Defence Science Journal, Vol. 74, No. 1, January 2024, pp. 46-52, DOI : 10.14429/dsj.74.18421

RAZOR: A Lightweight Block Cipher for Security in IoT

Dheeraj Singh[#], Manoj Kumar[$,*] and Tarun Yadav[$]

[#]*Department of Mathematics, University of Delhi, Delhi - 110 007, India*

[$]*DRDO-Scientific Analysis Group, Delhi - 110 054, India*

[*]*E-mail: manojkumar.sag@gov.in*

ABSTRACT

Rapid technological developments prompted a need to do everything from anywhere and that is growing due to the modern lifestyle. The Internet of Things (IoT) technology is helping to provide solutions by interconnecting smart devices. Lightweight block ciphers are deployed to enable security in such devices. In this paper, a new lightweight block cipher RAZOR is proposed that is based on a hybrid design technique. The round function of RAZOR is designed by mixing the Feistel and substitution permutation network techniques. The rotation and XOR-based diffusion function is applied on the 32-bit input with 8 branches to optimize the security. The strength of RAZOR is proven against differential, linear, and impossible differential attacks. The number of active S-boxes in any 5-round differential characteristic of RAZOR is 21 in comparison to the 10, 6, 4, 7, and 6 for PRESENT, Rectangle, LBlock, GIFT, and SCENERY respectively. RAZOR provides better security than the existing lightweight designs. The average throughput of 1.47 MB/second to encrypt large files makes it a better choice for software-oriented IoT applications.

Keywords: Feistel structure; Lightweight cryptography; Substitution permutation network; IoT

NOMENCLATURE

K	:	128-bit master key
RK_i^{64}	:	64-bit subkey for i^{th} round
P	:	64-bit plaintext
C	:	64-bit ciphertext
P_i^{64}	:	64-bit input to round function in i^{th} round
D	:	Diffusion function applied on 32-bit input
$\ll$	:	Bitwise left rotation
$\oplus$	:	Bitwise XOR operation

1. INTRODUCTION

Smart devices are controlled using mobile phones through the Bluetooth and internet. Smart home appliances and switches are being introduced bydevice makers to ease the modern lifestyle. Nowadays, IoT technology is being enabled in newly launched home appliances. In India, the IoT market size was five billion in 2020 and it is expected to reach 9.3 billion U.S. dollars by 2025[1]. These devices have many practical applications in humanlife, and hence their security against unwanted leakage of secured data is an essential concern. Lightweight cryptography emerged to cater to the security issues in resource-constrained IoT-enabled smart devices, healthcare services[2], and cloud computing[3]. The first notable lightweight block cipher for these environments was PRESENT[4] and thereafter many lightweight block ciphers have been published in the open literature to meet the platform-specific requirements.

Received : 22 August 2022, Revised : 12 September 2023
Accepted : 20 October 2023, Online published : 12 January 2024

Block ciphers are versatile cryptographic primitives that are used in various practical applications[5]. A block cipher encrypts the input plaintext by dividing it into pre-defined fixed-size blocks. For each block, a pre-fixed k-bit secret key is used to output the n-bit ciphertext by applying the round function r times iteratively. Each round consists of a key addition layer, a non-linear substitution layer, and permutation operations. Generally, S-boxes are used in a substitution layer and bit/byte-wise permutation or the maximum distance separable matrix is used in a diffusion layer. The diffusion functions are designed to enhance the security bounds introduced by the S-box layer.

Many lightweight block ciphers *e.g.* PRESENT[4], CLEFIA[6], LBlock[7], HIGHT[8], TWINE[9], RECTANGLE[10], PICO[11], GIFT[12], and SCENERY[13] have been published in the last two decades. The design of PRESENT curated a new path in the history of lightweight cryptography. It has been standardized by International Organisation for Standardization and International Electro-Technical Commission (ISO/IEC 29192-2:2012) for lightweight cryptographic applications. In most of the existing lightweight block ciphers, 4-bit S-boxes are used but a variety of diffusion layers are proposed in these designs. The bit permutation is effective to achieve hardware efficiency whilebyte/nibble permutations are preferred for better software performance.

Present paper proposes a new lightweight block cipher is proposedfor software-oriented IoT environments. It is based on a hybrid structure.The 4-bit S-box is applied on the full input block in parallel similar to the substitution

layer of the SPN structure. The diffusion function is applied similarly to the Feistel structure by dividing the input into two halves. Since rotation and XOR operations can be implemented in software applications more efficiently than the bit permutation-based diffusion layers. So, the diffusion function for 32-bit input is designed using the rotation and XOR operations only. Security analysis of RAZOR against basic cryptanalytic attacks asserts that it attains enough security margins against such attacks. The cipher is named 'RAZOR'due to rotation and XOR operations-based diffusion layer.

The remaining part of the paper is organised as follows. The design specifications of lightweight block cipher RAZOR are discussed in Section 2. The security analysis of RAZOR against some known attacks viz. linear, differential, and impossible differential attacks are presented in Section 3. The hardware and software performance analysis of lightweight block cipher RAZOR is presented in Section 4. The paper is summarised with a conclusion in Section 5.

2. SPECIFICATION OF RAZOR

RAZOR encrypts the 64-bit plaintext blocks using the 128-bit master secret key and consists of 32 rounds. In each round, key addition, substitution, and diffusion layers are applied (Fig. 1). In the substitution layer, a 4-bit S-box is applied 16 times in parallel. The diffusion layer divides the 64-bit input into two 32-bit words and applies the rotation and XOR-based function on each word. In the key addition layer, bitwise XOR of the current 64-bit state and 64-bit round subkey is performed.The key expansion, encryption, and decryption process with the test vectors for RAZOR are described in the following subsections.

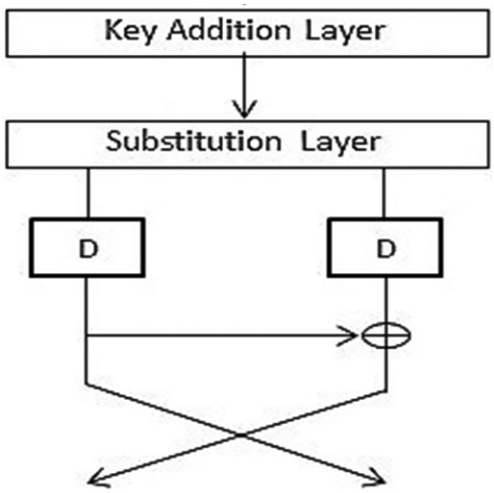


Figure 1. Round function.

2.1 Key Expansion

The initial 128-bit user-supplied master secret key is stored in a key register K. The bitwise representation of this 128-bit key is $k_0k_1k_2\ldots k_{127}$. There are 32 rounds in RAZOR, so one 64-bit round subkey for each round and one additional round subkey for key whitening purposes are required. In total, 33 round subkeys RK_i^{64} of size 64-bit each are generated for this purpose. The rightmost 64 bits of the current contents of the key register are stored as the roundsubkey $RK_1^{64} = k_0k_1k_2 \cdots k_{63}$. Then, key register K is updated to get the next 64-bit round subkey RK_i^{64} $(2 \le i \le 33)$:

- $K \ll 17$
- $(k_0k_1k_2k_3) = S(k_0k_1k_2k_3)$, $(k_4k_5k_6k_7) = S(k_4k_5k_6k_7)$
- $(k_{92}k_{93}k_{94}k_{95}k_{96}k_{97}k_{98}k_{99}) = (k_{92}k_{93}k_{94}k_{95}k_{96}k_{97}k_{98}k_{99}) \oplus [i]_2$
- RK_i^{64} is the leftmost 64 bits of the current content of the key register K

2.2 Encryption Process

The 64-bit plaintext block is encrypted by mixing the expanded thirty-three round subkeys.The subkey is mixed using the XOR operation in the key addition layer and the 4-bit S-box (Table 1) is applied 16 times in parallel in the substitution layer. The 64-bit output from the S-box layer is divided into two 32-bit words (left and right). The diffusion function D is applied to each 32-bit word. Then, left and right words are XORed to produce a new left 32-bit word. The new right 32-bit wordis the output of the diffusion function applied on the left 32-bit word. This process is repeated 32 times and the last 64-bit round subkey is used as a post-whitening key producing the ciphertext (Algorithm 1).

Input: *Plaintext* $P = P_1^{64}$ *&* *Round Subkeys* RK_i^{64} $(1 \le i \le 33)$
Output: *Ciphertext* $C = (P_{33}^{64} \oplus RK_{33}^{64})$
for $i = 1$ *to* 32 ***do***
$T_i^{64} = S(P_i^{64} \oplus RK_i^{64})$
$T_i^{64} \rightarrow (T_L^{32} || T_R^{32})$
$P_{i+1}^{64} = (D(T_L^{32}) \oplus D(T_R^{32})) || D(T_L^{32})$
end

Algorithm 1. Encryption.

The S-box: The 64-bit input is divided into 4-bit nibbles and a substitution table is used to map the 4-bit input x to a 4-bit output $S(x)$. The 4-bit S-box (Table 1) is used in the substitution layer.

The Diffusion Function. Let A and B be two 32-bit words, then diffusion function D is applied to A

Table 1. S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 2. Inverse S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S^{-1}(x)$	5	E	F	8	C	1	2	D	B	4	6	3	0	7	9	A

to get the output B. The diffusion function D is designed to provide the branch number 7 when input and output are divided into 8 branches each. The diffusion function D performs the XOR of A with the shifted versions of A so that $B = D(A)$.

$D(A) = A \oplus (A \ll 1) \oplus (A \ll 4) \oplus (A \ll 8) \oplus (A \ll 12) \oplus (A \ll 17) \oplus (A \ll 22)$

2.3 Decryption Process

RAZOR is based on a hybrid structure and its decryption process will use the inverse of the substitution box and diffusion function. The decryption process is applied to the 64-bit ciphertext using the 128-bit master key to get the original 64-bit plaintext. The key expansion algorithm is applied on the 128-bit masterkey to generate the thirty-three round subkeys. In the decryption process, the round subkeys are used in reverse order. The round subkey RK_{33}^{64} is XORed with the 64-bitciphertext and thereafter the inverse diffusion (D^{-1}) and inverse substitution (S^{-1}) operations are applied. In the last iteration, round subkey RK_{1}^{64} is applied as a whitening key to retrieve the original plaintext.

2.3.1 Inverse S-box

The S-box (Table 1) is used to generate the inverse substitution mapping (Table 2). In the decryption process, the inverse S-box (S^{-1}) will be used.

2.3.2 Inverse Diffusion Function

The diffusion function (D) consists of six XORs while the inverse of this diffusion function D^{-1} consists of ten XOR operations. The branch number of the inverse diffusion layer is also 7. Let A and B be two 32-bit words, then the output of the inverse diffusion layer will be obtained as follows $A = D^{-1}(B)$:

$D^{-1}(B) = B \oplus (B \ll 5) \oplus (B \ll 6) \oplus (B \ll 10) \oplus (B \ll 14) \oplus (B \ll 20) \oplus (B \ll 21) \oplus (B \ll 22) \oplus (B \ll 24) \oplus (B \ll 28) \oplus (B \ll 30)$

2.4 Test Vectors

The sample of plaintext, ciphertext, and key combinations is given in Table 3 which can be used to verify the encryption and decryption implementation of the lightweightblock cipher RAZOR.

3. SECURITY EVALUATION

There exist various cryptanalytic techniques to break the security of block ciphers. The strength of lightweight block cipher RAZOR is proven against differential[14], linear[15], impossible-differential[16], and related-key[17] cryptanalysis in this section. The following results are used to calculate the branch number of a word-oriented diffusion layer (D).

Definition 1. If $A = a_1 \| a_2 \| a_3 \| \cdots \| a_8$ be a 32-bit word, then the weight of A is defined by the number of non-zero nibbles a_i in A and denoted by $\mathrm{Wt}(A)$.

Definition 2. If A is an input to the diffusion layer D: $\{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$, then the branch number of D is defined as $\beta_D = \min \{\mathrm{Wt}(A) + \mathrm{Wt}(D(A)\}$, where minimum runs over all the non-zero values of 32-bit word A.

3.1 Differential Cryptanalysis

This is a chosen plaintext attack and requires the encryption of plaintext pairs under a fixed difference. The differential characteristics suggesting the occurrence of particular input and output differences with a high probability are used to distinguish the output of a block cipher from the random text. The data complexity of this attack is inversely proportional to the probability of optimal differential characteristic[14]. To apply this attack on a new cipher, a lower boundon the number of active S-boxes in any differential characteristic is obtained. The difference distribution table[4] (DDT) of S-box provides the maximum differential probability as 2^{-2} for one application of S-box[4]. The number of active S-boxes and maximum probability in DDT is used to calculate an upper bound on the probability of differential characteristic. This upper bound is used to calculate the data complexity of a differential attack on RAZOR. For a 64-bit block size, 2^{64} plaintext pairs can be generated. Hence, an adversary with a differential characteristic having 32 or less numb of active S-boxes can succeed with the differential attack. A bound on the numberof active S-boxes in a differential characteristic is provided by Theorem 1.

3.1.1 Theorem 1

Any 10-round differential characteristic of RAZOR has at least 35 active S-boxes.

3.1.2 Theoretical Bounds

The probability of any 10-round differential characteristic will be 2^{-70} (Theorem 1). Hence, at least 2^{70} plaintext pairs are required to distinguish the output of 10-round RAZOR using the differential attack. This is more than the total available plaintexts and therefore 32-round RAZOR is secure against this attack.

Table 3. Test vectors (Hex)

Key	Plaintext	Ciphertext
0x00000000000000000000000000000000	0x0000000000000000	0x4da588acdbe65ee3
0x00000000000000000000000000000000	0xffffffffffffffff	0xb8f3dd4c2d72ca01
0xffffffffffffffffffffffffffffffff	0x0000000000000000	0x16412af27a27b29e
0xffffffffffffffffffffffffffffffff	0xffffffffffffffff	0xf2e22b899037fa79

Table 4. Five round differential characteristic

Round	Input Difference	#Active S-box	Probability
1	0x0000000000000003	1	2^{-3}
2	0x0108444c00000000	6	2^{-18}
3	0x0880c0000880c000	6	2^{-35}
4	0x000000001550073c	6	2^{-51}
5	0x0c00500000000000	2	2^{-55}
6	0xd3cc0a64d3cc0a64	–	–

3.1.3 Practical Bounds

The differential characteristic search is implemented using the branch-and-bound technique[18,19] to obtain the actual differential characteristic. An optimal differential characteristic for 5-round RAZORwith a probability of 2^{-55} is presented in Table 4.

3.1.4 Key Recovery Attack

An adversary can use the 5-round differential characteristics with the probability of 2^{-55} to attack reduced round RAZOR. The subkeys involved in outermost rounds will be recovered using this attack and an exhaustive key search will be required to get the remaining subkeys. The subkey bits are guessed corresponding to the active S-box only and RAZOR uses a 4-bit S-box, so 4 subkey bits can be guessed corresponding to each active S-box. Since any two consecutive rounds differential characteristic of RAZOR have at least 7 active S-boxes. Hence, at most 28 subkey bits can be guessed as corresponding to any two additional outermost rounds of the characteristic. If two rounds are added on top and bottom of the characteristic, then 56 subkey bits used in these 4 outermost rounds can be recovered. It follows that an adversary can use this attack against 9-round RAZOR to recover 56 bits of the round subkey. Hence, a differential attack will not be useful beyond 9 rounds on the lightweight block cipher RAZOR.

3.1.5 Comparison of Active S-box Bound

The lower bounds on the number of active S-boxes in a 5-round differential characteristic of RAZOR are comparedwith the lightweight block ciphers PRESENT, Rectangle, LBlock, GIFT, and SCENERY. SCENERY has 6 active S-box in 5-round differential characteristic whereas RAZOR has 21 active S-boxes. Hence, RAZOR has more active S-boxes than SCENERY and other lightweight block ciphers. This comparison shows that the security of RAZOR is more than other ciphers (Table 5).

3.2 Linear Cryptanalysis

This is a known plaintext attack and the existence of high probability linearexpressions with bias ϵ among plaintext, ciphertext, and key bits is utilized in this attack[15]. The data complexity of linear attack is inversely proportional to ϵ^2. So, a larger bias of the linear expression means a lesser number of plaintexts willbe required to distinguish the cipher. So, to ensure that RAZOR is secure fromlinear cryptanalysis, the number of active S-boxes in the linear characteristic of RAZOR is estimated. The branch number of a diffusion layer is used to determine the minimum number of active S-box contributing to the linear characteristic and the branch number of the diffusion layer in RAZOR is 7. The maximum bias in the linear approximation table[5] of RAZOR is 2^{-2}. The security bound against linear attack is estimated using the following theorem.

3.2.1 Theorem 2

Any 10-round linear characteristic of RAZOR will contain at least35 active S-boxes. The bias of any 10-round linear characteristic using the Piling-Up lemma will be $2^{34} * (2^{-2})^{35}=2^{-36}$. The data complexity of the 10-round linear attackon RAZOR will be $(2^{-36})^{-2}=2^{72}$ known plaintexts.

3.3 Impossible Differential Cryptanalysis

The differential characteristics of zero probability are used to recover the roundsubkeys in this attack[16]. Unlike differential cryptanalysis, it sieves out the wrong keys from the key list and the keys that are remaining in the list are the correct options for the secret key. To ensure the security of RAZOR from this attack, an impossible differential characteristic covering the maximum number of rounds is searched. The following 6-round impossible differential characteristic is obtained using the miss-in-the-middle technique. By adding 4 outer rounds, an impossible differential attack cannot be applied to RAZOR beyond 10 rounds.

$$(000000000000000\alpha) \rightarrow_{6R} (\alpha000000000000000)$$

3.4 Related Key Cryptanalysis

This attack utilizes the linearity in the key scheduling algorithm and it has been applied to many existing block ciphers with linear and non-linear key schedules[17]. In this design, a non-linear key scheduling algorithm is used. The S-box and round constants are applied to extract the round keys from the master key. It is therefore expected that a related-key differential attack will pose no threat to the security of lightweightblock cipher RAZOR.

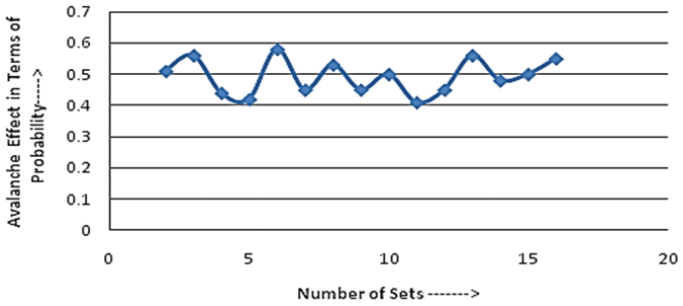
Table 5. Number of active S-boxes in five round differential characteristic

Round	PRESENT[4]	Rectangle[10]	LBlock[7]	GIFT[12]	SCENERY[13]	RAZOR
1	1	1	0	1	0	1
2	2	2	1	2	1	7
3	4	3	2	3	2	13
4	6	4	3	5	4	19
5	**10**	**6**	**4**	**7**	**6**	**21**

3.5 Avalanche Analysis

A cipher exhibits a good avalanche effect if the one-bit change in the plaintext/key affects almost half bits of the ciphertext. A block cipher that does not show an avalanche effect up to a significant degree is called a poor randomizer and will be prone to statistical analysis. The avalanche effect is tested on RAZOR and confirmed that it passes this test up to a significant degree.

Thousands of distinct plaintext pairs differing with a single bit only are generated. Each pair is encrypted using a fixed key to get the corresponding ciphertext pair. The percentage change in the ciphertexts is noted down is approximately 50 per cent in each case. The results are shown in Fig. 2.



3.6 Statistical Evaluation

The NIST Statistical Test Suit (SP800-22) for the randomness test is applied to the output obtained from RAZOR. The suit consists of 15 distinct randomness tests to check the bit string generated using a block cipher. For this purpose, one hundred distinct 64-bit plaintexts are encrypted using the arbitrary 128-bit keys in output feedback mode and stored in the output bit strings in different files. Each file consists of 10^7 bits of binary string. The experimental results (P-value and pass percentage) for some basic tests are shown in Table 7 which shows that data generated with RAZOR is completely random.

Table 7. Statistical results

Statistical Tests	P-Value	Proportions
Frequency	0.062821	97/100
Block frequency	0.699313	96/100
Cumulative sums	0.739918	97/100
Cumulative sums	0.224821	97/100
Runs	0.699313	100/100
Longest run	0.678686	100/100
Rank	0.249284	98/100
FFT	0.574903	97/100

4. PERFORMANCE EVALUATION

The performance evaluation of lightweight block cipher RAZOR is provided for software and hardware environments in this section. The hardware implementation of the substitution layer is provided that can be used to implement the cipher in hardware-oriented platforms. The software efficiency of RAZOR is evaluated by encrypting a set of files several times.

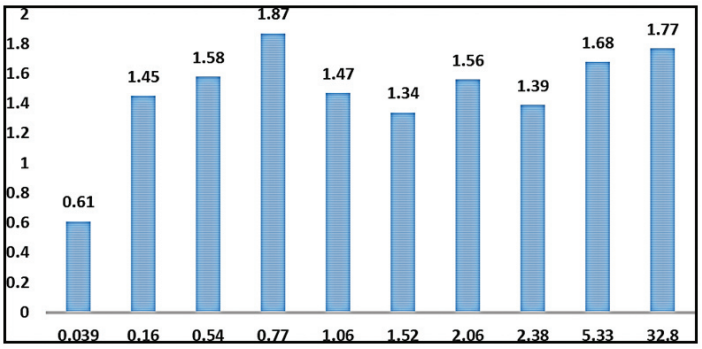


Figure 3. Throughput (MB/Sec).

4.1 Software Performance

To measure the throughput of RAZOR, 10 files of different sizes each are used. Each file is encrypted several times and encryption time is noted for each execution on i7-37770 CPU with 6 GB RAM and 3.40 GHz processor. The time required to encrypt the files is averaged and used to measure the throughput of the proposed lightweight block cipher. The throughput of RAZOR varies between 0.6 to 1.77 MB/sec which is shown in Fig. 3 and the average throughput is 1.47 MB/sec.

4.2 Hardware Implementation (S-box)

The area-optimized hardware implementation of the 4-bit S-box is presented that is used in the round function and key scheduling algorithm of RAZOR. The hardware circuit corresponding to this in-place implementation of the S-box is shown in Fig. 4.

4.3 Hardware Implementation of Diffusion Function

The rotation and XOR operations are costly in hardware implementations in comparison to the bit permutation-based diffusion functions. An alternate representation of the diffusion function is provided for efficient hardware implementations. The diffusion function D can be represented using XOR of various input bits. We can construct the 32-bit output B of diffusion function D using certain XOR operations on the selective bits in input A. The output bit b_i $(0 \le i \le 31)$ is calculated as follows.

$b31||b30||\ldots||b0 = A \oplus (A<<<1) \oplus (A<<<4) \oplus (A<<<8) \oplus (A<<<12) \oplus (A<<<17) \oplus (A<<<22)$

where $b_i = A_i \oplus A_{(31+i)\%32} \oplus A_{(28+i)\%32} \oplus A_{(24+i)\%32} \oplus A_{(20+i)\%32} \oplus A_{(15+i)\%32} \oplus A_{(10+i)\%32}$

5. CONCLUSION

In this paper, a new lightweight block cipher RAZOR is designed for software-oriented IoT applications. The main aim is to design a cipher that provides better security than the existing lightweight block ciphers for IoT-enabled devices. The rotation and XOR operations-based diffusion layer are used in the design for efficient software

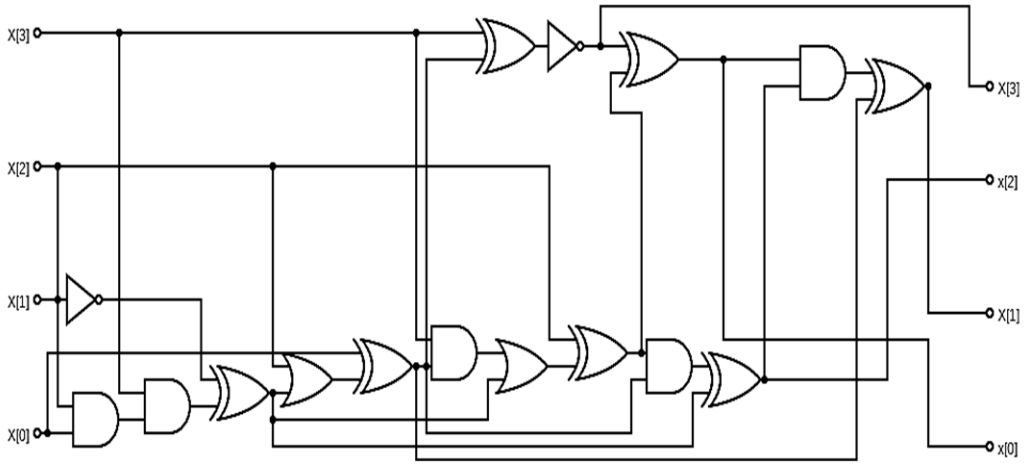


Figure 4. Hardware circuit (S-box).

implementations. This diffusion layer also increased the security strength of the proposed design. The security of RAZOR is proven against linear, differential,and impossible attacks. The number of active S-boxes in a 5-round differential characteristic of RAZOR is compared with the other lightweight block ciphers.RAZOR contains the highest number of active S-boxes in 5-round differential characteristics among these ciphers.

REFERENCES

1. IoT Market Size in India 2020-2025, Statista. https://www.statista.com/statistics/1183084/india-iot-market-size/, 2022. (Accessed on 13 July 2022).
2. Chinnasamy, P. & Deepalakshmi, P. Design of secure storage for health-care cloud using hybrid cryptography. Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), 2018, pp. 1717-1720 doi: 10.1109/ICICCT.2018.8473107
3. Chinnasamy, P.; Padmavathi, S.; Swathy, R. & Rakesh, S. Efficient data security using hybrid cryptography on cloud computing. In: Ranganathan, G., Chen, J., Rocha, Á. (eds) Inventive Communication and Computational Technologies. *Lecture Notes in Networks and Systems*, **145**. Springer, Singapore. doi:10.1007/978-981-15-7345-3_46
4. Bogdanov, A.; Knudsen, L.R..; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.B.; Seurin, Y. & Vikkelsoe, C. Present: An Ultra-Lightweight Block Cipher, CHES 2007, LNCS, 2007, 4727, pp. 450-466. doi:10.1007/978-3-540-74735-2_31
5. Knudsen, L. & Robshaw, M.J.B. Block cipher companion. Book Springer, 2011.
6. Shirai, T.; Shibutani, K.; Akishita, T.; Moriai, S. & Iwata, T. The 128-bit Block Cipher CLEFIA, FSE, LNCS, 4593, 2007, pp. 181-195. doi:10.1007/978-3-540-74619-5_12
7. Wu, W.; Zhang, L. LBlock: A lightweight block cipher. Proceedings of International Conference on Applied Cryptography and Network Security, 2011, pp. 327-344. doi:10.1007/978-3-642-21554-4_19
8. Hong, D.; Sung, J.; Hong, S.; Lim, J.; Lee, S.; Koo, B. Lee, C.; Chang, D.; Lee, J.; Jeong, K.; Kim, H.; Kim, J. & Chee, S. Hight: A new block cipher suitable for low-resource device, CHES, LNCS, 2006, 4249, pp. 46-59. doi:10.1007/11894063_4
9. Suzaki, T.; Minematsu, K.; Morioka, S. & Kobayashi, E. Twine: A lightweight, versatile Block cipher. Ecrypt Workshop on Lightweight Cryptography, 2011.
10. Zhang, W.; Bao, Z.; Lin, D.; Rijmen, V.; Yang, B. & Verbauwhede, I. Rectangle: A bit-slice ultra-lightweight cipher suitable for multiple platforms, Science China, Information's Sciences, 2015, **58**. doi: 10.1007/s11432-015-5459-7
11. Bansod, G.; Pisharoty, N. & Patil, A. Pico: An ultra lightweight and low power encryption design for ubiquitous computing. *Def. Sci. J.*, 2016, **66**, 259-265. doi: 10.14429/dsj.66.9276
12. Banik, S.; Pandey, S.K.; Peyrin, T.; Sasaki, Y.; Sim, S.M. & Todo, Y. Gift: A small present, CHES 2017, LNCS, 2017, 321-345. doi:10.1007/978-3-319-66787-4_16
13. Feng, J. & Li, L. Scenery: A lightweight block cipher based on feistel structure,Front. *Computer Science*, 2022, **16**(3). doi: 10.1007/s11704-020-0115-9
14. Biham, E. & Shamir, A. Differential cryptanalysis of the full 16-round DES, CRYPTO 92, LNCS, 1992, **740**, 487-496. doi: 10.1007/3-540-48071-4_34
15. Matsui, M. Linear cryptanalysis method for DES Cipher, Advances in Cryptology, Eurocrypt 93, LNCS,. Springer-Verlag, 1994, 765, 386-397. doi: 10.1007/3-540-48285-7_33
16. Biham, E.; Biryukov, A. & Shamir, A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials, Eurocrypt'99, LNCS, 1999, 1592 pp. 12-23. doi: 10.1007/3-540-48910-X_2
17. Biham, E. New types of cryptanalytic attacks using related *Keys. J. Cryptol.*, 1994, **7**(4), pp. 229-246. doi: 10.1007/BF00203965

18. Matsui, M. On correlation between the order of S-boxes and the strength of DES,EUROCRYPT 1994, 366–375. doi: 10.1007/BFb0053451
19. Sun, S.; Hu, L.; Wang, P.; Qiao, K.; Ma, X.; & Song, L. Automatic security evaluation and (Related-key) Differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers, ASIACRYPT 2014, LNCS, Springer, 2014, 8873, 158–178. doi:10.1007/978-3-662-45611-8_9

CONTRIBUTORS

Mr Dheeraj Singh completed his M.Phil from the University of Delhi and pursuing PhD from the University of Delhi. His research area includes: Design and analysis of block ciphers.
In the current study, his contributions are in the design and analysis of the lightweight block cipher and the implementation of various security analysis.

Dr Manoj Kumar obtained his PhD from the Department of Mathematics, University of Delhi. He is currently working as a Scientist in the DRDO-SAG. His research area includes: Design and analysis of symmetric cryptographic primitives.
In the current study, his contributions are in the overall design sketch and implementation of various attacks on the lightweight block cipher.

Mr Tarun Yadav completed his BTech in Computer Science and Engineering from IIT Ropar. He is currently working as a Scientist at DRDO-SAG. His research area includes: Protocol analysis and cryptanalysis of block ciphers.
In the current study, his contributions are in hardware implementation of S-box and diffusion layer & analysis of the lightweight block cipher.