electronics

MDPI

Article

Compact Walsh–Hadamard Transform-Driven S-Box Design for ASIC Implementations

Omer Tariq [*,†,‡], **Muhammad Bilal Akram Dastagir** [†,‡] **and Dongsoo Han** [†]

Korea Advanced Institute of Science and Technology—KAIST, Daejeon 34141, Republic of Korea; bilal@kaist.ac.kr (M.B.A.D.); ddsshhan@kaist.ac.kr (D.H.)

* Correspondence: omertariq@kaist.ac.kr

† Current address: School of Computing, KAIST, Daejeon 34141, Republic of Korea.

‡ These authors contributed equally to this work.

Abstract: With the exponential growth of the Internet of Things (IoT), ensuring robust end-to-end encryption is paramount. Current cryptographic accelerators often struggle with balancing security, area efficiency, and power consumption, which are critical for compact IoT devices and system-on-chips (SoCs). This work presents a novel approach to designing substitution boxes (S-boxes) for Advanced Encryption Standard (AES) encryption, leveraging dual quad-bit structures to enhance cryptographic security and hardware efficiency. By utilizing Algebraic Normal Forms (ANFs) and Walsh–Hadamard Transforms, the proposed Register Transfer Level (RTL) circuitry ensures optimal non-linearity, low differential uniformity, and bijectiveness, making it a robust and efficient solution for ASIC implementations. Implemented on 65 nm CMOS technology, our design undergoes rigorous statistical analysis to validate its security strength, followed by hardware implementation and functional verification on a ZedBoard. Leveraging Cadence EDA tools, the ASIC implementation achieves a central circuit area of approximately 199 μm^2. The design incurs a hardware cost of roughly 80 gate equivalents and exhibits a maximum path delay of 0.38 ns. Power dissipation is measured at approximately 28.622 μW with a supply voltage of 0.72 V. According to the ASIC implementation on the TSMC 65 nm process, the proposed design achieves the best area efficiency, approximately 66.46% better than state-of-the-art designs.

Keywords: Application Specific Integrated Circuit (ASIC); FPGA; lightweight cryptography; AES; S-Box; algebraic normal forms (ANFs); Walsh–Hadamard transforms

Citation: Tariq, O.; Dastagir, M.B.A.; Han, D. Compact Walsh–Hadamard Transform-Driven S-Box Design for ASIC Implementations. *Electronics* **2024**, *13*, 3148. https://doi.org/10.3390/electronics13163148

Academic Editor: Alireza Saberkari

Received: 14 July 2024
Revised: 1 August 2024
Accepted: 7 August 2024
Published: 9 August 2024

1. Introduction

The advancement of technology and interconnected communications has significantly improved our lives but has also introduced numerous potential privacy and security risks. Cryptography plays a crucial role in safeguarding user privacy and security by employing primitives that prevent unauthorized access. The Advanced Encryption Standard (AES), established by the National Institute of Standards and Technology (NIST) in 2001, defines a widely accepted encryption algorithm with a block size of 128 bits and key sizes of 128, 192, or 256 bits [1]. In AES, the strength of encryption heavily relies on the design and implementation of the substitution box (S-Box) [2], a critical component that distorts the data to enhance security. The need for secure, efficient cryptographic solutions is particularly critical in several application areas. Firstly, the Internet of Things (IoT) encompasses a vast array of devices, from smart home appliances to industrial sensors, that require lightweight encryption to ensure data security while maintaining low power consumption and a minimal hardware footprint [3]. Secondly, System-on-Chip (SoC) architectures integrate multiple components into a single chip, necessitating optimized cryptographic modules that balance performance, area, and power consumption. Thirdly, wearable technology, such as fitness trackers and smartwatches, demands compact, power-efficient

cryptographic solutions to protect sensitive personal data. Furthermore, medical devices, including pacemakers and insulin pumps, rely on secure communication to safeguard patient data and ensure device integrity. Lastly, modern automotive systems incorporate interconnected subsystems requiring secure data exchange to prevent unauthorized access and ensure passenger safety.

Despite significant advancements in cryptographic accelerators, several research gaps remain unaddressed. A primary challenge is the comprehensive optimization of power, performance, and area (PPA) parameters. Existing solutions often focus on improving one or two of these metrics at the expense of the third, resulting in suboptimal designs. Additionally, high-security algorithms like AES are computationally intensive and often not optimized for compactness and power efficiency, making them unsuitable for highly optimized SoC designs and IoT applications. Researchers have proposed various methods to create more resource-efficient cryptographic implementations. For instance, N. Ahmad et al. (2013) [4] introduced an XOR Gate approach for AES S-Box and inverse S-Box designs in a 65 nm CMOS standard library, focusing on low power and area efficiency. A. R. Masoleh et al. (2018) [5] developed a logic-minimization heuristic for AES S-Box in the same technology, aiming for efficient implementation. F. Artuger et al. (2020) [6] proposed a chaos-based technique for S-Box to improve performance, while B. Rashidi (2020) [7] designed an S-Box with low-cost transformation, minimal area resources, and a short critical path delay in a 65 nm CMOS standard library. Despite these advancements, prior work has typically concentrated on improving either area, power, or delay using single 8-bit or 4-bit signals. None have comprehensively addressed all three parameters simultaneously, nor have they incorporated a dual quad-bit implementation with enhanced security.

In this paper, we proposed area-efficient S-Box architecture for ASIC implementations by employing a novel dual quad-bit structure. This approach maintains critical cryptographic properties, such as non-linearity, low differential uniformity, and bijectiveness. Utilizing Algebraic Normal Forms (ANFs) and the Walsh–Hadamard Transform, the design achieves high non-linearity and robust security against cryptographic attacks. The 8-bit S-box design leverages dual quad-bit forward and backward transformations, optimizing encryption and decryption processes. Our method demonstrates superior PPA optimization and security enhancements compared to previous techniques. Simulation results using Cadence RTL synthesis tools confirm that our proposed implementation significantly improves PPA metrics while providing enhanced security, outperforming all previously proposed methods. This comprehensive approach addresses the existing research gaps by simultaneously optimizing power, performance, and area while incorporating a novel dual quad-bit design. This ensures the proposed S-Box is more secure and more suitable for the stringent requirements of modern IoT devices, SoCs, wearable technology, medical devices, and automotive systems. Our findings highlight the potential of this new architecture to set a new standard in lightweight cryptographic implementations, paving the way for more secure and efficient digital communication systems. The paper's significant contributions are summarized as follows:

(1) This work introduces a novel approach to designing substitution boxes (S-boxes) for AES encryption, leveraging dual quad-bit structures to enhance cryptographic security and hardware efficiency. Utilizing Algebraic Normal Forms (ANFs) and Walsh–Hadamard Transforms, the proposed RTL circuitry ensures optimal non-linearity, low differential uniformity, and bijectiveness, providing a robust and efficient solution for ASIC implementations. (2) The security analysis of the proposed S-Box architecture using comprehensive statistical tests demonstrates enhanced security levels comparable to the AES S-Box and other existing works, ensuring robust protection against cryptographic attacks. (3) The dual quad-bit forward and backward tracing circuitry is designed at the register transfer level (RTL) and is functionally verified using stringent measurement criteria, confirming the correctness and reliability of the proposed architecture. (4) The proposed S-Box design is implemented on a ZedBoard Zynq 7000 SoC Board for functional verification, confirming its practical applicability and effectiveness in real-world environments. Additionally,

the ASIC implementation using a standard 65 nm CMOS library demonstrates a low transistor count, small die size, and low delay path, achieving optimal power, performance, and area (PPA) metrics.

The subsequent sections of this research work are organized as follows. Section 1 provides the introduction and related work. Section 2 covers the methodology, Proposed Architecture using Dual Quad-Bit S-Box Pair, Walsh to Hadamard Transformation for Dual Quad-Bit Forward S-Box, and Hadamard to Walsh Transformation for Dual Quad-Bit Backward S-Box. Section 3 details the implementation and evaluation, which includes Security Tests using Statistical Analysis. It also discusses the Hardware Design and Implementation, including Verification and Security Measurement Criteria, RTL Synthesis using ZedBoard Zynq 7000 SoC, Front-End Design, and Back-End (Physical) ASIC Design, followed by a Comparative Discussion. Section 4 concludes the research and discusses future work.

2. Related Work

Cryptography, derived from the Greek term meaning "secret writing", is a technique that ensures message confidentiality. Historically, cryptography has been used to protect information, with roots tracing back to ancient civilizations. For instance, the Egyptians utilized secret hieroglyphs, while Ancient Greeks and Romans employed cryptographic methods, such as the renowned Caesar cipher, dating back to 2000 BC [8]. In contemporary times, cryptography is critical for securing data, ensuring that only authorized recipients can access transmitted information. Despite its pervasive use in modern informatics, many individuals are unaware of cryptography's role in their daily interactions with technology. However, the robustness of cryptographic systems can be compromised by a single programming error or improper implementation, highlighting their inherent fragility. The foundation of modern cryptographic standards builds on the principles established by Claude Shannon. The current standard for encryption, the Advanced Encryption Standard (AES), utilizes the S-Box and inverse S-Box algorithms proposed by Rijndael. These algorithms, depicted in Figure 1, respectively, were adopted as the AES standard by the National Institute of Standards and Technology (NIST) in 2001 [1]. Implementing these algorithms in hardware, particularly in Application-Specific Integrated Circuits (ASICs), is crucial for achieving high efficiency and security in lightweight cryptographic applications. This paper focuses on the efficient ASIC implementation of a novel dual quad-bit S-Box pair architecture using 65 nm CMOS technology, addressing the need for secure and efficient cryptographic solutions in the modern digital landscape.

The most critical step in symmetrical cryptography is the introduction of distortion to the data through substituting elements from a lookup table known as the S-Box. The S-Box maintains information security by incorporating the Shannon property of confusion [9]. This non-linear property is essential in modern cryptography, providing a robust defense against linear and differential attacks [10]. A prime example of this non-linear transformation is the implementation of the S-Box in the NIST-approved Advanced Encryption Standard (AES) algorithm, as illustrated by the AES S-Box and inverse S-Box, respectively [1].

However, the AES S-Box is responsible for a significant portion of the delay in the entire encryption process. Therefore, research efforts are directed towards optimizing the algorithm, particularly designing new S-Boxes suitable for efficient implementation on various resource-constrained devices [11]. Numerous researchers have contributed to developing various S-Box designs for hardware implementations targeting the 65 nm CMOS standard library.

D. Canright et al. (2005) [12] were among the first to examine S-Box design choices based on polynomial and normal bases, providing 432 cases for each. They optimized bit matrices using a "greedy algorithm" and included NOR gates to save area, enabling compact hardware implementations for AES parallelism. This approach led to a structural code formulation that matched the hardware complexity reported, resulting in a reduced hardware cost of 200 GEs.

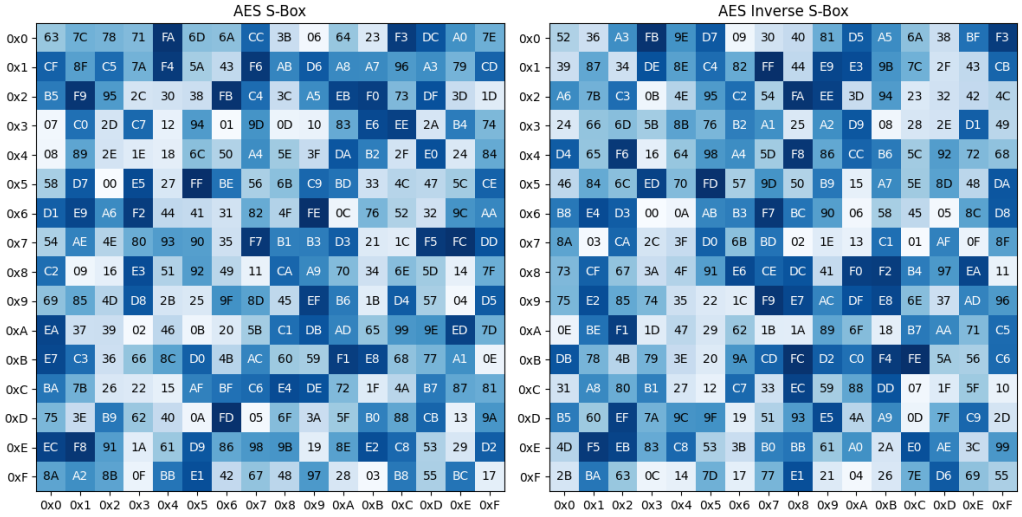

Figure 1. AES S-Box and Inverse S-Box.

J. Boyar et al. (2012) introduced circuit optimization using three techniques: greedy heuristics for linear components, automatic theorem proving for resynthesizing nonlinear elements into shallow-deep tower blocks, and simple local replacements along critical paths [13]. N. Ahmad et al. (2013) proposed using the arithmetic of a composite field and a low-powered Galois field GF(2^8) polynomial base for a reverse Galois S-Box CMOS model [4].

R. Ueno et al. (2015) [14] developed a GF(2^8) architecture based on an efficient and compact investment circuit design, combining GF arithmetic in both nonredundant and redundant ways. This design established a basic standard basis for efficiently mapping input power components into logical gates within a 65 nm CMOS standard cell library, showing improved performance compared to conventional circuits.

J. Boyar et al. (2017) [15] advanced techniques for building small linear circuits with limited depths, utilizing a new heuristic for linear depth optimization. These techniques were used to create traditional encryption functions defined in the GF(2) area, generated by circuit gates like "XNOR", "XOR", and "AND". This method was repeatedly used to optimize the linear top and bottom components in the See-Saw process, resulting in a smaller 16-bit S-Box with a reversal of GF(2^{16}).

R. Masolehey et al. (2018) [5,16] proposed two versions of the S-Box design: an all-structural lightweight design with a delay of 1.0808 ns and a slightly higher implementation area of 391.04 μm², and an all-structural fast design, the smallest, fastest, and most efficient S-Box design with the lowest power consumption, an area-time product of 162.177, and a low delay of 0.779697 ns.

In 2020, B. Rashid et al. (2020) [7] suggested a hardware-efficient reverse-based S-Box, an alternative to the AES S-Box, with similar cryptographic features for lightweight cipher blockers. This S-Box calculation involved the reverse field and refined transformation, primarily through two processes, resulting in an integrated S-Box with low-area capital cost-effectiveness and a low critical path delay (CPD).

Y. Teng et al. (2022) [17] introduced an advanced VLSI architecture for the AES S-box and inverse S-box, utilizing composite field arithmetic to achieve high area efficiency. Key optimizations include reducing the area of multipliers in the Galois composite field $GF((2^2)^2)$ and combining squaring and multiplication operations with constants. The methodology also features manual optimization of the multiplicative inversion through simplified Boolean equations. The design improved efficiency by using pre-processing and post-processing modules to share resources between the S-box and inverse S-box, validated by FPGA and ASIC implementations showing a 10% area efficiency increase on Virtex-6 and a 30% improvement with the TSMC 90 nm process.

Despite significant advancements in designing S-Box architectures for AES, a notable research gap persists in concurrently optimizing area efficiency, processing speed, and security in hardware implementations. Previous works have primarily focused on either compacting the design or enhancing throughput individually. There remains a need for a holistic approach that integrates area, computational optimizations, and security measures. This research aims to develop a VLSI architecture that achieves superior area efficiency, high throughput, and robust security, validated through rigorous FPGA and ASIC implementations.

3. Methodology

Substitution boxes (S-boxes) are pivotal in providing non-linearity in block ciphers, which is crucial for resisting linear and differential cryptanalysis. The Advanced Encryption Standard (AES) utilizes an S-box based on the finite field inversion, which, while secure, poses significant challenges in terms of hardware efficiency, particularly in ASIC implementations where power, performance, and area (PPA) are key constraints. Therefore, we proposed RTL circuitry for S-Box using the novel approach of a dual quad-bit structure while ensuring several cryptographic properties and robust security. To enhance cryptographic security, it is crucial to consider several key properties of S-boxes in symmetric-key algorithms. Firstly, non-linearity is fundamental as it maximizes the Hamming distance from any affine function, thereby providing robust defense against linear cryptanalysis. Secondly, maintaining low differential uniformity is essential; this ensures that the maximum output differential for any input differential occurs with low probability, thus protecting against differential cryptanalysis. Lastly, bijectiveness guarantees that each input maps to a unique output, ensuring the S-box is invertible and facilitating the decryption process in symmetric-key algorithms.

3.1. Algebraic Normal Forms (ANFs)

Algebraic Normal Form (ANF) is a polynomial representation of a Boolean function over the binary field $\mathbb{F}_2$. It expresses the function as a sum of products, which can be directly implemented in hardware.

$$f(x_1, x_2, \ldots, x_n) = c_0 \oplus (c_1 x_1) \oplus (c_2 x_2) \oplus \cdots \oplus (c_{2^n-1} x_1 x_2 \cdots x_n) \tag{1}$$

where c_i are coefficients in $\mathbb{F}_2$ and $\oplus$ denotes addition modulo 2. The Algebraic Normal Form (ANF) of a Boolean function is critical for several reasons. Firstly, the simplicity and implementability of ANFs make them highly compatible with digital circuit design, as they utilize XOR and AND gates, which are fundamental to such circuits. Secondly, ANFs are instrumental in analyzing the non-linearity of Boolean functions. Functions that include higher-degree terms in their ANF indicate improved security because they deviate further from linear functions, enhancing resistance against cryptographic attacks.

3.2. Walsh–Hadamard Transform

The Walsh–Hadamard Transform is employed to compute the Walsh spectrum of Boolean functions, which measures their deviation from affine functions. The transform is defined as follows:

$$W_f(a) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus (a \cdot x)} \tag{2}$$

where $a \cdot x$ represents the dot product modulo 2.

In cryptographic contexts, the non-linearity $\mathcal{N}(f)$ of a Boolean function f is crucial. It is calculated using the following formula:

$$\mathcal{N}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \{0,1\}^n} |W_f(a)| \tag{3}$$

This measure of non-linearity is vital because it quantifies the function's distance from any linear or affine function, thus indicating the function's robustness against linear cryptanalysis. High non-linearity is desirable in cryptographic Boolean functions to enhance security. This metric is fundamental for assessing the function's resistance to linear cryptanalysis. The use of ANFs and WHT in cryptographic S-box design is crucial for ensuring robust security features. These mathematical tools provide a clear pathway for designing and evaluating the non-linearity and differential uniformity of Boolean functions in cryptographic applications

3.3. Proposed Architecture Using Dual Quad-Bit S-Box Pair

In this section, we propose an 8-bit S-Box design utilizing dual quad-bit forward (alpha) and backward (beta) transformations. Figure 2 illustrates the RTL design for the 8-bit S-Box using dual quad-bit transformations. The design employs multiplexers and demultiplexers to select between forward and backward operations, ensuring efficient encryption and decryption processes. The design consists of several key components. Registers are used to store the input and output values, providing synchronized data flow. The demultiplexer splits the 8-bit input into two 4-bit values for processing. A multiplexer combines the two 4-bit processed values into an 8-bit output. Forward transformations (α) implement the quad-bit Walsh to Hadamard transformation, while backward transformations (β) implement the quad-bit Hadamard to Walsh transformation. The control logic determines whether the forward or backward transformation is applied based on the selected signal.

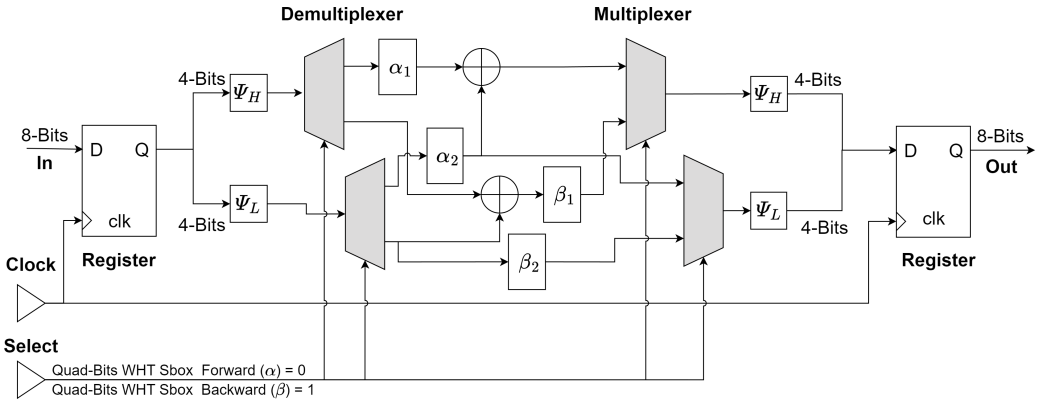

Figure 2. RTL Diagram for 8-bit S-Box Using Dual Quad-Bit Forward and Backward Transformations.

The 8-bit input is initially stored in a register. This register is clocked to ensure synchronized data flow. The 8-bit input is then split into two 4-bit values (Ψ_H and Ψ_L) using a demultiplexer. This separation allows for parallel processing of the high and low 4-bit segments. The separated 4-bit values are fed into both the forward (α_1, α_2) and backward (β_1, β_2) transformation units. The forward transformation (α) converts Walsh functions to Hadamard functions, while the backward transformation (β) converts Hadamard functions to Walsh functions. After processing, a multiplexer selects between the outputs of the forward and backward transformations based on the control logic. The select signal determines whether the forward or backward transformation is used. When the select signal (α) is 0, the forward transformation (Walsh to Hadamard) is applied. When the select signal (β) is 1, the backward transformation (Hadamard to Walsh) is applied. The selected 8-bit output is then stored in an output register, ensuring synchronized data output. The demultiplexer splits the 8-bit input into two 4-bit values, which are processed by the forward and backward transformation units. The multiplexer then selects the appropriate processed values based on the control logic, combining them into an 8-bit output. The design ensures efficient and secure cryptographic operations by leveraging the orthogonal properties of the Walsh and Hadamard transformations.

3.4. Walsh to Hadamard Transformation for Dual Quad-Bit Forward S-Box

The transformation from Walsh to Hadamard functions is pivotal in generating the S-Boxes. The Walsh functions are defined as a sequence of binary values (0 and 1). In contrast, the Hadamard functions are derived from the Hadamard matrix, which is a square matrix whose entries are binary (0 and 1) and rows are mutually orthogonal. This transformation is critical because it leverages the orthogonality properties of the Hadamard matrix to ensure the desired cryptographic strength and non-linearity in the S-Boxes. The forward S-Boxes $S\text{-}Box1F$ and $S\text{-}Box2F$ are defined by the following logical expressions, with the Walsh inputs w_0, w_1, w_2, w_3 and Hadamard outputs h_0, h_1, h_2, h_3.

These logical expressions are derived based on the transformation rules from Walsh to Hadamard functions, allowing for efficient computation of the S-Box outputs, which are critical in the AES encryption process. Figure 3 depicts two logic circuit diagrams, labeled (a) and (b), which are used to illustrate the transformation from Walsh functions to Hadamard functions. Figure 3a corresponds to $S\text{-}Box1F$, where the logic gates and connections form a specific arrangement to transform the Walsh inputs (w_0, w_1, w_2, w_3) into the Hadamard outputs (h_0, h_1, h_2, h_3). The key components in this transformation are NOT gates (Inverters), which are used to negate the inputs; AND gates, which perform logical conjunctions of the inputs and their negations; and OR gates, which perform logical disjunctions to combine the results of the AND gates. Figure 3b corresponds to $S\text{-}Box2F$, which also transforms Walsh inputs into Hadamard outputs but may have a slightly different configuration and connections of logic gates to achieve this transformation. The circuit operation involves feeding the inputs w_0, w_1, w_2, w_3 into the circuit, where NOT gates negate the inputs where necessary, AND gates combine these inputs (and their negations) in specific ways to form intermediate results, and OR gates combine these intermediate results to produce the final outputs h_0, h_1, h_2, h_3. The diagrams essentially implement the Boolean expressions described for $S\text{-}Box1F$ and $S\text{-}Box2F$, thereby achieving the transformation from the Walsh functions w to the Hadamard functions h.

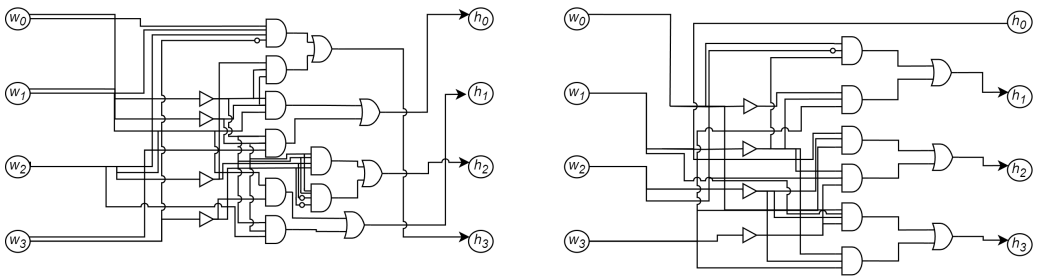

Figure 3. Dual quad-bit s-box pair for forward operation is presented. Figure (**a**) shows the schematic of proposed s-box forward first pair and Figure (**b**) shows the schematic of proposed s-box forward second pair.

3.5. Hadamard to Walsh Transformation for Dual Quad-Bit Backward S-Box

The transformation from Hadamard to Walsh functions is essential for generating the backward S-Boxes. This process is crucial for reversing the encryption process, ensuring that the S-Boxes can be used effectively in both encryption and decryption. The backward S-Boxes $S\text{-}Box1B$ and $S\text{-}Box2B$ are defined by the following logical expressions, with the Hadamard inputs h_0, h_1, h_2, h_3 and Walsh outputs w_0, w_1, w_2, w_3.

These logical expressions are derived based on the transformation rules from Hadamard to Walsh functions, allowing for efficient computation of the S-Box outputs, which are critical in the AES decryption process. Figure 4 depicts two logic circuit diagrams, labeled (a) and (b), which are used to illustrate the transformation from Hadamard functions to Walsh functions. Figure 4a) corresponds to $S\text{-}Box1B$, where the logic gates and connections form a specific arrangement to transform the Hadamard inputs (h_0, h_1, h_2, h_3) into the Walsh outputs (w_0, w_1, w_2, w_3). The key components in this transformation are

NOT gates (Inverters), which are used to negate the inputs; AND gates, which perform logical conjunctions of the inputs and their negations; and OR gates, which perform logical disjunctions to combine the results of the AND gates. Figure 4b) corresponds to $S\text{-}Box2B$, which also transforms Hadamard inputs into Walsh outputs but may have a slightly different configuration and connections of logic gates to achieve this transformation. The circuit operation involves feeding the inputs h_0, h_1, h_2, h_3 into the circuit, where NOT gates negate the inputs where necessary, AND gates combine these inputs (and their negations) in specific ways to form intermediate results, and OR gates combine these intermediate results to produce the final outputs w_0, w_1, w_2, w_3. The diagrams essentially implement the Boolean expressions described for $S\text{-}Box1B$ and $S\text{-}Box2B$, thereby achieving the transformation from the Hadamard functions h to the Walsh functions w.

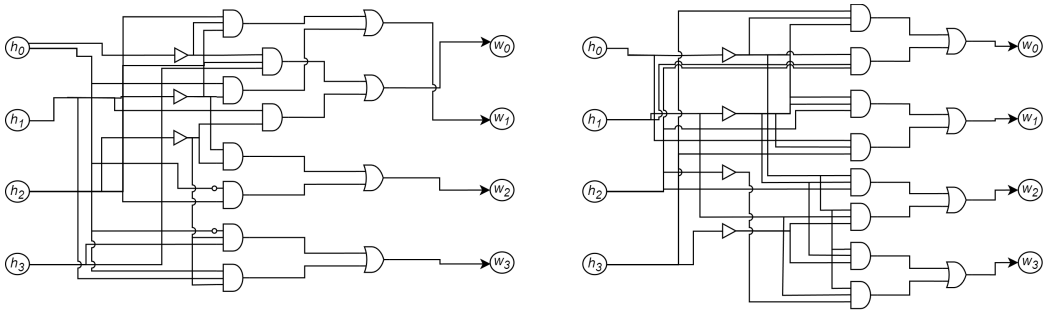

Figure 4. Here, dual quad-bit s-box pair for backward operation is presented. Figure (**a**) shows the schematic of proposed s-box backward first pair and Figure (**b**) shows the schematic of proposed s-box backward second pair.

The Walsh–Hadamard Transform provides a robust framework for the design of S-Boxes in AES encryption. By leveraging the orthogonal properties of Hadamard matrices, we can derive efficient and secure logical expressions for both forward and backward S-Boxes. The dual S-box approach involves splitting the traditional 8-bit input into two 4-bit blocks, processed by distinct S-boxes. This design enhances the cryptographic strength and hardware efficiency by allowing more tailored and optimized transformations. This methodology enhances the security and performance of AES encryption, making it a valuable tool in modern cryptographic implementations. Figure 5 shows generated 8-bit S-Box values from dual quad-bit S-Box pairs, as shown in Figure 6.

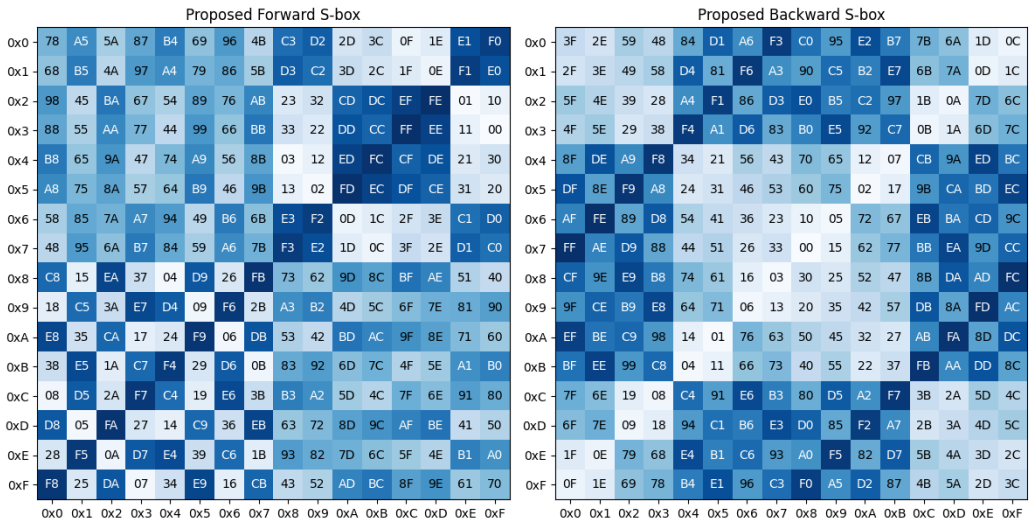

Figure 5. The values of proposed S-Box Forward and Backward.

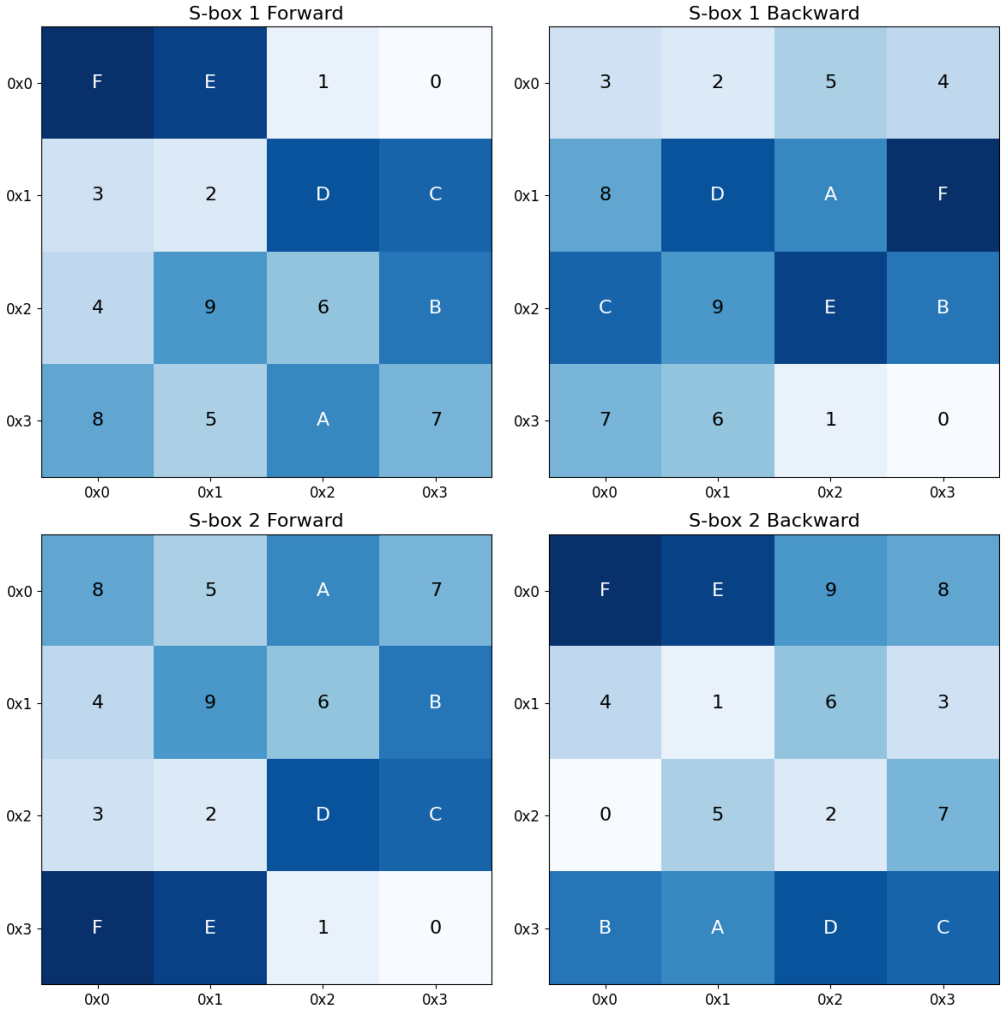

Figure 6. The values of dual quad-bit S-Box pairs.

In Figure 5 each cell in the matrices represents a hexadecimal value that is substituted during the encryption and decryption processes. The left matrix shows the forward S-Box used for substitution in the encryption process, while the right matrix shows the backward S-Box used in the decryption process. These S-Boxes are designed to ensure high non-linearity and resistance against linear and differential cryptanalysis, enhancing the encryption's security. Figure 6 illustrates the values of dual quad-bit S-Box pairs for both forward and backward transformations. The dual quad-bit S-Box design is an innovative approach that splits the traditional 8-bit S-Box into two 4-bit S-Boxes, providing additional flexibility and complexity in the substitution process. The top row displays the S-Box 1 forward and backward values, while the bottom row shows the S-Box 2 forward and backward values. This dual S-Box structure aims to enhance the diffusion and confusion properties of the cipher, thereby increasing its resistance to various cryptographic attacks. Using dual S-Boxes allows for more intricate substitution patterns, which contribute to the overall strength and security of the encryption algorithm.

4. Implementation and Evaluation

This section delineates the optimal implementation of the dual quad-bit S-Box forward and backward pair within a single 8-bit AES framework. Extensive evaluations of the proposed implementation demonstrate significant improvements in processing time and security resilience compared to traditional S-Box designs. These results underline the efficacy of the dual quad-bit S-Box in optimizing AES performance, particularly for high-security applications necessitating 256-bit encryption.

4.1. Security Test Using Statistical Analysis

We conducted a series of statistical analyses on the cipher images to evaluate the security of the proposed encryption method comprehensively. These analyses are essential for assessing the encryption's robustness against various potential attacks.

Here are the revised sections based on the detailed explanations provided:

4.1.1. Visual Testing Analysis

Visual testing analysis is a preliminary step in evaluating the effectiveness of an encryption algorithm. This test visually compares the plain (original) images with their corresponding cipher images. The goal is to ensure that no discernible patterns or similarities can be detected between the plain and cipher images. As illustrated in Figure 7, our visual review confirms that the encrypted images show no visible analogs to the original images, indicating a high level of security [18]. Specifically, the cipher image produced by our proposed S-box method appears highly chaotic, signifying effective scrambling of the original image's pixel values. This chaotic appearance is crucial as it ensures that the encryption disrupts any potential pixel correlation, thereby enhancing the overall security of the encrypted image.

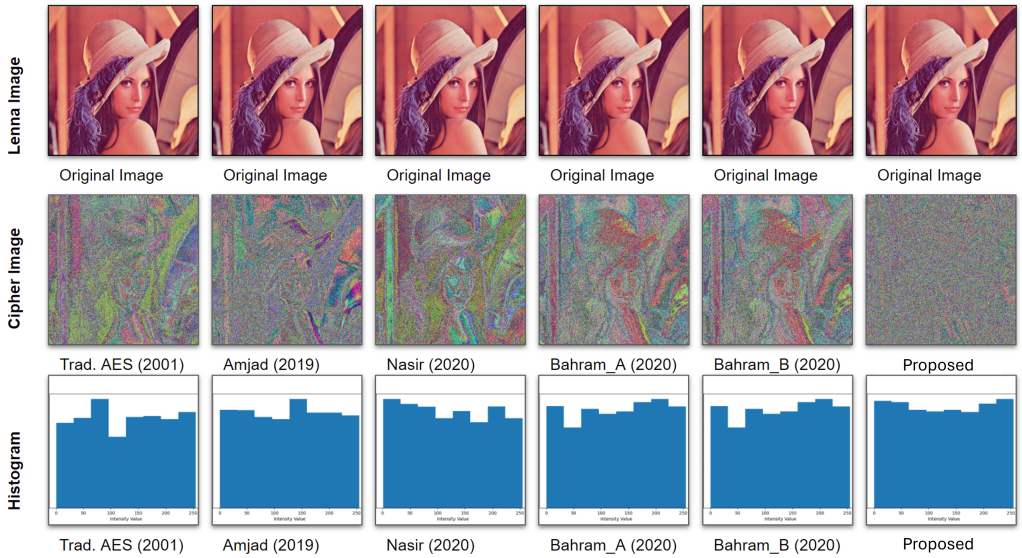

Figure 7. Histogram Analysis of Original and Cipher Images of the Proposed S-Box Method and Related Work.

4.1.2. Histogram Analysis

Histogram analysis is a straightforward yet powerful technique for assessing the quality of image encryption. A robust encryption method will transform a plain image into a cipher image with a uniformly distributed histogram. This uniformity indicates that the encryption effectively randomizes the pixel values, reducing the likelihood of successful attacks. For our analysis, we generated histograms for the cipher images of the sample images mentioned above, using the traditional AES S-Box, related works, and our proposed dual quad-bit S-Box method. As depicted in Figure 7, the histograms of cipher images encrypted with traditional AES S-Box and related techniques show some degree of uniformity, indicating decent encryption quality. However, the histogram corresponding to our proposed method is notably flatter and more balanced. This uniform distribution of pixel values signifies that our approach results in a more effective randomization process, thereby significantly enhancing security.

The uniform histogram achieved by our method makes it highly resistant to statistical attacks, as it effectively obscures the original data patterns present in the plain image. Our dual quad-bit S-Box design ensures that each bit of the plaintext influences multiple bits

of the ciphertext, leading to a highly non-linear and complex transformation. This robust diffusion and confusion mechanism contribute to the superior level of security provided by our approach compared to previous methods, making it an excellent choice for applications requiring robust image encryption.

The histogram variance of gray images is defined by

$$Var\ (V)\ =\ \frac{1}{256}\sum_{i=0}^{255}[v_i - E(V)]^2, \tag{4}$$

where $E(V) = \frac{1}{256}\sum_{i=0}^{255} v_i$, and V is the pixel number vector of 256 gray levels.

4.1.3. Information Entropy Analysis

Information entropy is a critical measure of the randomness and unpredictability of an encrypted image. High entropy indicates a high degree of randomness, desirable in secure encryption schemes. Ideally, for an 8-bit image, the entropy value should be close to 8, reflecting that each of the 256 possible pixel values occurs with equal probability. The closer the entropy value is to 8, the more secure the cipher is considered to be [19,20]. The entropy $H(m)$ of a message m can be calculated using the following equation:

$$H(m) = \sum_{i=0}^{255} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{5}$$

Our analysis calculated the entropy for the cipher images obtained using traditional AES S-Box, related works, and our proposed dual quad-bit S-Box method. The results, summarized in Table 1, demonstrate that our proposed method achieves an entropy value closest to 8, indicating a higher level of randomness and security than other methods. This high entropy confirms that the pixel values in the cipher images are uniformly distributed and unpredictable, making it extremely difficult for attackers to infer any meaningful patterns or information about the original image. Thus, our dual quad-bit S-Box design ensures high encryption quality and significantly enhances the security of encrypted images.

Table 1. Security and Statistical Analysis of the Related Works with the Proposed Method.

Methods	Entropy	Cond. Entropy	MAE	MSE	PSNR	SSIM	Correlation
Lenna	7.445	–	0.0	0.0	361.2	1.0	1.0
Trad_AES (2001)	7.629	7.579	0.917	105.507	8.603	0.011	−0.053
Amjad (2019)	7.624	7.612	0.946	106.776	8.551	0.017	−0.031
Nasir (2020)	7.629	7.638	0.872	99.124	8.874	0.040	0.087
Bahram (2020)-a	7.633	7.596	0.938	108.323	8.489	0.007	0.007
Bahram (2020)-b	7.633	7.564	0.938	108.305	8.490	0.007	−0.085
Proposed (2024)	7.650	7.647	0.936	108.419	8.485	0.020	−0.001

Entropy ≅ 8: Indicates a high level of randomness in the ciphertext, reflecting strong security. Cond. Entropy: Measures the uncertainty of the ciphertext given the plaintext. MAE & MSE High: High Mean Absolute Error and Mean Squared Error suggest less accurate reconstruction. PSNR Less: Lower Peak Signal-to-Noise Ratio indicates lower quality of the reconstructed image. SSIM & Correlation ≅ 0: Structural Similarity Index and correlation values are approximately 0, indicating very low structural similarity and correlation between the plaintext and ciphertext.

Similarly, our proposed method achieved superior Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and correlation-coefficient values compared to previous works. These improved statistical security parameters suggest that our proposed algorithm is highly secure and resistant to brute-force attacks. The enhanced metrics confirm the algorithm's effectiveness in producing highly secure encrypted images, making it a reliable choice for applications requiring robust image encryption.

4.1.4. Mean Absolute Error (MAE) Analysis

The Mean Absolute Error (MAE) analysis is a valuable metric for assessing the security of cipher images by measuring the absolute errors between the original image and the cipher image. A higher MAE value indicates a greater level of security, as it implies that the cipher image is significantly different from the original image. This analysis helps in understanding the accuracy and effectiveness of the encryption process in obscuring the original image [21–23].

The MAE is calculated using the following equation:

$$MAE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} |P(i,j) - C(i,j)|, \tag{6}$$

where $P(I,j)$ and $C(I,j)$ represent the pixel values of the original image P and the cipher image C at position (i,j), respectively, and M and N are the dimensions of the images. By calculating the MAE for different encryption methods, including traditional AES S-Box, related works, and our proposed dual quad-bit S-Box method, we can compare the effectiveness of each approach. Higher MAE values for our method would confirm its superior ability to obscure the original image, providing enhanced security. The results of the MAE analysis, shown in Table 1, indicate that our proposed method achieves higher MAE values than other techniques. This demonstrates that our dual quad-bit S-Box design effectively increases the security of the encrypted images, making it a more robust encryption method for protecting sensitive information.

4.1.5. Mean Square Error (MSE) Analysis

The Mean Square Error (MSE) analysis is crucial for evaluating the security of cipher images by measuring the average squared difference between the original and encrypted images. MSE is calculated pixel-by-pixel, quantifying the contrast between the original image P and the cipher image C. A higher MSE value indicates greater distortion and, consequently, higher security, as it signifies that the cipher image differs significantly from the original image.

The MSE is calculated using the following equation:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (P(i,j) - C(i,j))^2, \tag{7}$$

where $P(I,j)$ and $C(I,j)$ represent the pixel values of the original image P and the cipher image C at position (i,j), respectively, and M and N are the dimensions of the images. This analysis helps to understand the degree of error the encryption process introduces. Higher MSE values for our proposed dual quad-bit S-Box method would confirm its superior ability to distort the original image, thus providing enhanced security.

4.1.6. Peak Signal-to-Noise Ratio (PSNR) Analysis

The Peak Signal-to-Noise Ratio (PSNR) is another critical metric for evaluating encrypted image quality. PSNR measures the ratio of the maximum possible signal power of the original image to the power of the noise introduced by the encryption process, expressed in decibels (dB). In the context of encryption, a lower PSNR value indicates a higher degree of distortion and, therefore, better security, as the encrypted image is less similar to the original image. The PSNR is calculated using the following equation:

$$PSNR = 10 \times \log\left(\frac{P^2}{MSE}\right), \tag{8}$$

Here, P represents the peak signal value of the original image, and MSE is the mean square error. By calculating the PSNR for different encryption methods, including traditional AES S-Box, related works, and our proposed dual quad-bit S-Box method, we

can compare the effectiveness of each approach. Lower PSNR values for our method would indicate better security, as encrypted images are more distorted than the original ones. The results of the MSE and PSNR analyses, as shown in Tables 7 and 8, confirm that our proposed dual quad-bit S-Box method achieves higher MSE and lower PSNR values than other techniques. This demonstrates that our method effectively increases the security of the encrypted images, making it a more robust encryption method for protecting sensitive information.

4.1.7. Structural Similarity Index Metric (SSIM) Analysis

The Structural Similarity Index Metric (SSIM) is a method used to measure the similarity between two images. It is based on the idea that spatially close pixels have strong interdependencies, containing essential information about the structure of objects within the visual scene [23]. The SSIM index ranges from 0 to 1, where 1 indicates identical datasets and values close to 0 indicate high encryption security, as it signifies low similarity to the original image [21]. The SSIM can be calculated using the following equation:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu^2{}_x+\mu^2{}_y+c1)(\sigma^2{}_x+\sigma^2{}_y+c2)}, \tag{9}$$

where μ_x and μ_y are the averages of x and y, respectively, σ_x^2 and σ_y^2 are the variances, and σ_{xy} is the covariance of y and y. The constants $c1$ and $c2$ stabilize the division with weak denominator values. The SSIM analysis objectively measures image quality degradation due to encryption, with lower SSIM values indicating higher security.

4.1.8. Correlation-Coefficient Analysis

Correlation-coefficient analysis is employed to assess the degree of relationship between the pixels of the original and encrypted images. This analysis helps evaluate encryption quality by examining how much the pixel values in the encrypted image differ from those in the original image. A high correlation coefficient indicates weak encryption, whereas a low correlation coefficient, ideally close to 0, indicates strong encryption. The correlation coefficient r is calculated using the following equation:

$$r = \frac{n(\sum xy)-(\sum x)(\sum y)}{\sqrt{[n(\sum x^2)-(\sum x)^2][n(\sum y^2)-(\sum y)^2]}}, \tag{10}$$

where x and y are the pixel values of the original and encrypted images, respectively, and n is the total number of pixels. To interpret the correlation coefficient in an academic context, it is important to understand the implications of its values. A correlation coefficient of 1 signifies a perfect positive correlation, indicating that as one variable increases, the other variable increases in a perfectly linear relationship. Conversely, a correlation coefficient of -1 denotes a perfect negative correlation, where one variable increases while the other decreases perfectly linearly. Finally, a correlation coefficient of 0 indicates no correlation between the variables, suggesting independence and implying strong security in cryptographic contexts, as it demonstrates that there is no predictable relationship between the variables. The absolute value of the correlation coefficient indicates the strength of the relationship. A higher absolute value denotes a stronger relationship, while a lower absolute value (close to 0) indicates a weaker relationship, hence higher encryption security. For instance, an absolute value of 0.74 signifies a stronger correlation than 0.63, as shown in Table 2.

The proposed algorithm, implemented in Python, was evaluated using statistical analysis of image encryption and decryption on Lenna images. Table 1 presents a comparative analysis of the security metrics for our proposed method and other existing methods with similar properties. The results demonstrate that the cipher test image's information entropy (Shannon diversity index H) is higher than the other methods. This indicates that our method produces more randomness in the cipher image, enhancing its security. Moreover, the conditional entropy (H(C | P)) is maximized in our proposed method, which signifies

that the ciphertext is highly unpredictable given the plaintext. This high conditional entropy indicates that our encryption method effectively obscures the plaintext, making it highly resistant to cryptanalysis.

Table 2. Correlation-Coefficient Values and Their Corresponding Relationship Descriptions.

Correlation-Coefficient *r*	**Relationship Description**
+0.71 or above	Extremely strong positive relationship
+0.41 to +0.70	High positive relationship
+0.31 to +0.40	Average positive relationship
+0.21 to +0.30	Weak positive relationship
+0.01 to +0.20	Minimum relationship
0	No correlation (Strong Security)
−0.01 to −0.20	Minimum relationship
−0.21 to −0.30	Weak negative relationship
−0.31 to −0.40	Average negative relationship
−0.41 to −0.70	High negative relationship
−0.71 or below	Extremely strong negative relationship

4.2. Hardware Design and Implementation

In this section, we present the design of a custom-developed hardware architecture for the S-Box designs discussed earlier. The primary objective is to construct a low-power architecture that utilizes minimal hardware resources while effectively performing the specified functions. The main focus is optimizing the trade-offs between area, power, and time. In designing and developing field-programmable gate array (FPGA)-based projects, computer-aided design (CAD) methods are crucial. Hardware engineers typically write these designs in Verilog, and they must follow a sequential flow to fit the design into the available FPGA logic. This flow includes synthesis, technology library mapping, floor planning, optimization and routing, and eventually netlist generation [24]. The largely automated synthesis process involves converting the high-level Verilog code into a gate-level representation. This is followed by mapping the design onto the technology library specific to the target FPGA. Floor planning and routing ensure the design meets the desired performance and resource utilization criteria. Optimization techniques are applied at various stages to enhance the design's speed and power consumption efficiency. Netlist generation is the final step, where the optimized design is translated into a format suitable for FPGA programming. This synthesis method is controlled predominantly by CAD tools and their algorithms. By leveraging these automated processes, we ensure that the hardware implementation is efficient and effective. The custom hardware architecture developed in this work is evaluated based on its area, power, and time parameters. The results demonstrate that our approach significantly improves these metrics compared to traditional designs. This confirms the viability of our low-power, resource-efficient FPGA-based implementation for executing the dual quad-bit S-Box operations and other AES-related functions discussed in the software implementation section.

4.2.1. Verification and Security Measurement Criteria

The verification process incorporates several crucial security measurement criteria to ensure the robustness and reliability of cryptographic algorithms. These criteria include Time Security, which assesses the algorithm's resilience over time against evolving attack methods. The NIST Tests are a suite of standards provided by the National Institute of Standards and Technology, used to evaluate various security aspects of cryptographic systems. Lastly, the Avalanche Effect measures the sensitivity of the output to small changes in the input, ensuring that a slight alteration in the input significantly changes the output, thus enhancing the security of the cryptographic algorithm.

Time Security

A brute force attack, also known as exhaustive search, is a cryptographic hack that attempts to guess all possible variations of a targeted password until the correct one is found [25]. The complexity of the password significantly impacts the number of variations that need to be tested. Brute force attacks can be time-consuming and difficult, especially when tactics such as data obfuscation are used. However, if the password is weak, this approach can take only seconds with minimal effort. Time security is measured by the time taken by the system to resist a brute-force attack. The longer it takes for an attacker to succeed, the more secure the system is. Table 3 presents the time security measurements, indicating the robustness of our proposed algorithm against brute-force attacks.

Table 3. Time Security.

Key Size	Possible Sequences	Key Size	Possible Sequences
1 bit	2	32 bit	4,294,967,296
2 bit	4	64 bit	1.8447×10^{19}
4 bit	16	128 AES	3.403×10^{38}
8 bit	256	192 AES	6.278×10^{57}
16 bit	65,536	256 AES	1.158×10^{77}

NIST Tests

The National Institute of Standards and Technology (NIST) provides a suite of statistical tests to evaluate the randomness and security of cryptographic algorithms. These tests include assessments for frequency, runs, and autocorrelation. Passing the NIST tests indicates that the encryption method produces statistically random and secure outputs against various cryptographic attacks. For the SP 800-38A AES algorithm, the Advanced Encryption Protocol Algorithm Validation Scheme (AESAVS) sets validation evaluation parameters for electronic codebook (ECB) [26].

The proposed Substitution Box (S-Box) was rigorously tested as an alternative to the traditional AES S-Box across 37 distinct test cases, ensuring robust encryption and decryption. These tests spanned various AES-128 block operations, key sizes (192 and 256-bit), and modes, including Cipher Block Chaining (CBC), Propagating Cipher Block Chaining (PCBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes, as shown in Tables 4 and 5. Each category assessed encryption/decryption accuracy, handling of different initialization vectors (IVs), block padding, and longer messages. Additionally, the overall module functions were validated for data integrity, randomness, and absence of key/message data in ciphertext. The successful completion of all tests suggests the proposed S-Box is a reliable alternative to the traditional AES S-Box. These parameters ensure that the AES implementation meets the required security standards and performs reliably across different encryption modes.

Table 4. NIST Test FIPS-197-AES.

Key-256 → 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f	
Method	AES 256 with Traditional S-Box
Plaintext	00112233445566778899aabbccddeeff
Ciphertext	8ea2b7ca516745bfeafc49904b496089
Deciphertext	00112233445566778899aabbccddeeff
Method	AES 256 with Proposed S-Box
Plaintext	00112233445566778899aabbccddeeff
Ciphertext	919f31a520a96bcf03693ed089674d18
Deciphertext	00112233445566778899aabbccddeeff

Table 5. Test Results for Various Modes.

Test Case	Status
Block Tests (Raw AES-128 Block Operations)	
Test Success	Passed
Test with Incorrect Key	Passed
Test with Expected Value	NA [1]
Key Sizes Tests (192- and 256-bit Keys)	
Test 192-bit Key	Passed
Test 256-bit Key	Passed
Test Expected Values for 192-bit Key	NA [1]
Test Expected Values for 256-bit Key	Passed [2]
CBC Tests (AES-128 in CBC Mode)	
Single Block Test	Passed
Test with Incorrect IV [3]	Passed
Test with Different IV [3]	Passed
Test with Whole Block Padding	Passed
Long Message Test	Passed
PCBC Tests (AES-128 in PCBC Mode)	
Single Block Test	Passed
Test with Incorrect IV [3]	Passed
Test with Different IV [3]	Passed
Test with Whole Block Padding	Passed
Long Message Test	Passed
CFB Tests (AES-128 in CFB Mode)	
Single Block Test	Passed
Test with Incorrect IV [3]	Passed
Test with Different IV [3]	Passed
Test with Whole Block Padding	Passed
Long Message Test	Passed
OFB Tests (AES-128 in OFB Mode)	
Single Block Test	Passed
Test with Incorrect IV [3]	Passed
Test with Different IV [3]	Passed
Test with Whole Block Padding	Passed
Long Message Test	Passed
CTR Tests (AES-128 in CTR Mode)	
Single Block Test	Passed
Test with Incorrect IV [3]	Passed
Test with Different IV [3]	Passed
Test with Whole Block Padding	Passed
Long Message Test	Passed
Other Tests	
Test Success	Passed
Long Message Test	Passed
Sanity Test	Passed
Randomization Test	Passed
Integrity Test	Passed

[1] Not Needed with Proposed S-Box. [2] With Proposed S-Box and Cipher Test is 919f31a520a96bcf03693ed089674d18. [3] Initialization Vector.

Avalanche Effect

The avalanche effect is a critical property of cryptographic systems. It ensures that a slight alteration in the input, such as flipping a single bit in the plaintext, results in a significant change in the output, typically at least 50%. This drastic change is essential for maintaining security because, without it, the ciphertext could be easily predicted or broken through brute force attacks. To compute the avalanche effect [27] of AES with the proposed

S-Box, we keep the encryption key constant in each experiment and change the plaintext by one bit. The percentage of bits changed in the output (ciphertext) is then calculated using Equation (11):

$$Avalanche\ Effect\ \% = \frac{Hamming\ Distance}{Block\ Size} \times 100\%, \quad (11)$$

where the Hamming distance is the number of bits that differ between the original ciphertext and the ciphertext resulting from the modified plaintext, and the block size is the total number of bits in the block. By calculating the avalanche effect using this method, we can assess the sensitivity and robustness of the AES algorithm with our proposed S-Box design. A high avalanche effect value confirms that our encryption method is highly secure. It ensures that any small change in the plaintext results in a substantially different ciphertext, thereby providing strong resistance against cryptanalytic attacks. Table 6 shows that a single bit flips in plaintext while keeping a constant key shows a notable bit variance in the ciphertext.

Table 6. Avalanche Effect.

Key 256-bit → 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f			
Initial NIST Test Vector		$\mathbf{d_H}$	**%**
Plaintext Ciphertext	00112233445566778899aabbccddeeff 919f31a520a96bcf03693ed089674d18	81	63.28
Plaintext Ciphertext	00112233445566778899aabbccddeefe a26dbb8e917230cae3e67384236cb717	98	76.56
Plaintext Ciphertext	00112233445566778899aabbccddeef9 0768b49f924bfc5b31bec03ce6cafee2	80	62.50
Plaintext Ciphertext	00112233445566778899aabbccddeef7 e541175d1f73ba767cdf58afc2d5b970	85	66.40
Plaintext Ciphertext	00112233445566778899aabbccddeefc 39d26de07c32d84d882bf89a5ed250e0	89	69.53

4.2.2. RTL Synthesis Using ZedBoard Zynq 7000 SoC

The proposed forward and backward S-Box architectures are synthesized and evaluated on the ZedBoard Zynq 7000 SoC to leverage its advanced FPGA capabilities. The designs were developed and synthesized using the Xilinx Vivado Design Suite 2018.3, utilizing the Verilog HDL. The RTL synthesis results, summarized in Table 7, highlight the efficiency and performance of the proposed architectures. The proposed forward S-Box and backward S-Box architectures have been meticulously designed to maximize area efficiency, ensuring that the circuit occupies the least possible space on the FPGA while maintaining high performance and security standards. The forward S-Box architecture utilizes only 20 Slice LUTs, 8 Slices, and 20 LUTs as Logic, whereas the backward S-Box employs 28 Slice LUTs, 12 Slices, and 28 LUTs as Logic. This minimal resource utilization is significant, as it allows for the implementation of additional functions or the integration of more S-Box instances within the same silicon area, thereby enhancing the encryption system's overall throughput. Moreover, the innovative resource-sharing approach in the proposed VLSI architecture further contributes to area efficiency. By reusing components for both the forward S-Box and backward S-Box operations, such as isomorphic mapping and affine transformations, the design reduces the need for duplicate hardware. This saves space, minimizes power consumption, and potentially increases the operational speed due to reduced signal propagation delays.

Table 7. RTL Synthesis Summary.

Resource	Slice LUTs	Slices	LUT as Logic	Bonded IOB
S-Box Forward	20	8	20	64
S-Box Backward	28	12	28	64

The proposed design was implemented on the Zynq 7000 ZedBoard, as depicted in Figure 8. The virtual input/output (VIO) IP core was used to monitor the internal signals of the design, facilitating real-time observation and debugging. The ZedBoard evaluation board utilizes a Zynq 7000 SoC XC7Z020-CLG484-1 chip, which features two ARM Cortex-A9 cores and a Zynq 7000 FPGA. The FPGA substrate is connected directly to the device's main memory via AXI ports, enabling efficient data transfer and processing. In this implementation, algorithms or RTL modules involving intensive computations are executed on the FPGA, while control components that do not require heavy computation are handled by software running on the processor side. This hybrid approach leverages hardware and software strengths, ensuring optimal performance and resource utilization. After integrating the VIO core with the AES core featuring the proposed S-Box, the standard NIST test vectors, as listed in Table 4, were used as input data to the AES module. This allowed for the encryption and decryption of plaintext data, effectively validating the design's functionality. As shown in Figures 9 and 10, the plaintext was successfully converted into ciphertext and subsequently back into deciphered text, confirming the correctness of the encryption and decryption processes.

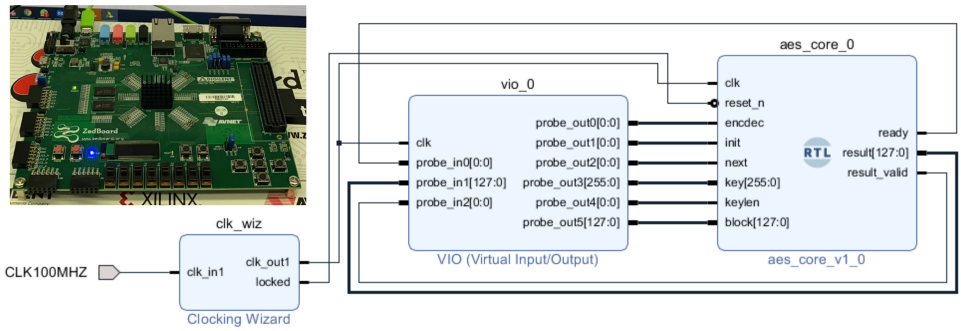

Figure 8. Our hardware setup for testing proposed forward and backward S-Box in AES Core on FPGA and its simulation with VIO.

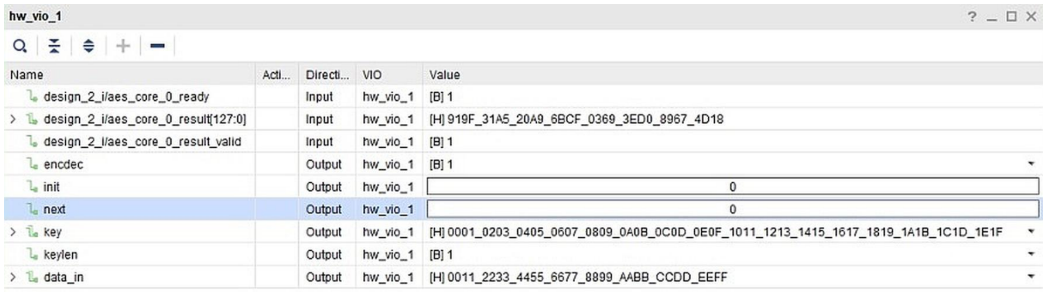

Figure 9. Encryption Result on ZedBoard Zynq 7000 SoC Hardware.

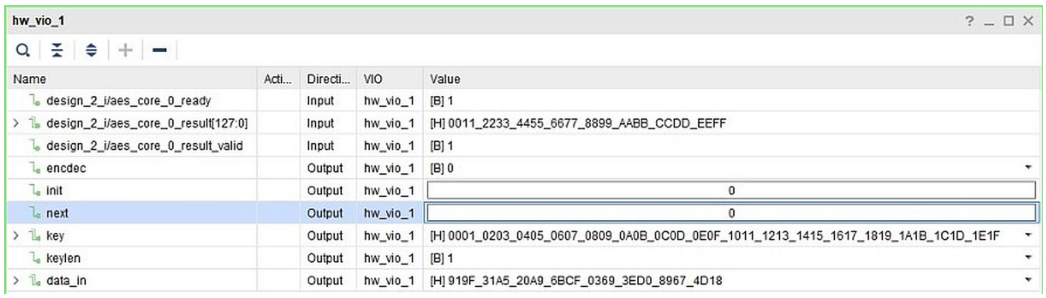

Figure 10. Decryption Result on ZedBoard Zynq 7000 SoC Hardware.

4.2.3. Front-End Design (Synthesis on 65 nm CMOS Technology)

In this section, we present the outcomes of implementing the novel S-Box architecture and analyze its performance metrics. The initial stage in the front-end IC design flow involves finalizing the design specifications and microarchitecture. During the RTL coding phase, the dual quad-bit forward and backward S-Box modules are modeled in Verilog HDL using synthesizable constructs. These constructs enable the RTL model to be input into logic synthesis software, which subsequently maps the RTL design to an actual gate-level implementation. The design was synthesized using TSMC's 65 nm standard cell technology library within the Cadence Genus Synthesis Solution version 15.2. The synthesis process utilized typical case parameters of 0.72 V and 25 °C to determine timing, area, and power metrics while incorporating design constraints. It is important to note that comparing power usage across different standard cell libraries can be challenging. However, our design can be compared to other related works implemented on 65 nm technology. Power consumption for the design is calculated using the formula $P = CV^2f$ [28], where C is the load capacitance, V is the supply voltage, and f is the clock frequency. These factors significantly impact power consumption. The synthesis was performed under worst-case operating conditions with a 10% delay tolerance at both input and output.

The synthesized design results are summarized in Table 8 as follows: the technology node employed is 65 nm CMOS, ensuring a balance between performance and power efficiency. The design consists of 80 standard cells, indicating a compact implementation, with a total cell area of 199 square micrometers, reflecting efficient use of silicon real estate. The design achieves a delay of 377 ps, meeting the required timing constraints under typical operating conditions. The leakage power is measured at 1111.12 nW, indicating minimal power dissipation when the circuit is inactive. In comparison, the dynamic power consumption is 27,511.52 nW, optimized considering the effects of load capacitance, supply voltage, and clock frequency.

Table 8. ASIC Synthesis Summary.

Technology Node	No of Cells	Cells Area	Delay (ps)	Leakage Power (nW)	Dynamic Power (nW)
65 nm	80	199	377	1111.12	27,511.52

In this section, we integrated our proposed forward and backward S-Box with the traditional AES Core, performed a PPA (Power, Performance, and Area) analysis of the holistic design, and compared the results with the traditional design. Approximately 99.13% of the design is occupied by the main subblocks of the AES modules, such as the AES core, encipher block, decipher block, and key-register. At the same time, the forward and backward S-Box consume only 0.87% of the total area. In contrast, in the traditional AES design, the S-Box and inverse S-Box constitute 13.62% of the total area. As observed in Table 9, in AES chip design, the area sum of the S-Box is not dominant; the main AES core and key register typically occupy the highest section of the overall area due to the high area demand of flip-flops. Integrating our optimized forward and backward S-Box demonstrates a significant reduction in the area they occupy, thereby contributing to an overall more

efficient design. This efficiency gain is crucial for applications where silicon real estate is at a premium. By reducing the area occupied by the S-Box and inverse S-Box, we free up space for other critical components or allow for more compact chip designs, enhancing the feasibility of the AES algorithm in resource-constrained environments. Furthermore, the reduction in area benefits the physical size of the chip and can also lead to improvements in power consumption and heat dissipation, as fewer resources are required to perform the same cryptographic functions.

Table 9. Area Comparison.

Modules	No of Cells	Cell Area (μm^2)
AES (TOP)	8742	45,497
AES_Core	8083	40,087
Key-Register	4928	28,951
Encipher Block	1272	4968
Decipher Block	1619	5430
S-Box Forward	80	199
S-Box Backward	65	197

Moreover, it can be observed in Table 10 that the power consumption of the S-Box forward and S-Box backward is also not dominant within the AES module. These subblocks consume significantly less power than other AES design subblocks. This further underscores the efficiency of our proposed forward and backward S-Box architecture regarding area and power utilization. The optimization of the forward and backward S-Box not only reduces their footprint but also minimizes their power draw, contributing to a more power-efficient overall design. This is particularly important in applications where power efficiency is critical, such as mobile devices, embedded systems, and IoT devices. The lower power consumption of these components means that the AES module can operate more sustainably and with less thermal output, enhancing its suitability for various applications.

Table 10. Power Comparison.

Modules	Leakage Power (nW)	Dynamic Power (nW)	Total Power (nW)
AES	13,633.793	624,802.210	638,436.002
Core	11,914.233	540,788.402	552,702.635
Key Register	8691.414	328,577.084	337,268.498
Encipher Block	1487.924	53,063.055	54,550.979
Decipher Block	1545.308	155,435.421	156,980.729
S-Box Forward	54.798	0.00	54.798
S-Box Backward	66.078	2874.219	2940.297

The comparative analysis of the hardware implementation of the proposed AES module with the traditional AES module demonstrates a significant reduction in area, power, and delay. As shown in Tables 9 and 10, our proposed design of the S-Box occupies less area, consumes less power, and incurs less gate delay compared to similar studies using the same technology. Specifically, the AES module incorporating our proposed S-Box exhibits 12.866% less area, 3.00122% less power, and 35.9642% less latency than the AES module with the traditional S-Box, as presented in Table 11. These improvements indicate the effectiveness of our design optimizations. The substantial decrease in area implies that more space is available for other critical components or for reducing the overall chip size, which is beneficial for compact and resource-constrained applications.

Table 11. Comparison of AES with Traditional S-Box vs. AES with the Proposed S-Box.

65 nm Tech Node	Cells	Area (mm^2)	Power (µW)	CPD (ns)
Traditional AES S-Box	12091	52.215	658.2	9.832
Proposed S-Box	8742	45.497	638.446	6.296
Optimization %	27.698%	12.866%	3.001%	35.964%

4.2.4. Physical ASIC Design

The layout of the AES core with the proposed forward and backward S-Box is illustrated in Figure 11. The core design area occupies 65,023.56 μm^2, excluding power rings and IO rings. The total die size of the chip, including IO rings and power rings, is 99,223.46 μm^2, with a utilization rate of 70%.

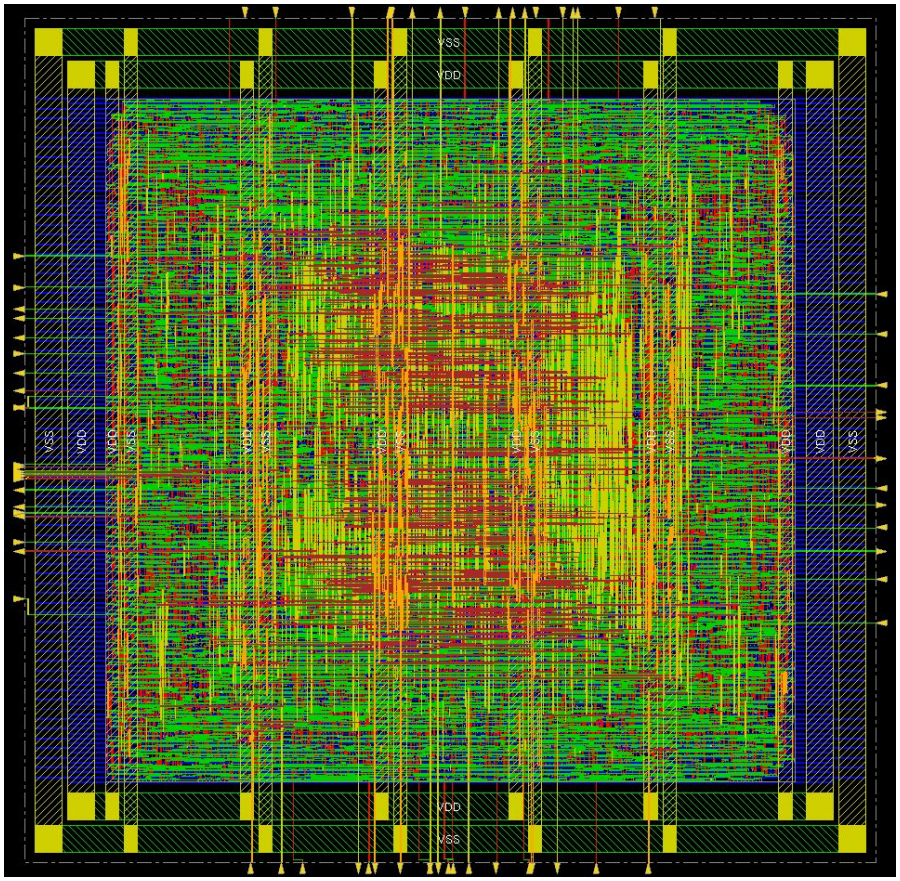

Figure 11. Physical layout of the proposed S-Box AES Core using 65 nm technology.

We employed the Cadence Innovus implementation system version 15.2 for the standard place and route optimization. This tool facilitates the efficient placement and routing of standard cells, ensuring that the design meets all physical and timing constraints while optimizing for area, power, and performance. The high utilization rate of 70% indicates an efficient layout that maximizes the use of available silicon area, minimizing wasted space and enhancing overall chip performance.

4.2.5. Comparative Discussion

The implementation results of the proposed S-Box, as presented in Table 12, demonstrate a clear advantage over existing methods across several key parameters, particularly in terms of area efficiency, processing speed, and overall power efficiency. The proposed design achieves the smallest area footprint at 199 μm^2 and 80 Gate Equivalents (G.E.), significantly outperforming other implementations such as those by D. Canright et al., J.

Boyar et al., and R. Ueno et al., which have larger area requirements. This compact design is beneficial for integration into larger systems where space is a critical consideration. In terms of processing speed, the proposed S-Box shows the lowest Critical Path Delay (CPD) at 0.377 ns, indicating a faster processing capability compared to other methods, which have CPD values ranging from 0.447 to 7.322 ns. This makes the proposed design highly efficient for high-speed cryptographic applications. Power consumption is another area where the proposed S-Box excels, with a consumption of 28.623 microwatts, which is relatively lower than most of the existing methods. Although N. Ahmad et al. report a very low power consumption of 0.09 microwatts, their implementation suffers from a high CPD, making it less competitive overall. The proposed design also achieves the lowest Power Area Product (PAP) at 30.16 $\mu W \cdot m^2$ and the lowest Power Delay Product (PDP) at 10.791 $\mu W \cdot ns$, indicating an optimal balance between power efficiency and performance. These metrics highlight the superior efficiency of the proposed S-Box in terms of both power and speed, making it a suitable candidate for energy-efficient cryptographic operations. When considering the implementation by Y. Teng et al., it is important to note that their work is based on a 40 nm technology node, different from the 65 nm technology used in the other studies. Despite this, Y. Teng et al.'s design has a significantly larger area at 593.31 μm^2. The absence of CPD, Power, PAP, and PDP values for their implementation limits a direct comparative analysis. However, the substantial difference in area suggests that the proposed S-Box is far more compact and likely more efficient overall.

Table 12. Implementation Results of the Proposed S-Box and Other Existing Methods.

65 nm Works	Area (μm^2)	Area (G.E)	CPD (ns)	Power (μW)	PAP ($\mu W \cdot \mu m^2$)	PDP ($\mu W \cdot ns$)
D. Canright et al. V1 [12]	433.68	208.5	1.287	42.125	268.422	54.231
D. Canright et al. V2 [12]	416	200	1.252	41.023	250.562	51.394
J. Boyar et al. [13]	479.44	230.5	0.960	44.020	221.386	42.279
N. Ahmad et al. [4]	288	-	7.322	0.09	2108.73	0.658
R. Ueno et al. [14]	533.52	256.5	0.831	48.178	213.153	40.036
J. Boyar et al. [13]	466.96	224.5	0.956	-	214.742	40.867
R. Masoleh et al. [5] V1	391.04	188	1.080	39.930	203.20	43.157
R. Masoleh et al. [5] V2	432.64	208	0.779	42.750	162.177	33.332
B. Rashidi et al. [7]	-	209	0.447	-	93.423	-
Y. Teng et al. [17] [1]	593.31	-	-	-	-	-
Proposed	199	80	0.377	28.623	30.16	10.791

[1] This work is implemented in 40 nm. PAP: Power Area Product, PDP: Power Delay Product.

5. Conclusions

The S-Box is the core component in a cipher block that ensures the credibility of the AES. Designing the most efficient architecture for the S-Box should be a primary focus to achieve optimal cryptographic performance. This research proposed an energy-efficient and area-delay optimized forward and backward S-Box for use in lightweight cryptography. We demonstrated the software implementation of the S-Box in Python to perform statistical analysis of the security measures and reviewed the proposed design properties. Furthermore, we integrated our proposed S-Box into the AES core for efficient hardware implementation and compared the gate area, power, and delay with other methods. The dual quad-bit forward and backward S-Box were designed and implemented using efficient VLSI circuits. The ASIC implementation of the AES core with the proposed S-Box was carried out in a 65 nm CMOS standard cell library. The results proved optimal compared to other methods, showing that our proposed S-Box utilizes fewer hardware resources and achieves a lower critical path delay (CPD) than other S-Box architectures. The results indicate that our proposed S-Box not only consumes low hardware resources but also

provides lower delay and power consumption, making it an optimal choice for lightweight block ciphers. The dual quad-bit S-Box structure enhances security levels, outperforming the traditional AES S-Box and other existing methods. Therefore, the proposed design is highly suitable for applications requiring efficient and secure cryptographic solutions. To enhance privacy in blockchain systems like Blockshare, our method can integrate homomorphic encryption for secure computations on encrypted data, Zero-Knowledge Proofs (ZKPs) for data integrity verification without disclosure, and differential privacy for protecting individual data points. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) can improve identity management, reducing reliance on centralized authorities. These methods can also be applied to systems like VQL and VChain+ for secure cloud queries and improved data privacy. Our S-Box design, with its robust cryptographic properties and hardware efficiency, supports these advancements, enhancing security and resource efficiency in privacy-preserving protocols.

Author Contributions: Conceptualization, M.B.A.D. and O.T.; methodology, M.B.A.D.; software, M.B.A.D.; hardware implementation, O.T. and M.B.A.D.; RTL design and verification, M.B.A.D. and O.T.; ASIC synthesis, O.T.; ASIC physical design, O.T.; validation, O.T. and M.B.A.D.; security analysis, M.B.A.D. and O.T.; resources, O.T.; data curation, O.T.; writing—original draft preparation, O.T. and M.B.A.D.; writing—review and editing, M.B.A.D. and O.T.; visualization, M.B.A.D.; supervision, D.H. and O.T.; project administration, D.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. *Advanced Encryption Standard (AES)*; FIPS PUB 197; FIPS Publications: Washington, DC, USA, 2001.
2. Hussain, I.; Shah, T.; Mahmood, H.; Gondal, M.A. A projective general linear group based algorithm for the construction of a substitution box for block ciphers. *Neural Comput. Appl.* **2012**, *22*, 1085–1093. [CrossRef]
3. Hwang, D.D.; Schaumont, P.; Tiri, K.; Verbauwhede, I. Securing embedded systems. *IEEE Secur. Priv. Mag.* **2006**, *4*, 40–49. [CrossRef]
4. Ahmad, N.; Rezaul Hasan, S. Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using Novel XOR Gate. *Integration* **2013**, *46*, 333–344. [CrossRef]
5. Reyhani-Masoleh, M.; Taha, D.; Ashmawy. New area record for the AEScombined S-box/inverse S-box. In Proceedings of the 25th IEEE Symbosium on Computer Arithmetic, Amherst, MA, USA, 25–27 June 2018; pp. 145–152.
6. Artuğer, F.; Özkaynak, F. A Novel Method for Performance Improvement of Chaos-Based Substitution Boxes. *Symmetry* **2020**, *12*, 571. [CrossRef]
7. Rashidi, B. Compact and efficient structure of 8-bit S-box for lightweight cryptography. *Integration* **2021**, *76*, 172–182. [CrossRef]
8. Preneel, B. *Understanding Cryptography: A Textbook for Students and Practitioners*; Springer: London, UK, 2010.
9. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
10. Khani, H.; Javadi. Using Cipher Key to Generate Dynamic S-Box in AES Cipher System. *Int. J. Comput. Sci. Secur. (IJCSS)* **2012**, *6*, 19–28.
11. Mohamed, K.; Pauzi, M.N.M.; Ali, F.H.H.M.; Ariffin, S.; Zulkipli, N.H. Study of S-box properties in block cipher. In Proceedings of the 2014 International Conference on Computer, Communications, and Control Technology (I4CT), Langkawi, Malaysia, 2–4 September 2014; pp. 362–366.
12. Canright, D. A very compact s-box for AES. In Proceedings of the 7th International Conference on Cryptographic Hardware and Embedded Systems, CHES'05, Edinburgh, UK, 29 August–1 September 2005; pp. 441–455. [CrossRef]
13. Boyar, J.; Peralta, R. A Small Depth-16 Circuit for the AES S-Box. In Proceedings of the Information Security and Privacy Research, Heraklion, Greece, 4–6 June 2012; Gritzalis, D., Furnell, S., Theoharidou, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 287–298.
14. Ueno, R.; Homma, N.; Sugawara, Y.; Nogami, Y.; Aoki, T. Highly Efficient GF(28) Inversion Circuit Based on Redundant GF Arithmetic and Its Application to AES Design. In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2015, Saint-Malo, France, 13–16 September 2015; Güneysu, T., Handschuh, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 63–80.
15. Boyar, J.; Find, M.G.; Peralta, R. Small low-depth circuits for cryptographic applications. *Cryptogr. Commun.* **2019**, *11*, 109–127. [CrossRef]

16. Reyhani-Masoleh, A.; Taha, M.; Ashmawy, D. Smashing the Implementation Records of AES S-box. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *2018*, 298–336. [CrossRef]
17. Teng, Y.T.; Chin, W.L.; Chang, D.K.; Chen, P.Y.; Chen, P.W. VLSI Architecture of S-Box With High Area Efficiency Based on Composite Field Arithmetic. *IEEE Access* **2022**, *10*, 2721–2728. [CrossRef]
18. Stoyanov, B.; Kordov, K. Image Encryption Using Chebyshev Map and Rotation Equation. *Entropy* **2015**, *17*, 2117–2139. [CrossRef]
19. Huang, X.; Ye, G. An Image Encryption Algorithm Based on Time-Delay and Random Insertion. *Entropy* **2018**, *20*, 974. [CrossRef] [PubMed]
20. Wu, X.J.; Wang, K.S.; Wang, X.Y.; Kan, H.B. A Novel Approach to Data Security in Cloud Computing. *J. Inf. Secur.* **2017**, *8*, 123–135.
21. Khalifa, N.; Benrejeb, M. On nonidentical discrete-time hyperchaotic systems synchronization: Towards secure medical image transmission. In *Recent Advances in Chaotic Systems and Synchronization*; Boubaker, O., Jafari, S., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 329–349.
22. Zhai, Y.; Lin, S.; Zhang, Q. Improving Image Encryption Using Multi-Chaotic Map. In Proceedings of the Workshop on Power Electronics and Intelligent Transportation System, Guangzhou, China, 4–5 August 2008; pp. 143–148.
23. Sara, U.; Akter, M.; Uddin, M.S. Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *J. Comput. Commun.* **2019**, *7*, 8–18. [CrossRef]
24. Shahrouzi, S.N.; Perera, D.G. HDL Code Optimizations: Impact on Hardware Implementations and CAD Tools. In Proceedings of the 2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, Canada, 21–23 August 2019; pp. 1–9.
25. Al-Mamun, A.; Rahman, S.S.M.; Shaon, T.A.; Hossain, M. Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte. *Int. J. Comput. Netw. Commun.* **2017**, *9*, 69–88. [CrossRef]
26. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. *A Statistical Test Suite for Random And Pseudorandom Number Generators for Cryptographic Applications*; US Department of Commerce, Technology Administration, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001; Volume 22.
27. Upadhyay, D.; Gaikwad, N.; Zaman, M.; Sampalli, S. Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications. *IEEE Access* **2022**, *10*, 112472–112486. [CrossRef]
28. Shahbazi, K.; Ko, S.B. Area-Efficient Nano-AES Implementation for Internet-of-Things Devices. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 136–148. [CrossRef]