Chakra-3: An Area-Efficient Lightweight Block Cipher for Resource-Constrained IoT Devices

Agnik Maity
Dept. of Electronics and Communication Engineering Institute of Engineering & Management, Kolkata School of University of Engineering & Management, kolkata
Kolkata, India
agnik.chakravyuha@gmail.com

Bhavishek Mishra
Dept. of Electronics and Communication Engineering Institute of Engineering & Management, Kolkata School of University of Engineering & Management, kolkata
Kolkata, India
bhavishek.chakravyuha@gmail.com

Swastika Pradhan
Dept. of Electronics and Communication Engineering Institute of Engineering & Management, Kolkata School of University of Engineering & Management, kolkata
Kolkata, India
swastika.chakravyuha@gmail.com

Prabaha Mondal
Dept. of Electronics and Communication Engineering Institute of Engineering & Management, Kolkata School of University of Engineering & Management, kolkata
Kolkata, India
prabaha.chakravyuha@gmail.com

Oindrila Dey
Dept. of Electronics and Communication Engineering Institute of Engineering & Management, Kolkata School of University of Engineering & Management, kolkata
Kolkata, India
oindrila.chakravyuha@gmail.com

Mihir Lal Saha
Dept. of Electronics and Communication Engineering Institute of Engineering & Management, Kolkata School of University of Engineering & Management, kolkata
Kolkata, India
mlsahaece@gmail.com

2026 9th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) | 979-8-3315-6339-4/26/$31.00 ©2026 IEEE | DOI: 10.1109/IEMENTECH202669403.2026.11434281

***Abstract*— The increase in the application of Internet of Things has increased the demand on cryptographic primitives that provide strong security and can be implemented on stringent hardware and resource constrained devices. This paper proposes Chakra-3, a new lightweight block cipher, which is specifically targeted at resource-constrained systems. Chakra-3 is a Feistel structure based block cipher, in which the same encryption and decryption structures are used and complex implementing the approach is minimized. The cipher is of 64-bit data block having the 256-bit secret key and runs 8 rounds of this cipher as an effective compromise between security and efficiency. The lightweight logical operations, compact substitution mechanisms, and regulated bit permutation are used in each round to increase the confusion and diffusion and reduce the hardware overhead. CMOS Hardware synthesis using GPDK 90nm technology node shows that Chakra-3 requires about 1100 gate equivalents with a peak operating frequency of about 120 MHz and a throughput of about 1 Gbps. Security analysis shows that the cipher has a large avalanche effect, with almost half the bits changing on a single bit input change, and passed NIST standard statistical tests of randomness. These findings demonstrate that Chakra-3 offers high-performance low-area cryptography implementation that can be used in secure communications in IoT and embedded systems.**

Keywords*— *Block Cipher, Cryptography, ASIC, Hardware Security, Image Encryption

I. Introduction and Related Works

The Internet of Things is a pervasive network based on the network of various physical entities like vehicles, devices, appliances, etc. which are embedded with the help of sensors, software, etc. which ensures connectivity and seamless data exchange across these entities. IoT devices (like actuators, sensors, processing software, etc.) which are used for exchanging data over the internet. They can be either rich in resources or resource constraint like barcodes, infrared sensors, Radio Frequency Identification (RFID) tags, etc. With the dawn of 5G (fifth generation) along with Artificial Intelligence (AI), the applications of Internet of Things (IoT) have tremendously evolved into various fields like smart healthcare system, smart cards, smart cities, smart agricultural systems, smart logistics, intelligent transport system, etc.

In the past decade numerous lightweight cryptographic block ciphers have been proposed and developed like DRCipher [6], IoVCipher [7], HDLBC [8], LELBC [9], IVLBC [10], SCENERY [11], SAND [12], Shadow [13], ACT [14], Loong [15], SFN [16], CHAM [17], PICO [18], Midori [19], HISEC [20], Halka [21], I-PRESENT [22], PRINCE [23], TWINE [24], KLEIN [25], LBlock [26], LED [27], etc. Some of these existing lightweight block ciphers can be implemented in hardware whereas some in software and few can be implemented in both hardware and software. The emergence of these various lightweight block ciphers has been gaining remarkable recognition in academia, industry and government ever since. There are two ground structures: Substitution-Permutation Network (SPN) and Feistel Network (FN) both of which are primarily used while making Lightweight Block Ciphers. The encryption and decryption algorithms in SPN are different. While the confusion and diffusion efficiency is excellent in SPN making them highly resistant to differential and linear cryptanalysis, some disadvantages still remain. The decryption process demands the inverse of the s-box and permutation layer which are usually computationally more complex and expensive. In this paper, a novel Lightweight Block Cipher, Chakra-3 has been proposed. It is based on the Feistel Network (FN) structure making it highly suitable for resource-constrained devices. Chakra-3 has a block size of 64 bits and the key size of 256 bits. It undergoes 8 iterative round transformations. The main module is Feistel-based. Therefore, the 64 bits input block is first divided into two equal blocks of size 32 bits each. Round operations performed on each of these blocks include XOR operations with the subkeys and F Block. Furthermore, the

979-8-3315-6339-4/26/$31.00 ©2026 IEEE

round transformation is followed by Bit Jumbling which in turn increases the confusion. The area constraint of Lightweight Block Cipher is up to 3000GE. Chakra-3 consumes 1097.86 GE (gate equivalents) in area on 90nm technology making it lightweight in nature. It has passes NIST tests and exhibits strong Avalanche effect.

Over the past decade the need for the use of resource-constrained devices has tremendously increased as mentioned earlier thereby increasing the need for better protection and security of data against breaches and theft. Consequently, the need for Lightweight Encryption algorithms has risen enormously. In the recent years several Lightweight Block Ciphers have been developed who find their application in various fields. For example, DRCipher [6] with a block size of 64 bits adopts GFN structure presenting a pseudo-random dynamic round algorithm and is highly secure against differential, algebraic and linear cryptanalysis but provides no information regarding the throughput and latency of the cipher which is very essential for determining the efficiency of the cipher. IoVCipher [7], applicable in the autonomous vehicle market, ensures the security of micro devices on the CAN bus system and uses the extended MISTI structure provides an effectively balanced low latency but the equivalent gate area appears to be higher than the range suitable for lightweight block ciphers. HDLBC [8] proposed by Li et al. overcomes the difficulty of changing only half of the plaintexts after each iteration thereby achieving a trade-off between high diffusivity and hardware resources. Though it is proven to be secure against several cryptanalytic attacks it lacks any information about the time delay, power and throughput. LELBC [9], a low energy lightweight block cipher which finds its application in smart agriculture. The implementation of a novel Permutation-Substitution-Permutation (PSP) structure and a 4-bit low energy s-box has contributed in achieving a low energy and gate area equivalent. However, the power, throughput and time delay of the cipher have not been provided. IVLBC [10], a SPN based involutive lightweight block cipher has proposed a Feistel with tree structure and a nibble-based involutive permutation. It provides high diffusion and is also resistant against various security attacks. However, it lacks any details on the power and delay. SCENERY [11] is a Feistel-based cipher which provides both hardware implementation on 0.18µm CMOS as well as software implementation on 8-b microcontrollers. Although it's resistance against some cryptanalytic attacks has been given, no data regarding the cipher's reliability against side channel attacks (SCAs) has been given.

II. Proposed Block Cipher Architecture

In this section the overall architecture of the Chakra-3 is elaborated. The proposed Algorithm is a Feistel structure in which the main block of plain text is divided into two equal sub-parts and then the various operations is carried on. It is also a symmetric encryption algorithm it means it requires only a single key to encrypt and decrypt the data. This architecture demonstrates the proper bit randomization using different types of operation. The proposed architecture has 8 iterations with 64-bit of plaintext, 32-bit of subkey and based on plaintext the ciphertext is also of 64-bit.

A. Main Algorithm

The more detailed architecture of the Chakra-3 can be obtained by investigating the internal structure of a single round. The first and initial phase explains the division of the plaintext in two equal subparts each having 32-bit and suppose both the subpart are known as Li and Ri. Then in the further step the Li XNOR with the subkey. The output of it can be called as wi. The output wi goes to the F-block where it is gone through certain steps and gain the output of the F-block XOR with the Ri and in its output Li+1 is obtained. The wi directly goes to the Ri+1. And in the last step the proper jumbling operation takes place in order to obtained a more random ciphertext. The schema of the round is shown the figure 1.

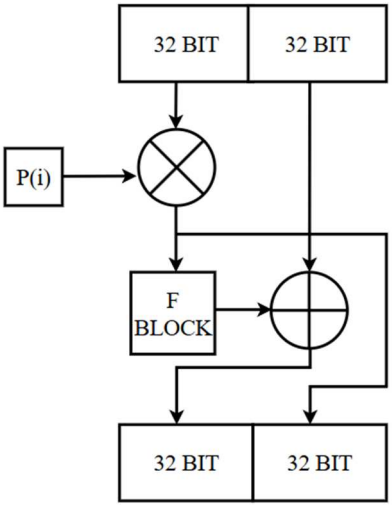

Fig. 1 Encryption Process of Proposed Cipher

B. F Block

It is simply a function block where actually the various operation takes place for the fulfillment of the confusion property. In this block the input is of 32-bit. From this 32-bit four 8-bit blocks are obtained and the first, third block is passed in the s-box

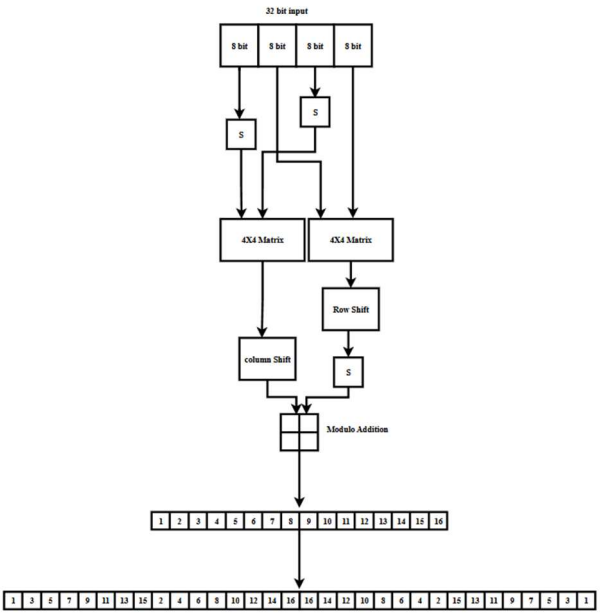

Fig. 2. F Block

[Where the changing of the bit index is performed]. Then with these two blocks a 4x4 matrix is formed then it gets in column shift block. On the other hand, the left two subblocks is used to form another 4x4 matrix and passed in a row shift block and again it goes in the S-box. Then both the output reaches the modulo addition block and in the output 16-bit block is obtained and then by arranging it to 32-bit the final output is obtained for the F-Block. The architectures of the F-block are shown in the figure 4.

C. Key Generation Algorithm

For processing the 8 rounds of iterations 32-bit subkey is required. And the subkeys are generated with the 256-bit of encryption key that is show in the figure 2. The procedure of the generation of subkeys is as follows:

- The 256-bit main key is equally divided into 4 subparts. Each subparts having the bit length of 64-bit.
- Each subpart is arranged in 8X8 Matrix form it is shown in the Figure 3.
- In the next step the subparts are passed through a block known as m-box.
- At the last step 64-bit subparts are further divided into two equal half 32-bit to fulfill the requirement of the subkeys for the round processing.

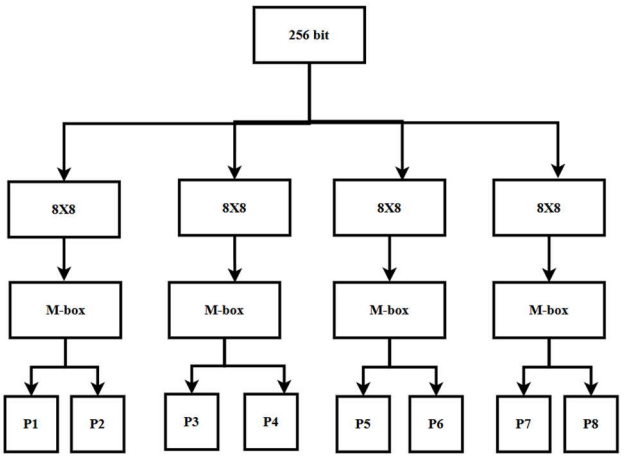

Fig. 3 Subkey Generation

a11	a12	a13	a14	a15	a16	a17	a18
a21	a22	a23	a24	a25	a26	a27	a28
a31	a32	a33	a34	a35	a36	a37	a38
a41	a42	a43	a44	a45	a46	a47	a48
a51	a52	a53	a54	a55	a56	a57	a58
a61	a62	a63	a64	a65	a66	a67	a68
a71	a72	a73	a74	a75	a76	a77	a78
a81	a82	a83	a84	a85	a86	a87	a88

Fig. 4 8x8 Matrix Block

III. MATLAB BASED IMAGE ENCRYPTION

Fig.5 represents the visual comparative study between the original medical image and its encrypted and decrypted counterparts. (α) shows the original image. Its encrypted image (β) shows a noise-like appearance without any recognizable structure thus, indicating effective confusion and diffusion properties of the proposed design making the image intelligible to attackers. In contrast (γ) represents the decrypted image which successfully reconstructs the original image without any degradation thereby verifying the reversibility process of the encryption and decryption of the proposed block cipher.

The RGB histograms of the original medical image as depicted in Fig.6 (A)-(C) indicates a highly non-uniform distribution with prominent peaks due to natural images possessing significant statistical predictability. The histograms of the encrypted image shown in Fig.6 (D)-(F) on the other hand, represent a much uniform distribution for the red, green and blue channels at all intensity levels. This demonstrates that the encrypted image successfully conceals the statistical information of the original image making the design resistant towards histogram-based attacks.

Fig.7 indicates the difference in values between the original and encrypted image with respect to entropy and correlation. The entropy of the original image is 6.0022 whose value rises to 7.5138 after encryption, the development indicating the high randomness of the encrypted algorithm making it immune to entropy-based attacks. Quantitatively the correlation reduces from 0.9450 in the original image to 0.0936 in the encrypted image.

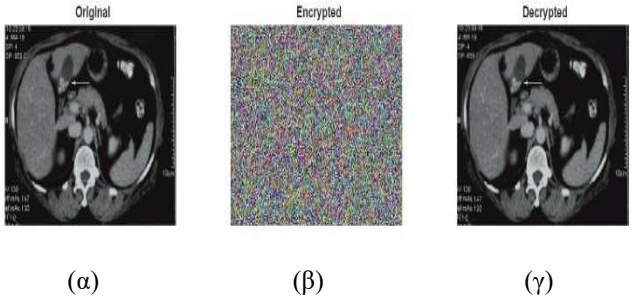

Fig. 5 (α), (β), (γ) depicts the Original, Encrypted and Decrypted version of the Medical Image.

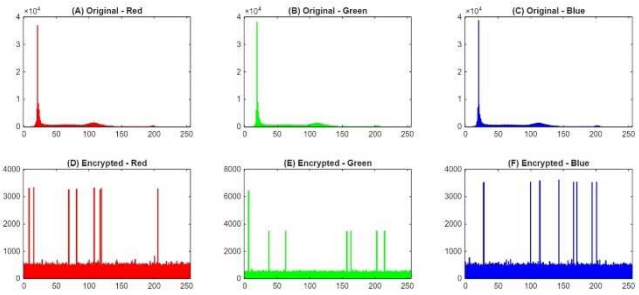

Fig.6 Original Medical Image Histogram for Red, Green and Blue components are depicted in (A), (B) and (C). Encrypted Image Histogram for Red, Green and Blue components are depicted in (D), (E) and (F).

```
Entropy  Original: 6.0022 | Encrypted: 7.5138
Corr(H) Original: 0.9450 | Encrypted: 0.0936
```

Fig.7 Correlation and Entropy values of Original and Encrypted Image

Fig.8 exhibits the adjacent pixels correlation analysis which has been done in horizontal, vertical and diagonal directions in order to assess its resistance against statistical attacks. It shows the distribution of adjacent pixel pairs on the original medical image where high linear correlation is observed across all the three-color channels. Fig.9 on the contrary, shows the corresponding distribution for the image encryption in the directions of horizontal, vertical and diagonal across the three-color channels where the pixel values are uniformly scattered resulting in near 0 correlation thereby ensuring that exploitation of statistical properties of the plaintext image by the potential attackers is prevented.

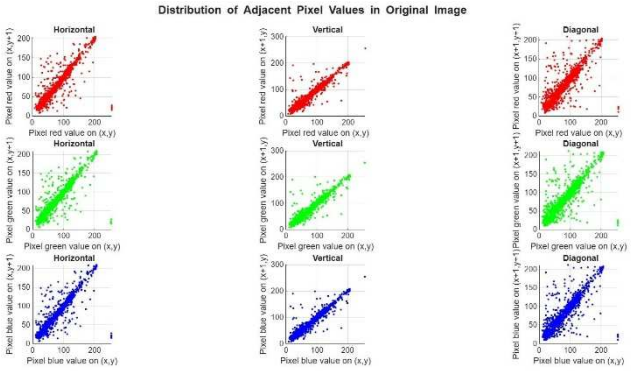

Fig.8 Adjacent Pixels Distribution of the Original Medical Image

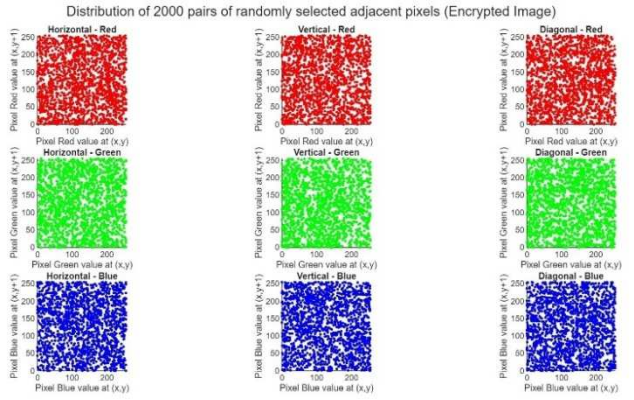

Fig.9 Randomly Chosen Adjacent Pixels Distribution of the Encrypted Medical Image

Fig.10 demonstrates the correlation between original and encrypted medical image across the green channel. The original image shows a strong linear relationship among neighboring pixel values. Conversely, the encrypted image shows a random distribution indicating that the encrypted image is statistically independent of the plaintext image.

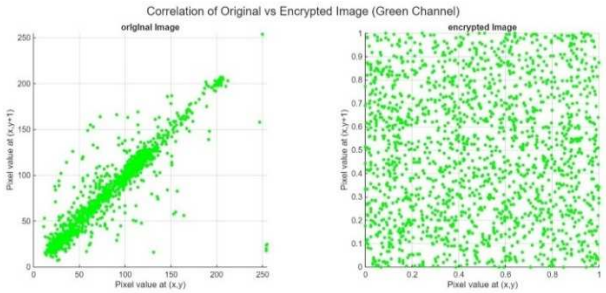

Fig.10 Correlation comparison between original and encrypted medical image

IV. Result and Discussion

The proposed novel block cipher, Chakra-3 has achieved a compact design with an equivalent gate area of 1097.86 GE which has been evaluated using a 90 nm process technology. As illustrated in Fig.11, in comparison to several existing block cipher, Chakra-3 has attained a much lower area thereby making its simplified and optimized 8 rounds Feistel architecture beneficial. Chakra-3 has furthermore attained a throughput of 0.952 Gbps, thereby, marking the highest throughput among various existing lightweight block ciphers as shown in Fig.12, most of them remaining in the kilobit-to-megabit range. With a maximum frequency of 119.05 MHz, it surpasses most reported lightweight ciphers, which typically operate only in the kilohertz to megahertz range. Moreover, achieving 867,489 kbps/kGE in hardware efficiency, the design sets a new benchmark, several orders of magnitude higher than many lightweight block ciphers. Fig.13 and 14 illustrates the comparison of frequency and hardware efficiency with the existing block cipher algorithms.

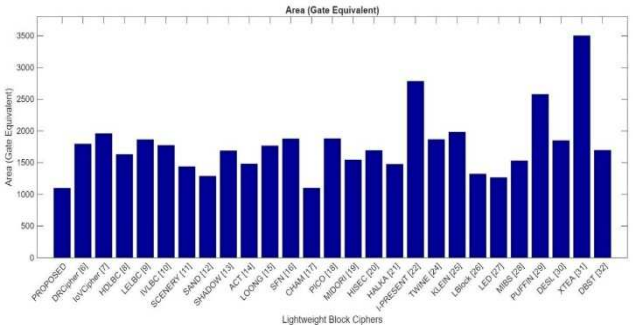

Fig. 11 Comparative Evaluation of Area with Existing Cipher

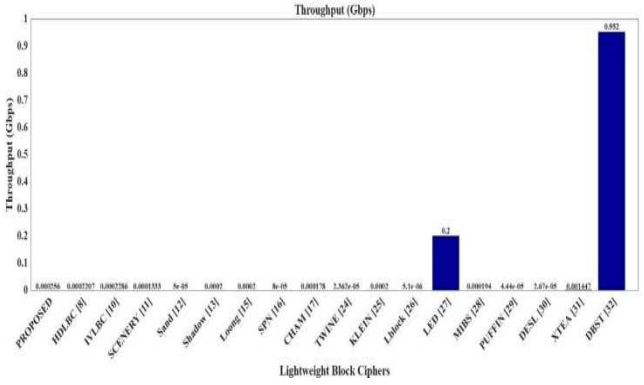

Fig. 12 Comparative Evaluation of Throughput with Existing Cipher

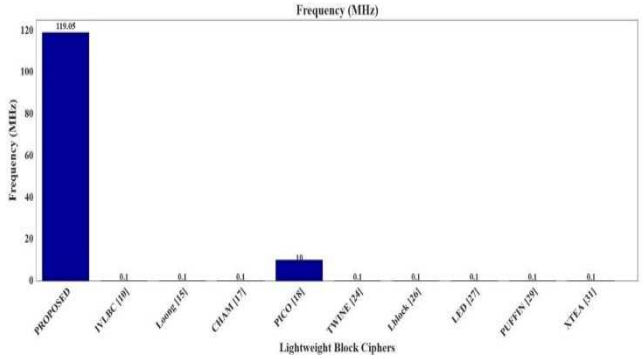

Fig.13 Comparative Evaluation of Frequency with Existing Cipher

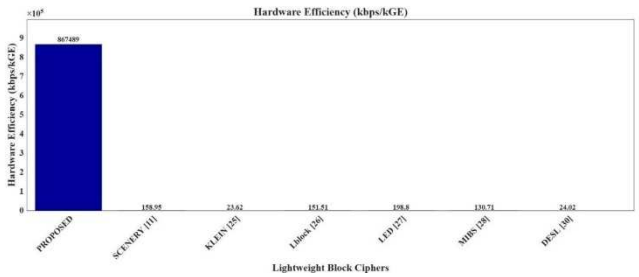

Fig. 14 Comparative Evaluation of Hardware Efficiency with Existing Cipher

V. CONCLUSION

This paper has presented an area optimized novel FN-based architecture, Chakra-3 which caters to the urgent requirement for reliable and secure encryption in resource-constrained devices. The proposed design will lead to significant reduction in cost with its lightweight nature. Its superior frequency, throughput, and efficiency metrics as compared to several existing lightweight block ciphers, along with the low chip area of 1097.86GE which was achieved using a 90 nm process technology, establishes it as one of the most effective lightweight cipher implementations to date. Therefore, the new introduced design can be a strong alternative to other well-known block ciphers for providing security for IoT-based resource-constrained devices. The MATLAB-based implementation of Chakra-3 also confirms the feasibility of this design. Furthermore, comprehensive security analysis of the proposed design by analyzing its security and resistance against various advanced cryptanalytic attacks will be considered for future research aspect.

REFERENCES

[1] A. Farooq, S. Riaz, A. Abid, S. F. Shah, and M. A. Iqbal, "A review on lightweight cryptography for Internet of Things based applications," *Journal of Network and Computer Applications*, vol. 181, 2021.

[2] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," IEEE Access, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[3] A. A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria, and M. Daud, "Trend analysis on the design of lightweight block cipher: A systematic literature review," J. King Saud Univ. – Comput. Inf. Sci., vol. 35, no. 5, Art. no. 101550, 2023, doi: 10.1016/j.jksuci.2023.04.003.

[4] Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," Future Generation Computer Systems, vol. 157, pp. 288–302, 2024, doi: 10.1016/j.future.2024.03.054.

[5] K. Saranya and K. Vijeyakumar, "A low area FPGA implementation of reversible gate encryption with heterogeneous key generation," Circuits, Systems, and Signal Processing, vol. 40, pp. 3836–3865, 2021, doi: 10.1007/s00034-021-01649-1.

[6] J. Kuang, X. Cao, S. Li, and L. Li, "DRcipher: A pseudo-random dynamic round lightweight block cipher," J. King Saud Univ. – Comput. Inf. Sci., vol. 36, no. 1, Art. no. 101928, 2024, doi: 10.1016/j.jksuci.2024.101928.

[7] X. Huang, L. Li, H. Zhang, J. Yang, and J. Kuang, "IoVCipher: A low-latency lightweight block cipher for Internet of Vehicles," Ad Hoc Networks, vol. 160, Art. no. 103524, 2024, doi: 10.1016/j.adhoc.2024.103524.

[8] Y. Li, J. Feng, Q. Zhao, and Y. Wei, "HDLBC: A lightweight block cipher with high diffusion," Integration, the VLSI Journal, vol. 94, Art. no. 102090, 2023, doi: 10.1016/j.vlsi.2023.102090.

[9] Q. Song, L. Li, and X. Huang, "LELBC: A low energy lightweight block cipher for smart agriculture," Internet of Things, vol. 25, Art. no. 101022, 2024, doi: 10.1016/j.iot.2023.101022.

[10] X. Huang, L. Li, and J. Yang, "IVLBC: An involutive lightweight block cipher for Internet of Things," IEEE Systems Journal, vol. 17, no. 2, pp. 3192–3203, Jun. 2023, doi: 10.1109/JSYST.2022.3227951.

[11] J. Feng and L. Li, "SCENERY: A lightweight block cipher based on Feistel structure," Frontiers of Computer Science, vol. 16, Art. no. 163813, 2022, doi: 10.1007/s11704-020-0115-9.

[12] S. Chen, Y. Fan, L. Sun, et al., "SAND: An AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations," Designs, Codes and Cryptography, vol. 90, pp. 155–198, 2022, doi: 10.1007/s10623-021-00970-9.

[13] Y. Guo, L. Li, and B. Liu, "Shadow: A lightweight block cipher for IoT nodes," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 13014–13023, Aug. 2021, doi: 10.1109/JIOT.2021.3064203.

[14] T. Kassim and K. Jithendra, "ACT: An ultra lightweight block cipher for Internet of Things," Int. J. Comput. Digital Syst., vol. 9, pp. 921–929, 2020, doi: 10.12785/ijcds/090512.

[15] B.-T. Liu, L. Li, R.-X. Wu, M.-M. Xie, and Q. P. Li, "Loong: A family of involutional lightweight block ciphers based on SPN structure," IEEE Access, vol. 7, pp. 136023–136035, 2019, doi: 10.1109/ACCESS.2019.2940330.

[16] L. Li, B. Liu, Y. Zhou, and Y. Zou, "SFN: A new lightweight block cipher," Microprocessors and Microsystems, vol. 60, pp. 138–150, 2018, doi: 10.1016/j.micpro.2018.04.009.

[17] B. Koo et al., "CHAM: A family of lightweight block ciphers for resource-constrained devices," in Proc. ICISC 2017, LNCS vol. 10779. Springer, 2018, pp. 3–25, doi: 10.1007/978-3-319-78556-1_1.

[18] G. Bansod, N. Pisharoty, and A. Patil, "PICO: An ultra lightweight and low power encryption design for ubiquitous computing," Defence Science Journal, vol. 66, pp. 259–266, 2016, doi: 10.14429/dsj.66.9276.

[19] S. Banik et al., "Midori: A block cipher for low energy," in Proc. ASIACRYPT 2015, LNCS vol. 9453. Springer, 2015, pp. 411–436, doi: 10.1007/978-3-662-48800-3_17.

[20] S. S. M. AlDabbagh, I. F. T. Al Shaikhli, and M. A. Alahmad, "HISEC: A new lightweight block cipher algorithm," in Proc. SIN 2014, ACM, 2014, pp. 151–156, doi: 10.1145/2659651.2659662.

[21] S. Das, "Halka: A lightweight, software friendly block cipher using ultra-lightweight 8-bit S-box," Cryptology ePrint Archive, 2014.

[22] M. Zaba et al., "I-PRESENT: An involutive lightweight block cipher," Journal of Information Security, vol. 5, pp. 114–122, 2014, doi: 10.4236/jis.2014.53011.

[23] G. Leander et al., "PRINCE: A low-latency block cipher for pervasive computing," in Proc. ASIACRYPT 2012, LNCS vol. 7658. Springer, 2012, pp. 208–225, doi: 10.1007/978-3-642-34961-4_14.

[24] T. Suzaki et al., "TWINE: A lightweight, versatile block cipher," in ECRYPT Workshop on Lightweight Cryptography, 2011.

[25] Z. Gong, S. Nikova, and Y. W. Law, "KLEIN: A new family of lightweight block ciphers," in Proc. RFIDSec 2011, LNCS vol. 7055. Springer, 2012, pp. 1–18, doi: 10.1007/978-3-642-25286-0_1.

[26] W. Wu and L. Zhang, "LBlock: A lightweight block cipher," in Proc. ACNS 2011, LNCS vol. 6715. Springer, 2011, pp. 327–344, doi: 10.1007/978-3-642-21554-4_19.

[27] J. Guo et al., "The LED block cipher," in Proc. CHES 2011, LNCS vol. 6917. Springer, 2011, pp. 326–341, doi: 10.1007/978-3-642-23951-9_22.

[28] M. Izadi et al., "MIBS: A new lightweight block cipher," in Proc. CANS 2009*, LNCS vol. 5888. Springer, 2009, pp. 334–348, doi: 10.1007/978-3-642-10433-6_22.

[29] H. Cheng, H. M. Heys, and C. Wang, "PUFFIN: A compact block cipher for embedded systems," in Proc. EUROMICRO DSD 2008, pp. 383–390, doi: 10.1109/DSD.2008.34.

[30] G. Leander et al., "New lightweight DES variants," in Proc. FSE 2007, LNCS vol. 4593. Springer, 2007, pp. 196–210, doi: 10.1007/978-3-540-74619-5_13.

[31] J. P. Kaps, "Chai-Tea: Cryptographic hardware implementations of xTEA," in Proc. INDOCRYPT 2008, LNCS vol. 5365. Springer, 2008, pp. 363–375, doi: 10.1007/978-3-540-89754-5_28.

[32] L. Yan, L. Li, and Y. Guo, "DBST: A lightweight block cipher based on dynamic S-box," Frontiers of Computer Science, vol. 17, Art. no. 173805, 2023, doi: 10.1007/s11704-022-1677-5.

[33] R. C. Phan and M. U. Siddiqi, "A framework for describing block cipher cryptanalysis," IEEE Trans. Computers, vol. 55, no. 11, pp. 1402–1409, Nov. 2006, doi: 10.1109/TC.2006.169.

[34] C. De Canniere, A. Biryukov, and B. Preneel, “An introduction to block cipher cryptanalysis,” Proc. IEEE, vol. 94, no. 2, pp. 346–356, Feb. 2006, doi: 10.1109/JPROC.2005.862300.

[35] E. Duan and W. Wu, “Invariant subspace of the P-SPN structure with a class of linear layer matrix,” Chinese Journal of Electronics, vol. 34, no. 5, pp. 1545–1558, 2025, doi: 10.23919/cje.2024.00.239.

[36] M. Cao and W. Zhang, “Related-key differential cryptanalysis of the reduced-round block cipher GIFT,” IEEE Access, vol. 7, pp. 175769–175778, 2019, doi: 10.1109/ACCESS.2019.2957581.