Qubahan Academic Journal
گوڤارا قبهان یا ئەکادیمی
مجلة قبهان الأكادمية
Doi: 10.48161/issn.2709-8206

FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review

https://doi.org/10.48161/qaj.v1n2a38

1st Abdulmajeed Adil Yazdeen
Dept. Information Technology Management
Duhok Polytechnic University
Duhok, Iraq
Abdulmajeed.adil@dpu.edu.krd

2nd Subhi R. M. Zeebaree
IT Dept.
Duhok Polytechnic University
Duhok, Iraq
Subhi.rafeeq@dpu.edu.krd

3rd Mohammed A. M.Sadeeq
Quality Assurance
Duhok Polytechnic University
Duhok, Iraq
mohammed.abdulrazaq@dpu.edu.krd

4th Shakir Fattah Kak
Dept. Information Technology
Duhok Polytechnic University
Akre-Duhok -Iraq
shakir.fattah@dpu.edu.krd

5th Omar M. Ahmed
Dept. *Information Technology*
Duhok Polytechnic University
Duhok, Iraq
omar.alzakholi@dpu.edu.krd

6th Rizgar R Zebari
Research and Development Center
Nawroz University
Duhok, Iraq
rzgarz11@gmail.com

***Abstract*— In recent days, increasing numbers of Internet and wireless network users have helped accelerate the need for encryption mechanisms and devices to protect user data sharing across an unsecured network. Data security, integrity, and verification may be used due to these features. In internet traffic encryption, symmetrical block chips play an essential role. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) ensure privacy encryption underlying data protection standards. The DES and the AES provide information security. DES and AES have the distinction of being introduced in both hardware and applications. DES and AES hardware implementation has many advantages, such as increased performance and improved safety. This paper provides an exhaustive study of the implementation by DES and AES of field programming gate arrays (FPGAs) using both DES and AES. Since FPGAs can be defined as just one mission, computers are superior to them.**

Keywords*— *Cryptography, DES algorithm, AES algorithm FPGAs Implementations, VHDL.

I. INTRODUCTION

The encryption algorithm is a method or a formula that secures the network or renders data protected with security. Cryptography is the science of developing methods that enable information to be transferred in a protected environment in such a way as to decipher the intended recipient [1]. Good networking helps to share network-wide data when connected to one computer and another [2]. messages really must be encrypted so that an assailant does not interpret the message [3]. Security of data is the mechanism of data protection for the whole of your life from all kinds of unapproved access and data corruption [4].

The consumer industry commonly uses communication technology to link devices without cables, namely, wireless communication. Wireless networking relies on cell technology. As the number of smartphone users has grown dramatically globally, other mobile commerce and wireless information services are required [5]. In the last two decades, cellular networks' transition from 2G, 3G, and 4G to 5G has been important [6].

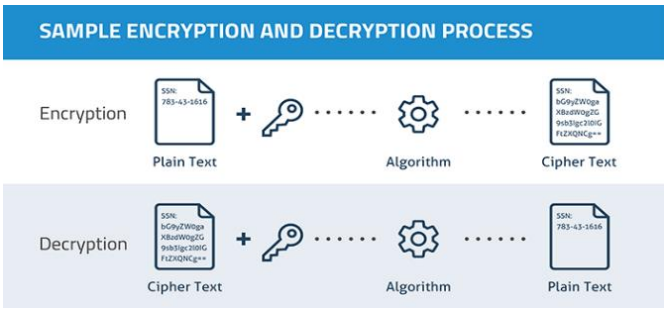

Fig. 1. Encryption and Decryption in Cryptography

Cryptography is the art of shielding information by encrypting the letter. The art of securing (encrypting) information, called ciphertext, in an unreadable format (encrypted text), only those that have a hidden key will decipher the message into plain text (decrypt) [5].

A cryptographic scheme is encrypted by the sender but decrypted in plain text by the recipient under this first details. Encrypted messages, often called code-breaking,

may also be opened by cryptanalysis[7]. Furthermore, if current methods of cryptography are practically unbreakable. With the Internet and other modes of electronic communication becoming more common, electronic security is becoming increasingly relevant [8, 9].

Data is a necessary commodity that must be prevented from unauthorized entry since cryptographic algorithms play an essential role in the secure transfer of information as a result [3]. Centered on remote vital systems and public critical systems, the encryption algorithms are confidential. Encryption algorithms Such as AES and camellia are used as cryptographic algorithms to preserve the data. As a basic algorithm to encrypt and decrypt secured data transmission to the standard of the new Data Encryption Standard (DES), the sophisticated encryption protocol was adopted by the National Institute of Standards and Technology (NIST) (AES) [10]. Data security has been a problematic area and is commonly used online to encrypt privacy for users. [11].

The rest of this work is organized as the following Concurrent and Parallel Computation in section two. In section three, Data Encryption and Decryption. In section four, DES Algorithm is illustrated. In section five, AES Algorithm is discussed. In section six, FPGA Implementations are illustrated. Literature Review in section seven. All mentioned and reviewed researches are compared and discussed in section eight. Finally, in section nine, the conclusion of this work is presented.

II. Concurrent and Parallel Computation

In the last decade, computation, networking, and storage systems have increased dramatically. The inherent variability and high dynamics of the phenomenon modeled on these applications are commonly used for dynamically adaptive technologies [12]. The increasingly complex, dynamic, and heterogeneous computer systems and the varied and heterogeneous [13]. Distributed computing systems have contributed to creating and introducing sophisticated computational architectures that enable such large-scale adaptive applications through scripting, execution, and runtime management [14, 15].

Scientists who want to write high-performance parallel applications now face the hierarchical architecture of systems also (or especially) in the "commodity" classes[16, 17]. Parallel hybrid platform programming styles are pure MPI, hybrid master only, overlap-hybrid hybrid, pure OpenMP cluster, and hybrid mapping. [18].

Several independent methods for the completion of the final calculation are used to transfer messages [19]. In calculating the patient's odds, many parallel procedures are generated, and the data involved is spread out over all of them using many different methods [20]. There are no standard data, and the second process must give it to the first process if a process wants data retained by another one [21]. A protocol to transmit an MPI message defines the internal methods and policies of an MPI to send messages [22]. Two traditional protocols, eager and appointing, are going through the message. Eager is an asynchronous protocol that requires a sending process to be completed without a corresponding acknowledgment [23]. Rendezvous is a synchronous protocol requiring corresponding receipt recognition to complete the transmission process [24]. As MPI allows the programmer in concurrent MPI systems to monitor the flow of data and the synchronization of the operation, problem decomposition and the coordination between processes pose two problems in writing. Without proper coding, the output of the software is influenced adversely [25].

III. Data Encryption and Decryption

For a deeper understanding of encryption algorithms, there are certain words that we can consider. It is imperative to understand this language since we will cover these familiar words in any algorithm overview [26].

- Plain text or Normal Text: The initial words or sentences used for correspondence are called "plain text." Example: Ahmad sends "Hello" to Jordi. Here "Hello" is Plain text or Original Message [27].
- Cipher Text: The plaintext is encrypted in incomprehensible characters. This cipher is considered 'meaningless.' For Example: "Hello" the message is translated. "+&tit%". This message is insignificant.
- Encryption: Encryption is the translation method of plain text to ciphertext. This un-readable message can be easily transmitted over an unreliable network. The encryption process requires encryption algorithms.
- Decryption: Decryption is the opposite of encryption. To transform plain text into ciphertext, use the algorithm.
- A Key: A key is a binary text (mathematical formula). In data encryption, it operates on plain text, and in decryption, it takes place on the ciphertext.
- Key Size: Key size, used in any algorithm, calculates required length in bits.
- Block Size: Key cipher is based on a fixed length of bits. It is a set length of bit "Block" in the machine. The block size depends on the algorithm selected.
- Round: Encryption round means that before it gives ciphertext as output, the encryption feature is performed in the complete encryption process.

With the exponential growth of technology, the primary need for data transmission through multimedia is stability. To be safe against unauthorized usage, multimedia data is required. Data security strategies are necessary to protect data from unauthorized users. One of the essential methods used for data security is the encryption of data [28]. Two fundamental forms of cryptography are available:

- Cryptography with Symmetric Key (Secret Key).
- Cryptography with Asymmetric Key (Public Key).

The sender and receiver use different keys to encrypt and decrypt the text in private key and encrypted in asymmetric cryptography. When hidden messages are exchanged from one end to another, this encryption and decryption process is used. In general, very confidential material is processed on the computer and distributed over

the Internet. Therefore, maintaining the integrity of data has become a crucial concern. There is a variety of image encryption and decryption algorithms listed in the next section [29].

IV. DES Algorithm

In cryptographic technology, the critical feature is description and encryption. Encryption is the translation of data into unknown types without a hidden key to guarantee protection. Meanwhile, a hidden key is called description to bring back data into the original form [30].

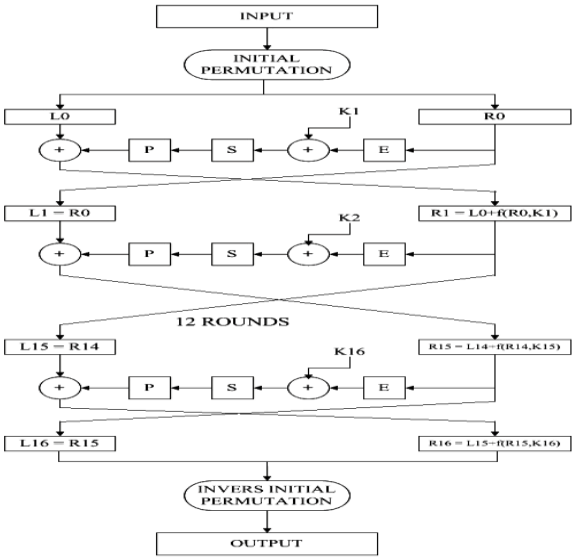

Fig. 2. DES Algorithm Scheme

Computer and Information Technology (EIConCIT) 2nd Eastern Indonesia Conference 2018; The objective of the encryption algorithm is to reach four main points: security of high-quality data leakage since cracking can be achieved with great complexity and costs, the defense of the DES algorithm is centered on the encryption key and the economic importance of the DES algorithm. The DES algorithm is acceptable for deployment in many various applications because the cost-effective and operational level is efficient [31].

In the Algorithm for DES, the main parameters are data, mode, and key. The DES algorithm works for bits or bytes of data units. The 64-bit key is the DES algorithm working key, 64-bit data is encrypted and decrypted, and DES algorithm processing mode, description, and encryption. The DES algorithm, working with permutation substitutions and XOR, is a repeating symmetric cipher block. In any operation and iteration in 16 rounds, the algorithm is sequential [32]. The Algorithm for DES structure on the is formed basis of Feistel chip structure principles [33]. In the DES algorithm, the model includes all operations which iterate in 16 rounds. The scheme for the DES algorithm is shown in Fig. 2.

V. AES Algorithm

It is an iterative cipher rather than Feistel. It is based on two standard methods known as the substitution and permutation network for encryption and decryption (SPN). SPN is a series of mathematical transactions in block cipher algorithms [34]. The AES will operate with the size of a 128-bit plaintext block (16 bytes). These 16 bytes are expressed in the 4x4 matrix, and AES operates on a byte matrix. Besides, the number of rounds is another prominent feature of AES. The round number depends on the size of the key. For Example, three different key sizes are used for encrypting or decrypting information (128, 192, or 256 bits). The critical dimensions are specified for rounds, including ten rounds for 128-bit, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys for the AES operation [35].

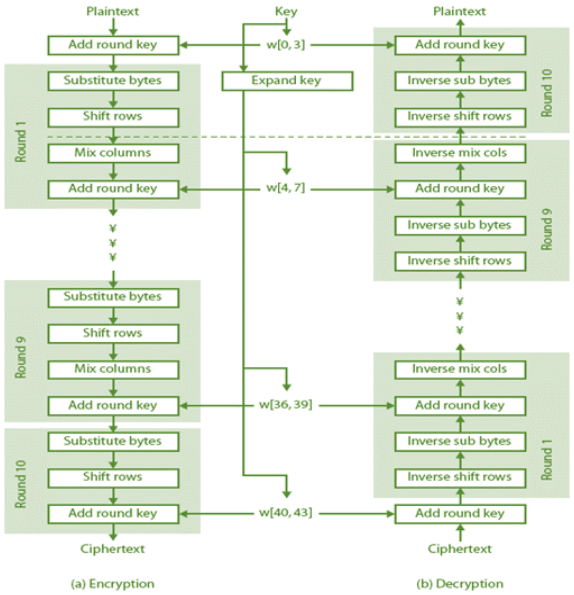

Fig. 3. Basic Structure of AES

VI. FPGA Implementations

Integrated digital circuits are Field Programmable Gate Arrays (FPGAs) (IC) manufactured from silicone modules containing configurable (programmable) logic blocks and configurable interconnections between these blocks. To perform large sets of tasks, these machines can be designed (programmed) by engineers. In order to execute the FPGAs, engineers can use different ways of programming. Some FPGAs can only be programmed once, and One-time programmable (OTP) is the term used, while some may be constantly reprogrammed. The "field-programmable" function for the FPGA name refers to the notion that its programming takes place "inside the disk" rather than the programs hardwired by the supplier's internal software. If a computer may be configured while it is in a higher-level structure, it is referred to in the system as programmable (ISP) [36].

The FPGA is a semiconductor device used for programmable lookup tables with a limited number of inputs to implement truth tables for logic circuits. In the form of block RAMs (BRAMs) and flip-flops, FPGAs can often provide memory, high-bandwidth on-chip memory [37].

The general structure architecture of FPGAs consisting of logic gates, embedded RAMs, multipliers, and blocks of I/O is seen in Figure (4).

A. *Programming Technologies*

For reconfigurable architectures, there is a range of programming technologies that have been used. Both of these architectures have distinct features that have a profound impact on the programmable architecture in turn. Any of the well-known methods include static, flash, and anti-fuse memory [38]. The Features of each technology can be summarized as follow:

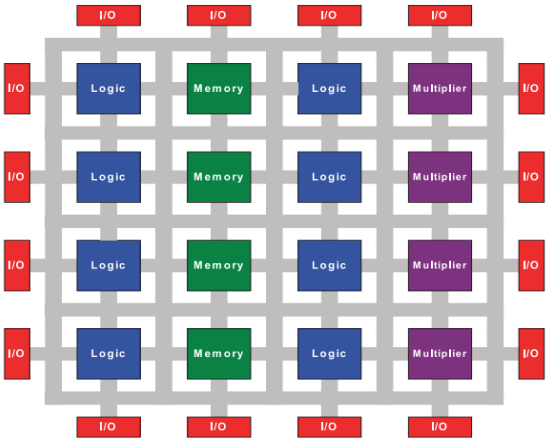

Fig. 4. Generic FPGA architecture

1) Antifuse FPGAs: For the device, fuse sets are used for initialization. If it has been programmed, the chip cannot be modified. Fortunately, recently printed circuit board (PCB) bugs can be modified and corrected. There is an overview of three widely used computing technologies where they have their advantages and disadvantages. Ideally, one would like to see a reprogrammable, non-volatile programming technology that uses a standard CMOS procedure. None of the innovations presented above meets these requirements. SRAM-based programming technology, however, is the programming technique that is most commonly used. The fundamental explanation is the use of the traditional CMOS process and, for this exact reason, the other two programming technologies are likely to continue to dominate this technology [39].

2) FPGAs Types: Some companies generate different FPGA families but typically follow the standard, scalable, regular, and programmable logic block (CLB) architecture covered by a programmable input/output block perimeter (IOBs). However, in future configuration and architecture, different FPGAs could have a slight variation [40]. Virtex Xilinx is one of the most renowned companies that primarily produces two FPGA family groups: Virtex and Spartan. The collection Virtex consists of (Virtex, Virtex-E, Virtex-Epro, Virtex-2, Virtex-4, Virtex-5, Virtex-6 and Virtex-7). Spartan's series consists of (Spartan-2, Spartan-3, Spartan-3L, Spartan-3E, Spartan-3A, Spartan -3A DSP, Spartan -3AN, and the extended Spartan -3A). Besides, Virtex and Spartan family systems can be reprogrammed to store the logic setup by SRAM. The Virtex series has high-performance FPGAs with the lowest strength. For, e.g., with over two million logic cells, Virtex-7 is built on a 28 nanometer (nm), Although the Spartan family is ideal for low-cost, high-volume applications. Spartan-3, for instance, is based on 90 nm [41]. The Configurable Logic Block (CLB), which includes practical elements for building logic, is based on Virtex and Spartan computers. Other essential functional elements that are programmable, such as Block RAMs, integrated multipliers, IBOs, and digital clock managers (DCMs), include CLBs, Virtex, and Spartan units [42].

B. *VHDL*

VHDL is a term for representing hardware. It defines how an electronic circuit or system can operate the physical circuit or system (implemented). VHDL stands for VHSIC hardware definition. VHSIC itself is the abbreviation for Very High Speed Integrated Circuits, a project launched in 1980 to promote the United States government's VLSI silicone chip design techniques. The initial version of VHDL 87 was finished up to the VHDL 93. Following the IEEE 1076 standard of the Institute of Electrical and Electronical Engineers (IEEE), the original and first Hardware classification language was VHDL. An additional standard, IEEE 1164, was later adopted for implementing a multi-value logic scheme [42]. In general, VHDL is partly known as a program as a language. In VHDL, only a declaration is made within a process, function, or protocol and is executed sequentially [43].

C. *Design Flow of VHDL*

VHDL is an expression for hardware representation. It defines how an electronic circuit or system can operate the physical circuit or system (implemented). VHDL stands for VHSIC hardware definition. VHSIC itself is the abbreviation for Very High Speed Integrated Circuits, a project launched in 1980 to promote the United States government's VLSI silicone chip design techniques. The initial version of VHDL 87 was finished up to the VHDL 93. Following the IEEE 1076 standard of the Institute of Electrical and Electronical Engineers (IEEE), the original and first Hardware classification language was VHDL. An additional standard, IEEE 1164, was later adopted for implementing a multi-value logic scheme [20]. VHDL is generally referred to as a program partly than a code. In VHDL, the only declaration is put and performed sequentially within a Method, FUNCTION, or Protocol [44].

D. *Design Flow of VHDL*

The main objective of VHDL is to allow a circuit or system to be synthesized on a programmable device (PLD or FPGA) or an ASIC [45].

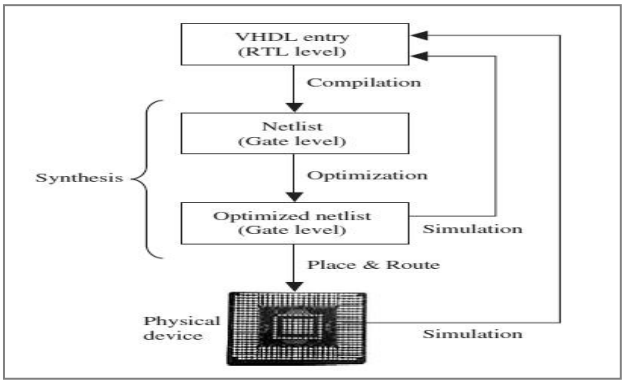

Fig. 5. Summary of VHDL Design Flow

VII. LITERATURE REVIEW

The spike in the number of scammers or crackers to target information and breach people's privacy. The main problem is, therefore, to enable the machine to encode data quickly. Because of the progress in computer screening and cracking, they analyzed the manner of ciphering quickly.

Zeebaree, Subhi, et al., [46] For high-performance computing, two systems based on FPGA, High-Performance Computing (HPC) code breaking was dependent upon the case analysis of the Simplified Data Encryption Standard (DES) algorithm. The first machine consists of a sequentially functioning FPGA unit. One FPGA interface includes sequentially one Processing Elements (PEs) job. This PE reflects a generalized two-round DES algorithm. Although the dual system is parallel, it also has one FPGA computer scheduled to be deployed in parallel. The FPGA computer includes 512 parallel-powered PEs. Each PE has two simpler DES algorithms completed. The FPGA unit functions in the second framework even faster than the first because it operates in parallel. It thus reflects a significant impact on the reduction of code break time and improved performance.

Kumar, Keshav, et al., [47] Used hardware FPGA systems because they are less complex, more compact, and more effective. In this job, one of the protection algorithms that is the AES algorithm is hardware execution. On Vivado 2014.2, the AES algorithm is performed, and findings of the Artix-7 FPGA are observed on 28 nanometers. This paper addresses the AES's development and the tools used to incorporate the Artix-7 FPGA AES architecture. The tools that are used are Slice Registry (SR), Lookup Tables (LUTs), Input/Output (I/O), and Global Buffer.

Sikka, Prateek, et al., [48] Offered a high-performance FPGA implementation based on high-level Advanced Encryption Standard (AES) algorithm synthesis. It uses a 128-bit key which is particularly suitable for telecommunication devices such as 5G. Investigators have designed and evaluated the setup to compare diverse HLS Recommendations according to their application using the Vivado High-Level Synthesis (HLS) platform. On Xilinx Kintex 7 and Virtex 6 FPGAs, the Verilog RTL was tested and applied. Because of using the same materials, we have seen substantial improvements compared to existing research approaches. The author also checked functionality design by testing the ciphertext of our design for the same plaintext.

Zope, Harshali, et al., [49] A new Hybrid unpipelined AES algorithm with improved security features is proposed, based on conventional AES algorithms. Abysmal AES research means that AES safety resides in activities in the S-box. This article presents a new method for generating S-box (modified S-box) values and the original key necessary to encrypt/encrypt (improved vital generation). Compared with the standard AES algorithm, the AES algorithm with the proposed changes significantly improves encryption Efficiency. The standard AES algorithm, fitted with new updated S-Box technology and advanced key generation technology, produces an avalanche effect of 60%, rendering attacks unavoidable. The proposed system is synthesized on many FPGA devices, and significantly improved performance is contrasted with the current designs. On the Spartan6 FPGA computer, the proposed concept is introduced.

Zeebaree, Subhi RM [50] High-performance Hardware implementation of DES Encryption reconfigurable. This was achieved by a new suggested implementation of the DES algorithm with a pipeline architecture. The use of the Spartan 3E family FPGAs (XC3S500E), one of the fastest and safest hardware applications, demonstrates the implementation of the proposed specification. The data blocks can be decoded or encrypted to 10688Mbps with an encounter speed of 167,448MHz and a decryption rate of 167,870MHz.

Hagras, Esam, et al., [51] A novel 4-dimensional high-speed FPGA chaotic memorandum system was proposed, based on a cubic nonlinear Xilinx System Generator (XSG) design. First, a pseudo-random number generator based on XSG FPGA's proposed implementation of a 4D Chaotic Memorizer scheme has been implemented in 32 fixed-point formats on the Xilinx Spartan-6 X6SLX45 board. The objective of the FPGA execution is to increase the random number generators of the memristor. FPGA application of the chaotic memristor systems findings reveals that the latest architecture solution reaches 393 MHz and dissipates 117 m watts. The traditional fifteen randomized experiments are used to calculate the proposed pseudo-random-number generator's consistency based on the chaotic 4D memory structure.

Furthermore, it has implemented a gray picture encryption method built on the chaotic 4D memristor system. The proposed encrypted scheme has a vast keyspace, shallow correlation values, much higher entropy, the optimal entropy value, a high change rate of pixels, and a tremendous unified average change in intensity values. The proposed encryption system's findings and its security review show that the encryption solution studied will protect high speed and safety against numerous attacks.

Zong, Jianyou, et al., [52] Proposed and demonstrated a reliable and safe data encryption communication method to improve physical layer protection in Orthogonal Frequency Division Multiplexing (OFDM)- Passive Optical Network (PON). The FPGA boards are used for optical network units and optical line terminal OFDM signal encryptions and decryption. The secrecy of physical layers is ensured through hyper-digital anarchy, which produces a large central area of 1045. The encrypted 16-QAM-OFDM signals at 435 Mb/s were successfully recovered after a 22-km SSMF transmission without any transmission loss. The digital chaos-based transmission of OFDM may be a robust and successful candidate for stable PON in the next decade.

Hashim, Ashwaq, et al., [53] Tried to develop the cryptographic algorithm simple, powerful and stable. The consequence of this effort is the 320-bit RC6-Cascade, the same as the cipher block. Up to 256 bytes will be essential. It is a hidden block chip with accurate RC6 algorithm characteristics, using a different overall structure architecture. Cascading of F-features instead of rounds is used in RC6-Cascade. The paper also examined the hardware architecture for the efficient implementation of the proposed FPGA cipher core of the RC6-Cascade stack. The F function of the above algorithm consists of an

effective compact iterative architecture. The objective is to develop a reliable algorithm for low-cost and small-scale applications with a high-speed encryption core.

Hasan, Fadhil, et al., [54] Utilized Xilinx System Generator (XSG) effectively, the latest stream cipher system model based on chaotic fixed-point maps are developed. The proposed Fixed Point XOR Chaotic Map-PRBG (FPXORCM-PRBG) and Fixed-Point Cascade Chaotic Map-PRBG (FPCCM-PRBG) are two Pseudo-Random Bit Generators (PRBGs) that rely on chaotic maps FPCCM-PRBG. The random trials in the NIST were used to evaluate the randomness metrics of the proposed PRBGs. For the proposed scheme study, security analyses are used, such as histogram, correlation coefficient, entropy information, and differential attacks (NPCR and UACI). Also, Xilinx SP605 XC6SLX45T FPGA Hardware Co-Simulation has been designed to evaluate the picture encryption truth. FXCM-PRBG and FPCCM-PRBG are appropriate for stream-based image encryption and outperform other encryption algorithms.

Madani, Mahdi, et al., [55] The two key targets have been identified for an optimized A5/3 algorithm architecture. The first part of the program is focused on the optimization of the kernel algorithm (the KASUMI block cipher). In contrast to the standard five-block KASUMI, the second tries to simplify the A5/3 algorithm with one block in the simplified KASUMI. The balance between high performance and hardware logic services in comparison with previous works was thus achieved by taking good performance into account. Several Xilinx Virtex FPGA technology devices implemented the proposed architecture. The synthesis findings from position and route have shown our solution's viability and effectiveness. This promising methodology can be used for the security of data in real-time on embedded mobile network applications.

Madhavapandian et al. [56] built an optimized FPGA implementation of AES goals to analyze an extensive range of security processes followed in the TCP/IP protocol suite. The first contribution of the experiments was to make the protection of the utility layer protocols. The AES cryptosystem for security protocols for the transmission control protocol/internet protocol (TCP/IP) protocol suite was implemented. AES is the most common cipher that is used for data protection. The configuration of the AES can be optimized to reduce the expense and use of electricity. Implementation of the Mix column in the AES techniques is carried out using an integrated system with the architecture for resource sharing and the door replacement process. This on-chip architecture provides a significant area and power savings compared to the initial hardware implementation. The current architecture is applied on the new Virtex 6 FPGA and compared with the previous works. It is proven that the proposed method has lower area utilization and ON-Chip utilization of power.

Visconti, Paolo, et al., [57] For a short and high-frequency communication system, the Wireless Connector is the high-speed implementation of the AES-128 algorithm. This communication system is based on the Xilinx ZCU102 FPGA platform. A pipelined implementation of the AES algorithm can handle different plaintext packets in different clock cycles for each round. This results in higher data throughput. It has the highest encryption and decryption speeds with 10s of clock cycles. The proposed solution will process data through pipelined and optimized solutions for the Substitute Bytes service, thereby providing maximum data throughput of more than 28 Gbit/s. In hardware capital, the proposed architecture needs only 1631 Configurable Logical Blocks (CLBs) and 3464 CLBs for decryption blocks.

Yang, Cheng, et al. [58] proposed a four-dimensional chaotic method to produce keys and boost the Advanced Encryption Standard. Using FPGA pipelines and parallel processing, the encryption algorithm is simplified as the secret to the encryption algorithm is the chaotic process. Block ciphers, Sub Byre, and Shift Rows are being converted to increase, and encryption rates are reduced. Instead of using the ARM-based SoC-FPGA for encryption and wired image transfer. The HPS kit works for Linux and monitors the encryption process with FPGA. The research has demonstrated a stable and robust proposed picture encryption algorithm.

Krishna, B Murali, et al., [59] The Image Cryptology (IC) is suggested by using a secret key in FPGA as a one-way FPGA Cryptographic feature, using the Runtime Linear Feedback Shift Register Logic (RLFSRL) as an Iteration Controller and a Reversible Logic Gate (RLG). ICRLG was planned for the syncretization, simulation, and implementation of the Vivado Hardware Description language (HDL) in Verilog, targeted to the architectural Artix-7 XC7A35T-1-CPG2, 36.

Li, Xiaochao, et al., [60] A new FPGA-based embedded along with a high-throughput, pipelined implementation of Linux Unified Key Setup (LUKS) is being introduced. The author designed a four-stage pipelined Secure Hash Algorithm-1 (SHA-1) module without the multiplexers between piecewise functions and a set of eight-stage pipelined Password-Based Key Derivation Feature-2 (PBKDF2) by reusing two hash results. Besides, we incorporate ST box-based AES decipher into the resource of block RAM (BRAM), which can boost the performance and leave much of the non-peripheral slice resource to the PBKDF2 model. With the aid of an FPGA and custom software, we can instantiate a high throughput LUKS co-processor in the Xilinx Zynq 7030 FPGA. In addition to a 16x speed increase over the previous work and 8x speed improvement over the previous work (the previous work was two times faster), the algorithm architecture is made using the FPGA. The speed of our LUKS leading recovery is quicker than the speed of the Nvidia GTX480.

Mhaouch, Ayoub, et al. [61] Proposed multiple trade-offs between the region and pace execution. In two different FPGA architectures, the author introduced the 128-bit Piccolo block cipher algorithm. The iterative and the four-bit serial architectures. Xilinx Spartan-3 was implemented as proposed. The iterative implementation achieves Seventy-six percent of resource use. It takes 31 clock cycles to execute the encryption or decryption. The result is a 151.1 Mbps output. In terms of cost reduction, the serial implementation was streamlined. The device completes 496 clock cycles and achieves a maximum output of 6.39 Mbps.

VIII. DISCUSSION

It can be concluded from the previous sections that researchers have used numerous approaches and strategies in different areas. Researchers have highlighted critical issues related to their plans' contrast. In Section VII, Table 1 is a comparison of the inquiries. The comparison consists of four main characteristics that comply with their trends to validate their Encryption and Decryption technique aims. The comparison was carried out concerning the fields of use, algorithms used, and significant satisfying targets.

It is evident from the table that the sources [47, 49, 50, 57] are depended directly on the Encryption and Decryption field. While reference [60, 61] work in the Encryption field, the remaining researcher worked in Code Breaking, Encryption Telecom Applications, Image Encryption, DATA Encryption, and Decryption and Security Processes in the TCP/IP Protocol field. Depending on the scientific area of DES Algorithms, AES Algorithms, and 4D memristor chaotic RNG, the researcher uses an important technique. Another method is used, such as Chaotic Data Encryption, RC6-Cascade, A5/3 algorithm, and so on. By using this methodology and techniques, both researchers have strong structures, frames, and functions. However, researchers' trend has been oriented for modern Image Encryption and Encryption and Decryption fields.

TABLE I. ENCRYPTION AND DECRYPTION DEPENDING ON FPGA

Researcher	Implementation Field	Used Algorithms	Significant Satisfied Aims
Zeebaree, Subhi et al, [46]	Code Breaking	DES Algorithms	For high-performance computing, two systems are based on FPGA, HPC.
Kumar, Keshav et al, [47]	Encryption and Decryption	AES Algorithms	Used hardware FPGA system because they are less complex, more compact and more effective
Sikka, Prateek et al, [48]	Encryption Telecom Applications	AES Algorithms	Offered a high-performance FPGA implementation based on high-level AES algorithm synthesis.
Zodpe, Harshali et al, [49]	Encryption and Decryption	AES Algorithms	A new Hybrid unpipelined AES algorithm with improved security features is proposed, based on conventional AES algorithms.
Zeebaree, Subhi RM [50]	Encryption and Decryption	DES Algorithms	Presented a high-performance reconfigurable DES Encryption algorithm hardware implementation.
Hagras, Esam et al, [51]	Image Encryption	4D memristor chaotic RNG	Proposed a novel high-speed FPGA low power 4-dimensional memristor chaotic system, based on Xilinx System Generator (XSG) concept with cubic non-linearity.
Zong, Jianyou et al,[52]	DATA Encryption and Decryption	Chaotic Data Encryption	Proposed and demonstrated a reliable and safe data encryption communication method to improve physical layer protection (OFDM)- PON.
Hashim, Ashwaq et al, [53]	Encryption and Decryption Cores	RC6-Cascade	Tried to develop the cryptographic algorithm simple, powerful and stable
Hasan, Fadhil et al, [54]	Image Encryption	stream cipher	Utilized XSG in an effective manner, the latest model of the stream cipher system based on chaotic fixed-point maps is developed.
Madani, Mahdi et al, [55]	Encryption Mobile Network Applications	A5/3 algorithm	The two key targets have been identified for an optimized A5/3 algorithm architecture.
Madhavapandian, et al, [56]	Security Processes in the TCP/IP Protocol	AES Algorithms	Optimized application of AES targets in the TCP/IP protocol suite for FPGA, to analyze a wide variety of security processes.
Visconti, Paolo et al, [57]	Encryption and Decryption	AES-128 Algorithms	For a fast and high-frequency communication device a high speed implementation of the AES-128 algorithm is indicated.
Yang, Cheng et al, [58]	Image Encryption	Chaotic-AES Algorithms	proposed a four-dimensional chaotic method to produce keys and boost the AES.
Krishna, B Murali et al, [59]	Image Cryptology	(RLFSRL) Algorithms	An image cryptology (IC)

			is suggested by the use of a secret key (RLFSRL).
Li, Xiaochao et al, [60]	Encryption	(LUKS) Algorithms	A new FPGA-based built-in system is implemented with a high performance, pipeline implementation (LUKS).
Mhaouch, Ayoub et al, [61]	Encryption	Piccolo Block Cipher Algorithm	Proposed multiple trade-offs between the region and pace execution.

IX. Conclusion

This paper addressed active approaches to developed FPGA Encryption/Decryption architectures. Depending on the reviewed researches, it can conclude that a variety of active mechanisms have an essential role in the FPGA Implementations for Data Encryption and Decryption implementation. These fields Code Breaking, Encryption Telecom Applications, Image Encryption, DATA Encryption, and Decryption and Security Processes in the TCP/IP Protocol. There are also powerful techniques in this area, such as Chaotic Data Encryption, RC6-Cascade, A5/3 algorithm, (RLFSRL) Algorithms, (LUKS) Algorithms. Nowadays, researchers are working more toward Image Encryption and DATA Encryption and Decryption fields. Therefore, efficient FPGA Security frames or systems have been developed, such as those making Proposed and demonstrated a reliable and safe data encryption communication method, high-performance computing, two systems based on FPGA HPC, novel high-speed FPGA low power 4-dimensional memristor chaotic system, based on Xilinx System. Adding to that, it can conclude that AES Algorithms is the most suitable technique for Encryption and Decryption. Both Chaotic-AES Algorithms and Runtime Linear Feedback Shift Register Logic (RLFSRL) Algorithms are suitable for Image Encryption. At the same time, the A5/3 algorithm is efficient for Encryption Mobile Network Applications.

References

[1] S. Zeebaree, S. Ameen, and M. Sadeeq, "Social Media Networks Security Threats, Risks and Recommendation: A Case Study in the Kurdistan Region," vol. 13, pp. 349-365, 07/04 2020.

[2] [W. Stallings, Data and computer communications: Pearson Education India, 2007.

[3] S. Zeebaree, R. R. Zebari, K. Jacksi, and D. A. Hasan, "Security Approaches For Integrated Enterprise Systems Performance: A Review," Int. J. Sci. Technol. Res, vol. 8, 2019.

[4] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocessors and Microsystems, vol. 77, p. 103201, 2020.

[5] W. Diffie and S. Landau, Privacy on the line: The politics of wiretapping and encryption: The MIT Press, 2010.

[6] A. A. Salih, S. R. Zeebaree, A. S. Abdulraheem, R. R. Zebari, M. A. Sadeeq, and O. M. Ahmed, "Evolution of Mobile Wireless Communication to 5G Revolution," Technology Reports of Kansai University, vol. 62, pp. 2139-2151, 2020.

[7] O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree, and F. Y. Ahmed, "A survey and analysis of the image encryption methods," International Journal of Applied Engineering Research, vol. 12, pp. 13265-13280, 2017.

[8] D. A. Zebari, H. Haron, S. R. Zeebaree, and D. Q. Zeebaree, "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 312-317.

[9] M. A. Hussain and R. Badar, "FPGA based implementation scenarios of TEA Block Cipher," in 2015 13th International Conference on Frontiers of Information Technology (FIT), 2015, pp. 283-286.

[10] G. MahendraBabu and K. Sridhar, "FPGA based Hybrid Random Number Generators," in 2020 4th International Conference on Electronics, Communication, and Aerospace Technology (ICECA), 2020, pp. 404-406.

[11] A. J. Abd El-Maksoud, A. A. Abd El-Kader, B. G. Hassan, N. G. Rihan, M. F. Tolba, L. A. Said, et al., "FPGA implementation of sound encryption system based on fractional-order chaotic systems," Microelectronics Journal, vol. 90, pp. 323-335, 2019.

[12] Z. N. Rashid, S. R. Zebari, K. H. Sharif, and K. Jacksi, "Distributed cloud computing and distributed parallel computing: A review," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 167-172.

[13] O. Alzakholi, H. Shukur, R. Zebari, S. Abas, and M. Sadeeq, "Comparison among cloud technologies and cloud performance," Journal of Applied Science and Technology Trends, vol. 1, pp. 40-47, 2020.

[14] S. Zeebaree and H. M. Yasin, "Arduino based remote controlling for home: power saving, security and protection," International Journal of Scientific & Engineering Research, vol. 5, pp. 266-272, 2014.

[15] H. Shukur, S. R. Zeebaree, A. J. Ahmed, R. R. Zebari, O. Ahmed, B. S. A. Tahir, et al., "A State of Art Survey for Concurrent Computation and Clustering of Parallel Computing for Distributed Systems," Journal of Applied Science and Technology Trends, vol. 1, pp. 148-154, 2020.

[16] S. R. Zebari and N. O. Yaseen, "Effects of Parallel Processing Implementation on Balanced Load-Division Depending on Distributed Memory Systems," J. Univ. Anbar Pure Sci, vol. 5, pp. 50-56, 2011.

[17] S. Zeebaree, L. M. Haji, I. Rashid, R. R. Zebari, O. M. Ahmed, K. Jacksi, et al., "Multicomputer Multicore System Influence on Maximum Multi-Processes Execution Time," TEST Engineering & Management, vol. 83, pp. 14921-14931, 2020.

[18] Z. N. Rashid, K. H. Sharif, and S. Zeebaree, "Client/Servers Clustering Effects on CPU Execution-Time, CPU Usage and CPU Idle Depending on Activities of Parallel-Processing-Technique Operations," Int. J. Sci. Technol. Res, vol. 7, pp. 106-111, 2018.

[19] Z. Ageed, M. R. Mahmood, M. Sadeeq, M. B. Abdulrazzaq, and H. Dino, "Cloud computing resources impacts on heavy-load parallel processing approaches," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 22, pp. 30-41, 2020.

[20] K. H. Sharif, S. R. Zeebaree, L. M. Haji, and R. R. Zebari, "Performance Measurement of Processes and Threads Controlling, Tracking and Monitoring Based on Shared-Memory Parallel Processing Approach," in 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), 2020, pp. 62-67.

[21] Z. N. Rashid, S. R. Zeebaree, and A. Sengur, "Novel Remote Parallel Processing Code-Breaker System via Cloud Computing."

[22] Z. S. Ageed, R. K. Ibrahim, and M. A. Sadeeq, "Unified Ontology Implementation of Cloud Computing for Distributed Systems," Current Journal of Applied Science and Technology, pp. 82-97, 2020.

[23] W. M. Abduallah and S. R. M. Zeebaree, "New Data hiding method based on DNA and Vigenere Autokey," Academic Journal of Nawroz University, vol. 6, pp. 83-88, 2017.

[24] H. M. Yasin, S. R. Zeebaree, and I. M. Zebari, "Arduino Based Automatic Irrigation System: Monitoring and SMS Controlling," in 2019 4th Scientific International Conference Najaf (SICN), 2019, pp. 109-114.

[25] D. Zebari, H. Haron, and S. Zeebaree, "Security issues in DNA based on data Hiding: A review," International Journal of Applied Engineering Research, vol. 12, pp. 0973-4562, 2017.

[26] N. Nayak, A. Chandak, N. Shah, and B. Karthikeyan, "Encryption and decryption using FPGA," in IOP Conference Series: Materials Science and Engineering, 2017, p. 052030.

[27] B. O'Sullivan, Mercurial: The Definitive Guide: The Definitive Guide: " O'Reilly Media, Inc.", 2009.

[28] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Machine learning models for secure data analytics: A taxonomy and threat model," Computer Communications, vol. 153, pp. 406-440, 2020.

[29] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," International Journal of Security and Its Applications, vol. 9, pp. 289-306, 2015.

[30] K. Lata, "An Approach Towards Resisting Side-Channel Attacks for Secured Testing of Advanced Encryption Algorithm (AES) Cryptochip," in 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), pp. 155-161.

[31] P. Srivastava, E. Chung, and S. Ozana, "Asynchronous Floating-Point Adders and Communication Protocols: A Survey," Electronics, vol. 9, p. 1687, 2020.

[32] J. Pandey, A. Gurawa, H. Nehra, and A. Karmakar, "An efficient VLSI architecture for data encryption standard and its FPGA implementation," in 2016 International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA), 2016, pp. 1-5.

[33] S. Vaudenay, A classical introduction to cryptography: Applications for communications security: Springer Science & Business Media, 2006.

[34] V. Lytvyn, I. Peleshchak, R. Peleshchak, and V. Vysotska, "Information encryption based on the synthesis of a neural network and AES algorithm," in 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 447-450.

[35] A. A. El-Moursy, A. M. Darya, A. S. Elwakil, A. Jha, and S. Majzoub, "Chaotic Clock Driven Cryptographic Chip: Towards a DPA Resistant AES Processor," IEEE Transactions on Emerging Topics in Computing, 2020.

[36] P. R. L. C. R. Check, "20VL004-FPGA Based System Design."

[37] C. Maxfield, The design warrior's guide to FPGAs: devices, tools and flows: Elsevier, 2004.

[38] H. Shinba and M. Watanabe, "Radiation-hardened configuration context realization for field programmable gate arrays," Applied Optics, vol. 59, pp. 5680-5686, 2020.

[39] J. Lambert, S. Lee, J. S. Vetter, and A. Malony, "In-depth optimization with the OpenACC-to-FPGA framework on an Arria 10 FPGA," in 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2020, pp. 460-470.

[40] V. Ivanov and E. Nosov, "Serial communication protocol for FPGA-based systems," in Journal of Physics: Conference Series, 2019, p. 012044.

[41] S. Setty, "Spartan: Efficient and general-purpose zkSNARKs without trusted setup," in Annual International Cryptology Conference, 2020, pp. 704-737.

[42] A. Ilyas, M. R. Khan, and M. Ayyub, "FPGA based real-time implementation of fuzzy logic controller for maximum power point tracking of solar photovoltaic system," Optik, vol. 213, p. 164668, 2020.

[43] D. Suratwala and G. Rahate, "A Comparative VHDL Implementation of Advanced Encryption Standard Algorithm on FPGA," in Machine Learning for Predictive Analysis, ed: Springer, 2021, pp. 343-351.

[44] F. M. Nascimento, F. M. dos Santos, and E. D. Moreno, "A VHDL implementation of the Lightweight Cryptographic Algorithm HIGHT," algorithms, vol. 2, p. 5, 2015.

[45] B. J. LaMeres, Introduction to logic circuits & logic design with VHDL: Springer, 2019.

[46] S. R. Zeebaree, A. B. Sallow, B. K. Hussan, and S. M. Ali, "Design and simulation of high-speed parallel/sequential simplified DES code breaking based on FPGA," in 2019 International Conference on Advanced Science and Engineering (ICOASE), 2019, pp. 76-81.

[47] K. Kumar, K. Ramkumar, and A. Kaur, "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), 2020, pp. 182-185.

[48] P. Sikka, A. R. Asati, and C. Shekhar, "Speed optimal FPGA implementation of the encryption algorithms for telecom applications," Microprocessors and Microsystems, vol. 79, p. 103324, 2020.

[49] H. Zodpe and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," Journal of King Saud University-Engineering Sciences, vol. 32, pp. 115-122, 2020.

[50] S. R. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," Indones. J. Electr. Eng. Comput. Sci, vol. 18, pp. 774-781, 2020.

[51] E. A. Hagras and M. Saber, "Low power and high-speed FPGA implementation for 4D memristor chaotic system for image encryption," Multimedia Tools and Applications, vol. 79, pp. 23203-23222, 2020.

[52] J. Zong, A. A. Hajomer, L. Zhang, W. Hu, and X. Yang, "Real-time secure optical OFDM transmission with chaotic data encryption," Optics Communications, vol. 473, p. 126005, 2020.

[53] A. T. Hashim, A. M. Hasan, and H. M. Abbas, "Design and implementation of proposed 320 bit RC6-cascaded encryption/decryption cores on altera FPGA," International Journal of Electrical and Computer Engineering (IJECE), vol. 10, pp. 6370-6379, 2020.

[54] F. S. Hasan and M. A. Saffo, "FPGA Hardware Co-Simulation of Image Encryption Using Stream Cipher Based on Chaotic Maps," Sensing and Imaging, vol. 21, pp. 1-22, 2020.

[55] M. Madani and C. Tanougast, "FPGA implementation of an optimized A5/3 encryption algorithm," Microprocessors and Microsystems, vol. 78, p. 103212, 2020.

[56] S. Madhavapandian and P. MaruthuPandi, "FPGA implementation of highly scalable AES algorithm using modified mix column with gate replacement technique for security application in TCP/IP," Microprocessors and Microsystems, vol. 73, p. 102972, 2020.

[57] P. Visconti, S. Capoccia, E. Venere, R. Velázquez, and R. d. Fazio, "10 Clock-Periods Pipelined Implementation of AES-128 Encryption-Decryption Algorithm up to 28 Gbit/s Real Throughput by Xilinx Zynq UltraScale+ MPSoC ZCU102 Platform," Electronics, vol. 9, p. 1665, 2020.

[58] C.-H. Yang and Y.-S. Chien, "FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm," Symmetry, vol. 12, p. 189, 2020.

[59] B. M. Krishna, K. C. S. Kavya, P. S. Kumar, K. Karthik, and Y. S. Nagababu, "FPGA Implementation of Image Cryptology using Reversible Logic Gates," Int. J. of Advanced Trendsin Computer Science and Engineering, vol. 9, 2020.

[60] X. Li, K. Wu, Q. Zhang, S. Lin, Y. Chen, and S. Y. Wong, "A High Throughput and Pipelined Implementation of the LUKS on FPGA," Journal of Circuits, Systems and Computers, vol. 29, p. 2050075, 2020.

[61] A. Mhaouch, W. Elhamzi, and M. Atri, "Lightweight Hardware Architectures for the Piccolo Block Cipher in FPGA," in 2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), 2020, pp. 1-4.