International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I8P128

Volume 72 Issue 8, 292-311, August 2024

Review Article

Design Advancements in Light-Weighted Symmetric Encryption for IoT applications on FPGA: Focusing on AES and DES Derivatives

Jasvir Singh Kalsi[1], Jagpal Singh Ubhi[2], Kota Solomon Raju[3]

[1,2]*Department of Electronics and Communication Engineering., SLIET Longowal.*
[3]*Aerospace Electronics & Systems Division, CSIR-NAL Bangaluru.*

[1]*Corresponding Author : jasvirkalsi@sliet.ac.in*

Received: 24 April 2024 Revised: 11 July 2024 Accepted: 31 July 2024 Published: 28 August 2024

Abstract *- The number of devices interconnected to share information in the Internet of Things (IoT) has seen an exponential rise in recent years. With the increase in complexity of the IoT network, the security of data is a major concern. Though strong security algorithms are available for conventional networking systems, these may not be directly used for IoT applications as resources are limited. Light-weight security algorithms are required for IoT applications. There are symmetric and asymmetric algorithms that are proposed from time to time by researchers to achieve a higher order of security, but these algorithms have to meet the requirements of resource-constrained devices at the IoT edge. This paper presents an overview of various research published in recent years, proposing the derivatives of symmetric algorithms using Rijndael-Cipher and Feistel-Cipher Structures. In conclusion, a proposal is also presented based on key generation that may be used to design a light weight security algorithm.*

Keywords *- AES, DES, Security algorithms, IoT security, FPGA.*

1. Introduction

Advances in the VLSI and IoT, alongwith communication technologies, led to a new era of intelligent technology usage in various automated processes in industry, health, housing and other day-to-day activities. These technologies use many sensors to control the actuators as per the application requirement. During this process lot of data is produced. This data has to be processed and transmitted to make useful service-oriented data using signal processing, AI, ML, DL and statistical dynamic learning techniques. Data transmission is one of the important issues not only to have reliable transmission and reception of the data but also to require safe and secured data through authentic and reliable modes or channels. To secure the data, providing encryption to data before transmission and decryption at the reception is one of the reliable solutions followed widely through various encryption techniques and standards. These encryption standards are broadly classified into symmetric and asymmetric. As per application requirements and available computational capabilities, symmetric or asymmetric standards, along with stream or block cipher processes, can be chosen to optimize the transmission of data securely [1]. On the other hand, IoT has mostly constrained devices at the edge node. A basic overview of the architecture is shown in Figure 1. These devices have very low data transmission rates along with larger transmission delays. Implementing the existing encryption techniques on power-constrained devices at the end node requires higher computational power, which increases the complexity and power usage. In addition to that, IoT devices are more vulnerable as far as hardware attacks are concerned since they are highly open and accessible to an intruder as compared to the other computing devices used for general purposes [2]. The limitations in implementation, along with the cost, make the design of a security platform for IoT devices quite a challenging task. Regardless of the limitations, IoT devices are bound to perform a required level of computation to provide security to the encryption algorithms [1][3]. The IoT end nodes are power-constrained with lower computational capabilities. Hence, the application of a high-performance security algorithm at transmission with a higher data rate and low latency is a challenge, even at 5G networks. To provide secure IoT solutions, the research community is looking at different aspects of secure communication by designing lightweight derivatives of existing algorithms which require less computation and are able to meet the constrained features of IoT devices and providing a reliable and robust hardware and software couplet [4]. Therefore, there is a dire need for lightweight security protocols and encryption techniques to be implemented. This paper aims to provide a systematic review of existing techniques of encryption, their complexity while being implemented at the edge node, and a birds-eye view of various techniques or variants of existing standards for IoT applications that are being proposed in the literature. The second section of the paper gives a detailed survey of the existing derivatives of the AES algorithm. The third section provides proposed algorithms from various authors based on the DES algorithm. A new key generation technique is also proposed in the future scope to provide an immediate option for constrained IoT applications.

2. Advanced Encryption Standard

Advanced Encryption Standard (AES) is an ISO/IEC 18033 symmetric encryption standard symmetric cipher and is one of the most used in data transmission for secure data transmission. AES encryption and decryption are frequently used in block-chaining modes of operation, such as cipher block chaining (CBC), cipher-based message authentication code (CMAC), and counter with CBC-MAC (CCM), for example, IEEE802.11 wireless LAN and EEE802.15.4 wireless sensor networks [4]. The basic AES algorithm flow diagram is shown in Figure 2. The parallel processing of key expansion and iterative execution rounds provides a secure ciphertext at the output. The implementation of the S-box is the most expensive as far as hardware is concerned. Moreover, the Key generation for each round also adds a significant amount of delay in the AES operation. Here, the integrity of transmission depends on the complexity and security of the key.

2.1. Discussion on Advancements in AES

A significant amount of work has been proposed by researchers in recent years in the development of light weighted security algorithm to be implemented over various layers of data transmission. Yu W. and Kose S. 2017 proposed a masking technique for implementing a false key-based AES to defend against the correlation power analysis attack (CPA) [1]. The authors proposed a WDDL (Wave Dynamic Differential Logic)- based XOR gate design. The work proposed to apply a false key to design and reconstruct using WDDL. The results showed that the minimum value of the measurement to disclose of proposed masked AES platform becomes over 150 million in case of CPA attacks as compared to the basic implementation of AES with negligible overheads to the performance [5]. The simulation results presented MTD (No. of measurements to disclose the secret key under first-order power analysis attack) analyses of the traditional AES-128, masked AES, and proposed WDDL-based AES. The results showed a power overhead of 2.4% and an additional delay of 2.55ns but provided a more secure environment as the IoT devices are highly vulnerable to hardware attacks, such for example CPA, with nearly no overhead [1].

U. Farooq and M.S. Aslam [6] implemented the operation of AES on FPGA in Block RAM (BRAM) mode and Configurable Logical Block (CLB) mode for the S-box and Key expansion process and found that there is an area-delay trade-off in AES implementation [6]. For faster operation parallel processing for S-box and Key Expansion leads to faster operations, but this requires more cache.

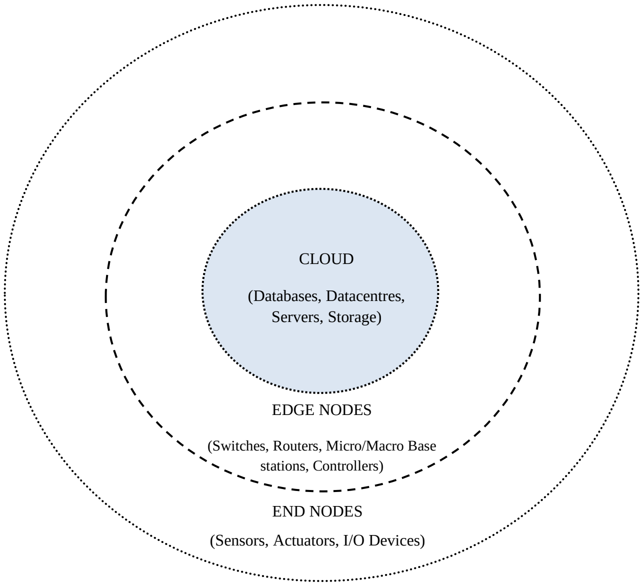


Fig. 1 Basic Cloud-Edge-End architecture of IoT

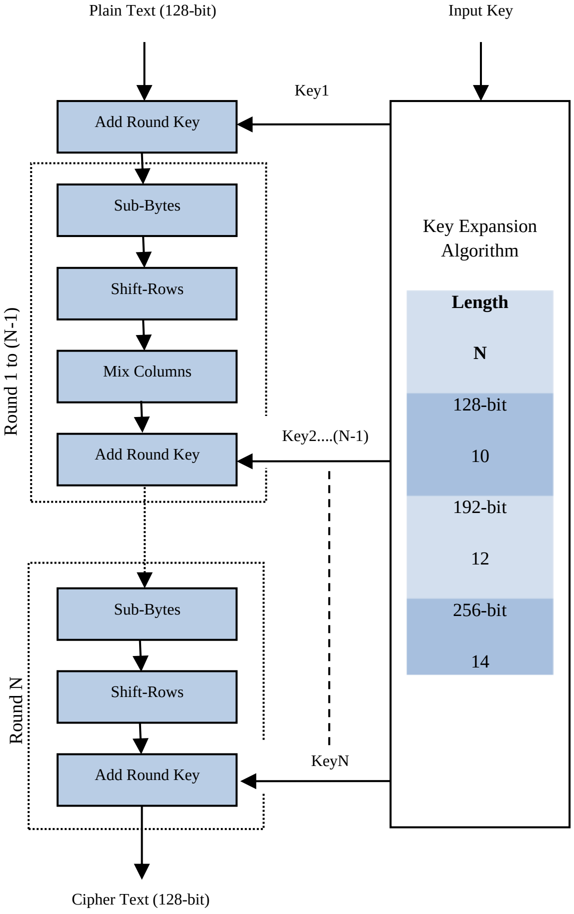


Fig. 2 AES Algorithm architecture [4]

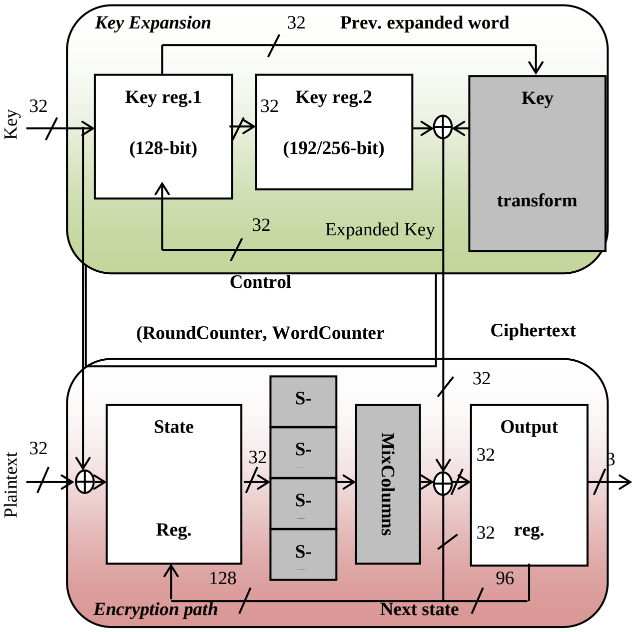


Fig. 3 A 32-bit datapath architecture [9]

The authors found that for remote applications best suitable mode of operations with the best resource usage and satisfactory throughput is to implement both algorithm processes in CLB mode [6]. In recent development trends, various authors have also designed lightweight block cipher algorithms based on reduction in memory footprints or software/hardware implementation such as PRESENT [7], but somewhere, the security or throughput is compromised. Mostly, they have been designed to have a smaller area of hardware and may have used more encryption rounds of smaller block sizes to lower the overhead, but this leads to lower throughput [8]. In 2017, Bui D.H. et al. presented an architecture based on a 32-bit datapath that supports multiple security levels through different key sizes, energy, and power optimization for key expansion and datapath [9]. AES can also be implemented using the hardware with the round-based, unrolled-round or pipeline architecture. Using a similar architecture, it is feasible to get a throughput of the range of Gb. The constraint of these platforms is majorly the higher power consumption. Such architectures are seldom suitable for embedded and constrained devices [8][9].

As the architecture of AES for computation is based on a 32-b instruction set, a major optimization in the process is a reduction in S-boxes. In round-based design, 20 S-boxes are required whereas, in the 32-b datapath, it uses only 4 (sharing with key expansion) or 8 (without sharing). The optimization in the datapath led to a power consumption of 20µW @ 0.6V [9]. In the process of designing lightweight security, the design should be rugged enough so that it maintains its data security and integrity when subjected to CRAs such as Jump-Oriented Programming (JOP) and Return-Oriented Programming (ROP) architecture approach of AES instruction set [10-12]. In 2017, Qiu P. et al. the authors presented and approach to design LEA-AES (Lightweight Encryption Architecture-AES) and evaluated it to measure the memory usage of the implementation and in-total run time. The proposed LEA-AES had, on average, a memory overhead of 0.62% with a loading-time overhead of 3.53%, along with a 3.19% run-time overhead [12]. A comparison was driven with the PUF method used by researchers but LEA-AES have a negligible architectural impact but is robust in the case of CRAs in Control Flow Integrity.

The robustness of the algorithm also depends upon the modes of operation of AES. In 2017, Fahd S. [13] derived an experimental comparison of the performance of Galois Counter Mode (GCM) with CPA against OFB (Output Feedback Mode), CFB Mode (Cipher Feedback Mode), CBC Mode (Cipher Block Chaining Mode), ECB Mode (Electronic Code Book Mode) and Counter Mode of operation of AES for SCA [14-19]. The AES is most vulnerable at counter mode last round leakage and lookup table access. The GCM is achieved by placing a parallel counter that provides a shield to the cipher counter, and the S-Box security is proposed by generating a Low SNR random S-Box with the help of a Pseudo-Random Number Generator (PRNG) proposed by Das S. [20] but again the memory requirement is to be compromised. This might enhance the security of IoT nodes from SCA but the hardware requirements and processor specifications are to be met.

Shahbazi K. et al., in 2017, designed an ASIP-based 32-bit cryptoprocessor for implementation of AES along with IDEA and MD5 on FPGA as Application Specific Integrated Circuits (ASIC) costs higher due to hardware approach rather than software approach designing on FPGAs [21,22]. The design allows the designer to use any of the encryption schemes and provides a higher order of secure data transmission as the information of the algorithm to generate cipher remains hidden from the intruder. Moreover, the authors have generated an instruction set for both general-purpose, i.e. common to all algorithms, and also specific purpose, i.e. algorithm-specific. This reduced the memory requirements as far as IoT applications are concerned, but the choice of encryption algorithm adds overhead to the process. The authors used the XC5VLX30 FPGA board, and have got the highest throughput at 166.916MHz frequency as compared to the same FPGA used by Mirzaee R.F. [23] and Granado J.M. [24]. Wang Y. et al. [25] used Stratix II GX hardware and got better results as compared to Shahbazi K. et al., but the highest operating frequency achieved was limited to 66.48MHz hence the design has better performance parameters as compared to the literature. Hoang V.P. et al. in 2017 designed ASIC based processor and have presented a comparison with existing literature, but the software approach presented by [21,23-25] provides better results. Moving on the same track, in 2018, Wanga P. [26] designed a crypto processor with improvements in the processes of inter-module interaction by putting the main emphasis on the encryption module and key extension module with the help of parallel and water technology [27]. The use of this technique enhanced the system operation speed, and the hardware encryption system achieved a more efficient and secure ciphertext generation process [26]. Strengthening the security of AES, Luo C. et al. [28] in 2018 has implemented XTS-AES (XEX-based tweaked-codebook mode with ciphertext stealing [29]) in an advanced mode, especially for sector-based storage devices such as hard disc devices or other solid-state discs. The feature of using two secret keys instead of one, along with an additional tweak used on each data block, makes the system highly resistant to SCAs and Crypto-analysis Attacks (CAs) [29]. The process was implemented on the SASEBOGII FPGA board. The analysis shows a successful and reliable implementation, but again, the delay and area requirements are to be compromised. This made the design unsuitable for IoT applications due to its complexity [28]. Another approach to strengthening the security of non-pipelined architecture AES was presented by Zodpe H. and Sapkal A. in 2018. The robustness of AES depends upon the security of the initial key as well as the s-box. The authors generated the S-box and initial key randomly using a PN sequence generator with the help of a Linear-Feedback Shift Register (LFSR), hence enhancing the strength of the cryptosystem [30].

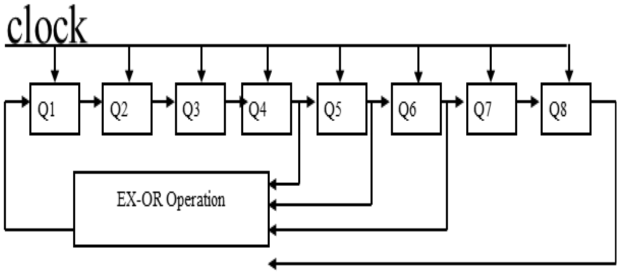


Fig. 4 An 8-bit PN sequence generator [30]

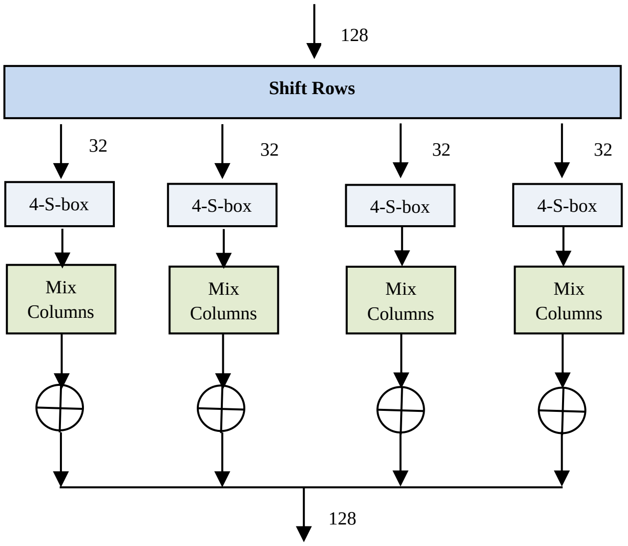


Fig. 5 AES Parallel architecture [32]

Although the different values of the generator polynomial can be selected, the authors used (8,6,5,4) taping to generate a random sequence. The algorithm was implemented on Spartan6 XC6SLX150-3FGG900 FPGA device, and throughput of 3.039 Gbps was achieved, achieving a 60% average percentage avalanche effect for the proposed AES as compared to traditional AES [30]. Although a higher degree of the strength of the key and s-box is achieved in the successful implementation of the proposed algorithm, it is observed that a system with higher computational configuration is required for the process. This makes the design unsuitable for remote nodes and sensors for IoT applications which require a light-weighted algorithm that must not only be secured in data transmission but also should not add overhead on the end and edge devices.

Approaching the lightweight characteristic and redefining parameters of AES, in 2018, Sheikhpour S. et al. proposed a High Throughput Fault Resilient AES (AES-HFA) in which parallel AES architecture is used. The proposed algorithm consists of four equivalent blocks followed by splitting each into two pipeline stages [31]. The authors inserted a single bit, multiple burst, and multiple random faults; the Fault Coverage (FC) would be 100 and 99.9939% for single and random faults, respectively [32].

The design implementations were tested on Virtex-5 (Xc5vlx110T), Virtex-6 (Xc6vcx130T), and Virtex-7 (Xc7vx330T, Xc7vx690T) FPGA families for evaluating parameters such as throughput, implementation area, maximum operating frequency, and power consumption. Even the proposed method is fast but it requires a heavier platform for computations. Moreover, the design is complex and needs a greater implementation area; hence power requirements are more as far as IoT applications are concerned. To make the process of AES more secure, authors such as Xu X. et al. [33] in 2014, Wan M. et al. [34] in 2015, and Kose S. et al. [35] in 2016 proposed and discussed Physical Un-clonable Function (PUF) based S-box architecture and in 2018 Yu W. et al. [36] presented a light-weighted masked AES-PUF architecture for high-security applications, especially for hardware-based authentication to avoid Side Channel Attacks (SCAs) and Machine-Learning Attacks (MLAs)[37-38].

The authors in [36] achieved 51.1% uniformity, 50.7% inter-hamming distance, and 98.1% reliability of the designed masked AES-PUF. Wei Y. et al. [39] also presented second-order threshold implementation of a masking AES architecture protecting the data against higher-order Differential Power Analysis (DPA). However, this ensures the security and integrity of the transmission of data without much overhead on the system but requires additional hardware for authentication that addon to the cost of the IoT edge and end. In 2019, the authors of [39] presented a new approach to optimizing the Mix-Column operation of AES. They used efficient mix column boolean expression using resource sharing architecture and Gate replacement technique in which the switching activity due to changing XOR gate is replaced by a combination of XOR, MUX, and OR gates, and redundant Look-Up-Table (LUT) bits are removed [39]. The architecture is implemented on Vertex-6 FPGA and evaluated for on-chip area and power. Total power is shown in Equation (1).

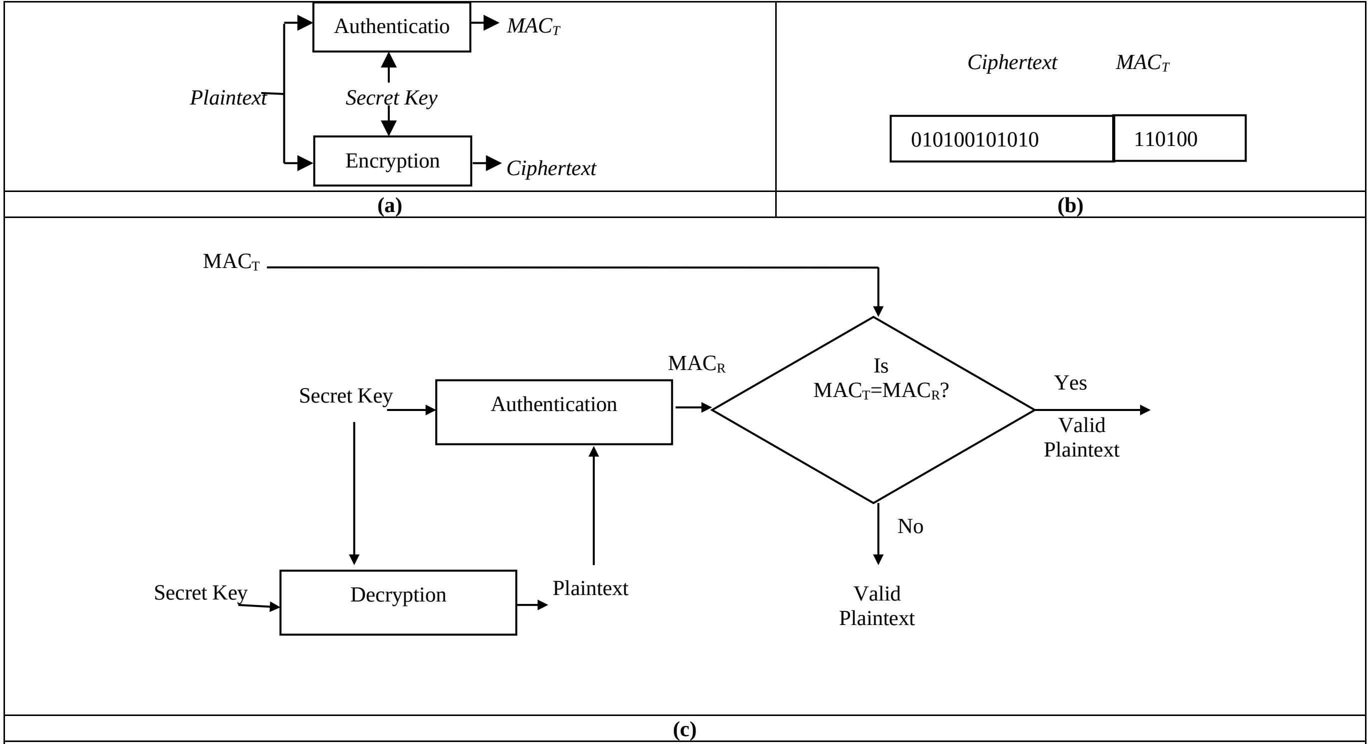
$$P_{total} = P_{switching} + P_{shortcircuit} + P_{leakage} .... (1)$$

With the optimization, the authors managed to reduce the $P_{switching;}$ hence, on-chip power consumption was reduced without overhead or any compromise in throughput [40].

Power optimization is one of the major concerns as far as IoT end devices, but due to on-chip resource sharing, delay is introduced in the process. In 2019, Pammu A. A. et al. designed an authentication-based parallel-encryption cum Matrix-transformation on an Asynchronous Multicore Processor (AMP-MP). Using the above method, the authors discussed the proposed algorithm for achieving a high throughput and highly secure AES that is based on Counter-Chaining Mode (AES-CCM) [41], shown in Figure 6. In Figure 6 (a), a Ciphertext, a Message Authentication Code (MAC), is generated and transmitted as a header of a message block, as shown in (b). At the receiver, again MAC is generated and is compared with the one sent from the receiver for authentication. In the concept, the encryption process involves operational computation at GF (28) for the transformation of 16 plain text. Due to this, the computation speed at the transmitter level and receiver level is jointly increased by a factor of 32 [41]. The process seems to be simple and verified by realizing it on an 8-bit asynchronous, 9-core processor (65nm CMOS technology node) and 13.54Gbps throughput is measured. As far as constrained IoT devices at the edge are concerned, the hardware might be able to cope with the design, but the hardware area, hence the power consumption, is increased.

This makes the design implementation at the IoT end a clumsy affair. A similar approach was followed in 2019 by Masoumi M. [42] and Lumbiarres-Lopez R. [43], in which they used a binary masking scheme in parallel to S-box substitution and implemented at a maximum clock frequency of 318.4 MHz on Virtex-5 FPGA but the area requirements and power consumption increases. Applying the same process, in 2019, Hameed M. E. et al. [44] designed a Lossless Compression and Encryption Mechanism (LCEM) for remote monitoring of ECG Data Using Huffman coding and Cipher-Block-Chaining Advanced Encryption Standard (CBC-AES). The designed application was robust, secure, and efficient but one has to compromise with the on-chip power consumption.

As discussed earlier, SCAs make use of emitted power for analyzing and reverting the steps or mathematical formulation of the process and extracting encryption keys. In 2019, Crocetti L. et al. [45] presented a software-based approach to avoid SCAs using Correlation and Differential-Power Analysis for the hardware-based implementations of AES architecture. Keeping in view the usage of random bitstreams, the authors made use of a True-Random-Number Generator (TRNG) based on [46].



(a) (b)

(c)

Fig. 6 (a) MAC generated at the Transmitter, (b) A message block, (c) MAC generated at the Receiver and authentication process [41]

The concept triggered a parallel operation-based Digital Ring Oscillator (DROs) that operates during the working of AES Core on an FPGA. The synthesis of the design was performed using the TRNG module on EP4SGX230KF40C2 (Intel FPGA platform), and then the required number sequence was gathered for enabling the AES core shown in Figure 7.

The work was partially funded by Intel Corporation (CG34441483) due to highly secure Ciphertext with almost no extra security hardware requirements, but a compromise on data transmission delay is concerned.

The IoT end nodes are already working at very low data transmission rates, and additional delay may cause undesirable results and data lag. Seghier A. et al. [47] 2019 proposed a method based on a key-dependent S-box cube, as shown in Figure 8. The process includes the construction of six S-boxes based on irreducible and distinct polynomials, and their selection is dependent on the key [48]. The S-BOXs are used in the selection during each round using the cube movement, which is being guided by a fragment of the round key process; hence, the initially selected S-BOX is processed using an around constant to generate a new S-BOX used in the operation [47].

In 2019, Shan W. et al. [49] introduced automated machine learning-assisted countermeasures for SCAs and implemented them on a 28-nm AES circuit. Although highly secure AES ciphertext is achieved, the process has the same problem as in [46-49]. The delay and complexity of the algorithm make it unsuitable for implementation at IoT nodes.

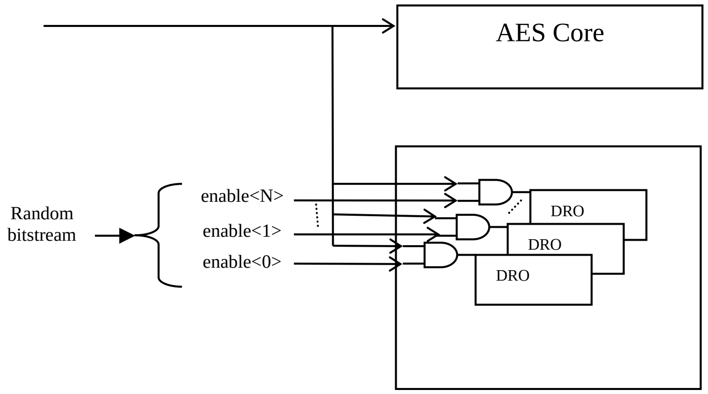


Fig. 7 High-level block diagram of the DROs based AES as a countermeasure against SCAs [45]

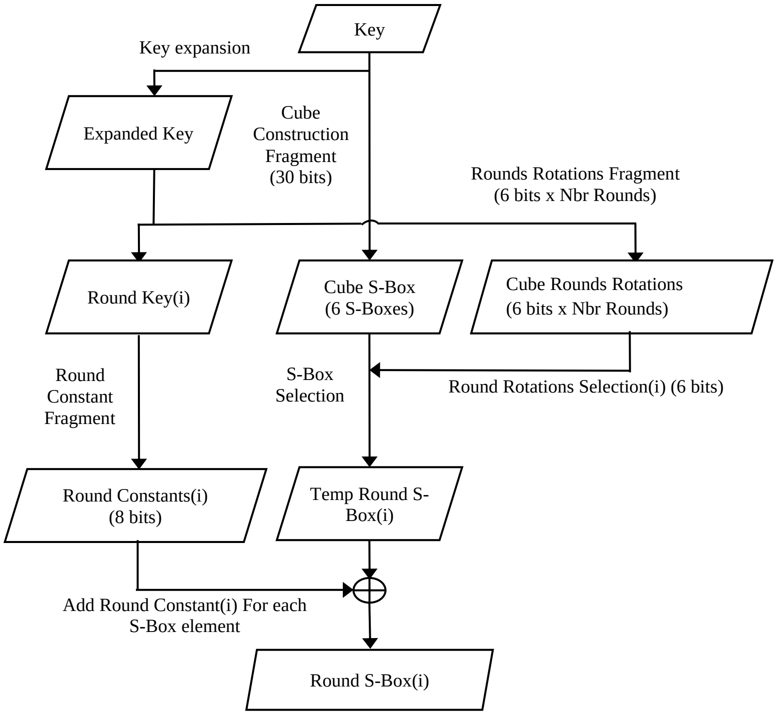


Fig. 8 Key-dependent S-Box selection AES architecture [47]

Although for minimizing power consumption, many authors have presented novel architectures, such as Nandan V. et al. in 2020, designed a low-power XOR gate-based design for AES algorithm consuming 45.5nW, which is much less as compared to the 692nW in actual AES design [50], even Kumar K. et al. in 2020 modified AES by skipping mix-column operation of traditional AES process [51]. The operation is validated on Artix-7 (xc7a200tlffg1156-2L) and Kintex-7 (xc7k160tffg676-2L) FPGAs, and there is a considerable improvement in the area required, power consumption as well as time delay hence increasing the throughput. The design was successfully tested for voice encryption. As far as security is concerned, the design is simpler and less secure for man-in-middle as well as SCAs. The authors suggested it for lightweight implementations such as constrained devices of IoT but at the risk of the security of data.

The literature published since 2015 showed a deviation of traditional AES encryption towards lightweight variants either by proposing parallel additions to existing processes or even modifications in the encryption-decryption. These led to an extensive emergence of variants, especially for power-constrained IoT devices and many works of literature since 2020 reflected the same. Recent publications presented concrete possible reflections of various threats which can occur in IoT networks. These may include a possibility but are not limited to replay attacks, man-in-the-middle attacks, impersonation in the network, Denial of Service (DOS), physically capturing IoT devices, privileged insider, and stolen-verifier attacks [52]. The various standards published for lightweight cryptographic standards, especially for IoT environments, are summarized in Table 1. Many researchers are not only working on the symmetric approach of the algorithm, but also the work is extended to design a lightweight security framework based on the asymmetric approach. Even Zeadally S. et al. [53] 2020 designed a mixed framework, not exactly combining or merging the symmetric and asymmetric approaches but near a parallel approach of implementation of both using different hardware.

This might be feasible as Zeadally S et al. [53] experimentally performed on the LPC1769 development board and UDOO Neo board under the "UMI-Sci-Ed (Exploiting Ubiquitous Computing, Mobile Computing and the Internet of Things to promote Science Education)" funded project (European Union's HORIZON 2020 research and innovation program under grant agreement No 710583). Following the research in [52][53], various researchers are looking for a hybrid algorithm based on both variants that must be lightweight, low cost, and compatible with IoT power-constrained devices with security be a major concern and without any compromise in it. Based on a similar concept, Hassan H. E. R. et al. 2020 proposed a robust Digital Right Management (DRM) based on a conflux of AES and ECC (Elliptical Curve Cryptography).

The basic proposed concept was based on partial encryption. The data was encrypted using AES-256, and the shared key was encrypted using the Elliptical Curve Diffie-Hellman (ECDH) and the Elliptic Curve Digital Signature Algorithm (ECDSA) used in the digital signature process. This Publisher-Server-Customer based approach was implemented on Audio and Video data files, and high performance is achieved keeping in view the author's right and precluding misuse of data in terms of altering and redistributing unauthorized persons. [54]. Still, these hybrid approaches need a great deal of hardware to be incorporated either at the edge or at the end layer, which not only makes the system complex and costly hence decreases the power backup as far as the IoT network is concerned. Extending the research further, to enhance security many algorithms are designed which are hardware-dependent [55][56]. The possibility of SCAs on a less secure IoT 8-bit microcontroller was implemented by Arpaia P. et al. in 2020 [57].

Table 1. Lightweight cryptographic standards for IoT environment [52]

Standard	Description
ISO/IEC–29192-1	"General information technology including security mechanisms, lightweight cryptography"
ISO/IEC–29192-2	"Information technology for security mechanisms, lightweight cryptography for block ciphers"
ISO/IEC–29192-3	"Information technology for security mechanisms, lightweight cryptography for stream ciphers"
ISO/IEC–29192-4	"Information technology for security mechanisms, lightweight cryptography for asymmetric techniques"
ISO/IEC–29192-5	"Information technology for security mechanisms, lightweight cryptography for hash functions"

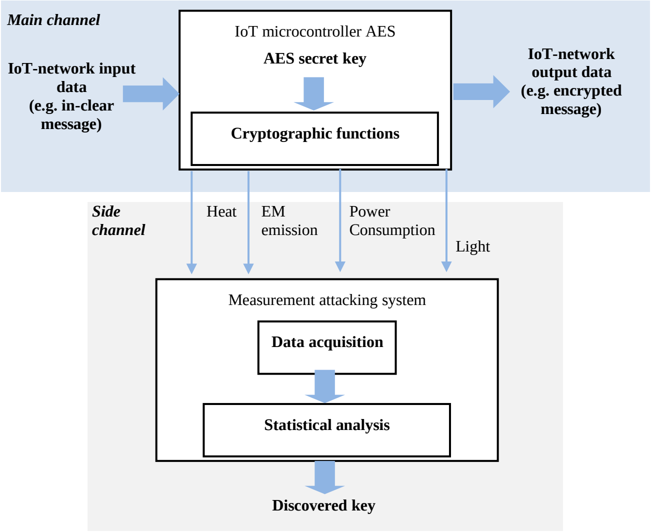


Fig. 9 A possible SCA on low secure IoT (8-bit) microcontroller [57]

The researchers used the TMS320F2803x series Texas Instruments controller for IoT application implementation and ARM Cotex (M4) based STM32F30x series for API sharing. The results showed the need for a highly secure system for IoT applications as the power-constrained devices are easily subjected to SCAs. Even Dhirendra et al. [58] presented a novel approach to performing the computational space for AES in the cloud. This led to a decrease in area requirements and power consumption transmitted at the cloud, which makes it vulnerable hence decreasing the security.

Moreover, as the frequency of the data communication between the edge and cloud is greater, it adds to a delay; hence, the process is not recommended for slow trans-receiving IoT applications. The researchers are looking forward to finding solutions to trade-offs between the parameters such as security, on-chip area, time delay, power consumption, and on-chip memory requirements as far as power and resource-constrained IoT devices [59-63].

In 2021, Shahbazi K. et al. [64] proposed a model to minimize the area requirements of IoT nodes. The authors used a reduced logic approach while implementing Vertex-6 FPGA. The shift-rows process is embedded inside the state register, the sub-byte block is shared with the key expansion process, and the 32-bit mix-column operation is divided into 4 phases of 8 bits each. Therefore, the add-round-key is processing byte by byte instead of a block of data. This reduces the memory requirement for the storage of results as 8-bit registers are used instead of 32-bit storage [64]. Although a great zeal of area reduction is nearly 15.5% and memory requirements are reduced this approach is a pipeline approach that adds delay in the process. Moreover, the computational facility may be available at the edge of the IoT framework but the scenario is different at the end devices.

A similar approach of area minimization is used in [4][65-67] but with a compromise either in power consumption or in delay for data encryption, hence resulting in a lag in the communication. On the other hand, research is going on to make data transmission faster, even for resource-constrained devices. The introduction of 5G technology may bridge this gap and narrows the boundaries of the trade-off between the power, area, and data transmission rate without any compromise in the security of plaintext or cipher. A similar approach was realized by Mamvong J et al. [68] to minimize the time delay and verified on ARM-Cortex M4-based ATECC608A controller for IoT applications. The authors reduced the number of rounds without adding to the security of the cipher; hence, there is a possibility of an attack and the integrity of the key and message.

In 2023, Proulx et al. [69] surveyed different attacks on low-power Xilinx AMD ZYNQ-7000 and Intel Startix-10 SoC boards and surveyed the possible physical layer attacks. The authors performed testing for Reverse Bitstream Engineering, Side Channel Attacks, Probing Attacks and Hardware Trojans using the AES algorithm. The authors discussed the use of low-power SoC modules based on ultra-scale technology for testing the algorithm. It was concluded that Physical security and active security measures play a significant role in protecting the device from malicious attacks [69,70].

Table 2. Performance comparison of recent development and implementation of the AES Algorithm

	Year	Encryption	HW/SW**	Technique	Arch.	Delay*	Area Req.*	Power Cons.*	Security
[1]	2017	AES-128	Cadance (CMOS)	WDDL-based XOR gates	Parallel	More (+2.55ms)	More (2.61%)	More (2.4%)	Enhanced
[6]	2017	AES-128	SPARTAN-6 VIRTEX-5	BRAM and CLB	Parallel	None	More	More	Enhanced
[9]	2017	AES-128/192/256	SNACk ST FDSOI (28nm)	32-bit datapath	Pipeline	More	More	More (+20μW)	Low
[12]	2017	AES-128	AES-128 built-in CPU	LEA-AES	Parallel	More (3.53%)	More (0.62%)	More	Low
[20]	2017	(AES/IDEA/MD5)	VERTEX-5 (XC5VLX30)	32-bit Crypto-processor	Parallel	More	More	More	Enhanced
[26]	2018	AES-128/192/256	QUARTUS-II	Parallel and Water operation	Parallel	Less	Less	More	Enhanced
[28]	2018	AES-128	FPGA (SASEBOG-II)	XTX-AES	Parallel	More	More	More	Enhanced
[30]	2018	AES-128	VIRTEX-6 (XC6XLX150)	Generation of Sbox using PN Sequence generator	Parallel	Less	More	More	Enhanced
[32]	2018	AES-128	VIRTEX-5 VIRTEX-6 VIRTEX-7	Fault Resilient	Parallel	Very Less	More	Less	Enhanced
[36]	2018	AES-128	Cadence (CMOS)	PUF based Sbox	Parallel	More	More	------	Enhanced

[37]	2018	AES-128	FPGA (SAKURA-G)	IInd order threshold PUF-based Sbox	Parallel	Less	More	------	Enhanced
[39]	2019	AES-128	VERTEX-6	Gate replacement technique	Parallel	More	Less	Less	------
[41]	2019	AES-128/192/256	Multicore ANoC (65nm)	Asynchronous Multicore Processor for AES-CCM	Parallel	Less	More	More	Enhanced
[42]	2019	AES-128	VIRTEX-5 (XC5vlx50)	Randomized SBox with a modified Boolean masking	Parallel	Less	More	More	Enhanced
[45]	2019	AES Core	Intel FPGA (EP4SGX230KF40C2)	Software-based approach (TRNG-Digital Ring Oscillator)	Parallel	More	Less	Less	Enhanced
[47]	2019	AES Core	VIRTEX-5	Key dependent Sbox generation	Pipeline	More	Less	More	Enhanced
[50]	2020	AES Core	Verilog	Use multiple gates instead of XOR (Low power Sbox with enhanced Galois-based transform)	Parallel	More	Less (10%)	Less (20%)	Low
[51]	2020	AES Core	ARTIX-7 KINTEX-7	Skipping MixColumn Operation	Parallel	Less	Less	Less	Very Low
[57]	2020	AES-128	TMS320F2803x series	Analyzing SCAs on less secure 8-bit IoT processor	Parallel	More	Less	More	Low
[58]	2020	AES-128	MATLAB	Cloud-based computational AES	Parallel	More	Less	-------	Very low
[63]	2020	AES-128	ESP8255	Eavesdropping and Brute-force attacks specifically, for IoT applications	Parallel	More (14.686ms)	-------	More	Enhanced
[64]	2021	AES Core	VIRTEX-5	Byte-by-byte processing instead of Block processing	Pipeline	More	Less (15.5%)	Less	-------
[68]	2021	AES Core	ARM-Cortex M4 (ATECC608A)	Reduction in AES rounds	Parallel	Less	Less	Less	Very Low
[70]	2023	AES Core	Intel Cyclone-V	AES operated in CTR (Counter) mode with RTL (Register Transfer Level)	Pipeline	------	Less (23%)	Less	-------
[71]	2024	AES Core	ARTIX-7 KINTEX-7	Reduction of 8x8 SBOX	Parallel	More	Less (11.76%)	Less (3.12%)	Low

* As compared with traditional AES **Hardware/Software

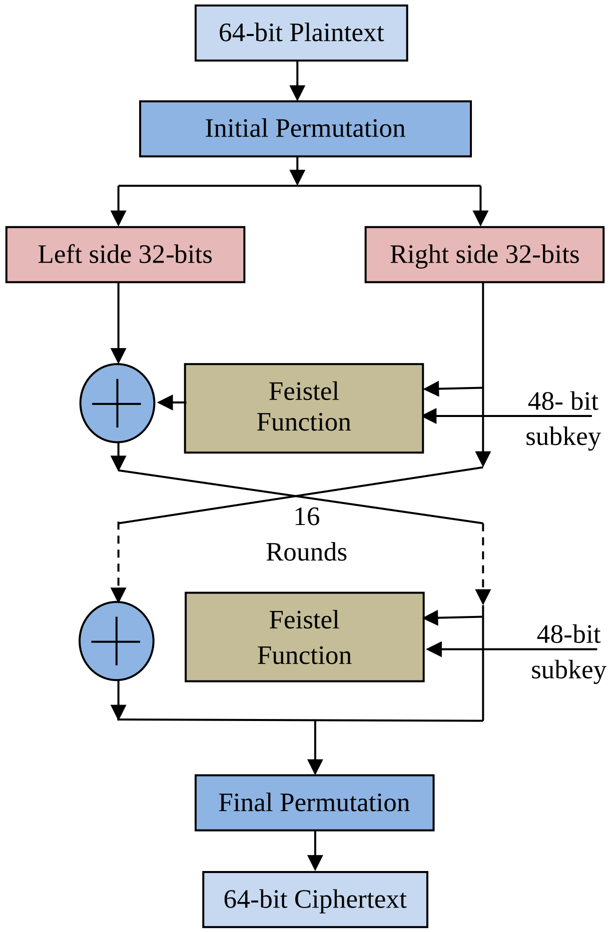


Fig. 10 Basic structure of DES

Reduction in power consumption during data communication has increased the interest of researchers in designing lightweight security algorithms. Malal et al. 2024 presented a compact and efficient AES-like 8x8 SBOX design and implemented it on Virtex-7 and Artix-7 FPGA boards. The authors achieved better throughput by reducing gate area by 11.76% using the parallel architecture of AES Core [17]. Hence evident that the researchers are working on the AES core algorithm to find a lightweight solution for power-constrained IoT devices. Table 2 shows the comparative analysis of advancements and developments approached by various authors and researchers during the last decade for making AES more power-efficient, lesser area requirement, and operating on low overhead to the system. The analysis is done on the research published in various reputed journals for authentic analysis. Many of them have successfully optimized one or two parameters, but still, the lightweight algorithm variant for specifically IoT applications and constrained devices has not been developed yet.

3. Data Encryption Standard

DES is a traditional block cipher algorithm that is based on Feistel Cipher Structure. Developed in March 1975 by IBM and adopted in 1977 by the National Bureau of Standards (NBS) of the United States published, DES is a secure mode of converting plain text into encoded text that the attackers can not intervene [72]. Since then, the encryption process has developed to a greater extent and has become a vital part of information security. The process of DES is summarized in Figure 10. Unlike the AES algorithm, the plain text datapath in DES is 64-bit, the key is 56-bit, and there are 16 iterations (rounds) in which the data is encrypted. The data is divided into two blocks of 32-bit each, and the 24-bit (expanded to 32-bit) key is used in the Feistel function during a single round of encryption. A structural overview of the Feistel function is shown in Figure 11.

There is a critical and time-consuming process of key generation and expansion that takes most of the memory and hence, the throughput of DES as compared to AES decreases [73][74]. Even after the complexity of DES with fewer benefits, still, the popularity of DES has led the researchers to find a derivative of DES that may be less time and power-consuming, reduced complexity, and lesser area requirements [75-78].

The 3-DES, derivative of DES, has inferior performance metric parameters, which makes this variant of minimum use as far as constrained IoT infrastructure is concerned. In this context, recent years have seen research publications regarding the design of light-weighted DES derivatives that may be used at the IoT edge or end layer. In 2014, Khan F. H. et.al. [79] showed that the implementation of DES can be optimized as it is hardware-dependent. The authors used Spartan 3e (XC3S1600E) FPGA for implementation and have generated a separate Key generation block that has not only saved the implementation time due to parallel processing but also saved the implementation area on-chip. This led to a better throughput at a higher frequency than the works of literature published [79].

3.1. Discussion on Advancements in DES

The minimization of power consumption at a remote node is also one of the prime requirements of IoT applications. Pandey B. et al. [80] 2015 analyzed and synthesized the power dissipation of DES on Artix-7 FPGA. The researchers used Stub-Series Terminated Logic (SSTL) as an input-output standard, keeping into consideration the variants, i.e. SSTL135, SSTL135_R, SSTL15, SSTL15_R, SSTL18_I, and SSTL18_II, and analysis of I/Os power, leakage power, clock power, logic power, and total power was performed [80]. The different SSTL logic represents the voltage associated with them. For example, SSTL18 has 1.8V I/O standards. The result analysis showed a variation of 50%-60% in total power dissipation against the selection of different I/O standards. There are other standards, such as TTL, GTL, GTLP, LVPECL, and LVDS, that can be explored for more energy-efficient options also [81,82]. Hence while designing a light-weighted algorithm for IoT, the selection of I/O standards also plays a major role as far as power is concerned.

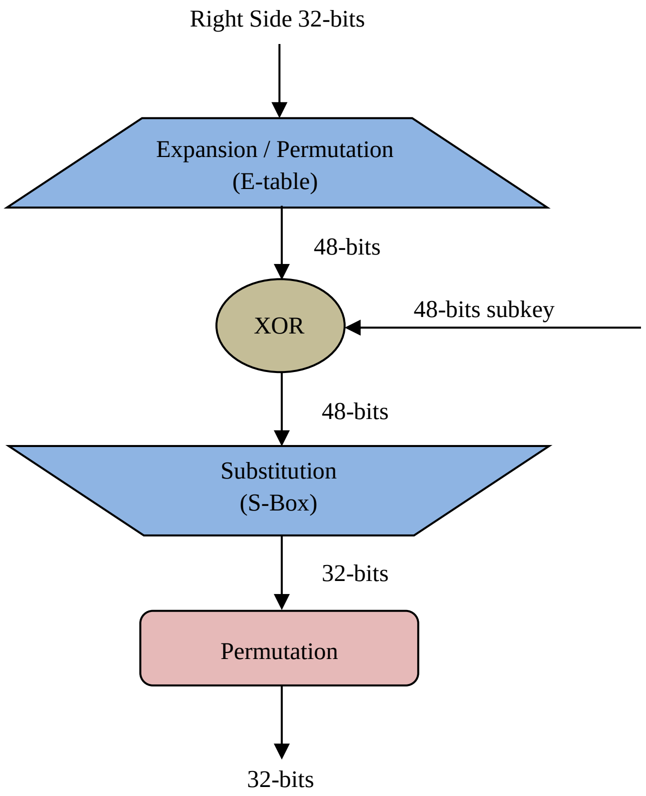


Fig. 11 Structural overview of Feistel function

A similar approach was presented in [83] by Singh D. et al. in 2015. The authors implemented DES on Vertex-6, Vertex-5, and Vertex-4 FPGAs upon LVCMOS15 and LVCMOS25 I/O standards and analyzed the power dissipation. The results were quite similar to those projected in [80]. The variation in reduction of power dissipation is 60%-65% as per the selection of hardware-I/O standard couplet. Hence, the authors projected the need for the selection of suitable I/O standards for the implementation of IoT architecture. The evolution of the light-weighted encryption technique has projected new and better ideas and gaps for researchers. Along with this, a primary concern is security, and many publications reflect the ideas that may enhance the security of existing databases but add overhead to the process, reducing throughput[84-88]. In 2016, Mitchell C. J. et al. presented two keys-based architectures [85] for the DES variant, but the enhanced security on the cost of complexity, power, area, and delay makes it unsuitable for IoT devices. Chabukswar P. M. et al. [89] 2017 proposed three key generation processes for DES apart from the traditional direct approach. This includes the generation of the key using Linear-Feedback-Shift-Register (LFSR) based on the generation of stream key, Chaotic encryption-based key generation, and 2's complement method. The dynamic key generation is summarized in Figure 12. The process provides a higher zeal of security, and the framework design is robust enough to withstand any kind of attack on the Cipher generated. Even the process is found to be energy efficient but as far as the IoT end is concerned, the memory requirements are more as the complexity in the process is observed. This approach might be implemented at IoT Edge due to the availability of higher configuration computational facilities.

The trade-off between area, memory, time delay, rate of transmission, complexity, cost, and power must meet a compromising stage. In 2017, Guler Z. et al. [90] experimented successfully with the 8-fold speed of transmission using Compute Unified Device Architecture (CUDA) designed by NVIDIA based on Single Instruction Multiple Data(SIMD) GPU. Here, the data transmission rate is high, and throughput is higher than traditional DES designs, but using a GPU at an IoT node is nearly impossible[91,92]. In 2017, Krishna B. et.al. used DNA-based cryptography in which the key generation process is modified using partially reconfiguring the FPGA (ZED board). Mathematically, they XOR the main key with a dummy key to generate a new key in between the process of data encryption, which makes it nearly impossible for an intruder and leaves him with confusion. Here LFSR is used to generate a dummy key as used by authors of [30] to generate the key for AES. The process has its demerit of higher computational requirements and power consumption.

The popularity of DES has never faded, although the evolution of 3DES and AES has captured the market. Even for computation facilities, memory and complexity are concerned, DES variants are preferred [93-96]. Following a similar approach, Tang H. et al. in 2018 used a dynamic concept-based 3-layered encryption using network coding on DES. The concept used a partial key update system to present a less complex process [97].

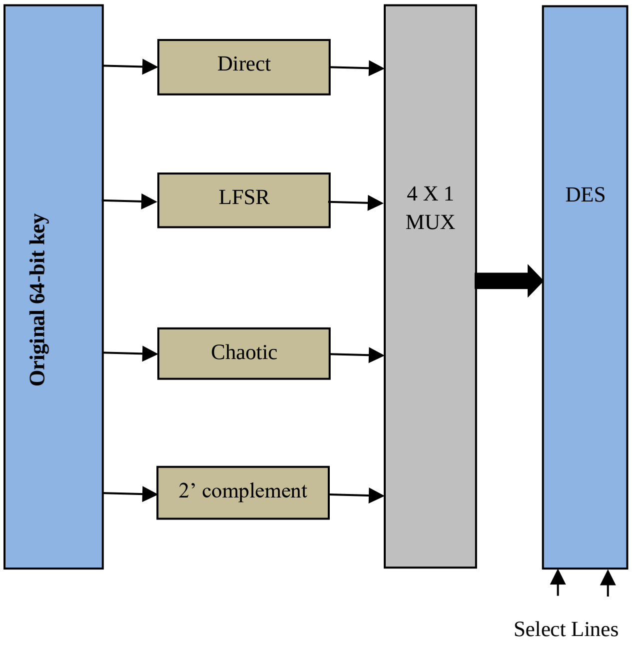


Fig. 12 Dynamic key generation [89]

The DES process has been bifurcated and at every step, the dynamics of the data are changed. The layer-based architecture led the DES into a robust design that can withstand both analysis and exhaustive attacks. The design was proposed theoretically for the Moving Target Defense (MTD) mechanism and the work has been appreciated and granted by various prestigious institutions such as the National Natural Science Foundation of China (61471034 and 61771045), Ministry of Education of China (6141A02033307), Fundamental Research Funds for the Central Universities (FRF-GF-17-B26) and Open Research Fund of Key Laboratory of Space Utilization, CAS (LSU-DZXX-2017-03)[99].

As the main concern of security algorithms for IoT applications is to be light-weighted. Kristianti V. E. et al. [100] 2018 proposed and verified a light-weighted DES by minimizing the number of rounds. The authors proposed the implementation of 8 rounds of the DES algorithm on FPGA rather than the traditional 16 rounds architecture. Figure 13 shows the parallel architecture where the 16 rounds are divided into 8 parallel rounds in even and odd patterns using internal registers of FPGA following pipelined architecture.

This approach led to minimizing the resources such as slice, flip flop, registers and LUTs, hence minimizing hardware complications. The 8-round design required an average of 9.7% of the resources available, while 16 rounds required 21.2% of them with Spartan 3e (XC3ES500E) FPGA used by the researchers without compromising the security aspects of data. The proposed approach has given a new insight into light-weighted designs. There are many kinds of research focused on minimizing the architectural iterations for decreasing overhead and increasing throughput, even based on cloud computing as proposed in [101-110] in previous years, but the distinctive featured algorithm could not be designed. Presently, researchers are developing and integrating a lightweight algorithm; Gao F. 2019 presented a blockchain-based DES for e-commerce platforms [111]. The idea is to omit the iterative stages and use a chaotic neural network before the key is introduced to the data. This enhances the security parameters and due to a single-stage process, presents a good amount of time-saving and needs lesser computational area. The signal-to-noise ratio (S/N) is analyzed on Tamcat6.0.32 software on the DELL SSL Test server and Weblogic12.1.1 and Oracle11g on HP servers with satisfactory security aspects. In 2019, Subhi R. M. et al. [112] tested sequential and parallel processing of DES on FPGA. The parallel and sequential architectural implementation is commonly used in the AES algorithm as per application requirements. The authors used XC3S1600E-4 Spartan-3e FPGA to test the security of a 12-bit datapath encrypted with a 9-bit key. The system design showed that the code-breaking time of parallel design is much less and presents better security [113-116]. However, the key length is very small and could be easily intercepted by an intruder.

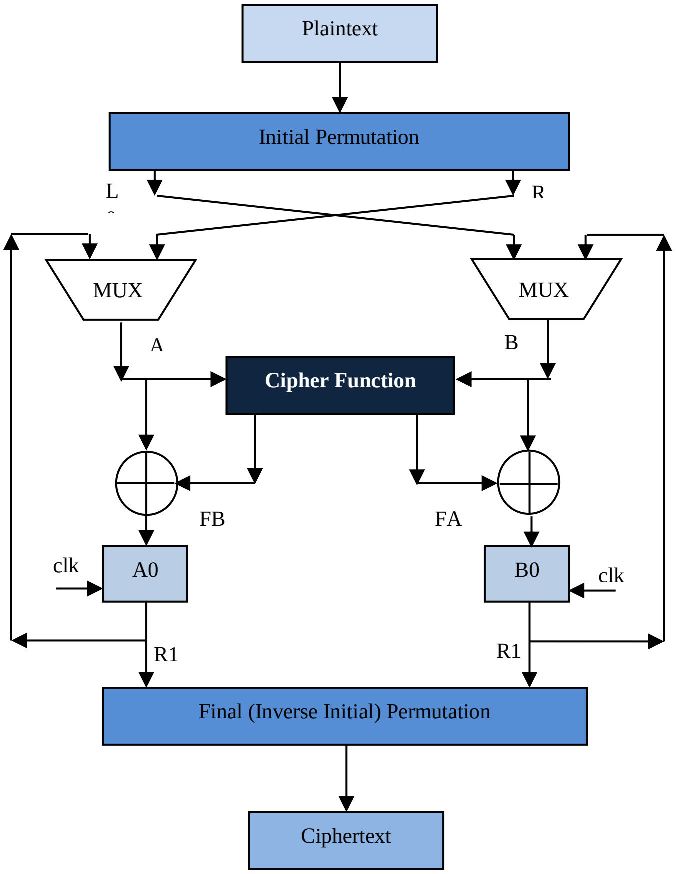


Fig. 13 DES 8-round algorithm architecture [100]

Amorado R. V. et al. in 2019 modified the concept of key expansion in DES. The researchers introduced the filtering and striding technique [117] in which the key matrix has a new column padded to the right of the key matrix. Each element of the column is filled with ‘0’ or ‘1’ by taking the average of the number of ‘1’ in that row. This strengthens the security aspects of the algorithm to a greater extent but again adds overhead to the design. Moreover, the concept is time-consuming and requires higher memory, which makes it unsuitable for IoT-constrained devices. Even Kester A. et al. [118] presented a conflux of Race Integrity Primitive Evaluation Message Digest (RIPEMD 128) [119], a hash function, and DES to establish node-node secure data communication for IoT applications, but the computational system requirements are higher. The overall scenario has seen a development of various variants that come out to be either lightweight or more secure in the case of SCAs, Power-based attacks, man-in-middle, and other software intrusions to crack the Ciphertext [120-127]. Due to the presence of remote nodes in IoT, there is a possibility of probing attacks. Wang H. et al. 2020 proposed FIB (Focused Ion Beam) based on a physical design flow based on anti-probing, which is evaluated to obtain the efficiency of the design flow. It is also helpful in determining the vulnerability of the area in the design flow to the probing attacks [128].

Table 3. Performance comparison of recent development and implementation of DES Algorithm

	Year	HW/SW	Technique	Delay*	Area Req.*	Power Cons.*	Security
[79]	2014	Spartan 3e (XC3S1600E)	Separate block for key generation process (H/W)	Less	Less	Less	High
[80]	2015	Artix-7	Stub-Series Terminated I/O Logic-based power analysis	Less	More	Very Less	-------
[83]	2016	Vertex-4 Vertex-5 Vertex-6	Power dissipation analysis of LVCMOS15 and LVCMOS25 I/O standards	Less	More	Very Less	-------
[89]	2017	Virtex-6 (xc6vlx75t-3ff484)	Dynamic Key generation (Direct, LFSR, Chaotic and 2’s Complement)	Less	More	More	High
[93]	2017	ZED board	Partially Reconfigurable concept of key generation	More	Less	Less	High
[100]	2018	Spartan 3e (XC3ES500E)	8-round DES implementation	Less	Less	Less	-------
[111]	2019	Tamcat6.0.32, Weblogic12.1.1 and Oracle11g	Use a chaotic neural network on the key before introducing it to the data path	Less	Less	More	High
[112]	2019	Spartan-3e(XC3S1600E-4)	Parallel and Sequential processing of 12-bit datapath with 9-bit key length	Less	More (parallel)	Less	Very low
[117]	2019	Python 3	Key modified using filtering and striding technique	More	More	More	High
[128]	2020	Synopsys Design Compiler (SAED 32nm)	FIB Physical design flow against probing attach	More	------	More	High
[134]	2024	Artix-7 Virtex-7		Less	Very Less	Very Less (86.07%)	------

* As compared with traditional DES

The design presented a hardware approach to implementing DES on FPGA and the results showed a vulnerable probing area decreased by 99% as compared to simple implementation along with a 4% overhead. A similar approach is presented by authors of [129-132]and found effective against probing. This technique can be used to strengthen communication where the cipher integrity of the application of an IoT network is critical. The evolution of cryptography has extended its application area, and due to the necessity of security aspects in data communication, the simple DES and its variants are still used in various fields such as e-commerce, banking/accounting [133], and even transportation.

The researchers are still working around DES to find a simpler, sustained, yet robust derivative for IoT applications. In recent research conducted by Ashish et al. in 2024, the authors performed a low-power implementation of Low Voltage Complementary Metal Oxide Semiconductor (LVCMOS) based DES algorithm on 28nm FPGA (ARTIX-7 and VIRTEX-7) [134]. The researchers were able to reduce the power consumption by 86.07% if we were using LVCMOS12. This was achieved by bifurcation of power, i.e. evidently, the dynamic power consumption is about 93%, whereas static power consumption is about 7%. Hence, the authors focused on the reduction of the dynamic power of the DES algorithm.

This highlights the interest of authors to work on derivatives of traditional symmetric algorithms such as DES to find a low-power lightweight security algorithm as a solution for power constrained devices [135-136]. Table 3 shows the hardware and software-based comparative analysis of the last decade, advancements, and developments approached by various authors and researchers for making Data Encryption Standard (DES) more power efficient with lesser area requirements.

4. Conclusion and Future Scope

The number of recent literatures published in various reputed platforms on AES and DES algorithms shows the growing interest of researchers in designing a lightweight solution for IoT devices. The publications recently have focused on hardware-based, software-based, and duo couplet-based algorithms that may be secure as well as robust without adding much overhead, taking lesser memory space for implementation, and minimizing the data transmission delay.

As the number of IoT sensors and devices, as well as their inter-communication, is increasing many folds, there is a huge potential in the area of research in designing an efficient and effective algorithm. In this regard, AES and DES algorithms can act as a pre-existing platform for the design due to their simplicity in understanding, ease of implementation, and robustness. Hence there is a predicted research area that requires to be emphasized to find new approaches or architectures that may be designed for constrained IoT applications. The key generating algorithm has a major part to play in encryption.

This algorithm requires a major computation and is time-consuming, making the existing systems unfavourable for IoT applications. We propose a key generation process in which the key will be generated from the data itself using the first and second levels of security. The first level may include an encoding technique that may be used to generate the key as the output of encoded data bits. Then the second level coding may be used to generate a final key. The key generated once could be used to encode a small chuck of data, probably the data that has been used to generate the key itself. This not only omits the operation of the key scheduling algorithm for encryption but also may enhance the security as every time; a new encryption key may be generated. The proposed algorithm will be lightweight and secure due to the variable key and data path size.

Abbreviations used

IoT:- Internet of Things
AES:- Advanced Encryption Standard
DES: Data Encryption Standard
FPGA: Field Programmable Gate Array
LUT:- Look-Up Table
ASIC: Application Specific Integrated Circuit
CBC:- Cipher Block Chaining mode
CMAC:- Cipher-based Message Authentication Code
NIST: National Institute of Standards and Technology (US.)
SBOX:- Substitution box
CPA:- Correlation Power Analysis attack
WDDL:- Wave Dynamic Differential Logic
BRAM:- Block Random Access Memory
CLB:- Configurable Logical Block
CRA:- Code Refusal Attack
ROP:- Return Oriented Programming
JOP:- Jump Oriented Programming
LEA:- Lightweight Encryption Architecture
GCM:- Galois Counter Mode
ECB:- Electronic Code Book
CFB:- Cipher Feed Back mode
OFB:- Output Feed Back mode
CCM:- Counter with Chaining Mode
PRNG:- Pseudo-Random Number Generator
TRNG:- True-Random Number Generator
Cas:- Crypto-analysis Attacks
SCAs:- Side Channel Attacks
MLAs:- Machine Learning Attacks
LFSR:- Linear Feedback Shift Register
HFA:- High throughput Fault-resilient
PUF:- Physically Un-coloneable Function
DPA:- Differential Power Analysis
AMP:- Asynchronous Multi-core Processor
MAC:- Message Authentication Code
DRO:- Digital Ring Oscillator
DOS:- Denial Of Service
DRM: Digital Right Management
ECC:- Elliptical Curve Cryptography
ECDH:- Elliptical Curve Diffie-Hellman
ECDSA:- Elliptical Curve Digital Signature Algorithm
SSTL:- Stub-Series Terminated Logic
CUDA:- Computer Unified Device Architecture
SIMD:- Single Instruction Multiple Data
MTD:- Moving Target Defence
RIPEMD:- Race Integrity Primitive Evaluation Message Digest
FIB:- Focused Ion Beam

References

[1] Sandip Ray, Yier Jin, and Arijit Raychowdhury, “The Changing Computing Paradigm with Internet of Things: A Tutorial Introduction,” *IEEE Design & Test*, vol. 33, no. 2, pp. 76-96, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[2] Weize Yu, and Selçuk Köse, “A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 11, pp. 2934-2944, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] Zeng Bohan et al., “Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530,” *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, pp. 1454-1457, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sanu K. Mathew et al., “53 Gbps Native GF$(2^4)^2$ Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors,” *IEEE Journal of Solid-State Circuits*, vol. 46, no. 4, pp. 767-776, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[5] Joan Daemen, and Vincent Rijmen, “Specifications for the Advanced Encryption Standard (AES),” *Federal Information Processing Standards Publication 197*, 2001. [Google Scholar]

[6] Umer Farooq, and M. Faisal Aslam, “Comparative Analysis of Different AES Implementation Techniques for Efficient Resource Usage and Better Performance of an FPGA,” *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 3, pp. 295-302, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[7] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," *Cryptographic Hardware and Embedded Systems-CHES 2007, Lecture Notes in Computer Science*, vol. 4727, pp. 450-466, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[8] Amir Moradi et al., "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," *Advances in Cryptology – EUROCRYPT 2011, Lecture Notes in Computer Science*, vol. 6632, pp. 69-88, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[9] Duy-Hieu Bui et al., "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3281-3290, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] Mehmet Kayaalp et al., "Branch Regulation: Low-Overhead Protection from Code Reuse Attacks," *2012 39th Annual International Symposium on Computer Architecture*, Portland, OR, USA, pp. 94-105, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[11] Pengfei Qiu et al., "Physical Unclonable Functions-Based Linear Encryption Against Code Reuse Attacks," *Proceedings of the 53rd Annual Design Automation Conference*, Austin Texas, pp. 1-6, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[12] Pengfei Qiu et al., "Control Flow Integrity Based on Lightweight Encryption Architecture," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 7, pp. 1358-1369, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Shah Fahd et al., "Correlation Power Analysis of Modes of Encryption in AES and its Countermeasures," *Future Generation Computer Systems*, vol. 83, pp. 496-509, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[14] François-Xavier Standaert, *Introduction to Side-Channel Attacks*, Secure Integrated Circuits and Systems, Springer, Boston, MA, pp. 27-42, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[15] Joan Daemen, and Vincent Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*, Springer Berlin Heidelberg, pp. 1-238, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[16] Peter Pessl, and Stefan Mangard, "Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability," *Topics in Cryptology - CT-RSA 2016: The Cryptographers' Track at the RSA Conference*, San Francisco, CA, USA, pp. 255-270, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sonia Belaïd, Pierre-Alain Fouque, and Benoît Gérard, "Side-Channel Analysis of Multiplications in GF (2^{128}): Application to AES-GCM," *Advances in Cryptology -- ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security*, Kaoshiung, Taiwan, China, pp. 306-325, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[18] Beibei Li et al., "DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415-2425, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[19] Beibei Li et al., "Distributed Host-Based Collaborative Detection for False Data Injection Attacks in Smart Grid Cyber-Physical System," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 32-41, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Das, "Generation of AES-like 8-Bit Random S-Box and Comparative Study on Randomness of Corresponding Ciphertexts with Other 8-Bit AES S-Boxes," *Proceedings of the International Conference on Advanced Computing, Networking, and Informatics*, India, pp. 303-318, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[21] V.P. Hoang, V.L. Dao, and C.K. Pham, "Design of Ultra-Low Power AES Encryption Cores with Silicon Demonstration in SOTB CMOS Process," *Electronics Letters*, vol. 53, no. 23, pp. 1512-1514, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[22] Karim Shahbazi, Mohammad Eshghi, and Reza Faghih Mirzaee, "Design and Implementation of an ASIP-Based Cryptography Processor for AES, IDEA, and MD5," *Engineering Science and Technology, an International Journal*, vol. 20, no. 4, pp. 1308-1317, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[23] Reza Faghih Mirzaee, Mohammad Eshghi, and Keivan Navi, "Design and Implementation of an ASIP-Based Crypto Processor for IDEA and SAFER K-64," *International Journal of Design, Analysis and Tools for Integrated Circuits and Systems*, vol. 3, no. 2, pp. 21-30, 2012. [Google Scholar]

[24] José M. Granado et al., "IDEA and AES, Two Cryptographic Algorithms Implemented Using Partial and Dynamic Reconfiguration," *Microelectronics Journal*, vol. 40, no. 6, pp. 1032-1040, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[25] Yuliang Wang et al., "Ultra High Throughput Implementations for MD5 Hash Algorithm on FPGA," *High Performance Computing and Applications, Lecture Notes in Computer Science*, vol. 5938, pp. 433-441, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[26] Pu Wang, Yuming Zhang, and Jun Yang, "Research and Design of AES Security Processor Model Based on FPGA," *Procedia Computer Science*, vol. 131, pp. 249-254, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[27] J.L. Imaña, "Low-Delay AES Polynomial Basis Multiplier," *Electronics Letters*, vol. 52, no. 11, pp. 930-932, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[28] Chao Luo et al., "Comprehensive Side-Channel Power Analysis of XTS-AES," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 12, pp. 2191-2200, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[29] "1619-2018 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices," *IEEE Std. 1619-2007, Standards*, pp. 1-32, 2008. [CrossRef] [Publisher Link]

[30] Harshali Zodpe, and Ashok Sapkal, "An Efficient AES Implementation Using FPGA with Enhanced Security Features," *Journal of King Saud University - Engineering Sciences*, vol. 32, no. 2, pp. 115-122, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Hadi Mardani Kamali, and Shaahin Hessabi, "A Fault Tolerant Parallelism Approach for Implementing High-Throughput Pipelined Advanced Encryption Standard," *Journal of Circuits, Systems and Computers*, vol. 25, no. 9, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[32] Saeide Sheikhpour, Ali Mahani, and Nasour Bagheri, "High Throughput Fault-Resilient AES Architecture," *IET Computers & Digital Techniques*, vol. 13, no. 4, pp. 312-323, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[33] Xiaolin Xu, and Wayne Burleson, "Hybrid Side-Channel/Machine-Learning Attacks on PUFs: A New Threat?," *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, Germany, pp. 1-6, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[34] Meilin Wan et al., "An Invasive-Attack-Resistant PUF Based On Switched-Capacitor Circuit," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 8, pp. 2024-2034, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[35] Weize Yu, and Selçuk Köse, "A Voltage Regulator-Assisted Lightweight AES Implementation Against DPA Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 8, pp. 1152-1163, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[36] Weize Yu, and Jia Chen, "Masked AES PUF: A New PUF Against Hybrid SCA/MLAs," *Electronics Letters*, vol. 54, no. 10, pp. 618-620, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[37] Ying Huang, Wei Li, and Jing Lei, "Concatenated Physical Layer Encryption Scheme Based on Rateless Codes," *IET Communication*, vol. 12, no. 12, pp. 1491-1497, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[38] Yongzhuang Wei et al., "New Second-Order Threshold Implementation of AES," *IET Information Security*, vol. 13, no. 2, pp. 117-124, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[39] 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, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] Safwat Mostafa Noor, and Eugene B. John, "Resource Shared Galois Field Computation for Energy Efficient AES/CRC in IoT Applications," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 4, pp. 340-348, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[41] Ali Akbar Pammu et al., "A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1023-1036, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[42] M. Masoumi, "A Highly Efficient and Secure Hardware Implementation of the Advanced Encryption Standard," *Journal of Information Security and Applications*, vol. 48, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[43] Rubén Lumbiarres-López, Mariano López-García, and Enrique Cantó-Navarro, "Hardware Architecture Implemented on FPGA for Protecting Cryptographic Keys Against Side-Channel Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 898-905, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[44] Mustafa Emad Hameed et al., "A Lossless Compression and Encryption Mechanism for Remote Monitoring of ECG Data Using Huffman Coding and CBC-AES," *Future Generation Computer Systems*, vol. 111, pp. 829-840, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[45] Luca Crocetti et al., "A Simulated Approach to Evaluate Side-Channel Attack Countermeasures for the Advanced Encryption Standard," *Integration*, vol. 68, pp. 80-86, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[46] Markus Dichtl, and Jovan Dj. Golić, "High-Speed True Random Number Generation with Logic Gates Only," *Cryptographic Hardware and Embedded Systems: 9th International Workshop*, Vienna, Austria, pp. 45-62, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[47] Athmane Seghier, Jianxin Li, and Da Zhi Sun, "Advanced Encryption Standard Based on Key Dependent S-Box Cube," *IET Information Security*, vol. 13, no. 6, pp. 552-558, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[48] Ziaur Rahaman et al., "A Novel Structure of Advance Encryption Standard with 3-Dimensional Dynamic S-Box and Key Generation Matrix," *International Journal of Advance Computational Science and Applications*, vol. 8, no. 2, pp. 314-320, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[49] Weiwei Shan et al., "Machine Learning Assisted Side-Channel-Attack Countermeasure and its Application on a 28-nm AES Circuit," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 3, pp. 794-804, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[50] V. Nandan, and R. Gowri Shankar Rao, "Minimization of Digital Logic Gates and Ultra-Low Power AES Encryption Core in 180CMOS Technology," *Microprocessors and Microsystems*, vol. 74, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[51] Keshav Kumar, K.R. Ramkumar, and Amanpreet Kaur, "A Lightweight AES Algorithm Implementation for Encrypting Voice Messages Using Field Programmable Gate Arrays," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 6, pp. 3878-3885, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[52] P. Panagiotou et al., "Cryptographic System for Data Applications, in the Context of Internet of Things," *Microprocessors and Microsystems*, vol. 72, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[53] Sherali Zeadally, Ashok Kumar Das, and Nicolas Sklavos, “Cryptographic Technologies and Protocol Standards for Internet of Things,” *Internet of Things*, vol. 14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[54] Heba El-Rahman Hassan, Mohamed Tahoun, and Gh.S. ElTaweel, “A Robust Computational DRM Framework for Protecting Multimedia Contents Using AES and ECC,” *Alexandria Engineering Journal*, vol. 59, no. 3, pp. 1275-1286, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[55] Xiongwei Fei et al., “Analysis of Energy Efficiency of a Parallel AES Algorithm for CPU-GPU Heterogeneous Platforms,” *Parallel Computing*, vol. 94-95, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[56] Zongchao Qiao, Safwan El Assad, and Ina Taralova, “Design of Secure Cryptosystem Based on Chaotic Components and AES S-Box,” *AEU - International Journal of Electronics and Communications*, vol. 121, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[57] Pasquale Arpaia, Francesco Bonavolontá, and Antonella Cioffi, “Problems of the Advanced Encryption Standard in Protecting Internet of Things Sensor Networks,” *Measurements*, vol. 161, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[58] Liandeng Li et al., “Efficient AES Implementation on Sunway TaihuLight Supercomputer: A Systematic Approach,” *Journal of Parallel and Distributed Computing*, vol. 138, pp. 178-189, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[59] Dhirendra K.R Shukla, Vijay K.R. Dwivedi, and Munesh C. Trivedi, “Encryption Algorithm in Cloud Computing,” *Materials Today: Proceedings*, vol. 37, no. 2, pp. 1869-1875, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[60] Rei Ueno et al., “High Throughput/Gate AES Hardware Architectures Based on Datapath Compression,” *IEEE Transactions on Computers*, vol. 69, no. 4, pp. 534-548, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[61] Yu Ou, and Lang Li, “Research on a High-Order AES Mask Anti-Power Attack,” *IET Information Security*, vol. 14, no. 5, pp. 580-586, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[62] Shotaro Sawataishi, Rei Ueno, and Naofumi Homma, “Unified Hardware for High-Throughput AES-Based Authenticated Encryptions,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 9, pp. 1604-1608, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[63] Zolidah Kasiran, Shapina Abdullah, and Normazlie Mohd Nor, “An Advance Encryption Standard Cryptosystem in IoT Transaction,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1548-1554, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[64] Karim Shahbazi, and Seok-Bum Ko, “Area-Efficient Nano-AES Implementation for Internet-of-Things Devices,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 1, pp. 136-148, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[65] Arash Reyhani-Masoleh, Mostafa Taha, and Doaa Ashmawy, “New Area Record for the AES Combined S-Box/Inverse S-Box,” *2018 IEEE 25th Symposium on Computer Arithmetic (ARITH)*, Amherst, MA, USA, pp. 145-152, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[66] Karim Shahbazi, and Seok-Bum Ko, “High Throughput and Area-Efficient FPGA Implementation of AES for High-Traffic Applications,” *IET Computers and Digital Techniques*, vol. 14, no. 6, pp. 344-352, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[67] Sanu Mathew et al., “340 mV–1.1 V, 289 Gbps/W, 2090-Gate NanoAES Hardware Accelerator With Area-Optimized Encrypt/Decrypt GF(2 4) 2 Polynomials in 22 nm Tri-Gate CMOS,” *IEEE Journal of Solid-State Circuits*, vol. 50, no. 4, pp. 1048-1058, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[68] Joseph N. Mamvong et al., “Efficient Security Algorithm for Power-Constrained IoT Devices,” *IEEE Internet Of Things Journal*, vol. 8, no. 7, pp. 5498-5509, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[69] Alexandre Proulx et al., “A Survey on FPGA Cybersecurity Design Strategies,” *ACM Transactions on Reconfigurable Technology and Systems*, vol. 16, no. 2, pp. 1-33, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[70] Ahmed Maache, and Abdesattar Kalache, “Design and Implementation of a Flexible Multi-Purpose Cryptographic System on Low Cost FPGA,” *International Journal of Electrical and Computer Engineering Systems*, vol. 14, no. 1, pp. 45-58, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[71] Ahmet Malal, and Cihangir Tezcan, “FPGA-Friendly Compact and Efficient AES-like 8 × 8 S-Box,” *Microprocessors and Microsystems*, vol. 105, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[72] National Bureau of Standards, “*Data Encryption Standard*,” U.S. Department of Commerce, Federal Information Processing Standards Publication 46, 1977. [Google Scholar] [Publisher Link]

[73] W.F. Ehrsam et al., “A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard,” *IBM Systems Journal*, vol. 17, no. 2, pp. 106-125, 1978. [CrossRef] [Google Scholar] [Publisher Link]

[74] J.H. Moore, and G.J. Simmons, “Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys,” *IEEE Transactions On Software Engineering*, vol. 13, no. 2, pp. 262-273, 1987. [CrossRef] [Google Scholar] [Publisher Link]

[75] I. Verbauwhede et al., “Security and Performance Optimization of a New DES Data Encryption Chip,” *IEEE Journal of Solid-State Circuits*, vol. 23, no. 3, pp. 647-656, 1988. [CrossRef] [Google Scholar] [Publisher Link]

[76] M.E. Smid, and D.K. Branstad, “Data Encryption Standard: Past and Future,” *Proceedings of the IEEE*, vol. 76, no. 5, pp. 550-559, 1988. [CrossRef] [Google Scholar] [Publisher Link]

[77] D. Coppersmith, "The Data Encryption Standard (DES) and its Strength Against Attacks," *IBM Journal of Research and Development*, vol. 38, no. 3, pp. 243-250, 1994. [CrossRef] [Google Scholar] [Publisher Link]

[78] Guang Gong, and S.W. Golomb, "Transform Domain Analysis of DES," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2065-2073, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[79] Fozia Hanif Khan et al., "Implementation of Data Encryption Standard (DES) on FPGA," *Journal of Computer Science of Newports Institute of Communications and Economics*, vol. 5, no. 1, pp. 47-59, 2014. [Google Scholar] [Publisher Link]

[80] Bishwajeet Pandey et al., "SSTL Based Power Efficient Implementation of DES Security Algorithm on 28nm FPGA," *International Journal of Security and its Applications*, vol. 9, no. 7, pp. 267-274, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[81] Tanesh Kumar et al., "LVTTL IO Standards and Capacitance Scaling Based Energy Efficient ALU Design on FPGA," *Ned University Journal of Research*, pp. 39-47, 2014. [Google Scholar] [Publisher Link]

[82] Suresh Manohar Menon et al., "Programmable Input/Output Circuit for FPGA for Use in TTL, GTL, GTLP, LVPECL and LVDS Circuits," *US6218858B1*, pp. 1-19, 2001. [Google Scholar] [Publisher Link]

[83] Deepa Singh et al., "Thermal Aware Internet of Things Enable Energy Efficient Encoder Design for Security on FPGA," *International Journal of Security and Its Applications*, vol. 9, no. 6, pp. 271-278, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[84] Prathyusha Uduthalapally, and Bing Zhou, "Improvement of ETSFS Algorithm for Secure Database," *2016 4th International Symposium on Digital Forensic and Security*, Little Rock, AR, USA, pp. 63-67, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[85] Chris J. Mitchell, "On the Security of 2-Key Triple DES," *IEEE Transactions On Information Theory*, vol. 62, no. 11, pp. 6260-6267, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[86] Elaine Barker, and Allen Roginsky, "*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*," NIST Special Publication 800-131A, Revision 1, National Institute of Standards and Technologies, USA, pp. 1-23, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[87] Elaine Barker, "*Recommendation for Key Management: Part 1: General*," NIST Special Publication 800–57 Part 1, Revision 4, National Institute of Standards and Technologies, USA, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[88] Maria Ellen L. Estrellado, Ariel M. Sison, and Bartolome T. Tanguilig, "Test Bank Management System Applying Rasch Model and Data Encryption Standard (DES) Algorithm," *International Journal of Modern Education and Computer Science*, vol. 8, no. 10, pp. 1-8, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[89] Punam Milind Chabukswar, Manoj Kumar, and P. Balaramudu, "An Efficient Implementation of Enhanced Key Generation Technique in Data Encryption Standard (DES)Algorithm Using VHDL," *2017 International Conference on Computing Methodologies and Communication*, Erode, India, pp. 917-921, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[90] Zafer Güler, Fatih Özkaynak, and Ahmet Cevahir Çınar, "CUDA Implementation of DES Algorithm for Lightweight Platforms," *Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics*, Bangkok Thailand, pp. 49-52, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[91] T.K. Sivakumar et al., "Enhanced Secure Data Encryption Standard (ES-DES) Algorithm Using Extended Substitution Box (S-Box)," *International Journal of Applied Engineering Research*, vol. 12, no. 21, pp. 11365-11373, 2017. [Google Scholar] [Publisher Link]

[92] Adeem Akhtar, Muhammad Zia Ullah Baig, and Waleej Haider, "Enhancing the Security of Simplified DES Algorithm Using Transposition and Shift Rows," *International Journal of Computer Science and Software Engineering*, vol. 6, no. 5, pp. 115-119, 2017. [Google Scholar] [Publisher Link]

[93] Luminiţa Scripcariu, Petre-Daniel Mătăsaru, and Felix Diaconu, "Extended DES Algorithm to Galois Fields," *2017 International Symposium on Signals, Circuits and Systems*, Iasi, Romania, pp. 1-4, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[94] B. Murali Krishna, "FPGA Implementation of DES Algorithm Using DNA Cryptography," *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 10, pp. 2147-2158, 2017. [Google Scholar] [Publisher Link]

[95] Rama Satya Nageswara Rao et al., "Wireless Secured Data Transmission Using Cryptographic Techniques through FPGA," *International Journal of Engineering and Technology*, vol. 8, no. 1, pp. 332-338, 2016. [Google Scholar] [Publisher Link]

[96] Surinder Kaur, Pooja Bharadwaj, and Shivani Mankotia, "Study of Multi-Level Cryptography Algorithm: Multi-Prime RSA and DES," *International Journal of Computer Network and Information Security*, vol. 9, no. 9, pp. 22-29, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[97] Hanqi Tang et al., "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense," *IEEE Access*, vol. 6, pp. 26059-26068, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[98] Karima Dichou, Victor Tourtchine, and Faycal Rahmoune, "Finding the Best FPGA Implementation of the DES Algorithm to Secure Smart Cards," *2015 4th International Conference on Electrical Engineering*, Boumerdes, Algeria, pp. 1-4, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[99] J.G. Pandey et al., "An Efficient VLSI Architecture for Data Encryption Standard and its FPGA Implementation," *2016 International Conference on VLSI Systems, Architectures, Technology and Applications*, Bengaluru, India, pp. 1-5, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[100] Veronica Ernita Kristianti et al., "Finding an Efficient FPGA Implementation of the DES Algorithm to Support the Processor Chip on Smartcard," *2018 2nd East Indonesia Conference on Computer and Information Technology*, Makassar, Indonesia, pp. 208-211, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[101] Muhammad Asif Habib et al., "Speeding Up the Internet of Things: LEAIoT: A Lightweight Encryption Algorithm Toward Low-Latency Communication for the Internet of Things," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 31-37, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[102] Yanyu Chen et al., "The Robustness and Sustainability of Port Logistics Systems for Emergency Supplies from Overseas," *Journal of Advanced Transportation*, vol. 2020, no. 1, pp. 1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[103] Murad Khan et al., "Context-Aware Low Power Intelligent SmartHome Based on the Internet of Things," *Computers & Electrical Engineering*, vol. 52, pp. 208-222, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[104] Muhammad Tausif et al., "Towards Designing Efficient Lightweight Ciphers for Internet of Things," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 8, pp. 4006-4024, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[105] David Park, "The Quest for the Quality of Things: Can the Internet of Things Deliver a Promise of the Quality of Things?," *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 35-37, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[106] Abdulatif Alabdulatif et al., "Privacy-Preserving Anomaly Detection in Cloud with Lightweight Homomorphic Encryption," *Journal of Computer and System Sciences*, vol. 90, pp. 28-45, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[107] Ruhul Amin et al., "A Light Weight Authentication Protocol for IoT-Enabled Devices in Distributed Cloud Computing Environment," *Future Generation Computer Systems*, vol. 78, no. 3, pp. 1005-1019, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[108] Muhammad Sheraz Mehmood et al., "A Comprehensive Literature Review of Data Encryption Techniques in Cloud Computing and IoT Environment," *2019 8th International Conference on Information and Communication Technologies*, Karachi, Pakistan, pp. 54-59, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[109] Abdulatif Alabdulatif et al., "Privacy-Preserving Anomaly Detection in Cloud with Lightweight Homomorphic Encryption," *Journal of Computer System and Sciences*, vol. 90, pp. 28-45, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[110] Qingchen Zhang et al., "Secure Weighted Possibilistic C-Means Algorithm on Cloud for Clustering Big Data," *Information Sciences*, vol. 479, pp. 515-525, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[111] Fei Gao, "Data Encryption Algorithm for E-Commerce Platform Based on Blockchain Technology," *Discrete and Continuous Dynamical Systems-S*, vol. 12, no. 4&5, pp. 1457-1470, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[112] Subhi R.M. Zeebaree et al., "Design and Simulation of High-Speed Parallel/Sequential Simplified DES Code Breaking Based on FPGA," *2019 International Conference on Advanced Science and Engineering*, Zakho-Duhok, Iraq, pp. 76-81, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[113] Johannes de Fine Licht, Michaela Blott, and Torsten Hoefler, "Designing Scalable FPGA Architectures Using High-Level Synthesis," *Proceedings of the 23rd ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*, Vienna, Austria, pp. 403-404, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[114] Yude Yang et al., "Parallel Computing of Multi-Contingency Optimal Power Flow with Transient Stability Constraints," *Protection and Control of Modern Power Systems*, vol. 3, no. 2, pp. 1-10, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[115] Mohamad Noura et al., "S-DES: An Efficient & Secure DES Variant," *2018 IEEE Middle East and North Africa Communications Conference*, Jounieh, Lebanon, pp. 1-6, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[116] Fatih Özkaynak, and Mukhlis I. Muhamad, "Alternative Substitutional Box Structures for DES," *2018 6th International Symposium on Digital Forensic and Security*, Antalya, Turkey, pp. 1-4, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[117] Ryndel V. Amorado, Ariel M. Sison, and Ruji P. Medina, "Enhanced Data Encryption Standard (DES) Algorithm based on Filtering and Striding Techniques," *Proceedings of the 2nd International Conference on Information Science and Systems*, Tokyo Japan, pp. 252-256, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[118] Kester Quist-Aphetsi, Bismark Tei Asare, and Laurent Nana, "IoT Node-Node Secure Communication Using RIPEMD-128 and DES," *2019 International Conference on Cyber Security and Internet of Things*, Accra, Ghana, pp. 62-65, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[119] Gaoli Wang, and Hongbo Yu, "Improved Cryptanalysis on RIPEMD-128," *IET Information Security*, vol. 9, no. 6, pp. 354-364, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[120] Constantinos Kolias et al., "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80-84, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[121] Arcelina Sukiatmodj, and YB Dwi Setianto, "Speed and Power Consumption Comparison between DES and AES Algorithm in Arduino," *Scientific Journal of Informatics*, vol. 6, no. 1, pp. 45-53, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[122] Amjad Yosef Hendi et al., "A Novel Simple and Highly Secure Method for Data Encryption-Decryption," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 232-238, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[123] Akshitha Vuppala et al., “An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm,” *Procedia Computer Science*, vol. 171, pp. 1054-1063, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[124] Fulei Ji, Wentao Zhang, and Tianyou Ding, “Improving Matsui’s Search Algorithm For The Best Differential/Linear Trails And Its Applications For DES, DESL And GIFT,” *The Computer Journal*, vol. 64, no. 4, pp. 610-627, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[125] Chunning Zhou et al., “Improving the MILP-based Security Evaluation Algorithm Against Differential/Linear Cryptanalysis Using A Divide-and-Conquer Approach,” *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 4, pp. 438-469, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[126] Lele Chen, Gaoli Wang, and GuoYan Zhang, “MILP-Based Related-Key Rectangle Attack and its Application to GIFT, Khudra, MIBS,” *The Computer Journal*, vol. 62, no. 12, pp. 1805-1821, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[127] Meichun Cao, and Wenying Zhang, “Related-Key Differential Cryptanalysis of the Reduced-Round Block Cipher GIFT,” *IEEE Access*, vol. 7, pp. 175769-175778, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[128] Huanyu Wang et al., “A Physical Design Flow Against Front-Side Probing Attacks by Internal Shielding,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 2152-2165, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[129] Michael Weiner et al., “The Low Area Probing Detector as a Countermeasure Against Invasive Attacks,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 2, pp. 392-403, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[130] Huanyu Wang et al., “Probing Attacks on Integrated Circuits: Challenges and Research Opportunities,” *IEEE Design & Test*, vol. 34, no. 5, pp. 63-71, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[131] Huanyu Wang et al., “Probing Assessment Framework and Evaluation of Antiprobing Solutions,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 6, pp. 1239-1252, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[132] Michael Weiner et al., “A Calibratable Detector for Invasive Attacks,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 5, pp. 1067-1079, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[133] Hongmei Yue, and Xin Zheng, “WITHDRAWN: Research on Encrypting Accounting Data Using Des Algorithm under the Background of Microprocessor System,” *Microprocessors and Microsystems*, pp. 1-2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[134] Ashish K Singh et al., " LVCMOS Based Low Power Implementation of DES Encryption Algorithm on 28nm FPGA," *2024 3rd International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control*, Mathura, India, pp. 383-386, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[135] Min-Yan Tsai, and Hsin-Hung Cho, “A High Security Symmetric Key Generation by Using Genetic Algorithm Based on a Novel Similarity Model,” *Mobile Networks and Applications*, vol. 26, pp. 1386-1396, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[136] Abdulmajeed Adil Yazdeen et al., “FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review,” *Qubahan Academic Journal*, vol. 1, no. 2, pp. 8-16, 2021. [CrossRef] [Google Scholar] [Publisher Link]