Chakra-1: Ultra-Lightweight Hybrid Cipher Architecture for Next Generation IoT Security

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

Agnik Maity
Dept. of Electronics & Communication Engineering
Institute of Engineering & Management, Kolkata, School of University of Engineering & management, Kolkata
Kolkata,India
agnikmaity12@gmail.com

Antarik Sinha
Dept. of Electronics & Communication Engineering
Institute of Engineering & Management, Kolkata, School of University of Engineering & management, Kolkata
Kolkata,India
antariksinha2017@gmail.com

Sayan Chatterjee
Dept. of Electronics & Telecommunication Engineering
Jadavpur University, Kolkata
Kolkata,India
sayan.chatterjee@jadavpuruniversity.in

2026 9th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) | 979-8-3315-6339-4/26/$31.00 ©2026 IEEE | DOI: 10.1109/IEMENTECH202669403.2026.11434099

***Abstract*—The prevalence of Internet of Things (IoT) in fundamental sectors such as health services, industrial automation, and smart infrastructure has intensified the demand of lightweight cryptography solutions with high security that operate with a very strict resource constraint. The current paper presents Chakra-1, a hybrid block cipher architecture which is extremely lightweight and combines the Substitution-Permutation Network (SPN) and Feistel models. A 64-bit data block is encrypted by the design with 128-bit master key by means of a bit-jumbling permutation as an alternative to traditional S-boxes to provide diffusion at the lowest hardware cost. A key scheduling algorithm without gates is proposed to avoid extra hardware expenses. The proposed cipher features a notably smaller hardware footprint of 448 Gate Equivalents (GE), extremely low power usage of 2.390 µW, and a minimal delay of just 3.374 ns when implemented using 90 nm technology. The proposed block cipher successfully completed all 15 evaluations from the NIST SP 800-22 suite using 1 billion cipher text outputs, demonstrating strong statistical randomness. Analysis of its performance reveals that it is more efficient than existing lightweight ciphers in terms of area, delay, and energy usage.**

Keywords— Lightweight cryptography, Hybrid block cipher, IoT Security, SPN- Feistel architecture, Low power encryption

I. Introduction and Related Works

In this era of advancing technologies, various different devices are linked and connected to each other, wireless through the internet, to build a smarter ecosystem of devices that will make tasks simpler, thus causing an advent of IoT. A question of privacy and security arises as the internet is used by the physical devices for interaction with each other [1]. In order to secure the ecosystem of devices through IoT a need for encryption of data comes into play. Lightweight cryptography is introduced to deal with the security level of the IoT constrained devices as the conventional cryptographic algorithms are unsuitable for IoT constrained devices [2]. NIST has provided certain criteria that are required to be fulfilled for making the cryptography algorithms lightweight which is suitable for IoT constrained overcoming the issue of space constraints whereas maintaining an efficient and smooth performance. These algorithms are perfect for applications such as embedded devices, tags with RFID, smart cards, and wireless sensors since they are especially designed to provide adequate security with minimal computational and hardware overheads [3].

In cryptography algorithms to make the exchange of information secure, a public or private key is used along with the plain text to obtain the cipher text in encrypted form. Primarily either of the two types of keys is used in any cryptography algorithms which are – symmetric key or asymmetric key. With the help of symmetric key, block cipher [4] or stream cipher can be generated of which block ciphers are more efficient and provide better performance [5]. In earlier days, Advanced Encryption Standard (AES) [6] and Data Encryption Standard (DES) [7] were used in which SPN and Feistel structure were used as the structure for algorithms respectively. SPN structure in the AES has multiple rounds that help in providing robust security but it cannot be used in the modern IoT constrained devices as it had greater power consumption and the gate area were rather high. The Feistel structure in DES was lighter in comparison of the AES but it was susceptible to brute force attack because of short key length. Thus, they were replaced by lightweight cryptography which is appropriate and suitable for IoT constrained devices. In the latest lightweight cryptography algorithm, the ciphers like - ANU [8], RECTANGLE [9], GIFT [10], SIMON and SPECK [11], ACT [12], BORON [13], and PICCOLO [14] are designed on the basis of SPN and Feistel structure. The SPN and Feistel structure are combined to form new cipher designs which are lightweight as well as provide robust security. They have lesser number of rounds than the AES but larger key size than DES making the newer cipher both robust and lightweight. This improvement in the cipher design over the conventional cryptographic algorithms has helped in the designing of lightweight block cipher which can be used in the IoT constrained devices. Furthermore, the landscape of lightweight ciphers has become even more varied with the introduction of new design philosophies including the utilization of ARX (Addition, Rotation, and XOR) structures and tweakable block ciphers [15].

Despite the presence of numerous cryptographic block cipher algorithms, a large amount of research work on lightweight cryptography needs to be done, as most of the existing algorithms possess some limitations and challenges that must

be overcome for efficient implementation in IoT-constrained devices. A novel cryptographic block cipher which is ultra-lightweight in nature has been proposed in this paper for IoT devices with resource-constrained by combining the SPN and Feistel structures to provide robust security while consuming less gate equivalent area and power.

II. Construction of Proposed Block Cipher

This work introduces a newly designed ultra-lightweight block cipher specifically aimed at IoT devices with low power, such as compact sensors, smart cards, and RFID systems, while still ensuring a satisfactory level of security. It has a unique hybrid design which combines both SPN and Feistel-based encryption designs with the ability to operate using a data block of 64-bit and a key size of 128 bits. This design does not have S Boxes unlike in traditional block ciphers that are used to provide confusion and diffusion in encryption. Rather, the bit diffusion jumbling process is applied during each round of iteration through bit permutation which essentially repeats the role of substitution boxes. A complete gateless key schedule algorithm is used to enhance security which does not require any additional hardware.

It is a block cipher which uses 64-bit plaintext blocks and 128-bit key, so it can be used in very light security implementations. It is a Feistel network that is created by combining substitution and permutation layers, which consists of eight encryption rounds. The encryption and decryption algorithms with detailed description is given in the following section.

A. Main Algorithm

The plaintext of 64-bit is split into four 16-bit plaintext blocks. These blocks may be referred to as: P1, P2, P3, P4.

A total of 8 encryption rounds is performed. Each round uses one round key (K_1 to K_8) and four F (jumbling) blocks. For each round (i = 1 to 8):

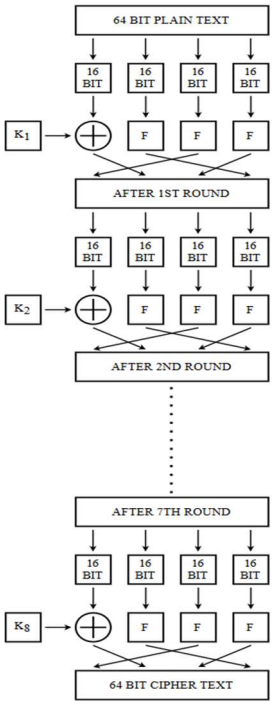


Fig. 1 Encryption Process of Proposed Cipher

Step 1: Take the first 16-bit block P1 and XOR it with the round key K_i.

Step 2: The result of XOR is passed through the F Block (permutation).

Step 3: Pass blocks P2, P3, and P4 through the F Block directly.

Step 4: Perform inter-block permutation between all four blocks as per the defined wiring scheme in the architecture diagram.

Step 5: The output becomes the new set of P1, P2, P3, P4 for the next round.

This process continues for 8 rounds, updating all blocks through XOR, F Block, and inter-permutation in each round. After the final (8^{th}) round, the 4 processed 16-bit blocks are concatenated to form the final 64-bit cipher text.

B. Jumbler Block

One input of 16 bits x[n] and Output of 16 bits y[n].

Y[n]=x[15], x[13], x[11], x[9], x[7], x[5], x[3], x[1], x[14], x[12], x[10], x[8], x[6], x[4], x[2], x[0]

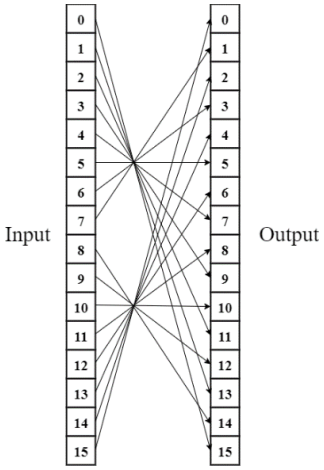


Fig. 2. F Block (Jumbler Block)

C. Key Generation Algorithm

A secret key of 128-bit is used to derive 8 round keys (K_1 to K_8), each of 16 bits.

Steps:

Eight 16-bit sub-blocks are formed by dividing the 128-bit key. Each 16-bit block is represented as a 4x4 matrix.

Each matrix is passed through a rotation operation, which scrambles the bits to enhance complexity. The rotation operation consists of eight step – row shift and column shift alternatively.

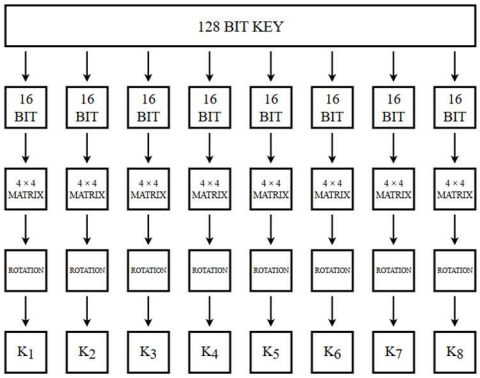


Fig. 3 Key Generation

In the row shift operation, the first row is shifted to its right (0,1,2,3) > (3,0,1,2) the remaining matrix remains unchanged.

In the column shift operation, the column row is shifted to its top (0,4,8,12) -> (12,0,4,8) the remaining matrix remains unchanged.

The output of each rotation gives a round key of 16-bit: K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8.

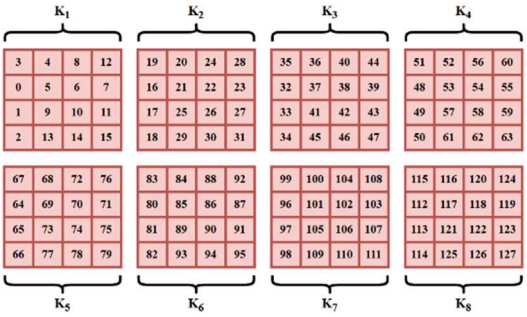


Fig. 4 Key Matrix Block

D. Encryption Procedure

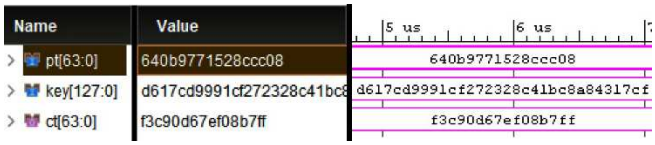
The method proposed uses jumbling of bits, matrix manipulations and simple logical XOR operations. Consequently, the data can only be decrypted by the authorized users to use it. The revealed system operates using 64 bits of plaintext data and was made as lightweight as possible. To enable this, the huge data block will be divided into several 16-bit segments with each segment being handled by different data channel. The same process is also repeated with other blocks of data. In the obtained output, the results of all the processed data block are added to obtain the encrypted data. The primary key is split into eight 16-bit sub keys used in several rounds of encryption. This will guarantee the method provides a high quality of performance on resource-restricted devices. The proposed encryption algorithm uses low power and needs minimal memory as well as low storage space.

E. Decryption

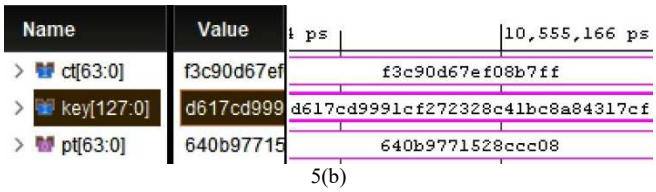
For decryption of data, the encryption process will be performed in the reverse sequence of the rounds that are used in encryption. The 16-bit blocks of cipher text are subjected to inverse inter-block permutations, inverse F block operations and XOR operations with the corresponding round keys in reverse order (K8 to K1) to basically reassemble the original 64-bit plaintext.

III. Simulation and FPGA Based Implementation

This section contains the results of the proposed architecture of an ultra-lightweight block cipher developed with the help of Verilog HDL. To confirm the performance of the cipher, all the simulations were performed in Xilinx Vivado 2018.2 web pack version where the implementation was done on the Artix-7 Xilinx FPGA.



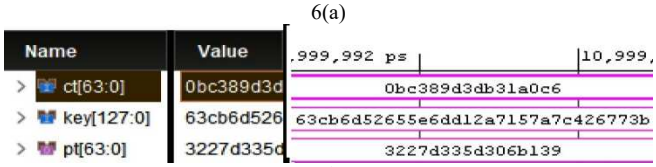
5(a)



5(b)

Fig. 5 (a), 5(b) Simulated Output of Test Case 1

6(a)



6(b)

Fig. 6 (a), 6(b) Simulated Output of Test Case 2

Figures 5(a) and 5(b) show an encryption and decryption process of test case 1 and Figures 6(a) and 6(b) represent an encryption and decryption process of test case 2. Table I represents the test cases, detailing the plaintext and keys utilized in the simulation process within the Xilinx Vivado tool. The test cases are presented in hexadecimal bit format.

TABLE I. Test Cases

Serial No.	Plain Text	Key	Cipher Text
Test Case 1	640b9771528ccc08	d617cd9991cf272328c41bc8a84317cf	f3c90d67ef08b7ff
Test Case 2	3227d335d306b139	63cb6d52655e6dd12a7157a7c426773b	0bc389d3db31a0c6

IV. Performance Evaluation

The newly developed method has attained a remarkably low equivalent gate count of just 448 GE and demonstrates impressive speed with a minimal computational time of 3.374 ns, alongside ultra-low power consumption of 2.390 µW when evaluated in Cadence Genus using Gpdk 90 nm process technology. Furthermore, it was synthesized on a Virtex 5 (xc5vlx30-3-ff324 - 65 nm) FPGA board utilizing Xilinx ISE 14.7. Table II displays the comparative analysis with the existing algorithms that were created utilizing either the SPN or Feistel architecture.

TABLE II. Comparison of Lightweight Block Cipher Algorithms

Ciphers	Block Size (Bit)	Key Size (Bit)	Structure	Area (GE)
PROPOSED	64	128	SPN, FEISTEL	448
SIMON[11]	32	64	FEISTEL	523
SPECK[11]	32	64	FEISTEL	580
GOST[30]	64	256	FEISTEL	651
PICCOLO[14]	64	80	FEISTEL	683
ANU[8]	64	80	FEISTEL	1015
QTL[29]	64	64	SPN, FEISTEL	1026
TEA[28]	64	128	FEISTEL	1140

ACT[12]	64	80	SPN	1481
TWINE[27]	64	80	FEISTEL	1503
MIDORI[26]	64	128	SPN	1542
SAND[25]	128	128	FEISTEL	1563
PRESENT[24]	64	80	SPN	1570
RECTANGLE[9]	64	80	SPN	1599.5
LOONG[23]	64	128	SPN	1766
SFN[22]	64	96	SPN, FEISTEL	1876.04
BORON[13]	64	128	SPN	1939
mCRYPTON[21]	64	64	SPN	2420
CLEFIA[20]	39	128	FEISTEL	2488
KLEIN[19]	64	80	SPN	2629
HIGHT[18]	64	128	FEISTEL	3048
AES[17]	8	128	SPN	3100
LED[15]	64	128	SPN	3407
PRINCE[16]	64	128	SPN	3491

Although not all published cipher research has provided details on all parameters—specifically area, delay, and power—we have compared the delay and power of existing algorithms that have been reported. Figures 7 and 8 illustrate the comparison of delay and power with the existing block cipher algorithm.

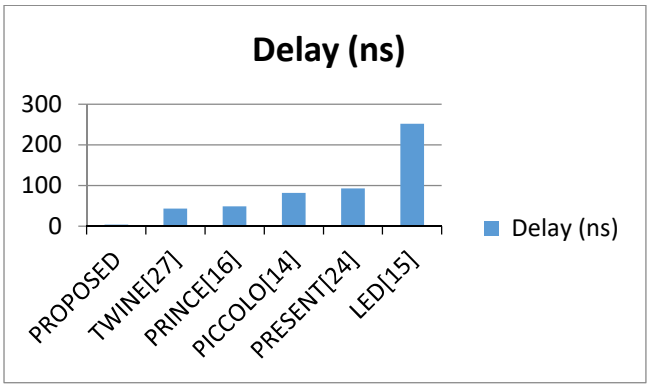


Fig. 7 Comparison of Delay with Existing Cipher

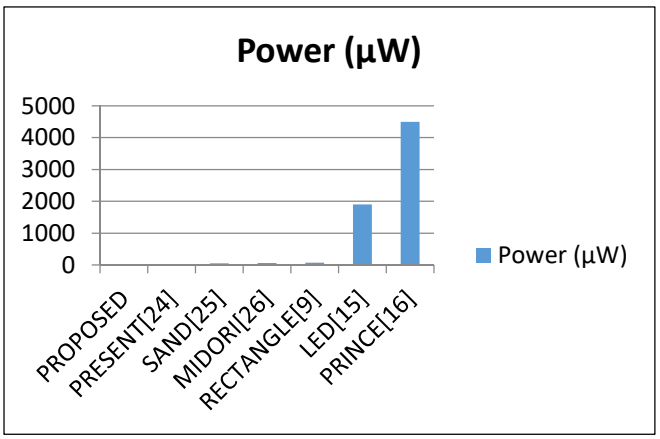


Fig. 8 Comparison of Power with Existing Cipher

NIST SP 800-22 consists of 15 standard tests typically employed to detect non-random sequences by examining specific patterns. For the analysis, 100 bit streams were produced using the proposed block cipher encryption algorithm. The proposed cipher mechanism is assessed for randomness through the 15 statistical tests provided by the National Institute of Standards and Technology (NIST) in the SP 800-22 suite. The testing was conducted with 1 billion cipher text outputs. All tests have been completed successfully. Table III displays the NIST test outcomes with their corresponding passed values.

TABLE III. NIST SP 800-22 RANDOM TEST ANALYSIS

NIST Test	P - Value	Results
Frequency	0.574903	Pass
Block Frequency	0.026948	Pass
Cumulative Sums	0.816537	Pass
Runs	0.637119	Pass
Longest Run	0.514124	Pass
Rank	0.455937	Pass
FFT	0.096578	Pass
Non-Overlapping Template	0.983453	Pass
Overlapping Template	0.514124	Pass
Universal	0.534146	Pass
Approximate Entropy	0.779188	Pass
Random Excursions	0.971699	Pass
Random Excursions Variant	0.911413	Pass
Serial	0.911413	Pass
Linear Complexity	0.334538	Pass

V. CONCLUSION

The design and development of Chakra-1 address the urgent need to have effective and safe encryption in IoT-like settings with limited available resources. The NIST SP 800-22 test suite verified the high level of statistical randomness in the algorithm as all 15 tests were successfully passed with a dataset of 1 billion cipher text outputs. The experimental results reveal that Chakra-1 has a 448 GE area, very low power consumption, and low delay, which is suitable in the low-power, memory-limited IoT devices. This, along with its better comparative performance values, highlights the possibility of it as an effective solution in the future of implementing IoT security. Future studies will focus on advanced cryptanalysis, integration of authenticated encryption and resistance against post quantum attacks.

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] G. T. Becker, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," *ACM Transactions on Embedded Computing Systems*, vol. 20, no. 4, 2021.

[3] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A secure sensor network communication architecture," in *Proceedings of the 6th International Conference on Information Processing in Sensor Networks*, 2007, pp. 479–488.

[4] S. Ali and M. Usman, "A review of lightweight block ciphers," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017.

[5] B. Chaitra, V.G. Kumar, R.C. Shatharama, "A survey on various lightweight cryptographic algorithms on FPGA," *IOSR Journal of Electronics and Communication Engineering*, vol. 12, no. 1, pp. 45–59, 2017.

[6] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001. DOI: 10.6028/NIST.FIPS.197-upd1.

[7] C. E. Shannon, "The Data Encryption Standard (DES) and its strength against attacks," *Bell System Technical Journal*, 1977.

[8] Bansod, G., Patil, A., Sutar, S., & Pisharoty, N. (2016). ANU: An ultra lightweight cipher design for security in IoT. Security and Communication Networks, 9, 5238–5251.

[9] Zhang, Wentao& Bao, Zhenzhen & Lin, Dongdai&Rijmen, Vincent & Yang, Bohan &Verbauwhede, Ingrid. (2015). RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences. 58. 10.1007/s11432-015-5459-7.

[10] Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y. (2017). GIFT: A Small Present. In: Fischer, W., Homma, N. (eds) Cryptographic Hardware and Embedded Systems – CHES 2017. CHES 2017. Lecture Notes in Computer Science(), vol 10529. Springer, Cham. https://doi.org/10.1007/978-3-319-66787-4_16.

[11] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404 (2013)

[12] T.Kassim, Shahana & Jithendra, K.. (2020). ACT : An Ultra Light Weight Block Cipher For Internet of Things. International Journal of Computing and Digital Systems. 9. 921-929. 10.12785/ijcds/090512.

[13] Bansod, G., Pisharoty, N. & Patil, A. BORON: an ultra-lightweight and low power encryption design for pervasive computing. J. Zhejiang Univ. - Sci. C 18, 317–331 (2017). https://doi.org/10.1631/FITEE.1500415.

[14] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T. (2011). *Piccolo*: An Ultra-Lightweight Blockcipher. In: Preneel, B., Takagi, T. (eds) Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011. Lecture Notes in Computer Science, vol 6917. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23951-9_23

[15] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M. (2011). The LED Block Cipher. In: Preneel, B., Takagi, T. (eds) Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011. Lecture Notes in Computer Science, vol 6917. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23951-9_22

[16] Borghoff, J. *et al.* (2012). PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications. In: Wang, X., Sako, K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34961-4_14

[17] P. Hamalainen, T. Alho, M. Hannikainen and T. D. Hamalainen, "Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core," *9th EUROMICRO Conference on Digital System Design (DSD'06)*, Cavtat, Croatia, 2006, pp. 577-583, doi: 10.1109/DSD.2006.40.

[18] Hong, D. *et al.* (2006). HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin, L., Matsui, M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11894063_4

[19] Gong, Z., Nikova, S., Law, Y.W. (2012). KLEIN: A New Family of Lightweight Block Ciphers. In: Juels, A., Paar, C. (eds) RFID. Security and Privacy. RFIDSec 2011. Lecture Notes in Computer Science, vol 7055. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25286-0_1

[20] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T. (2007). The 128-bit blockcipher CLEFIA (extended abstract). In: Fast Software Encryption (FSE 2007), Springer, LNCS, 4593 (pp. 181 195).

[21] Lim, C.H., Korkishko, T. (2006). mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors. In: Song, JS., Kwon, T., Yung, M. (eds) Information Security Applications. WISA 2005. Lecture Notes in Computer Science, vol 3786. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11604938_19

[22] Lang Li, Botao Liu, Yimeng Zhou, Yi Zou, SFN: A new lightweight block cipher, Microprocessors and Microsystems, Volume 60, 2018, Pages 138-150, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2018.04.009.

[23] B. -T. Liu, L. Li, R. -X. Wu, M. -M. Xie and Q. P. Li, "Loong: A Family of Involutional Lightweight Block Cipher Based on SPN Structure," in IEEE Access, vol. 7, pp. 136023-136035, 2019, doi: 10.1109/ACCESS.2019.2940330.

[24] Bogdanov, Andrey & Knudsen, Lars & Leander, Gregor & Paar, Christof & Poschmann, Axel & Robshaw, Matthew & Seurin, Yannick & Vikkelsoe, C.. (2007). PRESENT: an ultra-lightweight block cipher. Lect Note. Comput. Sci.. 4727. 450-466. 10.1007/978-3-540-74735-2_31.

[25] Chen, S., Fan, Y., Sun, L. et al. SAND: an AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations. Des. Codes Cryptogr. 90, 155–198 (2022). https://doi.org/10.1007/s10623-021-00970-9.

[26] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, ‘‘Midori: A block cipher for low energy,’’ in Proc. 21st Int. Conf. Theory Appl. Cryptol. Inf. Secur., Part II. Berlin, Germany: Springer, Nov./Dec. 2015, pp. 411–436. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3 662-48800-3_17.

[27] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, “Twine: A lightweight, versatile block cipher,” in Proc. of ECRYPT Work. pn Light. Cryptogr. LC11, pp. 146–169, 2011.

[28] M. B. Abdelhalim, M. El-Mahallawy, and M. A. A. Elhennawy, “Design and Implementation of an Encryption Algorithm for use in RFID System,” Int. J. RFID Secur. Cryptogr., vol. 2, pp. 51 57, 2013.

[29] Lang Li, Botao Liu, Hui Wang, QTL: A new ultra-lightweight block cipher, Microprocessors and Microsystems, Volume 45, Part A, 2016, Pages 45-55, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2016.03.011.

[30] Poschmann, A., Ling, S., Wang, H. (2010). 256 Bit Standardized Crypto for 650 GE – GOST Revisited. In: Mangard, S., Standaert, FX. (eds) Cryptographic Hardware and Embedded Systems, CHES 2010. CHES 2010. Lecture Notes in Computer Science, vol 6225. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15031-9_15.

[31] K. P. Raja, Z. Mishra, P. Singh, and B. Acharya, ‘‘Efficient hard ware implementations of lightweight simeck cipher for resource constrained applications,’’ Integration, vol. 88, pp. 343–352, Jan. 2023, doi: 10.1016/j.vlsi.2022.10.009.