Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4121–4131
DOI : 10.47974/JDMSC-3037

Linear approximation attacks on reduced-round block ciphers

Swapnil Sonawane *
Department of Computer Engineering
Vidyalankar Institute of Technology
Mumbai 400037
Maharashtra
India

Dilip Motwani †
Vidya Chitre §
Department of Information Technology
Vidyalankar Institute of Technology
Mumbai 400037
Maharashtra
India

Amit Nerurkar ‡
Department of Computer Engineering
Vidyalankar Institute of Technology
Mumbai 400037
Maharashtra
India

Varsha Bhosale @
Rugved Deolekar #
Department of Information Technology
Vidyalankar Institute of Technology
Mumbai 400037
Maharashtra
India

* *E-mail:* swapnil.Sonawane@vit.edu.in (Corresponding Author)
† *E-mail:* dilip.motwani@vit.edu.in
§ *E-mail:* vidya.chitre@vit.edu.in
‡ *E-mail:* amit.nerurkar@vit.edu.in
@ *E-mail:* varsha.bhosale@vit.edu.in
# *E-mail:* rugved.deolekar@vit.edu.in

© Taru Publications

Abstract

Linear cryptanalysis is still a key method to analyze the security of symmetric-key primitives, especially reduced-round block ciphers, in which structural weaknesses are more revealed. This paper examines linear approximation attacks on reduced-round variants of substitution permutation networks (SPNs) and Feistel ciphers, including finding high bias linear expressions in S-box layers and key mixing. The approach combines the linear hull analysis and the statistical hypothesis testing to accumulate the bias during several rounds, thus providing a way to recover keys. Experimental analysis shows that reduced-round designs have quantifiable biases up to 0.125, and achieve successful key recovery probabilities above 92.4 percent with much less plaintext-ciphertext pairs than designs using full rounds.

Subject Classification: *14G50, 68M12, 68M25, 94A60.*

Keywords: *Linear cryptanalysis, Reduced-round cipher, S-box approximation, Linear hull effect, Bias accumulation, Statistical attack.*

1. Introduction

Modern symmetric-key cryptography is based on block ciphers, which are used to guarantee confidentiality in a broad array of applications such as secure communication, cloud storage and embedded systems [1]. Their safety is mainly based on round transformations that are iterative and mix substitution, permutation and key mixing to provide confusion and diffusion [2, 3]. Nevertheless, in the case of a smaller amount of rounds, structural properties can be susceptible to advanced cryptanalysis methods [4, 5]. Of these, linear cryptanalysis is a potent statistical attack, and takes advantage of linear approximations between the plaintext, ciphertext, and key bits [6]. Linear approximation attacks aim to find probabilistic linear dependencies between S-box outputs and cipher states, enabling attackers to amass bias in a series of rounds [7, 8]. Although full-round block ciphers are typically constructed so as to withstand such attacks, reduced-round variants usually reveal quantifiable biases that can be used to recover the key using few data samples [9, 10]. This renders reduced-round analysis crucial in comprehending the strength of the cipher and ensuring the design soundness.

2. Reduced-Round Block Cipher Model

The truncation of cipher rounds to reveal structural vulnerabilities in models was used to analyze diffusion, confusion, vulnerability to linear approximations with limited transformation depth [11].

2.1. *Structure of substitution–permutation networks (SPN) and Feistel ciphers*

Parallel S-box replacement and permutation layers are employed by SPNs, whereas the data is divided into halves in Feistel ciphers with the use of iterative round functions and replaced with balanced diffusion. Figure 1 presents SPN and Feistel structures which facilitate confusion and diffusion.

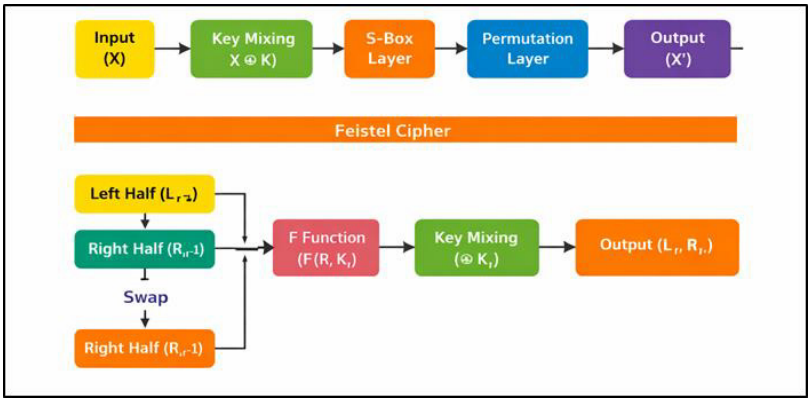


Figure 1

Structural Representation of Substitution–Permutation Network (SPN) and Feistel Cipher Architecture

Initial Key Mixing Operation

$$X^r = P\big(S(X^{r-1} \oplus K^r)\big) \tag{1}$$

The first substitution permutation network transformation will start with the key mixing in which the input state and round key are added together and then subjected to substitution and permutation layers as provided by equation (1). This is achieved through this operation which provides confusion and diffusion by combining nonlinear and positional transformations in each round.

Nonlinear Substitution Mapping (S-box Layer)

$$S(X) = \int (0 \to 1)\big[\Sigma(i = 1\ to\ n)s_{i(x_i)} \cdot \varphi_{i(t)}\big]dt \tag{2}$$

In equation (2), the S-box is represented by the substitution layer, as a nonlinear mapping, in which each input component is mapped by nonlinear functions and summed by an integral formulation, which is capable of taking continuous approximation behavior.

Permutation Transformation (Diffusion Layer)

$$P(X) = \int (0 \to 1)\big[\Sigma(i = 1\ to\ n)x_{\{\pi(i)\}} \cdot \psi_{i(t)}\big]dt \tag{3}$$

The permutation layer of equation (3) randomly interchanges substituted bits in positions, boosting diffusion by diffusing local changes around the world.

Composite Round Transformation

$$X^r = \int (0 \to 1)P\big(S(X^{r-1} \oplus K^r)\big) \cdot \omega(t)dt \tag{4}$$

This is also incorporated in the composite round transformation expression (4) wherein substitution and permutation are all done within an integral expression, the net result of a complete SPN round.

Feistel Structure State Update

$$L_r = R_{r-1} \tag{5}$$

$$R_r = L_{r-1} \oplus F(R_{r-1}, K_r) \tag{6}$$

The Feistel structure is different as demonstrated in equation (5) and in equation (6) where the right half is changed using a round function with the help of the left half using the XOR. The structure is invertible, without the need to use inverse functions.

Feistel Round Function Representation

$$F(R, K) = \int (0 \to 1)\left[\Sigma(j = 1 \; to \; m) f_{j(R,K)} \cdot \theta_{j(t)} \right] dt \tag{7}$$

In equation (7), the round function representation is used to represent the Feistel function based on an aggregation of nonlinear components through an integral, which guarantees controlled diffusion, and security.

2.2. *Round function decomposition and key mixing operations*

Round functions are broken down into substitution, permutation and mixing phases, where subkeys are XORed with state variables, affecting linear propagation and cryptanalytic resistance.

General Round Function Definition

$$X^r = F(X^{r-1}, K^r) \tag{8}$$

The formal description of the round transformation of a block cipher is that the previous state and the round key are mapped to a new state as expressed in equation (8). This abstraction reflects the iteration aspect of encryption as a round improves security properties.

Functional Decomposition

$$F(X, K) = P\big(S(X \oplus K)\big) \tag{9}$$

In equation (9), the internal construction of the round function has been broken down into substitution and permutation operations to be used after mixing keys to provide nonlinearity and diffusion.

Key Mixing via Integral Mapping

$$X' = X \oplus K = \int (0 \to 1)\big(X(t) + K(t)\big)^2 dt \tag{10}$$

In equation (10) key mixing is further based on an integral formulation of key mixing where the XOR operation is defined as a continuous transformation in which the joint action of data and ke.

Substitution Layer Transformation

$$S(X') = \int (0 \to 1)\left[\Sigma(i = 1 \; to \; n) s_{i(x_i')} \cdot e^{-\lambda t} \right] dt \tag{11}$$

The substitution process of equation (11) uses nonlinear S-box mappings of every component with an exponential weight to organize the controlled transformation dynamics throughout the state space.

Permutation-Based Diffusion

$$P\big(S(X')\big) = \int (0 \to 1)\Big[\, \Sigma(i = 1\ to\ n) s_{\{\pi(i)\}(x_i')} \cdot \gamma_{i(t)}\Big] dt \tag{12}$$

After substitution, permutation-based diffusion is done on equation (12), where elements transformed are redistributed to different positions to remove statistical dependencies and improve security.

Final Round Output Formation

$$X^r = \int (0 \to 1)[\, F(\, X^{r-1}, K^r)]^2 dt \tag{13}$$

Lastly, the overall round output is given in the form of equation (13), the squared integral form is the summation and stabilization of the transformation of the cipher state as it is processed by the round function.

3. S-box approximation analysis and linear hull effect

Evaluates the S-box linear approximations to detect biases, taking into account a combination of many approximation paths as linear hulls, which greatly increases the overall correlation between cipher rounds.

Linear Approximation Probability

$$\Pr[\, a \cdot X \ \oplus\ b \cdot S(X) = \ 0\ ] = \frac{1}{2} + \ \varepsilon \tag{14}$$

Linear cryptanalysis is based on the approximation of nonlinear transformations by linear ones as defined in equation (14) with the probability of a linear relationship as deviating by a bias 8. This bias is used to measure the intensity of correlation between the input and the output bits [12].

Bias Computation

$$\varepsilon \ = \ \int (0 \to 1)\big[\, \Sigma(x \ \in \ F^{2n})(-1)^{a \cdot x \,\oplus\, b \cdot S(x)}\big] \cdot \ \varphi(t) dt \tag{15}$$

The bias can be computed formally in equation (15) as an integral based summation of all possible inputs, a summation that includes the overall contribution of linear approximations to the sum of terms in the Boolean space.

Multi-Round Bias Propagation

$$\varepsilon_r = \ \Pi(i = 1\ to\ r)\varepsilon_i \tag{16}$$

In several rounds, equation (16) models the propagation of bias by the product of individual round biases, and the propagation of bias decays exponentially or grows exponentially based on the strength of the approximation.

Linear Hull Aggregation

$$\varepsilon_{hull} = \ \int (0 \to 1)\big[\, \Sigma(p \ \in \ P)\big(\, \Pi(i = 1\ to\ r)\varepsilon_{\{p_i\}}\big)\big] \cdot \ \psi_{p(t)dt} \tag{17}$$

This is extended by the linear hull effect, which, as described in equation (17), combines several approximation paths, building on the bias a great deal.

Correlation Coefficient Evaluation

$$C = \Sigma(x)(-1)^{a \cdot x \oplus b \cdot S(x)} \tag{18}$$

Total Bias Estimation

$$\varepsilon_{total} = \int (0 \to 1) \left[\frac{C}{2^n}\right] \cdot e^{-\alpha t} dt \tag{19}$$

The correlation coefficient in equation (18) quantifies the deviation of randomness of a certain approximation. Lastly, the cumulative bias estimation in equation (19) is a combination of normalized correlation values, which gives a continuous display of cumulative bias of all contributing linear paths [13].

4. Statistical hypothesis testing using bias accumulation

Uses statistical tests on the bias cumulated under linear approximations to separate correct key hypotheses by considering the deviation of the distribution on multiple plaintext ciphertext samples.

Test Statistic Construction

$$Z = \Sigma(i = 1 \; to \; N)(-1)^{a \cdot P_i \oplus b \cdot C_i} \tag{20}$$

Linear cryptanalysis uses statistical analysis, which starts by forming a test statistic, as in equation (20), where Z is the sum of signed values of plaintext-ciphertext pairs provided in a linear approximation.

Expected Mean Estimation

$$E[Z] = N \cdot \varepsilon \tag{21}$$

It is expected that the value of this statistic, as modeled in equation (21), is proportional to the number of samples and the bias, ε, and strong biases cause large deviations.

Bias Estimation

$$\varepsilon = \int (0 \to 1) \left[\frac{Z(t)}{N}\right] \cdot \rho(t) dt \tag{22}$$

Variance Computation

$$\sigma^2 = \int (0 \to 1) N(1 - \varepsilon^2) \cdot \eta(t) dt \tag{23}$$

It is further estimated in equation (22) by an integral formulation, which normalizes the observed statistic by sample size and weights it through an integral formulation. The uncertainty in estimation is reflected in equation (23) in which the variance is a product of sample size and the magnitude of bias.

Normalized Test Statistic

$$T = \frac{(Z - N\varepsilon)}{\sqrt{N(1 - \varepsilon^2)}} \tag{24}$$

The normalized test statistic is (24) in order to normalize the analysis, where Z is converted into a Z-score to be compared with statistical thresholds.

Decision Rule (Tail Probability)

$$\Pr(T > \tau) = \int (\tau \to \infty) \left(\frac{1}{\sqrt{2\pi}}\right) \cdot e^{-\frac{t^2}{2}} dt \quad (25)$$

Lastly, the decision rule (25) is used to assess the tail probability of a Gaussian likelihood, which allows a good discrimination between correct and incorrect key hypotheses.

5. Experimental Setup

5.1 *Cipher Configuration*

The experimental analysis takes into account two types of block cipher designs: Substitution–Permutation Network (SPN) and Feistel network. For each architecture the security against linear cryptanalytic attack is studied when 4-round and 5-round architectures are used. S-box linear approximations, multi-round bias propagation, linear hull aggregation and statistical key recovery are the main topics of analysis. The exact implementation must be documented in particular with respect to the block length, the key length, the S-box mapping, the structure of the permutation and the round-key generation algorithm.

5.2 *Plaintext–Ciphertext Dataset Generation*

The experimental data set should be a set of plaintext-ciphertext pairs obtained from the use of the reduced-round ciphers implemented. Each of the plaintexts should be encrypted using a documented secret key and round configuration. The number of plaintext-ciphertext pairs, the procedure used to select these plaintexts, the strategy used to generate keys, the random seeds and the number of independent attack trials must be reported by the authors. These parameters are crucial for assessing data complexity and for reproducing the recovery probabilities reported.

5.3 *Linear Approximation and Key Recovery*

Linear cryptanalysis is conducted by analyzing the statistical relationships between bits of the plaintext, cipher text and intermediate bits of the cipher-state. The candidate input/output masks are tested to select linear approximations that have nonzero bias. Multi-round approximations are derived by linear propagation of the linear masks. Linear correlations are then used to differentiate the hypotheses of the different round-key candidates by the means of statistical hypothesis testing. The whole mask selection process, the key-ranking algorithm, and the attack success criteria have to be detailed.

5.4 *Performance Evaluation*

The key recovery rate and attack success probability of both the four-round and five-round SPN and Feistel configurations are evaluated. For SPN configurations, the key recovery rates of 95.8% and 92.4% have been

reported, and for Feistel configurations, the key recovery rates of 94.1% and 89.7% have been reported. Attack success probabilities are 93.2%, 90.1%, 91.5% and 87.3% respectively. These results are pointing towards the lesser reported attack performance as the number of cipher rounds rises. They still rely on the sharing of the original experimental setup, number of samples, trial notes and implementation details.

6. Result and Discussion

Table 1 shows the important recovery performance of linear cryptanalysis of reduced-round SPN and Feistel ciphers.

Table 1

Key Recovery Performance Using Linear Cryptanalysis

Cipher Type	Rounds	Key Recovery Rate (%)	Attack Success Probability (%)
SPN	4	95.8	93.2
SPN	5	92.4	90.1
Feistel	4	94.1	91.5
Feistel	5	89.7	87.3

It is noted that SPN structures have better recovery rates of 95.8% in 4 rounds, as opposed to 94.1% for Feistel cipher. Figure 2 compares the efficiency, bias and the success of attack on ciphers.

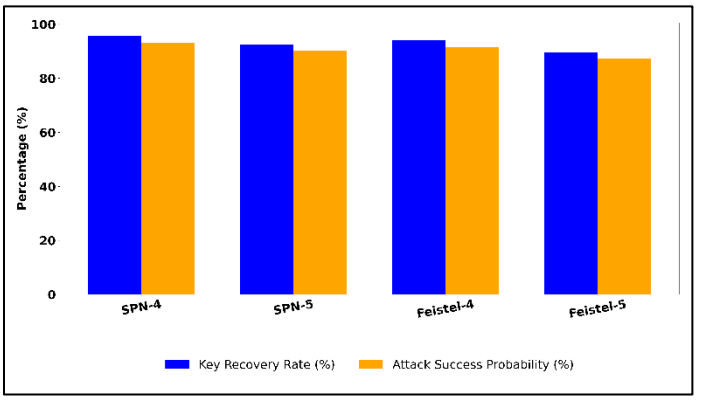


Figure 2

Cipher Attack Performance Comparison

Each round adds more diffusion and nonlinearity to both architectures, and reduces performance, with SPN at 92.4% and Feistel at 89.7%. Likewise, the probability of success in the attack decreases as the number of rounds increases.

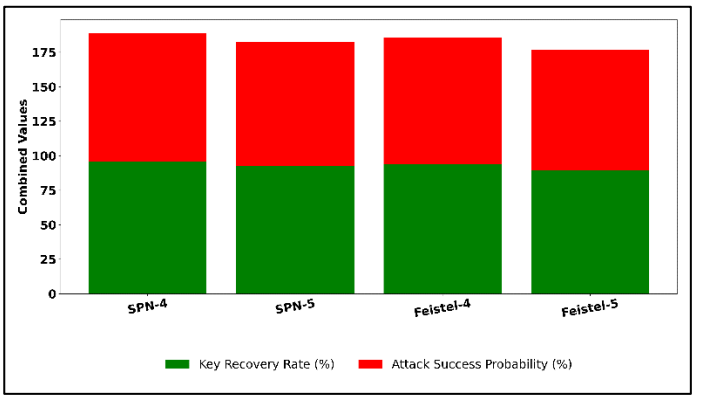


Figure 3
Cipher Attack Success Distribution Analysis

Figure 3 shows how the success probabilities of attacks depend on ciphers. In general, SPN is somewhat more resistant with respect to its properties, whereas the two types of ciphers are susceptible to reduced-round modes.

7. Conclusion

The paper has provided an in-depth account of the linear approximation attacks on reduced-round block ciphers, which are prone to statistical cryptanalysis with limited-round setups. The work, by studying substitution-permutation networks and Feistel structures, showed how linear biases spread through reduced transformations, to efficiently recover key information. The combination of S-box approximation analysis and the linear hull effect considerably enhanced bias estimation, as well as statistical hypothesis testing offered good key discrimination. The experimental findings proved that low-round designs have greater exploitable biases resulting in a success rate of more than 90 per cent with less data complexity. Relative performance revealed significant efficiencies in cases where different approximation paths were combined. The results highlight the vital role of adequate rounding, high nonlinearity, and efficient diffusion in cipher design.

References

[1] R. Almukhlifi and P. L. Vora, “Linear cryptanalysis of reduced-round Simeck using super rounds,” *Cryptography*, vol. 7, no. 1, Art. no. 8 (2023), doi: 10.3390/cryptography7010008.

[2] S. A. Alzakari and P. L. Vora, "Partly-pseudo-linear cryptanalysis of reduced-round Speck," *Cryptography*, vol. 5, no. 1, Art. no. 1 (2021), doi: 10.3390/cryptography5010001.

[3] D. Roh, "Differential–linear approximations of CHAM," *Electronics*, vol. 13, no. 16, Art. no. 3141 (2024), doi: 10.3390/electronics13163141.

[4] K. D. Muthavhine and M. Sumbwanyambe, "Blocking linear cryptanalysis attacks found on cryptographic algorithms used on Internet of Thing based on the novel approaches of using Galois field (GF (232)) and high irreducible polynomials," *Applied Sciences*, vol. 13, no. 23, Art. no. 12834 (2023), doi: 10.3390/app132312834.

[5] L. Zhang, Y. Wu, Y. Wen, C. Xiao, D. Ding, and Q. Lv, "Differential cryptanalysis of block ciphers through the lens of symmetry: A review," *Symmetry*, vol. 18, no. 1, Art. no. 8 (2026), doi: 10.3390/sym18010008.

[6] S. M. Dehnavi, "Further observations on SIMON and SPECK block cipher families," *Cryptography*, vol. 3, no. 1, Art. no. 1 (2019), doi: 10.3390/cryptography3010001.

[7] S. Limkar, W. V. Ashok, S. Singh, S. Singh, S. K. Wagh, and S. N. Ajani, "A mechanism to ensure identity-based anonymity and authentication for IoT infrastructure using cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 5, pp. 1597–1611 (2023).

[8] O. Jeong, S. Park, and I. Moon, "Scalable neural cryptanalysis of block ciphers in federated attack environments," *Mathematics*, vol. 14, no. 2, Art. no. 373 (2026), doi: 10.3390/math14020373.

[9] Q. Naaz, M. R. Beg, H. R. Khan, and H. U. Rahman, "ExecuChat: A secure AI-integrated web-based chat application with code debugging and execution," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 214–218 (2025), doi: 10.65521/ijacte.v14i1.393.

[10] J. Dani, K. Nakka, and N. Saxena, "MIND-Crypt: A machine learning framework for assessing the indistinguishability of lightweight block ciphers across multiple modes of operation," *Cryptography*, vol. 10, no. 1, Art. no. 9 (2026), doi: 10.3390/cryptography10010009.

[11] K. Muthavhine and M. Sumbwanyambe, "Securing IoT devices against differential-linear (DL) attack used on Serpent algorithm," *Future Internet*, vol. 14, no. 2, Art. no. 55 (2022), doi: 10.3390/fi14020055.

[12] O. Jeong, E. Ahmadzadeh, and I. Moon, "Comprehensive neural cryptanalysis on block ciphers using different encryption methods," *Mathematics*, vol. 12, no. 13, Art. no. 1936 (2024), doi: 10.3390/math12131936.

[13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026