ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14910222

Cryptography with Field Programmable Gate Arrays

Reena Kulkarni[1]; Dr. Keerti Kulkarni[2]

[1]Assistant Professor, Department of Electronics and Communication Engineering K.S. School of Engineering and Management Bengaluru, India
[2]Associate Professor, Department of Electronics and Communication Engineering B.N.M. Institute of Technology Bengaluru, India

Publication Date: 2025/02/22

Abstract: Cryptography is an important process of modern secure communication, and as the need for faster and more efficient encryption methods grows, hardware-based solutions have become significant. Field-Programmable Gate Arrays (FPGAs) offer flexible and efficient platform for implementing cryptographic systems and hence a promising solution for securing modern digital communications like, in Internet of Things and embedded system applications. This paper discusses the different cryptographic algorithms and how FPGAs are advantageous over other hardware-based security implementations.

Keywords: *Symmetric Key, Asymmetric Key, FPGAs, ASIC, Hardware Based Security.*

How to Cite: Reena Kulkarni; Dr. Keerti Kulkarni (2025). Cryptography with Field Programmable Gate Arrays. *International Journal of Innovative Science and Research Technology*, 10(2), 356-359. https://doi.org/10.5281/zenodo.14910222

I. INTRODUCTION

In most of the electrical and electronic applications, low power and security of data and network have become a significant consideration similar to the performance of the system. Cryptography, which is the art of securing data has led to evolution of modern techniques to ensure integrity, confidentiality and authentication of the data being transmitted [1],[2]. Field-Programmable Gate Arrays (FPGAs) offer a customizable environment as they are reconfigurable and the allow for rapid modifications without needing to produce new hardware.

This paper focuses on the various algorithms in cryptography and advantages of using FPGAs over other hardware-based implementations for cryptographic algorithm.

II. ALGORITHMS OF CRYPTOGRAPHY

Cryptographic algorithms provide the foundation for securing data in terms of Confidentiality, Integrity and Authentication of data being transmitted [1]. The algorithms can be broadly classified into two categories: symmetric-key and asymmetric-key algorithms.

The Symmetric–key algorithm [3],[4] rely on use of a single key for encryption and decryption. The most common algorithms include:

➢ *AES (Advanced Encryption Standard):*

- It has support for three-length keys: 128 bits, 192 bits, or 256 bits, with the most commonly used one being 128-bit key.
- It is used for data encryption in storage devices, internet browsers, file and disk compression. wireless networks, databases, etc.

➢ *DES (Data Encryption Standard) and Triple DES:*

- In DES, the 64-bit blocks of plaintext are encrypted using a 56-bit key.
- Triple DES applies DES thrice in a sequential manner on every plaintext block.
- Due to small key size DES algorithm is vulnerable to brute-force attacks.
- DES algorithms are used in random number generation and deployed in applications where not-so-strong encryption is needed.

➢ *RC4 (Rivest Cipher 4):*

- RC4 is a stream cipher, which uses a variable-length key, typically between 40 and 2048 bits.
- It was widely used in protocols like SSL/TLS (Secure Socket Layer/ Transport Layer Security) and WEP (Wired Equivalent Privacy), but is no longer considered secure due to security vulnerabilities.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14910222

In Asymmetric encryption [3],[4] (or public-key cryptography), two different keys are used: a public key for encryption and a private key for decryption. Some of asymmetric algorithms include:

➢ *RSA (Rivest-Shamir-Adleman):*

- RSA is based on the mathematical problem of factoring large prime numbers.
- RSA is commonly used for secure data transmission, digital signatures, and key exchange.

➢ *ECC (Elliptic Curve Cryptography):*

- ECC uses the mathematics of elliptic curves over finite fields for encryption.
- ECC is commonly used in modern cryptographic systems, especially in mobile devices and low-power systems.

➢ *DSA (Digital Signature Algorithm):*

- DSA is a standard for digital signatures based on the discrete logarithm problem and is used for verifying the authenticity and integrity of data.
- It's widely used in digital certificates, especially in conjunction with the SHA (Secure Hash Algorithm) family of hash functions (e.g., SHA-1, SHA-2).

➢ *ElGamal:*

- ElGamal encryption is based on the Diffie-Hellman key exchange protocol. It provides both encryption and digital signatures.
- It is used in is used as a part of the free GNU Privacy Guard Software, late forms of PGP, and different cryptosystems.

The other classification of cryptographic algorithms includes Key exchange, Hashing and Digital Signatures.The choice of algorithm depends on the specific security requirements, such as speed, resource availability, and the type of attack resistance needed.

III. IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS

The cryptographic algorithms can be implemented in software on a general-purpose hardware or dedicated hardware. The criterion to implement cryptographic algorithms in software versus hardware depends on several parameters like, performance, security, flexibility, cost, and power consumption.

➢ *Software Implementation of Cryptographic Algorithm:*

Software implementation of cryptographic algorithms includes writing code to perform the mathematical processes of cryptographic algorithm, ensuring data confidentiality, integrity, and authentication [5].

The various considerations in software implementations are efficiency, compliance to standards, security, key management and use of libraries and frameworks, like, PyCryptodome (Python library), OpenSSL (widely used C library), Bouncy Castle (Java library), libsodium (for modern cryptography).

➢ *Hardware Implementation of Cryptographic Algorithm:*

The most commonly used algorithms for securing data include Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA algorithm, Message Digest 5 (MD5), Secure Hash Algorithm (SHA) [6],[7]. All these algorithms are highly secured because of complex mathematical computations they possess, securing the data and hence making hacking a tedious job. The hardware implementation of algorithms presents enhancement in the speed of execution, efficiency and reliability of security standards.

The cryptographic algorithms can be implemented on ASICs (Application-Specific Integrated Circuits) and/or FPGAs; both of these are discussed in the following sections.

- *Application-Specific Integrated Circuits (ASICs):*

ASIC is a specialized integrated circuit (IC) designed for specific applications instead of general-purpose use. ASICs differ fundamentally from general integrated circuits like microprocessors and memory chips, designed for diverse applications and mass production. The primary objective of ASICs is to achieve a specific functionality with the highest possible efficiency, which can be in terms of power consumption, performance, and cost.

ASIC is optimized for speed, power, and size, and can offer the best performance and efficiency for a given task. However, an ASIC is expensive and time-consuming to design and manufacture, and it cannot be reprogrammed or modified once it is fabricated. ASICs can be broadly classified into two types: full custom ASICs and semi-custom ASICs.

ASICs find applications in diverse fields, including cryptocurrency mining, telecommunications, consumer electronics, automotive systems, AI/ML (Artificial Intelligence and Machine Learning), medical devices, and financial applications.

- *Disadvantages of ASICs:*

While ASICs offer exceptional performance, power efficiency, and tailored functionality, they come with several disadvantages that make them less suitable for certain applications. These include:

- High upfront costs for design and fabrication
- Lack of flexibility and limited reusability
- Long development time
- Risk of obsolescence as technologies evolve
- Volume dependence for cost-effectiveness
- Complexity in design and manufacturing

Hence, for applications where flexibility, low-volume production, or rapid prototyping is necessary, FPGAs can be more appropriate.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14910222

➢ *Field-Programmable Gate Arrays (FPGA)*

FPGA is a chip that is reprogrammable with a collection of hundreds of thousands of logic gates that are connected internally together to build a complex digital circuit. FPGAs can be broadly classified into two types: SRAM (static random-access memory)-based and flash-based.

FPGAs provide high performance, customization, and parallel processing capabilities [8], [9]. They offer a flexible and efficient solution for accelerating cryptographic operations, especially in cases where high throughput and low latency are critical, such as in security protocols, blockchain, network encryption, and secure communications.

Some of the commonly implemented cryptographic algorithms on FPGAs include AES, RSA, ECC, Hash functions, Public key cryptography (for key exchanges), Digital Signatures and Random Number Generation (RNG).

IV. IMPLEMENTATION FLOW FOR CRYPTOGRAPHIC ALGORITHMS

➢ *A Typical Flow for Implementing Cryptographic Algorithms on an ASIC Include the Following:*

- Requirement Analysis & Algorithm Selection
- Algorithm Design & Analysis
- High-Level Design & Architecture
- RTL Design (Register Transfer Level)
- Synthesis & Optimization
- Physical Design & Layout
- Verification & Validation
- Manufacturing & Packaging
- Deployment & Testing in Real-World Application

➢ *And a Typical flow for Implementing Cryptographic Algorithms on an FPGA Include the Following:*

- Requirement Analysis & Algorithm Selection
- Algorithm Design & Analysis
- High-Level Design & Architecture
- HDL Design (Register Transfer Level)
- Simulation & Functional Verification
- Synthesis & Design Optimization
- Implementation & Placement/Routing
- Post-Synthesis Simulation & Timing Verification
- Programming the FPGA & Real-World Testing
- Deployment & Integration

➢ *FPGA versus ASIC comparison summary*

Table 1 highlights the major differences between ASICs and FPGAs, focusing on their suitability for various applications and the trade-offs between performance, flexibility, cost, and development time.

Table 1 Summary comparing ASICs and FPGAs

Feature	ASIC	FPGA
Customization	Highly specialized, fixed design	Reconfigurable, flexible
Performance	High performance, power-efficient	Lower performance, higher power consumption
Cost	High initial cost, lower per-unit cost at scale	Lower initial cost, higher cost at large volumes
Development time	Long (months)	Short(weeks)
Power Efficiency	Very power-efficient	Higher power consumption
Application areas	Telecommunications, cryptocurrency mining, consumer electronics, automotive systems,	Smartphones, autonomous vehicles, cameras, displays, video and image processing, and security systems

V. CONCLUSION

The ASIC implementation flow for cryptographic algorithms is a rigorous process involving several detailed steps, from requirement analysis to final deployment. The upfront costs, long development time, and lack of flexibility make ASICs most suitable for high-volume, mission-critical applications. However, the FPGA implementation flow for cryptographic algorithms is a highly structured and multi-step process. With their high parallelism, low latency, and reconfigurability, FPGAs offer a flexible and powerful solution for implementing cryptographic functions that require high performance, security, and efficiency.

REFERENCES

[1]. Tushar, Aniket Sharma, Ankit Mishra, "Cryptographic Algorithm For Enhancing Data Security: A Theoretical Approach", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181 IJERTV10IS030158, Vol. 10 Issue 03, March-2021

[2]. Abdalbasit Mohammed, Nurhayat Varol, "A Review Paper on Cryptography", 7th International Symposium on Digital Forensics and Security (ISDFS), DOI:10.1109/ISDFS.2019.8757514, IEEE, 2019

[3]. Ridwan B. Marqas, Saman M. Almufti, Rasheed Rebar Ihsan, "Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms", Journal of Xi'an University of Architecture & Technology, Issn No: 1006-7930 Page No: 3110, Volume XII, Issue III, 2020

[4]. Priasnyomo Prima Santoso, Elkin Rilvani, Ahmad Budi Trisnawan, Krisna Adiyarta, Darmawan Napitupulu, Tata Sutabri, Robbi Rahim, "Systematic literature review: comparison study of symmetric key and asymmetric key algorithm", 2nd Nommensen International Conference on Technology and Engineering, IOP Conf. Series: Materials Science and Engineering 420 (2018) 012111 doi:10.1088/1757-899X/420/1/012111

[5]. Gerard Murphy, Aidan Keeshan, Rachit Agarwal, Emanuel Popovici, "Hardware – Software

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14910222

Implementation of Public-Key Cryptography for Wireless Sensor Networks", IEE Irish Signals and Systems Conference, Dublin, June 28-30, 2006

[6]. Hong-Jin Ryu, Samuel Sangkon Lee, "Design and Implementation of a Document Encryption Convergence Program Selecting Encryption Methods, and Integrating the Program into the Existing Office System", DOI: 10.5220/0012124000003541, Proceedings of the 12th International Conference on Data Science, Technology and Applications (DATA 2023), pages 452-459, ISBN: 978-989-758-664-4; ISSN: 2184-285X

[7]. Karim Shahbazi, Mohammad Eshghi, Reza Faghih Mirzaee, "Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5, Engineering Science and Technology, an International Journal 20 (2017) 1308–1317, https://doi.org/10.1016/j.jestch.2017.07.002

[8]. Prof. S. Venkateswarlu, Deepa G.M, G. Sriteja, "Implementation of Cryptographic Algorithm on FPGA", ISSN 2320–088X, IJCSMC, Vol. 2, Issue. 4, April 2013, pg.604 – 609