Indonesian Journal of Electrical Engineering and Computer Science
Vol. 41, No. 3, March 2026, pp. 946~953
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v41.i3.pp946-953

ARX based cipher with S-box augmentation: statistical and differential evaluation

Manita Rajput, Pranali Chaudhari
Department of Electronics and Telecommunication, University of Mumbai FCRIT, Navi Mumbai, India

Article Info

Article history:

Received Nov 9, 2025
Revised Jan 30, 2026
Accepted Feb 28, 2026

Keywords:

Differential trail
Index of coincidence
IoMT
Speck
STM32 Nucleo board

ABSTRACT

With the growth of internet of medical things (IoMT), the continuous transfer of vital biomedical data requires lightweight encryption with strong resistance to statistical and differential attacks. The Speck cipher is a suitable candidate because of its low memory and execution time. However, its vulnerability to differential cryptanalysis limits wider use in healthcare environments. In this work, a hybrid lightweight algorithm is proposed by integrating the PRESENT substitution box within the Speck64/96 round structure. The substitution layer was evaluated at three different positions in the round function. Statistical and differential analyses were performed on three sets of plaintext data, each containing 1,000 test pairs. Index of coincidence (IoC), entropy, and avalanche effect were used as the primary statistical metrics. Differential trail strength was assessed using ciphertext differences and round-wise differential probability (DP). The experimental results show that the proposed version, named Speckpres_S, achieves a 6.02% reduction in IoC, a 3.8% improvement in entropy, and a 1.7% rise in avalanche effect when compared with Speck64/96. The differential trail becomes weaker, with a 46% reduction in trail probability and a 12–15% increase in trail weight across all datasets. The execution time remained within IoMT limits. This indicates stronger resistance to differential attacks with predictable diffusion. The study demonstrates that Speckpres_S improves security while maintaining practical latency and throughput for IoMT applications. Although execution time increases marginally, the gain in differential resistance and statistical performance makes the proposed algorithm a more robust option for transmitting sensitive biomedical parameters.

Corresponding Author:

Manita Rajput
Department of Electronics and Telecommunication, University of Mumbai FCRIT
Navi Mumbai, India
Email: manita.rajput@fcrit.ac.in

1. INTRODUCTION

With the advent of internet of medical things (IoMT), vitals such as blood pressure, body temperature, heart rate of patients can be transmitted, stored on cloud and retrieved by the health care professional with speed and ease. The IoMT services have recently seen an exponential growth throughout the globe. The growth can be estimated from the fact that the global market size of IoMT services has been USD 60.33 billion in 2024 and it has been forecasted that the compound annual growth rate (CAGR) in IoMT services in the next 8 years will be 38.5% [1].

With petabytes of IoMT data in transit or at storage, data security is an important issue of concern. The IoMT data should be confidential, authenticated and correctly received by the medical health care

professional [2]-[4]. Data breaches have been recorded in IoMT networks in the recent years [5], [6], inspite of many existing lightweight security algorithms. Lightweight encryption algorithms are designed to minimize memory usage and latency and are well-suited for ensuring secure data transit from the IoMT sensor level to the cloud. Considering metrics of memory, latency and throughput, authors in [7] suggest that Present [8], Speck [9], Simon [9], Midori [10], and Piccolo [11] are the best suit algorithms for IoMT devices currently. Given the rapid growth of IoMT and the increasing attempts by attackers to access transmitted personal health information (PHI), there is a critical need for more number of robust encryption algorithms that surpass the security of existing solutions.

The objective of this paper is to propose a novel hybrid lightweight encryption algorithm which is developed from the base algorithm of Speck by the inclusion of S box of Present algorithm. Speck has been specifically selected for modifications as it is considered to be the most memory efficient algorithm occupying less than 200 bytes of ROM and zero bytes of RAM [7]. Speck also has a low latency (408 cycles/block) and high throughput (470.5 Kbps) [7]. Although Speck offers excellent performance in constrained environments, several studies report that it remains susceptible to differential attacks on a large subset of its rounds [12], [13]. Existing research largely focuses on analyzing these weaknesses rather than proposing modifications that improve differential resistance without compromising lightweight performance. This creates a clear research gap in developing an enhanced version of Speck that strengthens its security while remaining suitable for IoMT devices.

To address this gap, the present work investigates whether integrating a lightweight substitution box into the Speck 64/96 round structure can improve its statistical and differential strength. The S box of present is incorporated in the round structure of Speck 64/96. The block length choice has been made on the requirement of the vital parameters that are most frequently transmitted. The key length choice is based on impact level of biomedical data and it's confidentiality level requirements [4]. The S box has been included at various positions in the round structure of Speck. These versions are compared using statistical security metrics. The best performing hybrid algorithm is referred as Speckpres_S. The physical costs of Speckpres_S such as memory, latency and throughput has been computed and compared with original Speck. The differential trails of original Speck and Speckpres_S are compared. Lastly, a detailed comparative analysis has been done of Speck and Speckpres_S.

2. LITERATURE SURVEY

The literature survey covers Speck algorithm summary, it's vulnerability, methods to improve this algorithm against differential attacks and properties of S box.

2.1. Introduction and structure of Speck algorithm

Speck is a family of lightweight block ciphers publicly released by the National Security Agency (NSA) in June 2013 [8]. It has been optimized for performance in software implementations and is an add–rotate–XOR (ARX) cipher. The block size in Speck ranges from 32 bits to 256 bits. A block is always two words, but the words may be 16, 24, 32, 48 or 64 bits in size. The keyword size ranges from 64 to 256 bits. The key can be of 2, 3 or 4 words, depending upon the key length. To encrypt a block of 64 bits, there can be 2 different options of key size. The key size can be either 96 bits or 128 bits. While designing these rounds, major importance has been given to reducing the latency and memory requirements [14]. Due to simple linear and non-linear operations in round functions of Speck, it requires a lesser execution time and latency. Linear and differential attacks are the limiting attacks of Speck. Differential attacks on 70 to 75% rounds of all Speck variants have been possible [15]. 19 out of 26 rounds in Speck 64/96 which accounts to 73% of the rounds have already been attacked. Since Speck gives optimized performance with respect to execution speed, latency and memory, it can be a promisable cipher for IoT applications if it is made more robust to differential attacks. The next section elaborates on methods which can be used to make a cipher more robust to differential attacks.

2.2. Methods for enhancement of robustness of ciphers against differential attacks

Increasing the number of rounds in the cipher can make it more resistant to differential attacks [15]. Larger block sizes or an enhanced key scheduling algorithm [16] can also increase the complexity of potential differential characteristics, making it more challenging to perform differential cryptanalysis. Integrating S-boxes (substitution boxes) into the encryption rounds can add non-linearity to the cipher. For example, the granule cipher and the skinny cipher use a static Substitution box to improve its robustness against both linear and differential attacks [17].

As stated in section I, this paper analyses the performance of Speck 64/96 cipher with an inclusion of S box. The choice of S box and it's position in the round is crucial in deciding the security of the algorithm. The metrics used to decide the quality of an S box is given in sub-section 2.3.

2.3. Metrics used for substitution box selection

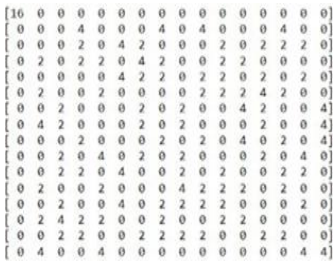
The difference distribution table (DDT) [18], linear approximation table (LAT) [18] and the Boomerang connectivity table (BCT) [19] constructed from the S box can help us evaluate the effectiveness of the S box towards certain attacks. Panchami and Mathew [20] has compared more than 20 S Boxes with respect to SNR (DPA), transparency order, confusion coefficient, algebraic degree, differential approximation probability (DAP), linear approximation probability (LAP). The DAP of Present S box was stated to be 0.657 and the LAP was 0.256 [20] which indicates the robustness of the Present S Box against differential and linear attacks respectively.

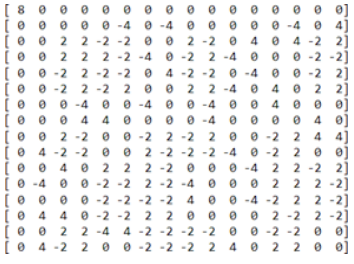
3. SOFTWARE IMPLEMENTATION

The tools and algorithms/methods used for Substitution box selection, hybrid algorithm development, formation of the plain-text data, differential cryptanalysis is briefed in this section.

3.1. Evaluating the properties of present S boxes

To validate the claims presented in paper [20], the DDT, LAT and BCT of the Present S box as shown in Figures 1-3 were constructed using SageMath tool [21].





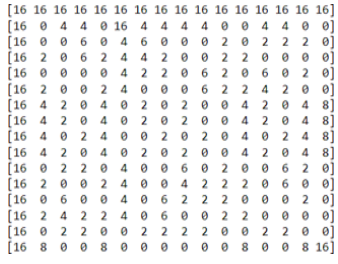


Figure 1. DDT of Present S box Figure 2. LAT of Present S box Figure 3. BCT of Present S box

From the DDT of the Substitution boxes, the differential branch number and differential uniformity was found. Likewise, the BCT and LAT was constructed. Metrics such as boomerang uniformity [21], linear branch number [21] and linearity was found. Table 1 shows the values of Present S box with respect to the metrics obtained from table.

The absolute value of maximum difference probability (MDP) is found to be 4 which is the minimum possible value. The differential uniformity (DU) which is a direct indicative measure of DAP is found to be 4. Both DU and DAP should be as low as possible. While other key properties (e.g., differential uniformity, boomerang uniformity, linearity) are equivalent across most S boxes given in [20], the Present S-box provides stronger non-linearity propagation without compromising balance or linear structure.

Table 1. Metrics of Present S-box

Metric	Present
Differential branch number	3
Differential uniformity	4
Boomerang uniformity	16
Maximal difference probability absolute	4
Linear structure	True
Balanced/Unbalanced	Balanced
Linear branch number	2
Linearity	8

3.2. Implementation of S box in Speck round

An attempt has been made to implement the S box of present algorithm at 3 different positions, S Box for half of plain text in each round, the complete plain text in every round of Speck and at the start of the rounds. Figures 4-6 show the positions of S box inclusion in the trials. All software implementations have been done in c programming with Visual Studio 2022 editor.

3.2.1. Structure and implementation of the algorithm

As shown in Figure 5, the 64 bits plain text is fed to the Substitution layer and then inputted for the regular operations of Speck. The substitution happens in every round of Speck algorithm. Other functions of modulo addition, right and left bit rotations are kept the same. 64 bit user defined block is divided into 2 halves, namely X and Y blocks of 32 bits each. This data is fed to the S box. The key scheduling algorithm is same as that of Speck. This version is henceforth called as Speckpres_S.

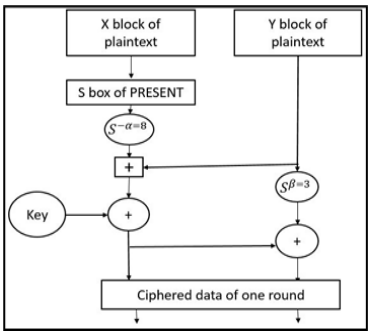


Figure 4. S box included for half plain text

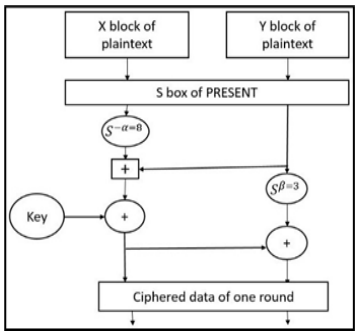


Figure 5. S box included for whole plain text (Speckpres_S)

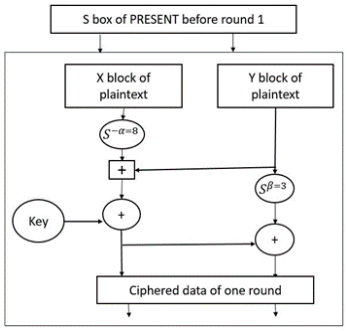


Figure 6. S box included at start of rounds

3.2.2. Formation of the test data

The test data which serves as a plaintext is taken in the hexadecimal format for compactness in representation. If a patient has a body temperature of 37.7 degrees Celsius, SPO_2 value of 94% and a random blood sugar of 550 mg/dL, then the sample of test data would look like as shown in Figure 7 [22]. As shown in Figure 7, part A of the data can be further used for ensuring integrity or sending more biomedical parameters. Part B is the concatenated biomedical parameters of temperature, SPO_2 and glucose level in hexadecimal format. For all testing purposes, part A of the plaintext in this paper is kept to be a series of "zeroes".

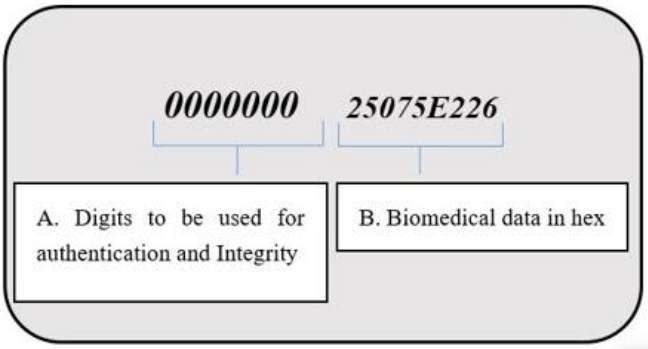


Figure 7. The format of plain text in hexadecimal

3.2.3. Differential trail of Speck and Speckpres_S

Differential trail of Speckpres_S was found primarily to assess its resilience to differential cryptanalysis. This differential trail should be as weak as possible. A cipher with a strong differential trail is more prone to attacks [23]. The differential trail was found using algorithm 1.

Algorithm for finding differential trails
Input:
1. A cryptographic algorithm E operating on n-bit plaintexts.
2. A specific plaintext difference ΔP , where $\Delta P = P1 \oplus P2$.
3. N : Number of plaintext pairs to analyze (e.g., N = 1000).

Output:
Observed differential trail $\Delta P \rightarrow \Delta C$ for each round of the algorithm.

Algorithm 1. Algorithm for finding differential trail of Speck and Speckpres S

Algorithm 1.1. Generate plaintext pairs:

```
Randomly generate N plaintexts P1,P2,...,PN of n-bits each.
for each plaintext Pi do:
Compute its pair P′ such that:
P′ = Pi ⊕ ΔP
where ΔP = 00000000 08000000 (as an example).
end for
```

Algorithm 1.2. Encrypt plaintext pairs:

```
for each plaintext pair (Pi, Pi′) do
Encrypt the pair using E to produce ciphertexts:
Ci = E(Pi),    C′ = E(Pi′)
end for
```

Algorithm 1.3. Compute ciphertext differences: for each ciphertext pair (Ci, C′) do:

```
Compute the ciphertext difference:
ΔCi = Ci ⊕ C′
end for
```

Algorithm 1.4. Map plaintext-ciphertext differences:

```
Record and analyze the relationships between ΔP and ΔC:
E
ΔP −→ ΔC
```

Algorithm 1.5. Repeat for each round:

```
for each round r of the algorithm E do
Observe and log the differential trail:
ΔPr = (ΔLi, ΔRi) → (ΔLo, ΔRo)
where ΔL and ΔR denote the left and right halves of the plaintext/ciphertext difference at
round r.
end for
```

Algorithm 1.6. Analyze differential trail:

```
Identify occurrences where specific ΔP consistently produce specific ΔC. Summarize the
probabilities for each trail ΔP → ΔC.
```

4. RESULTS AND DISCUSSIONS

This section tabulates and interpretes the statistical metrics, the differential cryptanalysis metrics and the performance costs of the hybrid cipher.

4.1. Comparison of Speck and modified Speck versions using security metrics

Index of coincidence (IoC) [24], Entropy and Avalanche effect [25] of all versions was computed and compared with Speck64/96. It is seen that when S box is included in the complete plain text, the percentage changes of the 3 metrics show the correct and desirable trend. Table 2 shows that Speckpres_S supercedes Speck algorithm in all 3-security metrics. The entropy has increased by 3.8% and the avalanche effect is also increased. The IoC also decreases by 6.02%.

Table 2. Comparison of statistical metrics for Speck with different S-box integration strategies

Algorithm	% change in IoC	% change in Entropy	% change in Avalanche
Speck with S-box for half of plain text	Increased by 25.45%	Increased by 0.4%	Decreased by 0.4%
Speckpres_S	Decreased by 6.02%	Increased by 3.8%	Increased by 1.7%
Speck with S-box at the start of the round	Decreased by 2.02%	Decreased by 3.3%	Decreased by 2.1%

4.2. Comparison of Speck and Speckpres_S using differential trail

Tables 3 and 4 show the details of the differential trail of Speck and Speckpres_S for a single data set of 1,000 pair of plaint-text samples. As shown in Table 3, differential probability (DP) and weight of Speck was computed from this differential trail.

Total DP of the trail is the product of the probabilities at each round and is expressed as:

$$DP_{trail} = P_{round1} \times P_{round2} \times ----\times P_{roundn} \quad (1)$$

the weight of a round which is the negative base-2 logarithm of its probability was computed as:

$$Weight(round) = -log2(Pround) \quad (2)$$

for the full trail:

$$Weight(round) = \sum_{rounds} Weight(round) \quad (3)$$

High-weight trails indicate that the cipher has strong diffusion and non-linearity, making it difficult for differences to propagate predictably. A higher weight also indicates that a much larger number of plain texts will be required for any type of attack. Thus, an algorithm having lesser value of trail DP and higher value of weight is considered to be robust against differential attacks. For Speck algorithm, the DP_{trail} was found to be 0.00805 and weight was calculated as 6.95. The DP_{trail} was found to be 0.00434 and weight was calculated as 7.844. This clearly shows that Speckpres_S has a weaker differential trail which indicates it will be more robust to differential attacks as compared to original Speck.

Table 3. Differential probability and weight of Speck

Rounds	Δx	Δy	Pround	Weight (round)
Round 1	00080000	00080000	1000/1000 = 1	0
Round 2	00080800	00480800	322/1000 = 0.322	1.634
Round 3	00480008	02084008	25/1000 = 0.025	5.32
			DPtrail = 0.00805	Total weight = 6.95

Table 4. Differential probability and weight of Speckpres_S

Rounds	Δx	Δy	Pround	Weight (round)
Round 1	00004000	00004000	217/1000 = 0.217	2.204
Round 2	000050C0	0002D0C0	20/1000 = 0.020	5.64
			DPtrail = 0.00434	Total weight = 7.844

As seen in Tables 3 and 4, DPtrail of Speckpres_S is 46% lower than that of Speck. The weight of Speckpres S is 12.86% higher than that of Speck. The differential trail, DPtrail and weight was found for 2 more sets of 1,000 pairs of plain text data. Figure 8 shows that all sets of inputs showed similar results with Speckpres S showing a 40% to 50% decrease in the of differential trail probability.

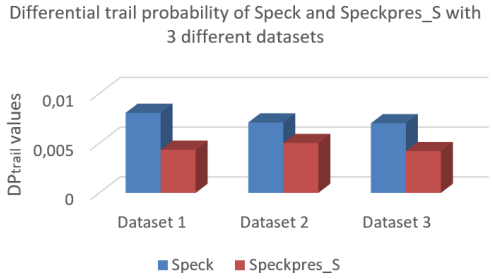


Figure 8. Comparison of differential trail probabilities of Speck and Speckpres_S

4.3. Comparison of Speck and Speckpres_S using performance costs such as execution time and latency on STM32 based boards

Execution time, latency was found of both algorithms on Nucleo F401RE development board. The STM32 Nucleo-F401RE development board is based on the STM32F401RE microcontroller, featuring an ARM Cortex-M4 core operating at a maximum clock frequency of 84 MHz [26], [27]. Table 5 compares the performance costs of the proposed hybrid algorithm with the original speck64/96. Results show that the execution time and latency are well within acceptable limits of IoMT transmission [28], [29].

Table 5. Execution time and latency comparison of Speck-64/96 and Speckpres-S-64/96 on STM32F401RE (84 MHz)

	Speck 64/96	Speckpres_S 64/96
Execution time	42 microseconds	93 microseconds
Latency	3,528 clock cycles	7,812 clock cycles

5. CONCLUSION

In this paper, a novel hybrid encryption algorithm tailored for IoMT was proposed and evaluated. The algorithm demonstrated significant improvements in critical cryptographic properties, including the IoC, avalanche effect, entropy and differential trail. These characteristics indicate an enhanced resistance to statistical and differential cryptanalysis. The IoC decreases by 6.02%, avalanche effect increases by 1.7% using the new hybrid algorithm Speckpres S. This algorithm also shows a weaker differential trail probability of only 0.00434 as compared to the DPtrail of Speck which is 0.00825. This reiterates the robustness of the Speckpres_S against differential attacks. These improvements contribute to stronger security guarantees, making the proposed algorithm suitable for sensitive medical data transmission. However, the trade-off for this increased security is a marginally higher execution time and latency, which is a common challenge in advanced encryption techniques. The execution time increases by 51 µs when tested on an STM32 Nucleo board. This marginally increased execution time is well within limits of IoMT data transfer rate requirements. Future work will focus on modifying the same algorithm for providing authentication and Integrity.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Manita Rajput	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Pranali Choudhari		✓						✓		✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [M.R], upon reasonable request.

REFERENCES

[1] "Internet of Medical Things (IoMT) Market Size, Share & COVID-19 Impact Analysis, By Component (Medical Devices, System and Software, Services, and Connectivity Technology), By Application (Patient Monitoring, Telemedicine, Connected Imaging, and Others)," Fortune Business Insights. Accessed: Jun. 18, 2024. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/internet-of-medical-things-iomt-market-101844.

[2] K. Stine, R. Kissel, W. C. Barker, A. Lee, and J. Fahlsing, "INFORMATION SECURITY," 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf.

[3] "Standards for security categorization of federal information and information systems," Washington, D.C., 2004. doi: 10.6028/NIST.FIPS.199.

[4] "Minimum security requirements for federal information and information systems," Washington, D.C., 2006. doi: 10.6028/NIST.FIPS.200.

[5] "Number of data breaches and individuals affected in the U.S. healthcare industry from 2009 to 2022," Statista. Accessed: Jun. 18, 2024. [Online]. Available: https://www.statista.com/statistics/798417/health-and-medical-data-compromises-united-states/.

[6] J. McKeon, "53% of connected medical devices contain critical vulnerabilities," Techtarget. Accessed: Jan. 21, 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/news/252511699/More-than-half-of-medical-devices-found-to-have-critical-vulnerabilities.

[7] 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.

[8] A. Bogdanov *et al*., "PRESENT: an ultra-lightweight block cipher," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4727 LNCS, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 450–466. doi: 10.1007/978-3-540-74735-2_31.

[9] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "SIMON and SPECK: block ciphers for the internet of things," 2015. [Online]. Available: https://eprint.iacr.org/2015/585.
[10] S. Banik *et al.*, "Midori: a block cipher for low energy (Extended Version)," 2015.
[11] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: an ultra-lightweight blockcipher," in *Lecture Notes in Computer Science*, vol. 6917 LNCS, 2011, pp. 342–357. doi: 10.1007/978-3-642-23951-9_23.
[12] F. Abed, E. List, S. Lucks, and J. Wenzel, "Cryptanalysis of the speck family of block ciphers," 2013. [Online]. Available: https://eprint.iacr.org/2013/568.
[13] Z. Feng, Y. Luo, C. Wang, Q. Yang, Z. Liu, and L. Song, "Improved differential cryptanalysis on SPECK using plaintext structures," in *Lecture Notes in Computer Science*, vol. 13915 LNCS, 2023, pp. 3–24. doi: 10.1007/978-3-031-35486-1_1.
[14] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "Notes on the design and analysis of Simon and Speck," 2017. [Online]. Available: https://eprint.iacr.org/2017/560.pdf.
[15] C. Song, K. Huang, L. Hu, and W. Yang, "Automatic differential attack on round-reduced speck," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 1, pp. 24–41, 2017.
[16] M. Imdad, S. N. Ramli, and H. Mahdin, "An Enhanced Key Schedule Algorithm of PRESENT-128 block cipher for random and non-random secret keys," *Symmetry*, vol. 14, no. 3, p. 604, Mar. 2022, doi: 10.3390/sym14030604.
[17] "A Substitution Box for Lightweight Ciphers to Secure Internet of Things," Journal of Computer Science".
[18] K. Mohamed, M. N. Mohammed Pauzi, F. H. Hj Mohd Ali, S. Ariffin, and N. H. Nik Zulkipli, "Study of S-box properties in block cipher," in *2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, IEEE, Sep. 2014, pp. 362–366. doi: 10.1109/I4CT.2014.6914206.
[19] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, "Boomerang connectivity table: a new cryptanalysis tool," 2018. [Online]. Available: https://eprint.iacr.org/2018/161.pdf.
[20] V. Panchami and M. M. Mathews, "A substitution box for lightweight ciphers to secure internet of things," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 4, pp. 75–89, Apr. 2023, doi: 10.1016/j.jksuci.2023.03.004.
[21] T. D. Team, "S-Boxes and their algebraic representations," Cryptography. Accessed: Aug. 15, 2023. [Online]. Available: https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/sbox.html.
[22] M. Rajput and P. Choudhari, "Comparative analysis of data security algorithms for IoMT applications," in *Lecture Notes in Networks and Systems*, vol. 1161, 2025, pp. 523–537. doi: 10.1007/978-981-97-8602-2_47.
[23] F. Abed, E. List, S. Lucks, and J. Wenzel, "Cryptanalysis of the speck family of block ciphers doble," 2013. [Online]. Available: https://eprint.iacr.org/2013/568.
[24] W. F. Friedman, "The index of coincidence and its applications in cryptography," Geneva, USA, 1922. [Online]. Available: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/publications/folder_233/41761039080018.pdf.
[25] K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, and S. Ariffin, "Analyse on avalanche effect in cryptography algorithm," in *Proceedings of the International Conference on Sustainable Practices, Development and Urbanisation (IConsPADU 2021), 16 November 2021, Universiti Selangor (UNISEL), Malaysia*, Oct. 2022, pp. 610–618. doi: 10.15405/epms.2022.10.57.
[26] STM32F401RE, "STM32 dynamic efficiency MCU, Arm Cortex-M4 core with DSP and FPU, up to 512 Kbytes of Flash memory, 84 MHz CPU, Art Accelerator." [Online]. Available: stm32f401re.pdf.
[27] "STM32 Nucleo-64 boards (MB1136)." [Online]. Available: um1724-stm32-nucleo64-boards-mb1136-stmicroelectronics.pdf.
[28] S. A. Ansari and S. Ali, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," *Discover Computing*, vol. 28, no. 1, p. 266, Nov. 2025, doi: 10.1007/s10791-025-09755-3.
[29] M. El-hajj, H. Mousawi, and A. Fadlallah, "Analysis of lightweight cryptographic algorithms on IoT hardware platform," *Future Internet*, vol. 15, no. 2, p. 54, Jan. 2023, doi: 10.3390/fi15020054.

BIOGRAPHIES OF AUTHORS

Manita Rajput is assistant professor at college of Father C. Rodrigues Institute of Technology. She is pursuing a Ph.D. degree in Electronics and Telecommunication with specialization in cryptography for IoT. Her research interests include security, biomedical engineering and wireless communication. She has authored a book on cellular Communication and several book chapters. She has co-authored at least 30 conference and journal papers. She has an H-Index of 6, i10 Index of 5 and Citation Counts of 340. She can be contacted at email: manita.rajput@fcrit.ac.in.

Dr. Pranali Chaudhari is working as an associate professor (Associate Dean of academics) at Father C. Rodrigues Institute of Technology. Sha has a doctorate's degree in Electronics and Telecommunication. Her research interests include security, biomedical engineering and IoT. She has more than 40 research publications and 2 patents. She has an H-index of 08. She can be contacted at email: pranali.choudhari@fcrit.ac.in.