Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3249–3257
DOI : 10.47974/JDMSC-2812

Spectral security analysis of cryptographic Boolean functions using discrete mathematical modelling and machine learning

Priya Mathur [@]
Department of Mathematics
Poornima Institute of Engineering & Technology
Jaipur 302022
Rajasthan
India

Pradeep Gupta [†]
Department of Computer Science and Engineering
Ajay Kumar Garg Engineering College
Ghaziabad 201015
Uttar Pradesh
India

K. Nandhini [§]
Lipika Goel [‡]
Department of Computer Science and Engineering (AIML)
Sridevi Women's Engineering College
Hyderabad 500075
Telangana
India

Satpal Singh Kushwaha *
Amit Kumar Gupta [#]
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[@] *E-mail:* drpriyamathur21@gmail.com
[†] *E-mail:* gupta.pradeep85@gmail.com
[§] *E-mail:* nandhukk28@gmail.com
[‡] *E-mail:* lipika.bose@gmail.com
* *E-mail:* satpal.singh@jaipur.manipal.edu (Corresponding Author)
[#] *E-mail:* amit.gupta@jaipur.manipal.edu

Abstract

This study investigates how the structural and spectral properties of Boolean functions influence their susceptibility to machine learning–based cryptanalysis. A comprehensive framework is proposed, combining Boolean function generation, truth table representation, Walsh–Hadamard spectral analysis, and machine learning evaluation. Using a dataset of 2000 functions (linear, balanced, bent-like, and random), results show that higher nonlinearity reduces learnability, while linear functions remain predictable. A strong negative correlation (–0.6499) between nonlinearity and learning accuracy is observed. Functions with large Walsh coefficients are more easily approximated. The findings confirm that machine learning exploits inherent structural weaknesses, aiding the design of more secure, learning-resistant cryptographic primitives.

Subject Classification: *94A60, 06E30.*

Keywords: *Boolean functions, Walsh spectrum, Nonlinearity, Machine learning cryptanalysis.*

1. Introduction

Modern cryptographic systems rely on discrete structures, especially Boolean functions and S-boxes, to resist attacks. Boolean functions provide the nonlinearity needed for Shannon's confusion, protecting against statistical and algebraic cryptanalysis [1], [2]. Their strength depends on Walsh spectrum, nonlinearity, correlation immunity, and algebraic degree [1]. Large Walsh coefficients increase vulnerability to linear cryptanalysis, while smaller ones enhance security [3], [4]. S-boxes, as vector Boolean functions, gain robustness from these properties [5]. Recent ML advances enable approximation of Boolean functions and detection of hidden patterns [6]-[8]. However, the relationship between spectral properties and ML learnability remains underexplored, motivating a unified framework combining spectral analysis and ML evaluation [18], [19], [20].

2. Literature Review

Boolean functions play a central role in symmetric cryptography due to their nonlinear properties, which enhance resistance to linear and differential attacks [1]. The Walsh–Hadamard transform is a key tool for analyzing spectral characteristics and evaluating resistance to linear cryptanalysis [3]. Foundational works highlight properties such as nonlinearity, correlation immunity, and algebraic immunity as critical for secure design [1], [2]. Recent studies focus on optimizing S-boxes and Boolean functions using spectral analysis and evolutionary methods [4], [9], [10], [11]. Meanwhile, machine learning–based cryptanalysis has shown the ability to detect patterns and approximate cryptographic functions [7], [8], [12], [13], [14], [15]. However, limited research directly connects spectral properties, such as Walsh coefficients and nonlinearity, with machine learning learnability, indicating a significant research gap.

3. Methodology and Mathematical Modelling

Proposes a framework combining Boolean theory, Walsh spectral analysis, and machine learning to evaluate learnability, correlation, and S-box vulnerabilities across generated Boolean functions and their structural properties as shown in Figure 1.

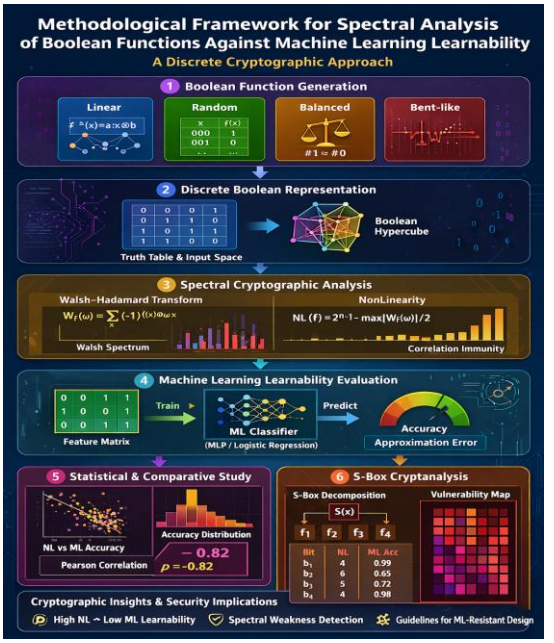

Figure 1

Methodological framework for spectral analysis of Boolean functions against machine learning learnability

3.1 *Boolean Function Generation*

Let $f:\{0,1\}^n \to \{0,1\}$ be an n-variable Boolean function, where the input space consists of 2^n binary vectors [1]. Boolean functions used in the experiments belong to four structural classes:

(a) Linear Boolean Functions: A Boolean function is linear if it can be written as

$$f(x) = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n \oplus b \tag{1}$$

for all $a_i, b \in \{0,1\}$ and $\oplus$ denotes addition modulo 2. Linear functions exhibit maximum correlation with affine functions, making them highly vulnerable to approximation and cryptanalysis [1].

(b) Random Boolean Functions: Random Boolean functions are generated by assigning outputs independently with equal probability:

$$P(f(x) = 0) = P(f(x) = 1) = \frac{1}{2} \quad (2)$$

These functions represent typical Boolean behavior in high-dimensional spaces [1].

(c) Balanced Boolean Functions: A Boolean function is balanced if the number of zeros and ones in the truth table are equal:

$$\sum_{x\in\{0,1\}^n} f(x) = 2^{n-1} \quad (3)$$

Balanced functions are essential for cryptographic primitives to prevent statistical leakage [1].

(d) Bent and Bent-like Functions: Bent functions achieve maximum nonlinearity and exist only for even n. Their Walsh spectrum satisfies

$$| W_f(\omega) | = 2^{\frac{n}{2}} \quad (4)$$

for all $\omega \in \{0,1\}^n$. Bent functions are maximally distant from affine functions and therefore highly resistant to linear cryptanalysis [1].

3.2 Discrete Boolean Representation

Boolean functions are represented explicitly using truth tables. For an n-variable function, the input space is $X = \{0,1\}^n$ and the truth table representation is

$$T_f = \{(x, f(x)) : x \in X\} \quad (5)$$

$$x = (x_1, x_2, \dots, x_n) \quad (6)$$

represents a vertex of the Boolean hypercube. This discrete representation allows exact computation of cryptographic metrics such as Walsh spectrum, nonlinearity, correlation immunity as described in classical Boolean cryptography theory [1].

3.3 Spectral Cryptographic Analysis

The spectral properties of Boolean functions are evaluated using the Walsh–Hadamard transform.

Definition 4.1: Walsh–Hadamard Transform. For a Boolean function f, the Walsh transform is defined as

$$W_f(\omega) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus(\omega\cdot x)} \quad (7)$$

$$\omega \cdot x = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n \quad (8)$$

The Walsh transform measures the correlation between f and linear functions. Large Walsh coefficients indicate strong linear correlation and potential cryptographic weakness [16], [17].

Definition 4.2: Nonlinearity: The nonlinearity of a Boolean function is defined as

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{\omega\in\{0,1\}^n} | W_f(\omega) | \quad (9)$$

Nonlinearity represents the minimum Hamming distance between f and all affine functions. Higher nonlinearity implies stronger resistance to linear cryptanalysis correlation attacks [1].

3.4 *Machine Learning Learnability Evaluation*

Machine learning classifiers are used to approximate Boolean functions. Let the training dataset be

$$D = \{(x_i, f(x_i))\}_{i=1}^{N} \tag{10}$$

where $x_i \in \{0,1\}^n$. The classifier learns a function h(x;θ) that approximates $f(x)$. In this work we use multilayer perceptrons (MLP), logistic regression classifiers. The prediction accuracy is defined by equation 11 where $\mathbf{1}(\cdot)$ is the indicator function and the the approximation error is defined by equation 12. Machine learning learnability is therefore quantified by classification accuracy.

$$Accuracy = \frac{1}{N} \sum_{i=1}^{N} \mathbf{1}(h(x_i) = f(x_i) \tag{11}$$

$$Error = 1 - Accuracy \tag{12}$$

3.5 *Spectral Learnability Theorem*

The following theorem establishes a connection between Walsh spectral properties and ML learnability.

Theorem 1: (Spectral Learnability Principle): *Let f be a Boolean function. If $\max_{\omega} | W_f(\omega) | = \lambda$ then a low-complexity classifier can approximate f with expected accuracy bounded by*

$$Accuracy \leq \frac{1}{2} + \frac{\lambda}{2^{n+1}} \tag{13}$$

A large Walsh coefficient indicates strong correlation with an affine function, which ML classifiers can exploit to reduce the hypothesis space. Similar links between spectral correlation and approximation have been studied in learning theory and Boolean function analysis [17].

3.6 *Nonlinearity–Learnability Trade-off*

Theorem 2: *For any Boolean function f, higher nonlinearity increases its Hamming distance from all affine functions, requiring greater ML model complexity for approximation and establishing a link between cryptographic strength and ML resistance.*

$$Accuracy \leq 1 - \frac{NL(f)}{2^{n-1}} \tag{14}$$

3.7 *Statistical Correlation Analysis*

To quantify the relationship between cryptographic strength and ML learnability, the Pearson correlation coefficient is computed. Let $X =$

$\{NL_1, NL_2, \ldots, NL_m\}$ be nonlinearity values and be ML accuracies. The correlation coefficient is

$$Y = \{Acc_1, Acc_2, \ldots, Acc_m\} \tag{15}$$

$$\rho = \frac{\sum(NL_i - \bar{NL})(Acc_i - \bar{Acc})}{\sqrt{\sum(NL_i - \bar{NL})^2 \sum(Acc_i - \bar{Acc})^2}} \tag{16}$$

A strong negative correlation indicates that higher nonlinearity leads to lower ML learnability.

3.8 *S-Box Cryptanalysis*

Substitution boxes are modeled as vector Boolean functions denoted by equation 17. Each component function is analyzed independently by $f_i: \{0,1\}^n \to \{0,1\}$.

$$S(x) = \big(f_1(x), f_2(x), \ldots, f_m(x)\big) \tag{17}$$

Theorem 3: (Bitwise Vulnerability). *An S-box is vulnerable to machine learning cryptanalysis if at least one component Boolean function satisfies where τ is a predefined security threshold. Even if an S-box appears globally secure, weak Boolean components may leak information. This observation aligns with prior research on S-box cryptographic design i.e. $NL(f_i) < \tau$.*

4. Results and Discussion

Experimental evaluation on 2000 Boolean functions (linear, balanced, bent-like, random) shows that Walsh spectral properties strongly influence learnability. Distributed Walsh coefficients indicate moderate resistance, while large coefficients correspond to lower nonlinearity and easier ML approximation (Figure 2 (a)). Most functions achieve 0.4–0.7 accuracy, whereas linear functions approach 1.0 (Figure 2 (b), Table 1). Nonlinearity distribution reveals two regions: zero (linear) and 20–24 (nonlinear), confirming structural diversity (Figure 2 (c), Table 1). A strong negative correlation between nonlinearity and ML accuracy indicates reduced learnability with higher nonlinearity (Figure 3(a), Table 1). Linear functions are highly learnable, while others approach random prediction (Figure 3 (b), Table 1). High nonlinearity is confirmed for balanced, bent-like, and random functions (Figure 3 (c)). Overall, results show that spectral properties govern learnability, with ML exploiting structural weaknesses rather than bypassing cryptographic principles.

Table 1
Shows ML Accuracy, Nonlinearity, Function-wise Analysis Statistics

ML Accuracy Statistics		**Nonlinearity Statistics**		**Function-wise Analysis**	
Metric	Value	Metric	Value	Type	Value
Mean Accuracy	0.5708	Standard Deviation	9.48	Balanced	21.40, 0.487

Standard Deviation	0.2052	Minimum	0	Bent	21.54, 0.498
Minimum	0.10	Median	21	Linear	0.00, 0.801
Median	0.50	Maximum	26	Random	21.61, 0.490
Maximum	1.00				

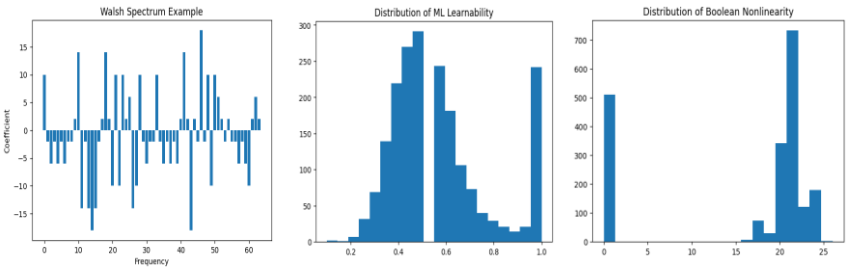

Figure 2

(a) Walsh spectrum obtained from a randomly generated Boolean function, (b) Distribution of Machine Learning Learnability, (c) Distribution of Boolean function nonlinearity

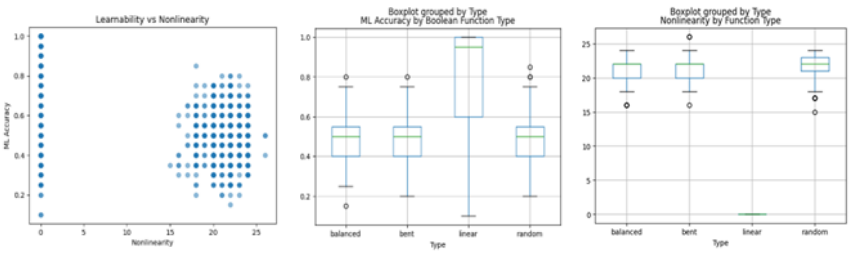

Figure 3

(a) Boolean nonlinearity and machine learning learnability, (b) Distribution of machine learning accuracy across different function types, (c) Distribution of nonlinearity across Boolean function types

5. Conclusion

This study presents a framework linking Boolean spectral properties with machine learning learnability for cryptographic security. Results show that linear functions are easily learned, while high nonlinearity improves resistance. A strong negative correlation confirms that ML exploits existing structural weaknesses. The framework supports designing cryptographic components resilient to both classical and learning based attacks, with future work extending to advanced properties and real-world ciphers. A strong negative correlation confirms that ML exploits existing structural weaknesses. The framework

supports designing cryptographic components resilient to both classical and learning-based attacks, with future work extending to advanced properties and real-world ciphers.

References

[1] C. Carlet, *Boolean Functions for Cryptography and Coding Theory.* Cambridge, U.K.: Cambridge University Press (2021).

[2] C. K. Wu, *Boolean Functions and Their Applications in Cryptography*. New York, USA: Springer (2016).

[3] O. S. Rothaus, "On bent functions," *Journal of Combinatorial Theory,* vol. 20, no. 3, pp. 300–305 (1976).

[4] J. A. Armario, M. Torres, and L. Hernández, "Boolean functions and permanents of Sylvester matrices," *Mathematics*, vol. 9, no. 2, pp. 1–15 (2021).

[5] J. Daemen and V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard. Berlin, Germany: Springer-Verlag, ser. *Information Security and Cryptography*, (2002), doi: 10.1007/978-3-662-04722-4.

[6] L. Franco, "Generalization ability of Boolean functions implemented in feedforward neural networks," *Neurocomputing*, vol. 70, pp. 351–361 (2006).

[7] A. Gohr, "Improving attacks on round-reduced SPECK32/64 using deep learning," in *Advances in Cryptology–CRYPTO 2019, Lecture Notes in Computer Science*, vol. 11692. Cham, Switzerland: Springer (2019).

[8] S. Wu and W. Wang, "A survey on the applications of artificial intelligence in cryptanalysis and cryptographic design," *Frontiers in Science and Engineering*, vol. 5, no. 3, pp. 390–399 (2025).

[9] P. P. Duong, N. T. Nguyen, and H. T. Nguyen, "Constructing 8×8 S-boxes with optimal Boolean function nonlinearity," *Cryptography,* vol. 9, no. 4, pp. 1–17 (2025).

[10] L. Rovito, A. De Lorenzo, and L. Manzoni, "Discovering Non-Linear Boolean Functions by Evolving Walsh Transforms with Genetic Programming," *Algorithms*, vol. 16, no. 11, Art. no. 499 (2023), doi: 10.3390/a16110499.

[11] M. Djurasevic, D. Jakobovic, L. Mariot, and S. Picek, "A survey of metaheuristic algorithms for the design of cryptographic Boolean func-

tions," *Cryptography and Communications*, vol. 15, no. 6, pp. 1171–1197 (Dec. 2023), doi: 10.1007/s12095-023-00662-2.

[12] D. Gerault, A. Hambitzer, M. Huppert, and S. Picek, "Survey: 6 years of neural differential cryptanalysis," *IACR Cryptology ePrint Archive*, Paper 2024/1300 (2024).

[13] B. D. Kim, V. A. Vasudevan, R. G. L. D'Oliveira, A. Cohen, T. Stahlbuhk, and M. Médard, "Cryptanalysis via Machine Learning Based Information Theoretic Metrics," arXiv:2501.15076 (Jan. 2025).

[14] C. Carlet, D. Jakobovic, and S. Picek, "Evolutionary algorithms-assisted construction of cryptographic Boolean functions," in *Proc. Genetic and Evolutionary Computation Conf. (GECCO),* Lille, France (Virtual), pp. 565–573 (Jul. 2021), doi: 10.1145/3449639.3459362.

[15] C. Carlet and D. Tang, "A general secondary construction of Boolean functions including the indirect sum and its generalizations," *IACR Cryptology ePrint Archive* (2025).

[16] K. Heuser and M. Zohner, "Spectral methods in cryptographic Boolean analysis," *Cryptography and Communications*, vol. 13, no. 5, pp. 725–747 (Sep. 2021), doi: 10.1007/s12095-021-00485-6.

[17] M. Erdal and F. Schwenker, "Learnability of the Boolean Innerproduct in Deep Neural Networks," *Entropy*, vol. 24, no. 8, p. 1117 (2022).

[18] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 5-A, pp. 1473–1486 (Aug. 2025), doi: 10.47974/JDMSC-2146.

[19] P. Mathur, F. Sheth, D. Goyal, and A. K. Gupta, "Deep insight: Mathematical modeling and statistical analysis for mango leaf disease classification using advanced deep learning models," *Journal of Interdisciplinary Mathematics,* vol. 27, no. 2, pp. 317–342 (2024).

[20] R. Joshi, P. Mathur, A. K. Gupta, S. Singh, V. Paliwal, and S. Nayar, "Mathematical modeling of intelligent system for predicting effectiveness of premenstrual syndrome," *Journal of Interdisciplinary Mathematics,* vol. 26, no. 3, pp. 551–562 (2023).

Received March, 2026