Цзян Сюе
PhD candidate
1.Bengbu University, Bengbu City, Anhui Province, China
2.National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID 0009-0000-1676-2331
jx1283@163.com
Lakhno Valerii
Doctor of Technical Sciences, Professor, Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID 0000-0001-9695-4543
lva964@nubip.edu.ua

SURVEY ON THE EVOLUTION AND KEY TECHNOLOGIES OF DIFFERENTIAL DISTINGUISHER DESIGN

Abstract. The differential distinguisher is pivotal in differential cryptanalysis, distinguishing authentic from random differential distributions. This paper surveys its evolutionary trajectory and key technologies, covering the paradigm shift from traditional manual-driven to neural network-aided methods. Traditional distinguishers rely on Differential Distribution Tables and manual high-probability paths, offering strong interpretability but poor efficiency and adaptability to complex ciphers like Speck and Simon. Neural network-aided designs innovate in input feature engineering and network architectures. The paper identifies challenges including poor cross-cipher generalisation and insufficient interpretability, proposing future directions like adaptive design and lightweight optimisation. It serves as a comprehensive reference for lightweight cipher security analysis.

Keywords: differential distinguisher; cryptanalysis; Neural network; Lightweight ciphers

1 INTRODUCTION

The differential distinguisher is a core component of differential cryptanalysis, whose primary function is to distinguish between the "authentic differential distribution" (generated by encrypting plaintext pairs with fixed differences) and "random differential distribution" (generated by encrypting random plaintext pairs) output by cryptographic algorithms, providing a critical basis for subsequent key recovery attacks [1]. Since Biham and Shamir proposed DES cryptanalysis based on differential distinguishers in 1991 [1], the design of differential distinguishers has undergone a paradigm shift from "traditional manual-driven" to "neural network-aided": traditional methods rely on manual exploration of high-probability differential paths, which are inefficient and struggle to handle high-round or complex-structure ciphers (e.g., lightweight block ciphers Speck and Simon); in 2019, Gohr introduced Deep Residual Networks (ResNet) into differential distinguisher design for the first time [3], breaking through traditional limitations and paving the way for a new direction in neural network-aided cryptanalysis. Focusing on the core design of differential distinguishers, this paper systematically organises their evolutionary context, key technologies, performance characteristics, and future challenges, providing a reference for the security analysis of lightweight ciphers.

2 EVOLUTION OF DIFFERENTIAL DISTINGUISHER DESIGN

2.1 Traditional differential distinguishers: based on DDT and high-probability paths

The core of traditional differential distinguisher design lies in the Differential Distribution Table (DDT) and high-probability differential paths. The DDT quantifies the probability that an input difference is transformed into an output difference via the cipher's round function, serving as a fundamental tool for distinguishing between authentic and random distributions [1]. The steps to construct an effective distinguisher are as follows:

Traditional design offers advantages of intuitive logic and strong interpretability, but suffers from significant limitations: first, it relies on manual experience to explore high-probability paths, leading to poor adaptability to complex ARX (Addition-Rotation-XOR) structures (e.g., Speck's modular addition + rotation + XOR); second, differential probability decays exponentially with increasing rounds, resulting in a sharp decline in discrimination performance (e.g., the accuracy of traditional distinguishers for 7-round Speck32/64 is less than 60% [3]); third, it has high data complexity, requiring a large number of plaintext-ciphertext pairs to verify differential paths.

2.2 Neural Network-Aided Differential Distinguishers: Design Innovation Driven by Features and Data

The introduction of neural networks has restructured the design logic of differential distinguishers—shifting from "manual path-finding" to "model-based feature learning". Core improvements focus on input feature design and network architecture adaptation, with specific evolutionary paths as follows:

2.2.1 Input feature design: from single-dimension to multi-dimension enhancement

Input features serve as the "information source" for neural network distinguishers, and their design directly determines feature utilisation and discrimination performance. Mainstream designs include:

Single Ciphertext Pair (SCP) Design [3]: A foundational paradigm proposed by Gohr, which takes raw bits of a single ciphertext pair as input. It first verified the effectiveness of neural networks on Speck32/64 (92.9% accuracy for 5 rounds). However, it only utilises surface-level bit information, leading to a drop in accuracy to 61.6% for high rounds (7 rounds).

Multiple Ciphertext Pairs (MCP) Design [4]: By concatenating k ciphertext pairs into a single sample, it leverages inter-sample derived features (e.g., differential statistical correlation) to enhance discriminability. For 5-round Speck32/64, accuracy reaches 99.99%, and for 7 rounds, it increases to 64.93%. Meanwhile, it reduces data complexity by 30% through a data reuse strategy.

Multi-Round Differential (MRMSD) Design [6]: Integrating the multi-round differential characteristics of Markov ciphers, it introduces differential information from the penultimate round via partial decryption with random pseudo-round keys, and converts ciphertext pairs into differential form. This design strengthens cryptographically core features, achieving 94.11% accuracy for 7-round Speck32/64 and enabling effective discrimination of 12-round Simon48/96 for the first time (61.59% accuracy).

Masked Output Distribution Table (M-ODT) Design [5]: To address the "black-box" issue, it compresses the DDT via masking, mapping input features to explicit differential probabilities. While maintaining performance (92.3% accuracy for 5-round Speck32/64), it reveals key differential bits relied on by the model, achieving a breakthrough in interpretability.

Random Key Multi-Cipher Pairs (RKMP) Design [7]: It introduces random keys for additional encryption of ciphertext pairs, enhancing feature diversity and improving generalisation. For 7-round Speck32/64, accuracy reaches 92.03%, and it enables effective discrimination of 8 rounds for the first time (63.32% accuracy), adapting to the needs of high-round cryptanalysis.

2.2.2 Network architecture adaptation: from ResNet to attention enhancement

Neural network architectures must match input features to maximise performance: ResNet mitigates the vanishing gradient problem via residual connections, adapting to deep feature extraction for multi-round differences [3]; 2D-CNN utilises local convolution kernels

to capture correlations between multiple ciphertext pairs [4]; attention mechanisms focus on key features and suppress noise introduced by random keys in RKMP [7]. For example, ResNet integrated with attention mechanisms enables RKMP to achieve 99.5% accuracy for 9-round Simon32/64, an improvement of 0.4% compared to MRMSD [7].

3 KEY DESIGN ELEMENTS AND PERFORMANCE COMPARISON

3.1 Core design elements

The design of differential distinguishers must balance three core objectives: feature effectiveness , data efficiency, and interpretability. Table 1 compares the core features and performance of mainstream designs:

Table 1

Performance indicators for various cryptanalytic designs

Design Type	Core Features	5-Round Speck32/64 Accuracy	7-Round Speck32/64 Accuracy	Maximum Supported Rounds (Simon32/64)
Traditional DDT-based	Single-round high-probability paths	~85%	~55%	6 rounds
SCP [3]	Raw bits of single ciphertext pair	92.9%	61.6%	8 rounds
MCP [4]	Concatenation of multiple ciphertext pairs	99.99%	64.93%	9 rounds
MRMSD [6]	Multi-round differences + differential form	-	94.11%	11 rounds
RKMP [7]	Random keys + attention mechanism	-	92.03%	9 rounds (99.5% accuracy)

3.2 Key performance conclusions

Expanding feature dimensions significantly improves performance: Multi-round differential (MRMSD) design increases accuracy by 32.5% for 7-round Speck32/64 compared to single-round feature (SCP) design;

Differential form outperforms raw bits: MRMSD improves accuracy by 29.18% for 7-round Speck32/64 compared to MCP;

Interpretability and performance can be balanced: While maintaining accuracy comparable to SCP, M-ODT reveals key differential bits, providing a theoretical basis for cryptanalysis [5].

4 CONCLUSIONS

The design of differential distinguishers has shifted from traditional manual-driven to neural network-aided feature and data-driven approaches. The core evolutionary logic is to "expand feature dimensions, improve data efficiency, and balance performance with interpretability". Designs such as MRMSD and RKMP have broken through the discrimination bottleneck for high-round ciphers, while M-ODT provides a new approach to interpretability. Future research should focus on cross-cipher generalisation, lightweight design, and interpretability, enabling differential distinguishers to play a greater role in the security verification of lightweight ciphers and providing stronger support for cryptographic security in scenarios such as the Internet of Things and embedded systems.

REFERENCES

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[2] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Workshop on the Theory and Application of Cryptographic Techniques - EUROCRYPT 1991*, 1991, pp. 17–38.

[3] A. Gohr, "Improving attacks on round-reduced Speck32/64 using deep learning," in *Advances in Cryptology - CRYPTO 2019*, 2019, pp. 150–179.

[4] Y. Chen, Y. Shen, H. Yu, and S. Yuan, "A new neural distinguisher considering features derived from multiple ciphertext pairs," *The Computer Journal*, vol. 66, no. 6, pp. 1419–1433, 2023.

[5] A. Benamira, D. Gerault, T. Peyrin, and Q. Q. Tan, "A deeper look at machine learning-based cryptanalysis," in *Advances in Cryptology - EUROCRYPT 2021*, 2021, pp. 805–835.

[6] J. S. Liu, J. J. Ren, S. Z. Chen, et al., "Improved neural distinguishers with multi-round and multi-splicing construction," J*ournal of Information Security and Applications*, vol. 74, pp. 103461, 2023.

[7] X. Jiang, M. Li, K. Makulov, et al., "Enhanced neural differential distinguisher for Speck32/64 using attention mechanisms and multi ciphertext inputs," *Informatica*, vol. 49, pp. 197–210, 2025.

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL UNIVERSITY OF LIFE AND ENVIRONMENTAL SCIENCES OF UKRAINE

FACULTY OF INFORMATION TECHNOLOGY

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

PROCEEDINGS

МАТЕРІАЛИ

XIII International scientific and practical conference

XIII Міжнародної науково-практичної конференції

GLOBAL AND REGIONAL PROBLEMS OF INFORMATIZATION IN SOCIETY AND NATURE USING '2025

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2025

13-14 November 2025

Kyiv, NULES of Ukraine

13-14 листопада 2025 року

Київ, НУБіП України

Kyiv 2025

Київ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XIII Міжнародної науково-практичної конференції

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2025

13-14 листопада 2025 року

Київ, НУБіП України

Київ 2025

УДК 004

Рекомендовано до друку вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 18.12.2025).

Укладач: д.т.н., доцент Шкарупило В.В.

Збірник матеріалів XIII Міжнародної науково-практичної конференції "Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2025", 13–14 листопада 2025 року, НУБіП України, Київ. – К.: НУБіП України, 2025. – 206 с.

Відповідальність за зміст публікацій несуть автори.