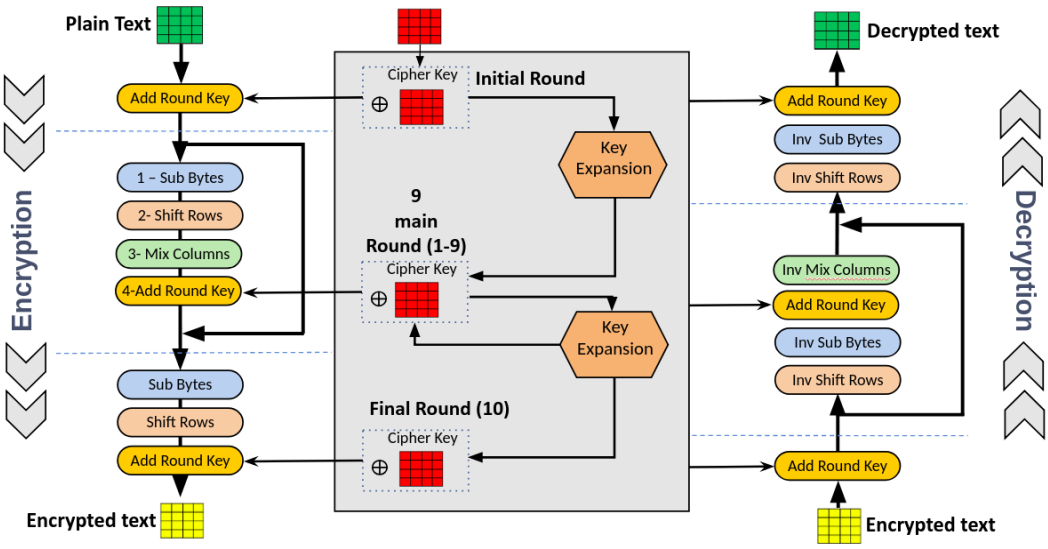

Fig. 4 AES Algorithm flow

3.1.2 Data Encryption Standard (DES) and Triple DES (3DES)

DES, though replaced by AES in most applications, still finds its usage in some legacy systems [1, 7]. The main concentration in the FPGA-based implementations of DES has been toward enhancing the performance of the encryption process. 3DES, which applies the DES encryption three times, is more resource-intensive and hence much benefits from the parallelism of FPGA. In figure 5 shown below using DES algorithm 64 bit plaintext can be converted in 64 bit cipher text using round key generation and encryption method whereas decryption process is exactly opposite to encryption i.e. it works in reverse order.

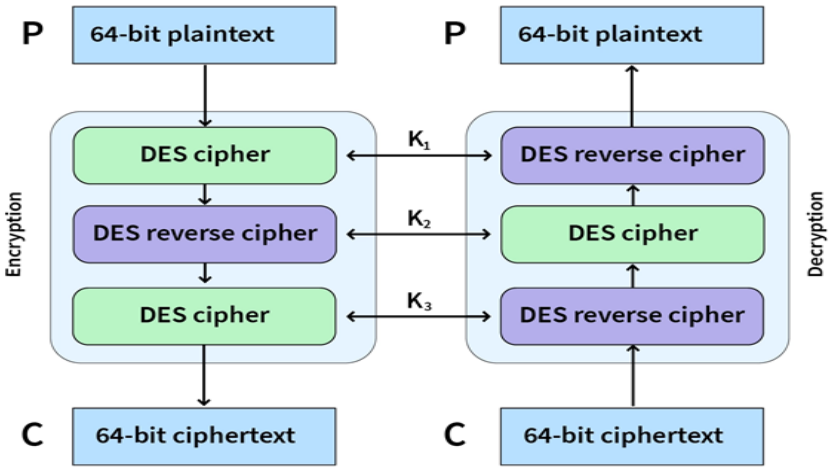

Fig. 5 DES Algorithm flow

3.1.3 RSA Encryption

RSA is a public-key encryption algorithm based on the computational intolerance of factorizing large prime numbers. Previous FPGA implementations of RSA are all based on efficient modulo exponentiation, as this phase is usually regarded as the most computation-intensive part of the whole RSA algorithm [12]. Using methods like Montgomery multiplication, an RSA implementation based on FPGA can be highly accelerated compared with a traditional microprocessor-based implementation.

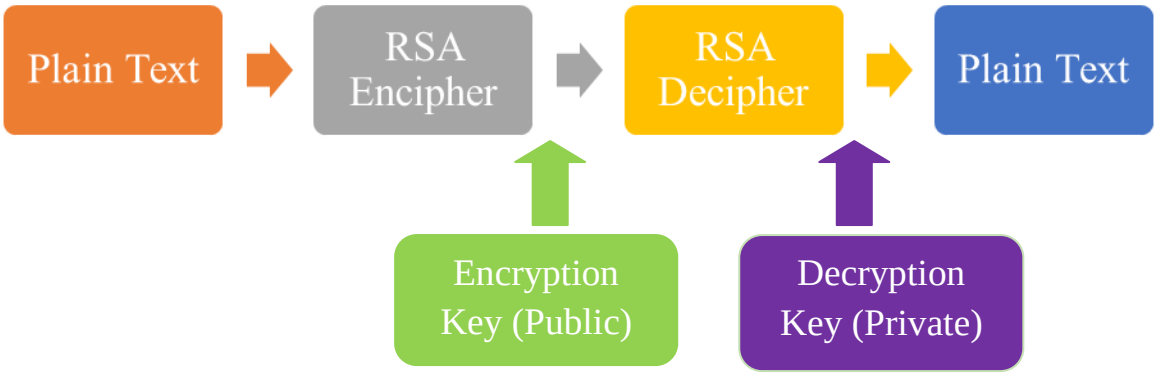

Fig. 6 RSA Algorithm flow

3.2 Recent Trends in Encryption

3.2.1 Elliptic Curve Cryptography (ECC)

Some would consider ECC more secure than RSA, since RSA bases its key strength on factoring large numbers, which is a problem computers have been able to solve. On the other hand, the problems that elliptic curve cryptography uses-namely the discrete logarithm problem-are much harder to solve [14]. ECC is an alternative public-key encryption technique that finds favor because key lengths are somewhat shorter compared to those of RSA for similar levels of security but far more moderate in their computational resource requirements. In fact, FPGA implementations of ECC also show pretty superior performance in constrained resource platforms such as mobiles and IoT devices. Most recently, several works have concentrated on improving the performance of the point multiplication operation lying at the heart of ECC on FPGA platforms.

3.2.2 Quantum-Resistant Cryptosystems

While quantum computing replaces traditional encryption methods, vulnerabilities in attacks are also growing. Lattice-based cryptography and hash-based cryptography have a big potential for developing novel methods of quantum resistance [13, 15].

FPGAs are a flexible platform for implementing such new cryptographic algorithms, which enables real-time testing and performance evaluation in a wireless communication environment [11].

3.2.3 Comparative observations of Encryption Methods on FPGA

Table-1 below summarizes a few points of difference between some commonly used encryption methods on FPGAs applied for different wireless communication systems. Each encryption technique is assessed based on performance, power efficiency on FPGA, and its typical applications [1, 7].

Table 1 Comparative highlights of Encryption Methods used for FPGA Implementation

Encryption Method	Key Features	FPGA Implementation	Performance (Throughput/Latency)	Power Efficiency	Applications
AES (Advanced Encryption Standard)	High security, 128/192/256-bit keys	Fully pipelined architectures	High throughput (several Gbps) with low latency	Moderate, depending on pipelining	Secure wireless communications, IoT, 5G
DES (Data Encryption Standard)	Outdated, 56-bit key, vulnerable	Requires additional layers (Triple DES)	Lower throughput compared to AES	Higher power consumption	Legacy systems, still in use for specific industries
RSA (Rivest-Shamir-Adleman)	Public-key, key lengths of 1024-4096 bits	Optimized through modular exponentiation on FPGA	High latency due to complex key processing	Moderate efficiency	Secure key exchange, VPNs, Digital Signatures
ECC (Elliptic Curve Cryptography)	Shorter keys, same security as RSA	Efficient implementation with reduced FPGA resource usage	Higher performance in constrained devices	High power efficiency due to short keys	Mobile devices, IoT, low-power applications
Quantum-Resistant Cryptography	Resistant to quantum computing attacks	FPGAs provide flexible testing for new algorithms	Varies by algorithm, ongoing research	Varies, still in development	Future wireless communication systems, post-quantum security

4. FPGA-BASED ENCRYPTION IN WIRELESS COMMUNICATION

4.1 Real-Time Encryption in 4G/5G Networks

These are also the encryption techniques carried out by FPGAs, widely adopted in modern 4G and 5G wireless communication networks [3]. All these wireless communication networks require secure data transmission among different nodes. In this regard, FPGA-based AES and ECC techniques showed paramount performances. These platforms can execute different encryption and decryption processes by exploiting parallelism and re-configurability with low latency for achieving secure and real-time communications [6].

4.2 IoT Security

New challenges for data security have been posed by the rapid emergence of IoT devices. In general, such devices possess very limited processing power and supplies of energy, so FPGA-based encryption seems to be the right answer [3]. Several IoT devices have introduced PRESENT and SPECK as FPGA implementations of light-weight cryptographic algorithms capable of offering a trade-off between security and energy efficiency [6, 9].

5. CHALLENGES AND FUTURE PERSPECTIVES

5.1 Challenges in FPGA-Based Encryption

While the advantages are not limited to the aforementioned, there are still several challenges in FPGA-based encryption. These include but are not limited to:

- **Power Consumption:** Although FPGAs are efficient and consume less power compared to general-purpose processors, the power consumption in battery-powered devices, such as mobile phones and IoT devices, is one of the top concerns.
- **Resource Utilization:** All heavy cryptographic algorithms, for instance, RSA and ECC, require heavy resources on an FPGA, which may be prohibited in resource-constrained environments [3, 9].

5.2 Future Perspectives

Future research is likely to concentrate on:

- **Integration with AI and Machine Learning:** FPGA-based encryption could also be combined with AI algorithms in developing adaptive security systems that can respond dynamically to new emerging threats [2, 3, 4, 6, 8].
- **Post-Quantum Cryptography:** Once quantum computers become reality, attention will be turned to implementing quantum-resistant cryptographic algorithms on FPGAs.

6. CONCLUSION

This work has identified the key role of FPGAs in implementing wireless communication data encryption techniques. Its flexibility, speed, and energy efficiency currently make FPGA a hot choice for various real-world applications in the fields of 5G, IoT, and secure military communication. To this end, even as new methods of encryption are beginning to be developed, including the development of quantum-resistant algorithms, FPGAs will still be considered a central player in ensuring secure communication in an increasingly connected world.

REFERENCES:

[1] NR Shetty, NH Prasad, HC Nagaraj, “Advances in Communication and Applications,” *Proceedings of ERCICA*, 2023.

[2] S Moradian, S Gharbia, AI Olbert, “Enhancing the accuracy of wind power projections under climate change using geospatial machine learning models,” *Energy Reports*, 2024 - Elsevier.

[3] SB Akinpelu, SA Abolade, E Okafor, “Interpretable machine learning methods to predict the mechanical properties of ABX3 perovskites,” *Results in Physics*, 2024 - Elsevier.

[4] J Finkelstein, A Gabriel, S Schmer, “Identifying Facilitators and Barriers to Implementation of AI-Assisted Clinical Decision Support in an Electronic Health Record System,” *Journal of Medical Systems*, 2024 - Springer.

[5] A Chierici, F Lareyre, “Vascular liver segmentation: a narrative review on methods and new insights brought by artificial intelligence,” *Journal of Medical Case Reports*, 2024.

[6] S Shahpouri, D Gordon, “Transient NOx emission modeling of a hydrogen-diesel engine using hybrid machine learning methods,” *International Journal of Engine Research*, 2024.

[7] J Yang, J Yu, D Tang, “An interpretable precursor-driven hierarchical model for predictive aircraft safety,” *Expert Systems with Applications*, 2024 - Elsevier.

[8] D Freedman, B Bagga, “Quality assessment of expedited AI generated reformatted images for ED acquired CT abdomen and pelvis imaging,” *Abdominal Radiology*, 2024.

[9] M Kattih, M Bressler, “Artificial Intelligence-Prompted Explanations of Common Primary Care Diagnoses,” *PRiMER*, 2024.

[10] A Sarajlić, I Plaščak, "The use of acoustic technology for monitoring biodiversity in the Kopački Rit Nature park (project WatchOut)," *Proceedings of Croatian Conference on Plant Protection*, 2024 - Croris.

[11] R Saed, "The impact of artificial intelligence on the jurisprudential research industry between prohibition and permissibility," *Annals of the Faculty of Arts, Ain Shams University*, 2024.

[12] JF Ramírez-Vasquez, EJ Carlock-Acevedo, "Inverse kinematics using neural networks and random forests for trajectory tracking of a three-degree-of-freedom robotic arm," *BUAP Institutional Repository*, 2024.

[13] KA Einarson, "Molecular representations in computational drug design-from early stage protein functions to machine learning based prediction of pharmacokinetic parameters," *Technical University of Denmark*, 2024.

[14] J Mirabet Herranz, "Application of machine learning techniques to detect malware on Android devices," *Universitat Politècnica de València*, 2024.

[15] S Minoo, F Ghasemi, "Automated Teeth Disease Classification using Deep Learning Models," *International Journal of Applied Data Science*, 2024.

BIOGRAPHIES

	Mr. Vijay Santosh Tawar has experience of 13 Years in Teaching, currently working as Assistant Professor Approved by KBCNMU, Jalgaon and DBATU, Lonere, in Department of Electronics & Telecommunication Engineering in SSVPS' Bapusaheb Shivajirao Deore College of Engineering, Dhule (MS). He perceived M.Tech. in Digital Communication in 2015. His domain of research is VLSI Design, Date Encryption & Decryption and Communication.
	Dr. Nafees Ahmed M. Kazi has vast experience of 25 Years in Teaching, currently working as Associate Professor, in Department of Electronics & Telecommunication Engineering in SSBT' SSBTs College of Engineering and Technology Bambhori Jalgaon (MS). He perceived PhD in Electronics Engineering from KBCNMU, Jalgaon in 2022. His domain of research is Software Defined Network, Computer Networking, Satellite Communication, CMOS Design, Automotive Electronics and Electric Vehicle