WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Closing the Gap: Comparative Analysis of Deep Learning with Traditional Techniques Used in Differential Cryptanalysis of AES

***Rajat Chandel[1], Chhavi[2], Lakshay Mukheria [3]***

Maharaja Agrasen Institute of Technology Delhi-110062, India
chandelrajat003@gmail.com, chhavitomar711@gmail.com, lakshaymukheria35@gmail.com

**ABSTRACT—**

Differential cryptanalysis is still a basic method for estimating the security of block ciphers. Classical algebraic approaches have been successful in cryptanalyzing up to 7 rounds of AES, while the recent breakthroughs in deep learning have the promise to be effective as powerful tools to identify complex differential patterns, but up to only 2-3 rounds. This paper surveys the current state of differential cryptanalysis against AES, compares the advantage and disadvantage of the classical algebraic and recent deep learning methods, and points out significant research gaps. We explain the reason behind the limitation of deep learning beyond 3 rounds and point out directions of future work towards making it useful for deeper rounds of AES.

***Index Terms***—Differential Cryptanalysis, AES, Deep Learning, Cryptanalysis, Block Ciphers, Convolutional Neural Networks, Machine Learning, Hybrid Models.

## Background

The Advanced Encryption Standard (AES) is one of the most widely used encryption standards globally, known for its strong resistance against most known cryptanalytic attacks [3], [4]. One of the most powerful attack methods on block ciphers is differential cryptanalysis, which explores how differences in plaintexts influence differences in ciphertexts through the encryption rounds. Over the years, several advances have been made in differential cryptanalysis to analyze the security of AES, especially for reduced rounds. While classical algebraic methods have been effective in analyzing up to 7 rounds of AES, recent studies have highlighted the potential of deep learning methods to find differential patterns for AES encryption. However, the application of deep learning methods has shown promising results only for up to 3 rounds. This paper aims to compare the efficacy of both classical algebraic techniques and deep learning methods in AES cryptanalysis and discuss the significant challenges faced by deep learning approaches in attacking deeper rounds.

## Classical Algebraic Differential Cryptanalysis

Classical algebraic differential cryptanalysis techniques have been extensively used in cryptanalysis to investigate how differences propagate through the encryption rounds of AES. A notable approach was introduced by Phan [1], who proposed an impossible differential cryptanalysis attack that was able to break up to 7 rounds of AES-192 and AES-256. However, this method requires the use of specific impossible differential paths, which are computationally expensive and infeasible for real-world applications due to the massive computational resources required, such as $2^{186}$ encryptions. Zhang et al. [2] extended this attack and demonstrated that it could also be applied to AES-128 for up to 7 rounds. Although successful in breaking several rounds, these methods still face limitations due to the high computational complexity involved in finding impossible differential paths and analyzing key scheduling vulnerabilities.

Despite these challenges, classical algebraic methods pro- vide a systematic approach to attack deep rounds of AES. These methods, being based on well-understood algebraic structures, offer a reliable mechanism for cryptanalysis, al- though they are heavily dependent on the availability of large amounts of plaintext-ciphertext pairs and require significant computational resources.

## Deep Learning-Based Differential Cryptanalysis

In recent years, deep learning techniques have emerged as a promising alternative to traditional algebraic cryptanalysis methods. Several studies [6], [7] have explored the applica- tion of convolutional neural networks (CNNs) for differential cryptanalysis of AES, with remarkable results in distinguishing differences between ciphertext pairs for reduced rounds. These studies have shown that CNNs can automatically extract fea- tures from pairs of ciphertexts with known input differences, allowing them to achieve high accuracy for up to 2 or 3 rounds of AES.

One notable approach is the use of CNNs for output prediction attacks, where the network learns to differentiate between ciphertext pairs with certain input differences. These deep learning models are able to predict the output with nearly 100% accuracy for up to 3 rounds. However, these techniques encounter significant difficulties when attempting to generalize beyond 3 rounds. The primary reason for this limitation is that AES behaves almost randomly after 3-4 rounds, making it difficult for deep learning models to discern any meaningful patterns.

Moreover, as the number of rounds increases, the differential probability decreases exponentially, which further complicates the training process. The growing noise in the data results in the model struggling to differentiate between actual patterns and random noise. Consequently, deep learning techniques, while promising, have not yet shown the capability to break deeper rounds of AES, such as 7 rounds or more.

## Analysis of the Research Gap

The disparity between classical algebraic methods and deep learning-based approaches can be attributed to several key challenges in applying deep learning to AES cryptanalysis:

### *A. Increased Randomness*

AES approaches ideal random behavior as the number of rounds increases. After 3-4 rounds, the cipher becomes highly resistant to differential cryptanalysis as the differences in plaintext pairs have little effect on the ciphertext. The increased randomness in the cipher's behavior eliminates any distinguishable differential patterns, making it increasingly dif- ficult for deep learning models to find meaningful correlations.

### *B. Low Differential Probability*

The differential probability of AES decreases significantly as more rounds are added to the cipher. This reduction makes it increasingly difficult for deep learning models to extract any useful features from the data. As the differential probability becomes lower, the models are more likely to encounter noise in the training data, leading to poor generalization performance.

### *C. Insufficient Feature Acquisition*

Deep learning models, particularly CNNs, excel at automat- ically learning features from data. However, the complexity of AES's round transformations, including key expansion, substitution, and permutation, leads to highly nonlinear re- lationships between the plaintext and ciphertext. Standard deep learning models may struggle to capture these complex algebraic relationships, especially as the number of rounds increases.

### *D. Training Complexity*

Training deep learning models for differential cryptanalysis requires large amounts of data and substantial computational resources. For deep rounds of AES, the data complexity increases exponentially, and deeper models with more layers are needed to capture the intricate patterns. However, training deeper models can lead to overfitting or failure to converge, further limiting the effectiveness of deep learning in attacking deeper rounds of AES.

## Potential Solutions to Extend Deep Learning to More Rounds

To address the limitations of deep learning for attacking deeper rounds of AES, several strategies could be explored:

***Classical Differential Integration***

A promising approach is to combine classical algebraic differential cryptanalysis with deep learning techniques. For instance, high-probability differential paths could be used for the initial rounds, while deep learning models could be employed for the subsequent rounds. This hybrid approach could leverage the strengths of both methods, providing a more efficient attack strategy.

### *A. Hybrid Learning Models*

Another approach is to integrate algebraic information, such as properties of the MixColumns transformation, directly into the deep learning architecture. By embedding such algebraic information into the model, it may be possible to help the network capture complex relationships in the later rounds of AES, allowing it to generalize to deeper rounds.

### *B. Advanced Architectures*

Recent advances in deep learning architectures, such as Transformer models [**?**], could potentially improve the perfor- mance of differential cryptanalysis. Transformer models, with their ability to model long-range dependencies, may be better suited to capturing the complex interactions between rounds in AES. Additionally, deeper CNNs with attention mechanisms could help the model focus on the most relevant parts of the input, improving the performance of deep learning attacks on AES.

### *C. Curriculum Training*

Training deep learning models in a sequential manner, starting from 1-round distinguishers and gradually increasing the number of rounds, could help the model build a hierarchi- cal understanding of AES encryption. This curriculum-based approach could allow the model to progressively learn the more complex relationships between plaintext and ciphertext as the number of rounds increases.

### *D. Structured Training Data*

Another avenue for improving the performance of deep learning in AES cryptanalysis is to use structured training data. Instead of relying on completely random plaintext pairs, the training data could be generated from known structured variations in plaintexts. This approach could help the model focus on the most relevant features and reduce the noise in the data.

## Comparative Analysis: Traditional vs. Deep Learning Techniques

### *Future Research Directions*

Given the challenges faced by deep learning methods in attacking deeper rounds of AES, several research directions can help bridge the gap:

- Launch deep learning-based attacks on AES-192 and AES-256 to explore their potential for higher-round at- tacks.

| Dimension | Classical Algebraic Methods | Deep Learning Methods |
|---|---|---|
| **Methodology** | Manually crafted differentials and algebraic reasoning | Automated feature extraction from datasets |
| **Rounds Attacked** | Up to 7 rounds (AES-192/256) (Phan, 2004; Zhang et al., 2007) | Up to 3 rounds (Deep Learning AES Works, 2021–2024) |
| **Data Complexity** | Very high (e.g., 2^92 plaintexts) | Moderate for early rounds |
| **Computational Resources** | Extremely high (memory, computation) | High during training, moderate during inference |
| **Extensibility** | Systematic but complex | Very difficult beyond 3 rounds |
| **Expertise Required** | High cryptographic expertise | High machine learning expertise |

**Fig. 1. Comparative Analysis of Traditional and Deep Learning Techniques**

- Investigate side-channel-aided deep learning attacks by exploiting intermediate encryption states and partial in- formation from the encryption process.
- Develop cryptanalysis-oriented neural architectures that are sensitive to finite field operations, which are crucial in AES encryption.
- Explore transfer learning methods, leveraging knowledge from small block ciphers to improve the performance of deep learning models for AES.

## Conclusion

In this paper, we compared classical algebraic methods with deep learning techniques in the context of AES cryptanalysis. While traditional algebraic methods have been successful in analyzing up to 7 rounds, deep learning approaches are still limited to 2-3 rounds due to the increasing randomness and complexity of AES after several rounds. To overcome these limitations, hybrid approaches and advanced architectures may hold the key to extending deep learning methods to deeper rounds of AES, offering new opportunities for cryptanalysis in the future.

**REFERENCES**


1. Raphael C.-W. Phan, ”Impossible Differential Cryptanalysis of 7-round Advanced Encryption Standard (AES)”, Information Processing Letters, vol. 91, pp. 33–38, 2004.
2. Wentao Zhang, Wenling Wu, Dengguo Feng, ”New Results on Impossible Differential Cryptanalysis of Reduced AES”, ICISC 2007, LNCS 4817, Springer, 2007.
3. Joan Daemen and Vincent Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer, 2002.
4. Vincent Rijmen and Joan Daemen, ”The Advanced Encryption Standard (AES)”, Dr. Dobb’s Journal, 2001.
5. William Stallings, Cryptography and Network Security: Principles and Practice, 4th Edition, Prentice Hall, 2005.
6. Zhang et al., ”Output Prediction Attacks on Block Ciphers Using Deep Learning,” Collected Research, 2021-2024.
7. Various Authors, Cryptanalysis Papers on AES Based on Deep Learning, gathered from AES Related Work papers (2021–2024).
8. Jean-Philippe Joux, ”The Mathematics of Cryptography,” Handbook of Applied Cryptography, CRC Press, 2004.
9. Li, Y., Zhang, H., and Wang, Y., ”Deep Learning-based Cryptanalysis of Block Ciphers: A Survey,” Cryptography, vol. 6, pp. 85-102, 2021.
    a. Kim, S., ”Differential Cryptanalysis of AES Using Machine Learning,” Journal of Cryptology, vol. 33, pp. 476-497, 2020.
    b. Choi, W., Park, K., and Kim, H., ”Differential Cryptanalysis of AES with Deep Learning,” In Proc. of AsiaCrypt, Springer, 2019.
10. Liu, H., Chen, Y., and Hu, Y., ”Efficient Deep Learning for Cryptanalysis of AES with Reduced Rounds,” IEEE Transactions on Information Forensics and Security, vol. 13, pp. 1016-1029, 2018.
11. Chang, W., ”Neural Network-Based Cryptanalysis of Reduced AES Rounds,” In Proc. of Cryptography and Network Security, 2018.
    a.