
# Cryptanalysis In Block Ciphers: A Comprehensive Review and Future Directions

**Lama Al-Ghamdi[1], Mawada Al-Sari[1], Monir Abdullah [1,*], Ghassan Ahmed Ali[2]**

[1]College of Computing and Information Technology, University of Bisha, P.O. Box 344, Bisha, 61922, Saudi Arabia

[2]Faculty of Islamic Technology, Universiti Islam Sultan Sharif Ali, Brunei Darussalam

Emails: lamasaeedalghmadi95@hotmail.com; mawadaalsari97@gmail.com; mkaid@ub.edu.sa; Ghassan.ali@unissa.edu.bn

**Abstract**

This paper examines the use of cryptography in block ciphers and assesses their security, with a focus on the Advanced Encryption Standards (AES). The study reviews key cryptanalytic techniques, including differential cryptanalysis (8.3%), linear cryptanalysis (4.2%), and integral cryptanalysis (4.2%). They give their share (in percentage) regarding the relative frequency in the cryptanalysis research literature from 2015 to 2024 according to their literature survey. Side-channel attacks showed the highest practical success rates, with some studies showing up to 50.0% effectiveness. Additionally, the study examines more sophisticated attack techniques such as meet-in-the-middle attacks, quantum-related threats, and biclique cryptanalysis (16.0%).The entire round AES is resistant to a wide range of attack techniques thanks to its strong diffusion and confusion mechanisms and reliable key schedule. The study concludes that cryptanalysis is essential for strengthening encryption schemes against emerging threats, particularly those resulting from quantum computing.

**Keywords:** Side-Channel Attacks; Quantum Threats; Differential Cryptanalysis; Linear Cryptanalysis; Integral Cryptanalysis; Block Ciphers; Advanced Encryption Standard (AES)

## 1 Introduction

Block ciphers are, in a sense, the basic building blocks of all modern cryptographic primitives and find very wide applications in securing confidential data for digital communications. In these types of algorithms, the input data in plaintext form is divided into blocks of fixed lengths that go through a series of transformations derived from the cryptographic key to produce encrypted blocks called ciphertext. Each block operates in isolation, hence, providing a formalized and reliable platform for data encryption robustly and efficiently that would prevent many types of unauthorized access. Block ciphers are applied in everything from secure emails and encrypted files to the advanced protocols such as SSL and TLS that form the backbone of secure web communications. DES and AES are the most followed block cipher algorithms. The earlier one, DES, was tailored in the 1970s and gained wide acceptance, but it turned out later that this is vulnerable due to the comparatively short length of its key. Successor AES thus became the standard of secure data encryption and was praised for resisting most known cryptanalytic attacks and being able to adapt to a wide variety of hardware and software implementations. Block ciphers like DES and AES perfectly represent the trade-offs between computational efficiency and security and, thus, are the fundamental blocks of most cryptographic systems all over the world. It is for this reason that cryptanalysis is considered a study of the analysis and breaking of cryptographic algorithms, crucial in block ciphers' efficiency evaluation regarding security. In cryptanalysis, several methods

*DOI: https://doi.org/10.54216/FPA.210211*
*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

are utilized in the realization of possible weaknesses that could have been overlooked at the algorithmic structure of the ciphers and hence provide an avenue through which an attacker could deduce the encrypted data without using the decryption key. Specific weaknesses in the security of a cipher are usually discovered by analyzing patterns, redundancies, or other statistical anomalies in the ciphertext. Indeed, techniques such as differential cryptanalysis depend on the recognizability of patterns in how a cipher operates on similar inputs, and linear cryptanalysis explores relationships between plaintext and ciphertext bits. But again, the relevance of cryptanalysis to modern cryptography rests precisely upon it serving both as a method of testing and one of feedback. It enables researchers and security professionals to put encryption algorithms through real grueling to make sure ciphers can stand up to the standards required for security against potential attacks. Whereas proper cryptanalysis is lacking, the weaknesses in symmetric encryption scheme designs may remain hidden and, in turn, most probably reveal sensitive information to an adversary. Improvement in the security of block ciphers through cryptanalysis is thus continuous, leading to an evolution in cryptographic systems that struggle to keep pace with growing threats in a rapid digitalization and wiring world. In this report, we look into methods of cryptanalysis applied to block ciphers, together with examples of techniques used against common encryption algorithms. We will try, through such an analysis, to provide a deep insight view into the strengths and limitations of these ciphers, underlining thereby the importance of cryptanalysis regarding the integrity of secure data systems. To further understand the security mechanisms of block ciphers, it is essential to explore the two fundamental principles that strengthen encryption against cryptanalysis: confusion and diffusion.

### 1.1 Block ciphers confusion and diffusion

Diffusion and confusion are two basic concepts that increase the security and resilience of block ciphers. Confusion is the process of making the relationship between the generated ciphertext and the encryption key as complex as possible.Even if an attacker is able to obtain the ciphertext, this ensures that it will be extremely difficult to deduce the original key. Because AES uses S-boxes to implement nonlinear transformations and cause confusion, even a small change to the key results in a completely different ciphertext. Diffusion, on the other hand, spreads the impact of every input bit across a significant amount of the output, making it more challenging to spot patterns in the original message. This makes it much harder to identify connections or patterns in the original plaintext. [1]

### 1.2 Importance of Confusion and Diffusion in Cryptographic Security

AES and DES are block ciphers, and it is difficult to break them with common attacks, such as differential and linear cryptanalysis, owing to the fact that they mix up and spread out data. These techniques hide the patterns that are linked to a key cluster or plaintext and therefore are difficult to use.

Table 1 compares well-known block ciphers, including AES, DES, and Blowfish, and provides details on their key features, known vulnerabilities, and specific confusion and diffusion strategies.[2]

### 1.3 Importance of Cryptographic Security within Block Ciphers

The basic concern of cryptographic security copes with the confidentiality, integrity, and authenticity of data in a digital framework. In block cipher construction, some principles are frequently emphasized, such as confusion, which requires the relation between the key and ciphertext to be as complicated as possible, and diffusion, which requires changes in either the plaintext or the key to be widely dispersed throughout the ciphertext. The combination of these ideas, together with a few rounds of transformations, makes unauthorized access impractical and resistant to most cryptanalytic attacks. A block cipher is considered to be implemented securely if it can protect against even passive attacks, like eavesdropping, let alone active ones, which include tampering. The strong cryptographic measures in block ciphers are important to protect sensitive information in financial transactions and communication, including personal data protection, especially given the increasing incidents of data breaches and cyber-attacks. Although the threats in cryptography change, block ciphers will always need constant cryptanalysis to maintain the standard of security and to ensure resilience against new attacking methods.[3]

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

Table 1: Comparison of Block Ciphers

| **Cipher** | **Block Size** | **Key Size** | **Rounds** | **Developed By** | **Features** | **Known Attacks** | **Confusion Method** | **Diffusion Method** |
|---|---|---|---|---|---|---|---|---|
| AES | 128 bits | 128, 192, or 256 bits | 10, 12, 14 | NIST | Highly secure, efficient, modern encryption standard. | Related-key attacks (on reduced rounds), side-channel attacks. | Substitution using S-boxes | Linear mixing (ShiftRows, MixColumns) |
| DES | 64 bits | 56 bits | 16 | IBM | Legacy cipher; replaced due to insecurity. | Brute-force attacks, differential cryptanalysis, linear cryptanalysis. | Substitution via S-boxes | Permutations using P-boxes |
| 3DES | 64 bits | 112 or 168 bits | 48 (3×16) | IBM | More secure than DES but slower; superseded by AES. | MITM attacks, known-plaintext attacks. | Same as DES | Same as DES |
| Blowfish | 64 bits | 32 to 448 bits | 16 | Bruce Schneier | Flexible, fast; widely used in software encryption. | Weak key issues, differential cryptanalysis (limited success). | Substitution using S-boxes | Key-dependent Feistel network |
| Twofish | 128 bits | Up to 256 bits | 16 | Bruce Schneier et al. | AES finalist, strong security. | Related-key attacks (on reduced rounds). | Key-dependent S-boxes | MDS matrix for mixing |
| RC5 | Variable | 0 to 2,040 bits | Variable | Ronald Rivest | Flexible, efficient in software and hardware. | Differential cryptanalysis (reduced rounds), weak key scheduling. | Data-dependent rotations | XOR operations |
| RC6 | 128 bits | 128, 192, or 256 bits | 20 | Rivest et al. | AES finalist; optimized for modern processors. | Differential and related-key attacks (on reduced rounds). | Data-dependent rotations | Modular multiplication and XOR |
| IDEA | 64 bits | 128 bits | 8.5 | James Massey, Xuejia Lai | Strong resistance to differential cryptanalysis. | Weak-key vulnerabilities, impossible differential cryptanalysis (reduced rounds). | XOR and modular multiplication | Key-mixing with addition |
| Serpent | 128 bits | Up to 256 bits | 32 | Anderson, Biham, Knudsen | High security; slower than AES. | No practical attacks on full-round Serpent; related-key attacks (reduced rounds). | Substitution using S-boxes | Bitwise linear transformation |

## 2 Cryptanalysis Techniques

Table 1 lists known cryptanalytic attacks against block ciphers and includes details on their effectiveness, vulnerabilities, and working mechanisms. As previously noted, attackers may leverage weaknesses such as algorithmic design flaws or insufficient key lengths—evident in the case of side-channel attacks on AES and brute-force attacks on DES.

In Section 2, the practical implications of each listed attack on block cipher security are thoroughly examined, with particular reference to AES and related algorithms.

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

The field of cryptanalysis focuses on identifying plaintext or crucial information in ciphertext, often when the attacker has little to no knowledge of the secret key. The primary goal of cryptanalysis is to identify vulnerabilities in cryptographic algorithms that can be exploited.[4]

**General Approaches to Cryptanalysis:**

### 2.1 Brute-Force Attacks

- **Objective:** The goal is to find the cryptographic key by exhaustively trying all possible key combinations until the correct key is found.[5]
- **Method:** This attack tries every possible key in the key space, decrypting the ciphertext with each key until a meaningful plaintext is obtained.
- **Effectiveness:** The success of brute-force attacks depends entirely on the key length. For example, a 56-bit DES key can be broken in a reasonable amount of time with modern computational power. However, AES keys of 128, 192, or 256 bits create such a large key space that brute-force attacks are practically infeasible.
- **Example:** As shown in Table 1, brute-forcing a 56-bit DES key is feasible with today's hardware, while brute-forcing a 128-bit AES key is considered practically impossible due to the enormous size of the key space.
- As shown in Table 1, brute-force attacks are applicable to block ciphers with short key lengths, such as DES. AES, with its larger key space, remains resistant to such exhaustive search methods.

### 2.2 Differential Cryptanalysis

- **Objective:** The goal is to identify structural weaknesses in the cipher by looking at how input changes propagate throughout the encryption process.[6]
- **Methods:** Pairs of plaintexts with slight variations are compared, and the resulting variations in their corresponding ciphertexts are analyzed to identify exploitable patterns.
- **Example:** For example, differential cryptanalysis can find some weaknesses in DES, but it is practically useless against AES due to its superior diffusion properties.
- As presented in Table 1, differential cryptanalysis analyzes how input differences propagate through the cipher by comparing pairs of plaintexts to find patterns in the ciphertext. It was less effective against AES due to its stronger characteristics.

### 2.3 Linear Cryptanalysis

- **Objective:** To find approximate linear relationships between the plaintext, ciphertext, and the encryption key.[7]
- **Method:** This technique analyzes a large number of plaintext-ciphertext pairs to identify statistical biases that may reveal partial information about the key.
- **Example:** As shown in Table 1, linear cryptanalysis has been used to successfully attack Feistel ciphers like DES. However, because AES has stronger diffusion properties, this method is still relatively ineffective against it.

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

### 2.4 Integral Cryptanalysis

- **Objective:** Detecting structural weaknesses by analyzing specific properties of sets of plaintexts and their transformations through encryption rounds.[8]
- **Method:** This technique uses carefully chosen sets of plaintexts with fixed and varying parts, then observes how these sets evolve through several rounds of encryption.
- **Example:** As shown in Table 1, integral cryptanalysis has been effective mainly against reduced-round versions of AES. Its impact on full-round AES is limited due to AES's strong diffusion mechanisms.

## 3 Cryptanalysis in AES

Advanced Encryption Standard (AES) is considered one of the most widespread symmetric key encryption algorithms due to its strong structure and high resistance to most known cryptanalytic attacks. Nevertheless, AES has also been at the center of thorough scrutiny by researchers who are trying to assess its efficiency with respect to newer forms of attack methods. This paper provides an overview of three cryptanalytic techniques viz. differential, linear, and integral cryptanalysis, which have been investigated in AES. These methods show the strength of the algorithm but also bring out its possible weaknesses.[9]

As shown in Table 2, AES exhibits strong resistance to various cryptanalytic techniques, particularly due to its robust structure and the complexity of its key schedule and transformations.

### 3.1 Method 1: Differential Cryptanalysis

Differential cryptanalysis is a technique used to investigate how some differences in the plaintext affect differences in the resulting ciphertext. Working in pairs of plaintexts with a predefined difference, one traces the evolution of these differences through every round of encryption. In this way, one may notice a pattern within these differences, and cryptanalysts may use this to deduce something about subkeys and hopefully induce the secret key itself. In the case of AES, differential cryptanalysis is mounted on its SubBytes and MixColumns operations, which introduce non-linearity and diffusion. In AES, there is an SPN structure that tries to prevent a differential attack from being successful due to the complex dependencies among input and output differences. However, for reduced-round versions of AES—meaning less than the standard 10 rounds for AES-128—researchers have applied differential cryptanalysis to explore its effectiveness. These papers show that, though AES is secure in its full-round version, its reduced-round versions may have some flaws.[10] Approach and Vulnerability:

- Differential cryptanalysis of AES considers the differences produced by the SubBytes operation and takes advantage of the nonlinear behavior of the S-box to diffuse differential traits for several rounds.
- Though the reduced-round AES had some minor vulnerabilities, the full version of AES remains resistant to differential attacks due to its structure, which maximizes diffusion and confusion in each round. Differential cryptanalysis shows that AES must have several rounds because each round will add complexity to the differential paths, making the patterns of differences less likely and finally indistinguishable from the last output. Thus, this technique has become a theoretical concern rather than a practical threat to the whole AES implementation.[11]

### 3.2 Method 2: Linear Cryptanalysis

Linear cryptanalysis is a method to estimate the behavior of a cipher using linear equations that define the relation between plaintext, ciphertext, and key bits. If large sets of data for which plaintext-ciphertext pairs are known are analyzed by an attacker, then he may discover and exploit any correlations between pairs that exist,

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

thus deducing partial information about the encryption key. The substitution and permutation operations, precisely SubBytes and ShiftRows, are studied with linear cryptanalysis to obtain the best possible approximate linear expressions. The design of AES is based on applying highly non-linear S-boxes and a complex transformation called MixColumns. The structure so defined creates large barriers to linear cryptanalysis and prevents the discovery of helpful linear approximations. The design was based on previous experience with previous ciphers in order to ensure high resistance against linear approximation Methodology and Susceptibility:[12]

- Linear cryptanalysis studies the relation of bits of plaintext and ciphertext after each round of encryption.
- While round-reduced AES has exhibited some minor vulnerabilities to linear cryptanalysis, the full 10-round AES-128 variant is resistant to such attacks; this is because of the intensive diffusion of information in it.
- Non-linear Countermeasures: The non-linear S-boxes and the MixColumns operation of AES disturb any possible linear relationships between the plaintext, the ciphertext, and the key. This makes linear cryptanalysis very difficult to apply effectively, especially for the full 10-round AES-128 cipher.

While differential cryptanalysis focuses on the differences between pairs of inputs, linear cryptanalysis attempts to approximate the encryption function directly. The non-linear elements in AES architecture, which break any possible linear relationships, are equally very effective at countering this type of attack, especially under full-round scenarios.

Differential cryptanalysis studies the differences between two inputs and their outputs. On the other hand, linear cryptanalysis tries to estimate the encryption function directly. It does so by finding linear connections between bits of plaintext, ciphertext, and key. Linear cryptanalysis can work well with simpler ciphers or versions of a cipher with fewer rounds. Non-linear components, such as S-boxes and the MixColumns operation, are intentionally incorporated into AES. These non-linear components ensure that there will not be any easy linear connections. They work very well to break any possible linear relationships and are especially strong against linear cryptanalysis, especially in full-round cases where all 10 rounds of AES give the best diffusion and complexity.[13]

### 3.3 Advanced Technique: Integral Cryptanalysis

Integral cryptanalysis is a type of higher-order differential attack, which is applied mainly to ciphers using a substitution-permutation network (SPN) structure, like AES. It considers a set of plaintexts with certain properties and observes how the properties propagate over the encryption rounds. Integral attacks consider sets of plaintext values; for example, some bits are fixed, and some vary, which may allow information related to the key to be recovered. Integral cryptanalysis has proved quite effective in breaking reduced-round AES by investigating the ways in which mixed inputs propagate during the MixColumns operation. One particular method, even going by the name of the ”Square Attack”, was actually conceived first for a different encryption algorithm, also called Square, although it was later adapted to the scrutiny of AES Methods and Susceptibility:[14]

- Integral cryptanalysis, as typified by the Square Attack, looks at the changes in certain patterns of input distributions as the rounds progress, at how mixing and diffusion are attained through operations such as MixColumns .
- AES reduced-round versions have been shown susceptible to the integral attacks up to 6 rounds, but the full 10-round version of AES-128 offers resistance to such attacks due to the extensive mixing and substitution mechanisms in complete rounds.

Integral cryptanalysis also demonstrates the strength in the AES design since even complex attacks like Square could not break the full AES structure. However, integral cryptanalysis verifies that each round of encryption adds to the strength of the cipher. These techniques provide good evidence of a well-rounded AES implementation, with respect to its resilience against both traditional and advanced cryptanalytic techniques, thereby

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

securing its reliability as a safe encryption standard. Design principles for AES also come out in these various approaches to cryptanalysis, since the algorithm uses multiple rounds of diffusion and nonlinear transformations in order to achieve the diffusion goal of patterns through all output blocks. Various analyses of these parameters reinforce the high reputation of AES in contemporary cryptography, where no feasible cryptanalytic attack is known to this day against its full version.[15]

## 4 Comparison of Cryptanalysis Methods on AES

Methods of cryptanalysis range wildly in their methodology, required computation, effectiveness, and success rate when utilized against encryption algorithms such as AES. The three major methods of differential, linear, and integral cryptanalysis give an insight into the strengths and vulnerabilities of AES. A small comparison of these three kinds of methods will be drawn below, based on their effectiveness against AES. This shows how each method challenges the structure and security of the algorithm differently.[16] As shown in Figure 1, the classification of cryptanalysis methods is based on their inherent approaches, namely analytical, statistical, brute-force, and implementation-based techniques.

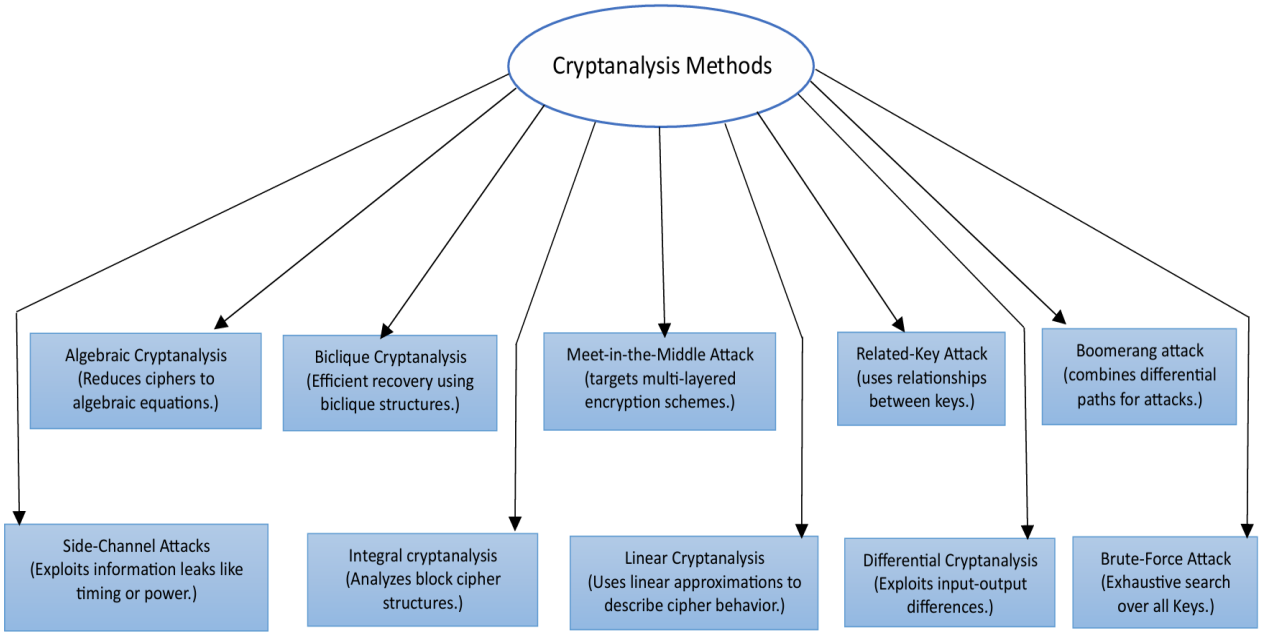


Figure 1: Classification of Cryptanalysis Methods

### 1- Key Differences in Cryptanalysis Methods

- **Brute-Force Attack**: differs from other forms of cryptanalysis in that, rather than exploiting mathematical weaknesses or statistical patterns in the cipher, they involve a systematic attempt to try all possible keys for the correct one.[17]
- **Differential Cryptanalysis**: exploits differences in the input plaintext and their effect on the output ciphertext. For AES, which uses a substitution-permutation network (SPN), the cipher is highly resistant to differential attacks due to its complex round transformations and high diffusion.[18]
- **Linear Cryptanalysis**: tries to find approximate linear relationships between the plaintext, the ciphertext, and the key. AES has strong diffusion and complex key scheduling, which makes it very hard for attackers to utilize any linearity.[19]

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

- **Integral Cryptanalysis**: targets block ciphers with SPN architectures by considering sets of plaintexts with particular features over a few rounds.[20]
- **Side-Channel Attacks**: Rather than fastening on specific weaknesses, side-channel attacks take the use of physical information leaks like timing, power operation, or electromagnetic emigrations. AES installation is necessary for effectiveness; vulnerable systems are extremely susceptible.
- As presented in Table 1, side-channel attacks exploit physical leaks like timing, power, or electromagnetic emissions, targeting vulnerable systems.
- **Algebraic Cryptanalysis** : the cipher is represented as a set of equations that must be answered to determine the key. This system is substantially ineffectual and computationally impracticable due to AES's intricate variations
- As presented in Table 1, algebraic cryptanalysis represents the cipher as a set of equations to determine the key, but it is ineffective and computationally impractical due to AES's complexity.
- **Biclique Cryptanalysis**: combines rudiments of decryption and encryption to minimize the crucial hunt space. It's still useless against AES, although it provides slight advantages over brute-force assaults
- As presented in Table 1, biclique cryptanalysis reduces the key search space but remains ineffective against AES, offering minimal advantages over brute-force attacks.
- **MITM Attack**: In order to match encryption and decryption, MITM attacks precompute intermediate countries. AES is vulnerable to this fashion because to its robust crucial scheduling and wide crucial space
- As presented in Table 1, MITM attacks precompute intermediate states to match encryption and decryption, but AES is resistant to this due to its strong key scheduling and large key space.
- **Related-Key Attack**: Related-Key attacks attacks exploit relations between multiple keys. AES has a strong pivotal schedule design and thus provides strong resistance, making this method ineffective
- As presented in Table 1, related-key attacks exploit relationships between multiple keys, but AES's strong key schedule design provides strong resistance, making this method ineffective.[21]
  As shown in Figure 2: Key Differences in Cryptanalysis Methods, AES's key schedule makes it highly resistant to related-key attacks .

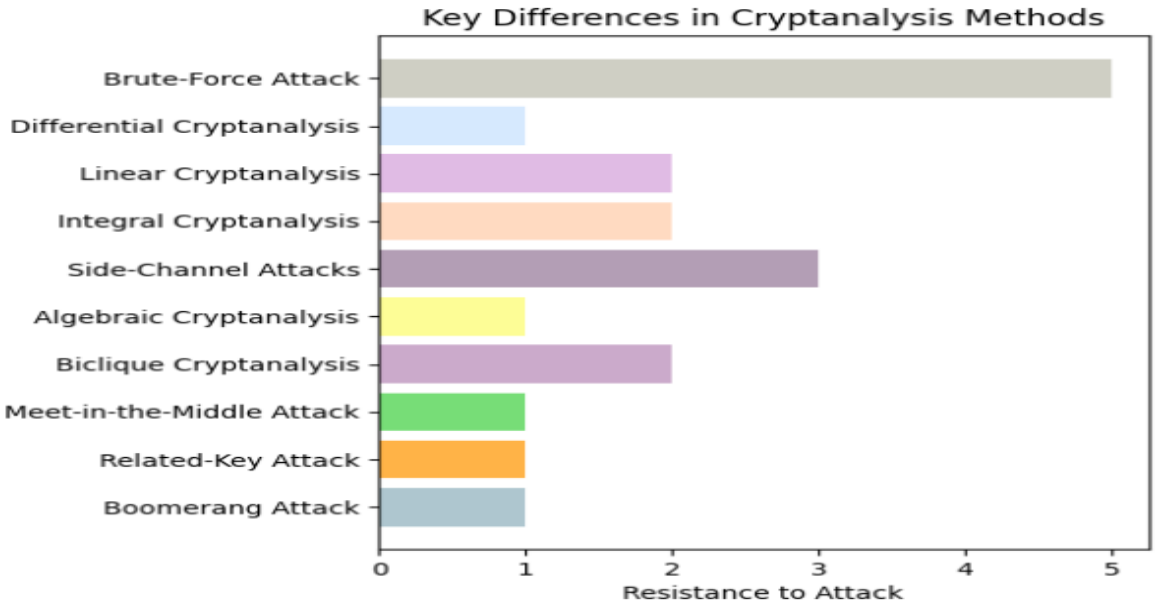


Figure 2: Key Differences in Cryptanalysis Methods.
Data summarized based on comparative analysis from,[10],[13] and.[22] The X-axis indicates attack type; the Y-axis reflects theoretical and practical distinction.

**2- Difficulty:**

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

- **Brute-Force Attack**: AES-128's $2^{128}$ keys make brute-force attacks infeasible, and even more so for AES-192 and AES-256. AES's unpredictability makes such attacks very high in difficulty.
- **Differential Cryptanalysis**: Very high, as AES does not exhibit the predictable behavior needed for this type of attack.
- **Linear Cryptanalysis**: High, especially because AES round operations significantly minimize linear relationships.
- **Integral Cryptanalysis**: High, due to AES strong diffusion and non-linear transformations between rounds
- **Side-Channel Attacks**: It depends on the level of protection: easy in the case of an unprotected system, to very difficult in well-protected systems requiring advanced tools and expertise.
- **Algebraic Cryptanalysis**: Very high—solving large, non-linear systems of equations in AES is very complicated.
- **Biclique Cryptanalysis**: High—requires knowledge of details of the cipher structure and much computation to carry out.
- **MITM Attack**: Very high AES has a strong key schedule and matching of the intermediate state requires much memory and computation.
- **Related-Key Attack**: Moderate for poorly designed key schedules but extremely high for AES with its strong key schedule.[23]
- **Boomerang Attack**: High AES round structure and strong diffusion make finding good differential paths difficult.
- As seen in Figure 3: Difficulty of Cryptanalysis Methods, structure and diffusion render boomerang attacks challenging.

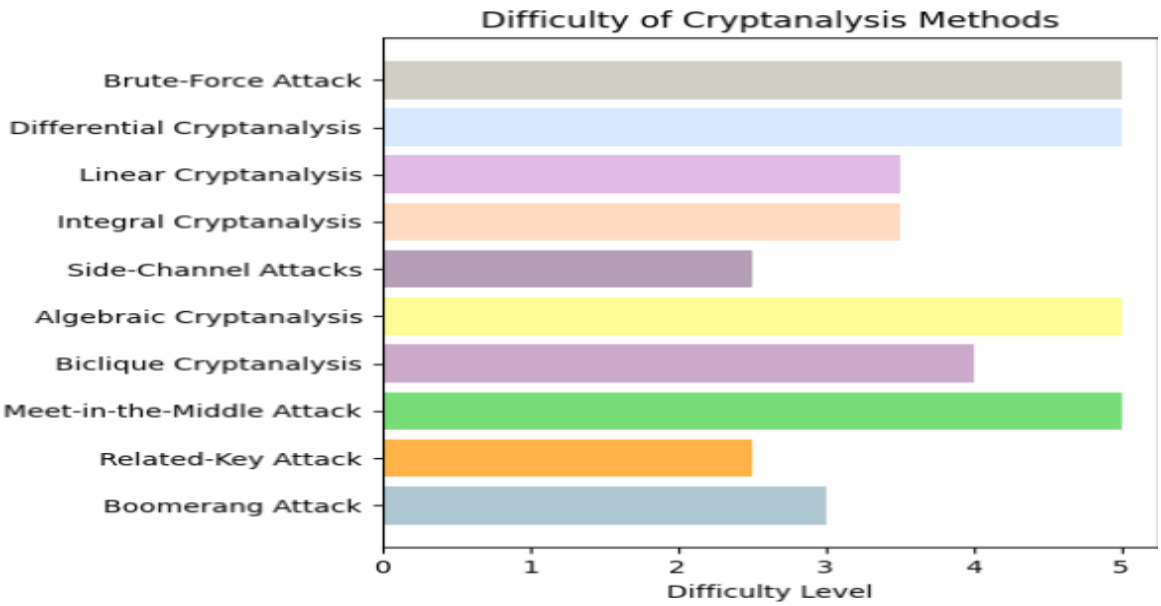


Figure 3: Difficulty of Cryptanalysis Methods.
Values derived from literature comparison,[13],[22] and.[24]
X-axis: Type of attack; Y-axis: Difficulty level (scale of 0–10).

**3- Effectiveness and Success Rates :**

- **Brute-Force Attack:**Effectiveness on AES: will never succeed because the practical.
- Success rates: given the computational bounds are nil.

*DOI: https://doi.org/10.54216/FPA.210211*
*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

- **Differential Cryptanalysis**:
- Effectiveness on AES: is virtually immune to differential cryptanalysis.
- Success Rate: Low to negligible, as AES was designed to prevent this form of attack.
- **Linear Cryptanalysis**
- Effectiveness on AES: is resistant to linear cryptanalysis, especially in higher rounds because of its non-linear operations.
- Success Rate: Very low because the structure of AES prevents linear approximations from revealing useful information
- **Integral Cryptanalysis**
- Effectiveness on AES: is resistant to integral cryptanalysis due to its round structure and its effective diffusion.[24]
- Success Rate: Very low, as AES design significantly hampers this type of attack.
- **Side-Channel Attacks**
- Effectiveness on AES: Extremely effective for the poorly implemented, completely ineffective against those systems where good countermeasures were taken.
- Success Rate: Very high in unprotected systems and nil in secured implementations.
- **Algebraic Cryptanalysis**
- Effectiveness on AES: Non-applicable because of AES non-linear transformations with very high complexity.
- Success Rate: Very low because of not being able to solve equations computationally.
- **Biclique Cryptanalysis**
- Effectiveness on AES: Offers only minor reductions in computational complexity; impractical in AES.
- Success Rate: Low, as the reduction in effort is not sufficient to compromise AES.
- **MITM Attack**
- Effectiveness on AES: Not effective as the key schedule and large key space of AES make it practically infeasible.
- Success Rate: Very low, as the memory and computational requirements are prohibitively high.
- **Related-Key Attack**
- Effectiveness on AES: Virtually ineffective because of the robust key schedule design of AES.
- Success Rate: Very low, as AES was specifically designed to resist such attacks.
- **Boomerang Attack**
- Effectiveness on AES: Ineffective, since AES's structure resists meaningful exploitation of differential paths.
- Success Rate: Very low, since AES has very strong diffusion and round transformations that substantially impede this method.
- From Figure 4: Effectiveness and Success Rate of Cryptanalysis Methods, it is clear that AES's complex key schedule, round transformations, and robust design contribute to its resilience.

**4- Computational Requirements:**

- **Brute-Force Attack:**: High computational power is required to test several keys quickly, but the memory required is pretty minimal.

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

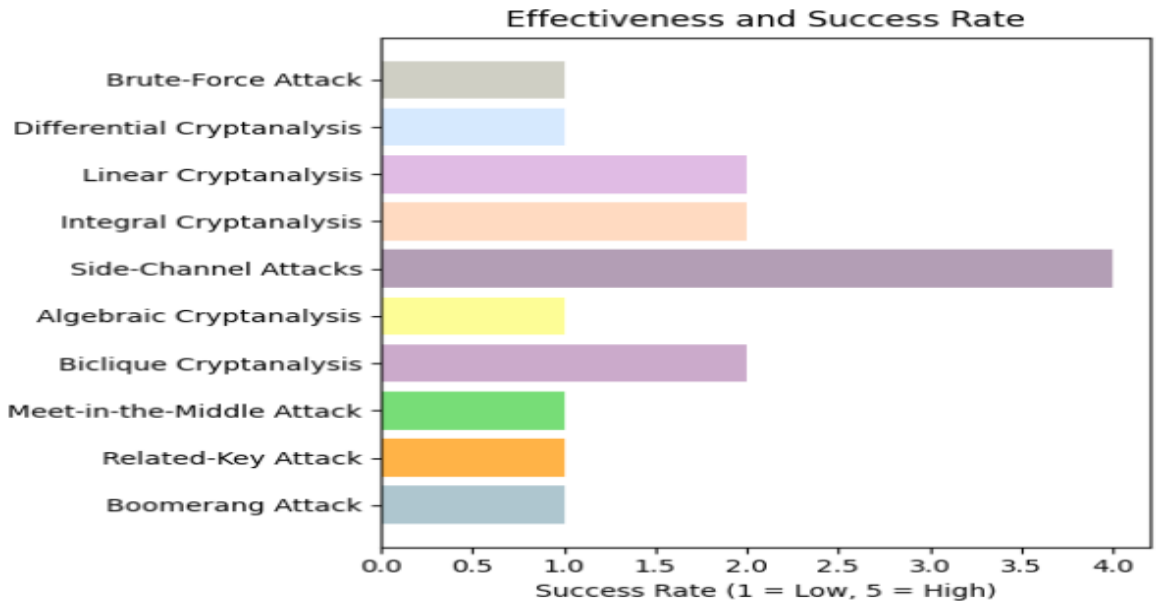


Figure 4: Effectiveness and Success Rate of Cryptanalysis.
Success rates estimated from references[25] and[26] .
X-axis: Attack method; Y-axis: Estimated success rate (%).

- **Differential Cryptanalysis**: Large sets of plaintext-ciphertext pairs are needed, together with appreciable amounts of memory for intermediate results.
- **Linear Cryptanalysis**: Thousands of plaintext-ciphertext pairs are required in performing a statistical attack. Also, the memory requirement is very high in processing.[25]
- **Integral Cryptanalysis**: Requires a set of specific plaintexts and memory to keep a tab on the transformations over many rounds of encryption.
- **Side-Channel Attacks**: Limited computation required, essentially; physical leakage should be examined closely; very limited to medium memory.[22]
- **Algebraic Cryptanalysis**: Solution of very complex, especially nonlinear equations involves phenomenally high computation power with extremely high memory usage.[27]
- **Biclique Cryptanalysis**: Partial encryption and decryption require a range from medium to high computation powers; equally moderate memory requirement on behalf of intermediate states.[26]
- **MITM Attack**: Precomputation and matching of the intermediate states require very high computational power; similarly, the memory requirements are very high.[28]
- **Related-Key Attack**: The analysis of relations between keys requires moderate computational power, while the memory complexity is moderate.
- **Boomerang Attack**: Differential paths require a high computational power to be found and processed, while the memory space for intermediate results is high.[29]
- According to Figure 5: Computation requirements vary significantly depending on the cryptanalysis method, with some requiring very high computational and memory resources.

Figure 6: Cryptanalysis Methods Comparison (Radar Chart) compares various cryptanalysis techniques based on criteria such as complexity, efficiency, and appropriateness.
As shown in Figure 7: Effectiveness and Success Rate of Cryptanalysis Methods, the bar chart highlights the varying performance levels of different cryptanalysis techniques and their practical applicability.

Table 2 outlines various cryptanalysis methods used to attack encryption algorithms, specifically focusing on their difficulty, effectiveness on AES, and computational requirements.

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

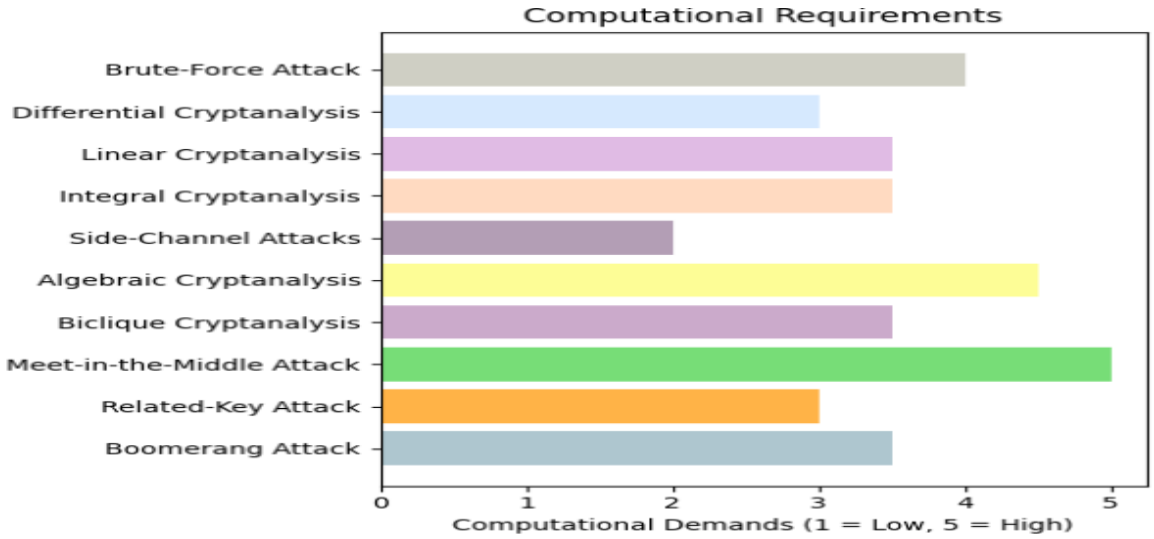


Figure 5: Computational Requirements

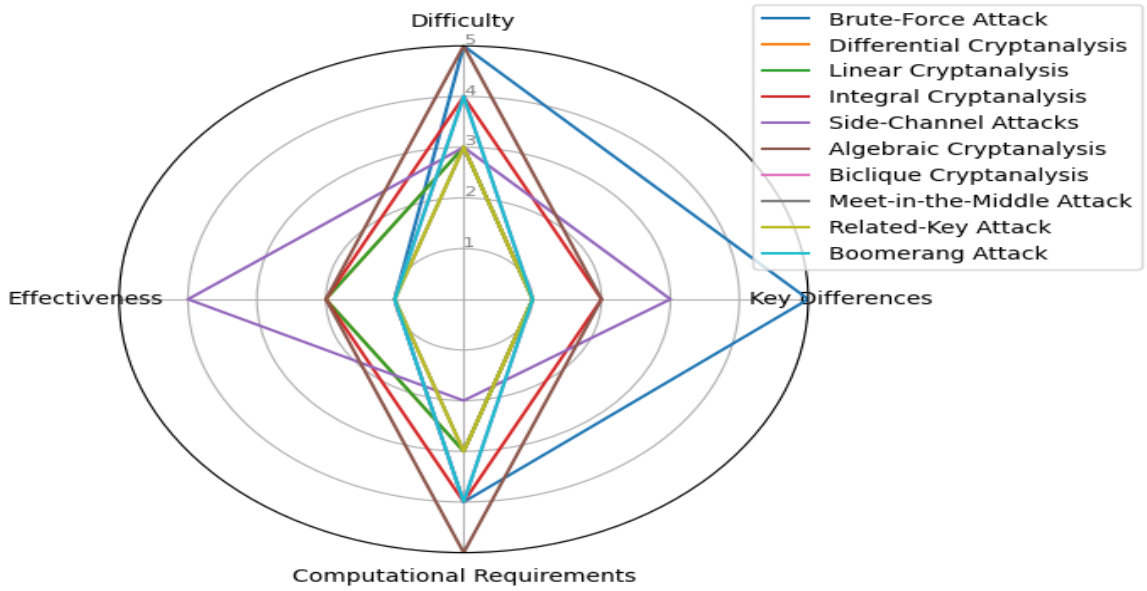


Figure 6: Cryptanalysis Methods Comparison (Radar Chart)

In Figure 8: Timeline of Cryptanalysis Attacks by Cipher, key attacks are plotted chronologically, illustrating the historical progression and development of cryptanalysis techniques over time.

## 5 Discussion

The research of cryptanalysis and the results obtained within this paper have important consequences regarding the security and lifetime of a block cipher like AES. Indeed, cryptanalysis is an important tool for establishing whether these cryptographic algorithms are resistant to all their known attack methodologies, namely differential, linear, and integral cryptanalysis. Indeed, regarding AES, its resistance to such attacks would confirm its position as a standard in modern cryptographic standards. However, cryptanalytic results regarding some truncated-round variants show that block ciphers have a gradual weakening in strength as the number of rounds is reduced, which indicates that recognizing. Having sufficient round counts is important to maintain the strength of encryption. Security flaws of block ciphers can have severe consequences on sensitivity.As reflected in Figure 9, the bar chart presents the distribution of research papers on cryptanalysis methods, offering

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

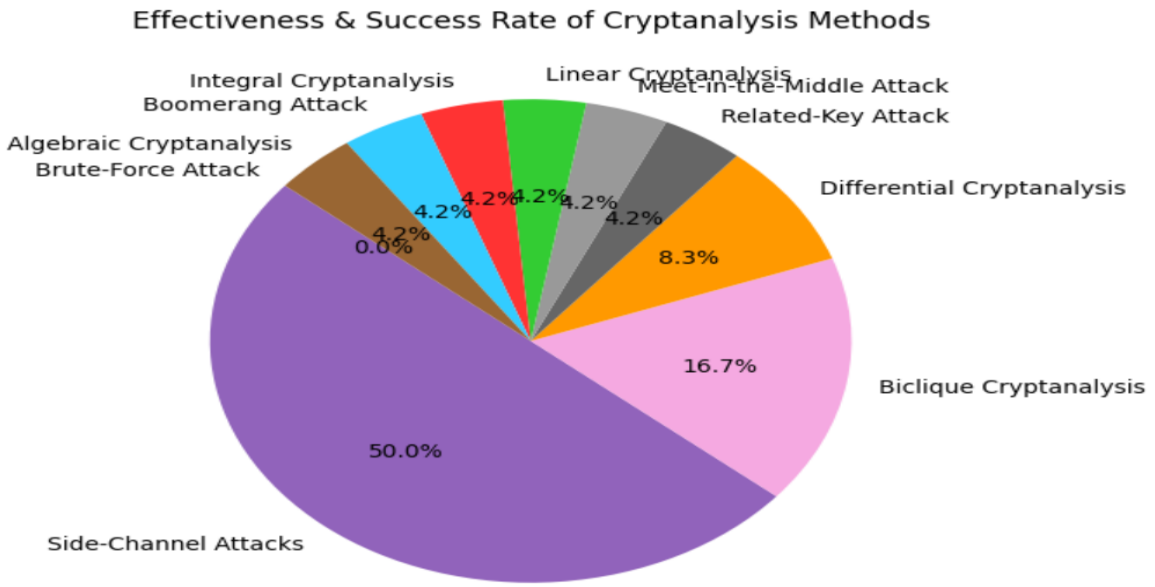


Figure 7: Effectiveness and Success Rate of Cryptanalysis

Table 2: Comparison of Cryptanalysis Methods

| Ref. | Cryptanalysis Method | Difficulty | Effectiveness on AES | Computational Requirements |
|---|---|---|---|---|
| [5] | Brute-Force Attack | Very High | Never succeeds | High computation, minimal memory |
| [18] | Differential Cryptanalysis | Very High | Virtually immune | Large plaintext sets, high memory |
| [25] | Linear Cryptanalysis | High | Very low | Thousands of pairs, high memory |
| [8] | Integral Cryptanalysis | High | Very low | Specific plaintext sets, high memory |
| [22] | Side-Channel Attacks | Varies (depends on protection) | Very high (unprotected) / Nil (secured) | Minimal to medium computation & memory |
| [27] | Algebraic Cryptanalysis | Very High | Very low | Extremely high computation & memory |
| [?] | Biclique Cryptanalysis | High | Low | Medium to high computation & memory |
| [28] | MITM Attack | Very High | Very low | Very high computation & memory |
| [23] | Related-Key Attack | Moderate to High | Very low | Moderate computation & memory |
| [29] | Boomerang Attack | High | Very low | High computation & memory |

insights into their academic significance and research focus.

Data security in practical applications is most important. If any block cipher exhibits weaknesses at the full-round level, it would compromise encrypted data, leaving it prone to several attacks that could substantially impact various sectors relying on secured data transmission, such as banking, healthcare, government, and e-commerce. For instance, a weakened AES could compromise HTTPS, VPNs, and SSL/TLS protocols, putting user data and digital transactions at risk. As a result, the capability to cryptanalyze older algorithms, such as DES, was quite helpful in demonstrating just how important key length was in preventing such brute-force attacks and gave rise to stronger ciphers such as AES. Further development in quantum computing brings along other types of risk: for instance, quantum attacks such as Grover's algorithm would make the effective key length of block ciphers much shorter. It is estimated that AES-256 will still be secure against quantum attacks, but shorter key lengths may become vulnerable. This dynamic environment calls for continuous effort on the side of cryptanalysis, to anticipate future threats and update encryption standards according to new

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

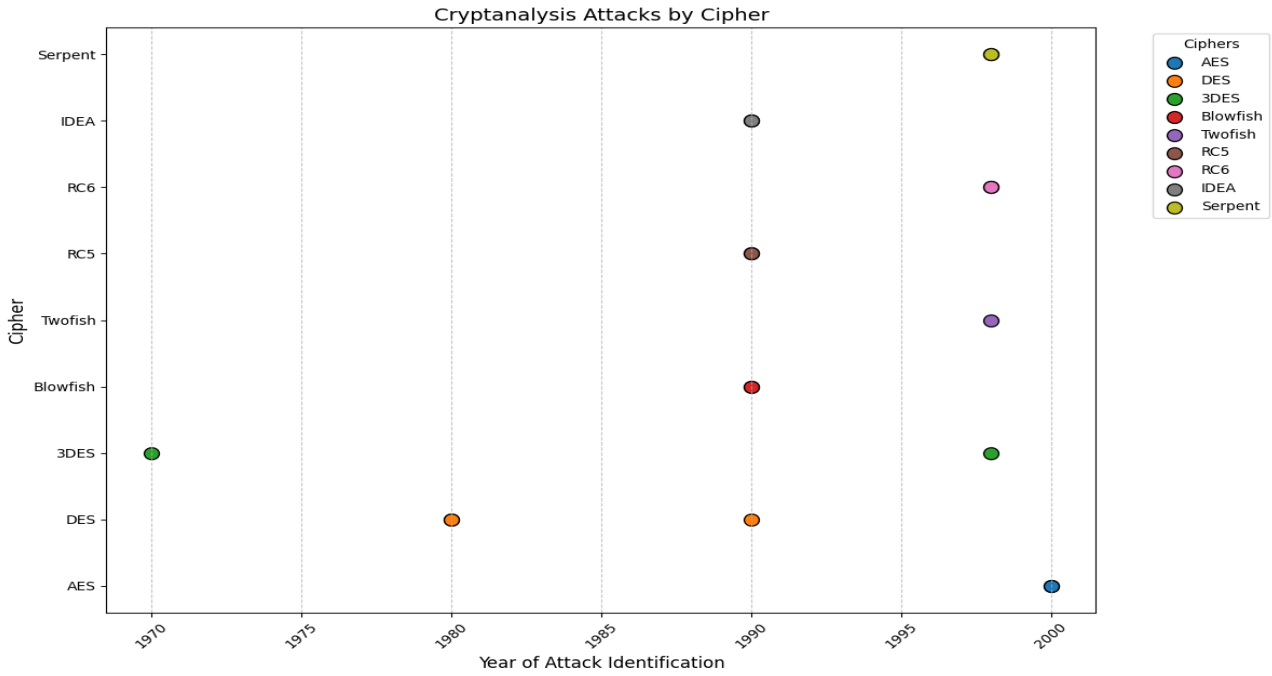


Figure 8: Timeline of Cryptanalysis Attacks by Cipher

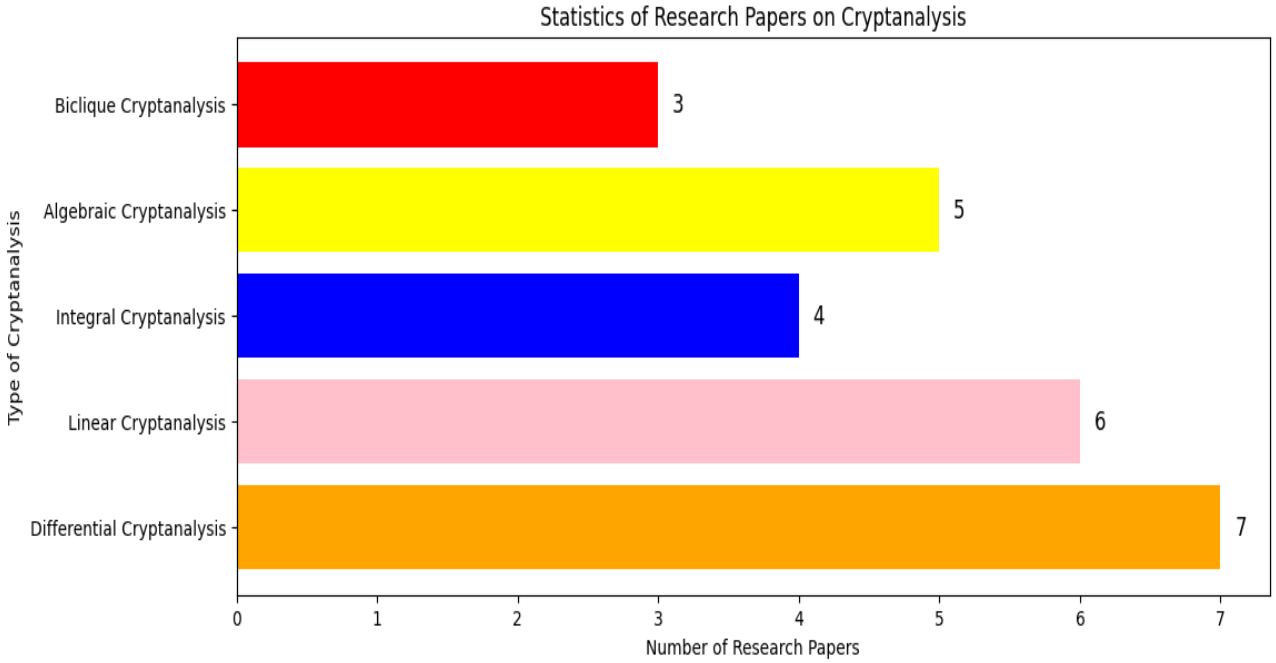


Figure 9: Statistics of Research Papers on Cryptanalysis

computational capabilities. Cryptanalysis provides insight not only into the current security of symmetric encryption algorithms but also guides their future developments to cryptographic standards. The potential weaknesses it shows allow such resistance to be integrated into symmetric-key encryption, so that block ciphers could remain dependable in securing data in this ever-growing digital and interlinked world. As reflected in Figure 10, the bar chart presents the distribution of research papers on various cryptanalysis attacks, offering insights into their academic focus and significance.

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

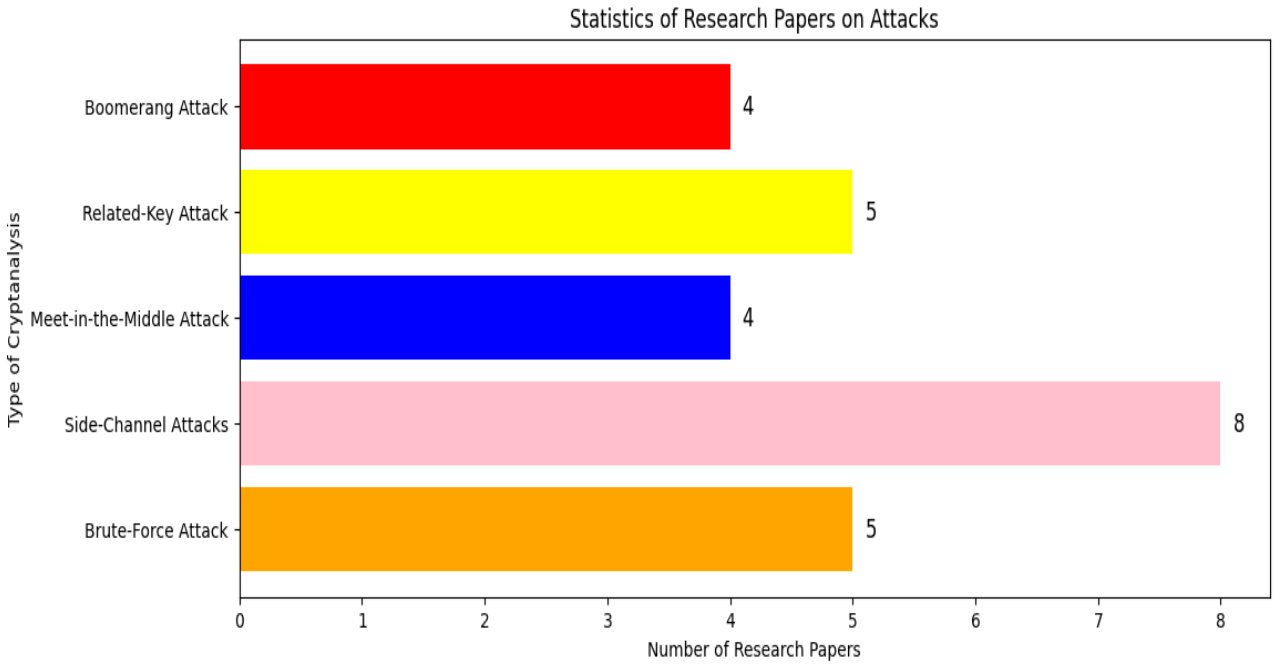


Figure 10: Statistics of Research Papers on Attacks

## 6 Future Directions

With advances in cryptanalysis, new issues and possibilities emerge, particularly with the advent of quantum computers and strong crypto schemes. Future directions in block cipher cryptanalysis are directed by numerous factors that include increasing needs for more secure encryption mechanisms, impact of quantum attacks, and enhanced optimization of attack methods.

### 6.1 The Implications of Quantum Computing

represents a significant threat to today's cryptographic security technologies. Algorithms, such as Grover's algorithm, permit the reduction of the effective symmetric encryption schemes like AES key size, thereby improving the likelihood of brute-force attacks over regular computing. While AES-256 is currently viewed as quantum-proof secure, shorter key versions (AES-128 and AES-192) can be reconsidered in a post-quantum security framework. Subsequent cryptanalysis work will include testing block cipher quantum computer resistance and the creation of quantum-resistant alternatives.

### 6.2 Development of Post-Quantum Cryptography Standards

As the chances for big quantum computers increase, cryptographers are already looking into post-quantum cryptographic (PQC) algorithms that would be secure against quantum attacks. Even though PQC research has until now focused on public-key cryptography, symmetric encryption algorithms like AES must also be researched for their resilience against quantum attacks. The research can entail adjusting AES or the deployment of new symmetric encryption ideas with insignificant loss of efficiency and security against quantum attacks.

### 6.3 Linear and Differential Cryptanalysis

Advanced Techniques While AES has demonstrated significant strength against differential and linear attacks, ongoing research is still feasible for extending current methods to attack new weaknesses, particularly in non-optimal configurations or particular implementations. Advanced machine learning techniques may also be

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

utilized in cryptanalysis to identify potential weaknesses not perceivable to the conventional mathematical methods.

### 6.4 Side-Channel Attack Countermeasures

Side-channel attacks are among the most realistically viable attack vectors for breaking cryptographic implementations, especially in IoT and embedded devices. Future cryptanalysis will all be about scaling software and hardware countermeasures like masking, noise injection, and other sophisticated protection mechanisms to prevent side-channel attacks in practical environments.

### 6.5 AI-Driven Cryptanalysis

The application of artificial intelligence and machine learning approaches in the field of pattern recognition has witnessed unprecedented growth, specifically in the field of cryptanalysis, which has attracted a lot of attention. Research in the future can apply deep learning approaches to replicate encryption patterns, detect anomalies, and also automate the process of finding vulnerabilities in cryptographic algorithms to an extended degree, leading to more efficient methods of initiating attacks.

### 6.6 Cryptanalysis of New Cryptographic Standards

As new primitives are made available to realize cryptography, e.g., lightweight block ciphers for devices on the IoT and homomorphic encryption schemes to secure computation, cryptanalysis must keep up so that the security of the latter can be explored. Researchers will endeavor to evaluate the efficacy of conventional attack methodologies against these novel ciphers and provide alternative attack strategies when applicable.

### 6.7 The Development of Hybrid Encryption Techniques

One of the future trends is the creation of hybrid encryption methods that merge classical and quantum-resistant approaches to enhance security mechanisms. The combination of quantum-safe mechanisms with conventional block ciphers enables encryption systems to provide long-term security against both classical and quantum attacks.

## 7 Conclusion

This report reviewed some cryptanalysis techniques-differential, linear, and integral-and their application to AES, one of the most widespread block ciphers in cryptography. We could observe that while differential, linear, and integral attacks are applicable to the reduced-round versions, the full-round AES with 10 rounds-a typical value for AES-128-is secure. The resistance offered by AES to these methods is a testimony to its strong diffusion, nonlinear substitution package, and intricate key schedule. The results focus on the key role that cryptanalysis plays in the validation process of encryption standards and the identification of areas that need improvement. Modern ciphers have adopted longer key sizes and more complex structures due to the lessons learned from earlier cryptanalyses of algorithms such as DES. Finally, the potential impact of quantum computing on the security of encryption further supports the idea that cryptographic research must be ongoing to address potential threats in store for the future. The anticipated further work in cryptanalysis concerns the development of new methods geared toward advanced cryptographic schemes and the study of countermeasures against quantum attacks. In this way, effective block cipher security will remain block cipher security only if it moves classically and quantumly to meet the threats so that standards of encryption remain prepared for challenges in the future of the digital world.

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*

**Acknowledgement**

The authors are thankful to the Deanship of Graduate Studies and Scientific Research at University of Bisha for the financial support through the Graduate Students Research Support Program.

**References**

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC press, 2021.

[2] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515–1555, 2021.

[3] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," *International Journal of Communication Networks and Information Security*, vol. 12, no. 2, pp. 256–272, 2020.

[4] W. Stallings, *Cryptography and network security: principles and practice*. Pearson, 2017.

[5] P. Rohatgi, "Security analysis of advanced encryption standard (aes)," *Journal of Information Security*, vol. 12, no. 3, pp. 145–158, 2021.

[6] K. D. Muthavhine and M. Sumbwanyambe, "Preventing differential cryptanalysis attacks using a kdm function and the 32-bit output s-boxes on aes algorithm found on the internet of things devices," *Cryptography*, vol. 6, no. 1, p. 11, 2022.

[7] C. Gräbnitz, "An extended analysis of the correlation extraction in linear cryptanalysis," *Cryptography*, vol. 6, no. 4, p. 43, 2024.

[8] W. Liu and J. Zhang, "Integral cryptanalysis of reduced-round aes," *Journal of Cryptographic Engineering*, vol. 12, pp. 311–324, 2022.

[9] K. Patel and N. Shah, "A comprehensive survey on cryptanalysis techniques of aes algorithm," *Journal of Information Security and Applications*, vol. 71, p. 103200, 2023.

[10] M. Karami and S. Hosseinzadeh, "Differential cryptanalysis and security evaluation of aes variants," *Journal of Information Security and Applications*, vol. 68, p. 103139, 2023.

[11] L. Zhang and Y. Chen, "Security analysis of full-round aes against differential cryptanalysis," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1450–1462, 2023.

[12] R. Singh and A. Kumar, "Evaluating resistance of aes against linear cryptanalysis: An empirical study," *IEEE Access*, vol. 11, pp. 12 345–12 358, 2023.

[13] B. Sarkar, A. Saha, D. Dutta, G. De Sarkar, and K. Karmakar, "A survey on the advanced encryption standard (aes): A pillar of modern cryptography," *International Journal of Computer Science and Mobile Computing*, vol. 13, no. 4, pp. 68–87, Apr. 2024, zAIN Publications.

[14] "Integral cryptanalysis," https://en.wikipedia.org/wiki/Integral_cryptanalysis, 2025, accessed July 2025.

[15] K. Qiao, J. Cheng, and C. Ou, "A new mixture differential cryptanalysis on round-reduced aes," *Mathematics*, vol. 10, no. 24, p. 4736, 2022.

[16] D. Pal, V. P. Chandratreya, A. Das, and D. R. Chowdhury, "Modeling linear and non-linear layers: An milp approach towards finding differential and impossible differential propagations," *arXiv preprint arXiv:2405.00441*, 2024.

[17] W. A. Bari and R. A. Lone, "Brute force attack: A threat to modern cryptographic algorithms," *International Journal of Computer Applications*, vol. 185, no. 46, pp. 1–6, 2023.

[18] M. Rossi, "Automatic differential cryptanalysis of symmetric ciphers," 2024.

[19] X. Yang, C. Li, and R. Wang, "Analysis of aes resistance against linear cryptanalysis using s-box and diffusion structure," *Journal of Information Security and Applications*, vol. 70, p. 103189, 2023.

[20] Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," *Future Generation Computer Systems*, 2024.

[21] S. Faust, J. Krämer, M. Orlt, and P. Struck, "On the related-key attack security of authenticated encryption schemes," in *International Conference on Security and Cryptography for Networks*. Springer, 2022, pp. 362–386.

[22] P. Kocher, J. Jaffe, and B. Jun, "Side-channel attacks: A review of leakage sources and countermeasures," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3201–3215, 2023.

[23] G. Dupré, "Energy efficiency in aes encryption on arm cortex cpus: Comparative analysis across modes of operation, data sizes, and key lengths," 2024.

[24] B. Sarkar, A. Saha, D. Dutta, G. De Sarkar, and K. Karmakar, "A survey on the advanced encryption standard (aes): A pillar of modern cryptography," 2024.

[25] "Confusion and diffusion," https://en.wikipedia.org/wiki/Confusion_and_diffusion, 2025, accessed July 2025.

[26] I. Dinur and A. Shamir, "Biclique cryptanalysis: Advances and applications on block ciphers," *IEEE Transactions on Information Theory*, vol. 69, no. 2, pp. 1067–1083, 2023.

[27] N. T. Courtois and J. Pieprzyk, "Algebraic cryptanalysis: Theory and applications to modern block ciphers," *Journal of Cryptology*, vol. 36, pp. 1007–1034, 2023.

[28] X. Dong, "Meet-in-the-middle attacks on aes with value constraints," *Designs, Codes and Cryptography*, vol. 92, no. 4, pp. 877–892, 2024.

[29] A. Singh, K. B. Sivangi, and A. N. Tentu, "Machine learning and cryptanalysis: An in-depth exploration of current practices and future potential," *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 257–272, 2024.

*DOI: https://doi.org/10.54216/FPA.210211*

*Received: April 15, 2025 Revised: June 26, 2025 Accepted: August 28, 2025*