Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 12** : 1–10.
ISSN-0037-8712
doi:10.5269/bspm.82399

Design and Analysis of Neural Distinguisher for Differential Cryptanalysis of Lightweight Block Ciphers

Praveen Kumar U. M.[1] and Venkata Sundaranand Putcha[2]

ABSTRACT: The design and analysis of small, low-power electronics, with limited memory and processing power is a niche area of research because of its wide range of applications. It is necessary to secure these devices and Lightweight ciphers will provide security for these devices (IoT, sensors, RFID). This paper deals with the neural distinguishers of lightweight block ciphers. A neural distinguisher scheme based on ResNet, Transformer, and a hybrid ResNet–Transformer model architectures for the ciphertexts is designed and the efficiency is demonstrated by considering the outputs of four lightweight block ciphers PRESENT, HIGHT, PRINCE, and TWINE. The results are obtained in the round-reduced environment and will provide empirical insights for the full-fledged differential cryptanalysis.

Keywords: Cryptanalysis, light weight cipher, distinguisher, neural cryptanalysis, ResNet, transformer.

Contents

2020 *Mathematics Subject Classification:* 94A60, 68T07.
Submitted March 04, 2026. Published June 08, 2026.

1. Introduction

Lightweight block ciphers are fundamental to security techniques utilized in limited environments, including RFID systems, sensor networks, and embedded devices, where efficiency and security must be carefully balanced [34].. A key element of security measures used in restricted settings like RFID systems, sensor networks, and embedded devices are lightweight block ciphers. As a result, understanding their resilience to both traditional and emerging cryptanalytic approaches remains a key research question. Differential, linear, and integral cryptanalysis are traditional methods that have been very important for judging how safe these systems are over the previous few decades [2,3,5,6] and have also been applied to analyze stream and block cipher constructions through state transition and structural properties [31,32]. With the fast development in machine learning, especially in deep learning area, neural network have recently been studied as automatic methods for cryptanalysis. Early research show that deep neural networks are able to distinguish between round-reduced block ciphers and random version, even when the traditional attack are not very effective [15]. Later works improve the dataset construction, network architecture, and training method, showing that neural distinguisher can work as complement to classical cryptanalytic techniques [18,21,23]. Most of the existing research on neural cryptanalysis have focus on a limited number of cipher family, mainly ARX-based design such as SIMON and SPECK [15,20]as well as other ARX-oriented constructions studied under classical cryptanalytic frameworks [33]. While these study provide useful insight, the diversity of lightweight cipher scheme is not fully covered. In real application, lightweight ciphers include different structural paradigm, such as substitution–permutation networks (SPNs), Feistel networks, ARX construction, and involutive design. Each paradigm shows different diffusion and algebraic property, which can significantly affect the neural distinguishability [17,20]. This article present a comparative experimental analysis of neural differential distinguisher applied to four representative lightweight block cipher: PRESENT , HIGHT , TWINE and PRINCE . Instead of optimizing for best attack performance on a single target cipher, these ciphers are selected to represent different design philosophy. The analysis is conducted in a unified experimental setting, which allow direct comparison between cipher structure and neural architecture.We evaluate three neural model: a ResNet architecture inspired by residual learning [25], a Transformer model based on self-attention mechanism [26], and a hybrid ResNet–Transformer architecture that combine local feature extraction with global dependency modeling. The cryptanalytic task is defined as a binary classification problem, where the network distinguish ciphertext difference generated from structured plaintext pair versus random pair. This formulation follow the common practice in neural differential cryptanalysis [15,19,21]. One important challenge addressed in this study is related to involutive cipher like PRINCE. Simple dataset generation may lead to trivial distinguisher that do not reflect real learning behavior due to the symmetry of the structure. To solve this problem, the PRINCE experiments apply random input whitening, making sure that the neural model learn statistical pattern instead of deterministic feature. Similar issue regarding dataset bias and experiment validity have been pointed out in recent studies on neural cryptanalysis methodology [18,23]. This work present a comparative study of neural differential distinguisher applied to lightweight block cipher with different structural design. A unified experimental framework are used to evaluate ResNet-only, Transformer-only, and hybrid architecture under consistent dataset and training condition. Cipher-specific pair-generation equation are formally defined, and whitening is applied when it is required to avoid trivial distinguisher. Experimental result on reduced-round PRESENT, HIGHT, PRINCE, and TWINE highlight how the cipher structure influence neural distinguishability, as well as the practical limitation of deep learning based cryptanalysis. Section 2 presents the methodology and experimental setup, including cipher formulation, dataset construction, neural architectures, and training procedure. Section 3 reports the experimental results and comparative analysis across the considered lightweight block ciphers. Finally, Sections 4 to 6 discuss the results, highlight limitations, and conclude the paper.

2. Methodology and Experimental Setup

This section describes the cryptanalytic setting, dataset construction, and neural models used in the experiments. The objective is to establish a standardized and reproducible framework for assessing neural differential distinguishers across various lightweight block cipher architectures.

2.1. Problem Formulation

Let $E_K(\cdot)$ denote a block cipher encryption function under secret key K, with block size $n = 64$. In classical differential cryptanalysis, the attacker studies how a fixed plaintext difference propagates through the cipher. Given a plaintext pair $(P, P \oplus \Delta)$, the corresponding ciphertext difference is defined as

$$\Delta C = E_K(P) \oplus E_K(P \oplus \Delta), \tag{2.1}$$

where Δ is a fixed input difference. If the cipher behaves as a random permutation, the distribution of ΔC is expected to be uniform. Deviations from uniformity indicate non-random behavior and can be exploited as a distinguisher [2].

Following prior work on neural cryptanalysis, the distinguishing task is formulated as a supervised binary classification problem [15]. Given a ciphertext difference ΔC, the neural network predicts whether it originates from a structured plaintext pair with fixed input difference (positive class) or from two independently random plaintexts (negative class). The classifier outputs a probability estimate

$$f_\theta(\Delta C) \in [0, 1],$$

where θ denotes the model parameters.

2.1.1. HIGHT. The HIGHT operates on a 64-bit block, represented as eight 8-bit words. Let the internal state at round i be:

$$X_i^0 X_i^1 X_i^2 X_i^3 X_i^4 X_i^5 X_i^6 X_i^7$$

where each $X_i^j \in \{0, 1\}^8$.

Rotation operators

$$\lll\text{: left rotation,} \qquad \ggg\text{: right rotation}$$

Nonlinear functions

$$f_0(x) = (x \lll 1) \oplus (x \lll 2) \oplus (x \lll 7)$$

$$f_1(x) = (x \lll 3) \oplus (x \lll 4) \oplus (x \lll 6)$$

Round equations

For round i, the state update is defined as:

$$X_{i+1}^0 = X_i^1$$

$$X_{i+1}^1 = X_i^2$$

$$X_{i+1}^2 = X_i^3$$

$$X_{i+1}^3 = X_i^4 \oplus \left(f_0(X_i^5) + K_i^{(1)}\right)$$

$$X_{i+1}^4 = X_i^5$$

$$X_{i+1}^5 = X_i^6$$

$$X_{i+1}^6 = X_i^7$$

$$X_{i+1}^7 = X_i^0 \oplus \left(f_1(X_i^1) + K_i^{(0)}\right)$$

where $+$ denotes addition modulo 2^8, and $K_i^{(0)}, K_i^{(1)}$ are round subkeys.

2.1.2. PRESENT. The PRESENT is a 64-bit substitution–permutation network (SPN). Let the internal state at round i be:

$$S_i \in \{0,1\}^{64}.$$

Round function

Each round consists of three steps:

Add Round Key

$$S_i' = S_i \oplus K_i$$

Substitution Layer

$$S_i'' = \|_{j=0}^{15} \text{SBox}\,(S_i'[4j+3:4j])$$

where each 4-bit nibble is substituted independently.

Permutation Layer

$$S_{i+1}[P(j)] = S_i''[j], \quad 0 \le j < 64$$

where $P(\cdot)$ is a fixed bit permutation.

2.1.3. PRINCE. The PRINCE operates on a 64-bit state and follows an involutive design. Let the state at round i be:

$$X_i \in \{0,1\}^{64}.$$

Whitening

$$X_0 = P \oplus K_0$$

Round function

For round i:

$$X_{i+1} = M\,(S(X_i \oplus RC_i)) \oplus K_1$$

where $S(\cdot)$ is a 4-bit S-box layer, $M(\cdot)$ is a linear diffusion layer, RC_i is the round constant, and K_0, K_1 are whitening keys.

2.1.4. TWINE. The TWINE is a 64-bit Feistel cipher operating on 4-bit nibbles. Let the state at round i be:

$$(L_i^0, R_i^0, L_i^1, R_i^1, \ldots, L_i^7, R_i^7)$$

where each element is a 4-bit value.

Round function

For each nibble pair j:

$$L_{i+1}^j = R_i^j$$

$$R_{i+1}^j = L_i^j \oplus S(R_i^j) \oplus K_i^j$$

After substitution, a fixed permutation π is applied:

$$X_{i+1} = \pi(X_{i+1})$$

where $S(\cdot)$ is a 4-bit S-box and K_i^j is the round subkey.

2.2. Dataset Construction

For each cipher and round configuration, a balanced dataset is generated. Each sample consists of a 64-bit ciphertext difference represented as a binary vector. Positive samples are constructed using plaintext pairs with a fixed input difference Δ, while negative samples are generated from independent random plaintexts. The dataset is defined as

$$\mathcal{D} = \{(\Delta C_i, y_i) \mid y_i \in \{0,1\}\},$$

where $y_i = 1$ and $y_i = 0$ denote a structured pair and a random pair respectively. By considering equal number of positive and negative samples in each experiment class imbalance is countered. The data is randomly divided into training and testing subsets in a 70/30 split. For involutive ciphers such as

PRINCE, simplistic dataset construction may lead to trivial distinguishers because of inherent structural symmetry. To address this issue, random input whitening is implemented. Specifically, a randomly generated mask W is XORed with both plaintexts prior to encryption:

$$\Delta C = E_K(P \oplus W) \oplus E_K((P \oplus \Delta) \oplus W).$$

This process avoids the deterministic leakage brought on by involution while maintaining the differential structure. Recent evaluations of neural distinguishers have brought up similar issues with dataset bias [18, 23].

Table 1: Dataset Parameters

Parameter	Description / Value
Cipher block size	64 bits
Input representation	Binary vector of ciphertext difference
Feature dimension	64 (one bit per position)
Dataset type	Supervised binary classification
Total samples	$2 \times N$ (balanced)
Positive samples	$(\Delta C = E_K(P) \oplus E_K(P \oplus \Delta))$
Negative samples	$(\Delta C = E_K(P_1) \oplus E_K(P_2))$
Output labels	$(y = 1)$ structured, $(y = 0)$ random
Class balance	50% positive, 50% negative
Dataset size per experiment	20,000 plaintext pairs
Train / Test split	70% / 30%

2.3. Neural Network Architectures

In this study, three neural architectures are evaluated, a ResNet model, a Transformer model, and a hybrid ResNet Transformer design. To ensure the comparison is fair, all the models use the same binary input representation and are trained in the same manner. The ResNet model use stacked one-dimensional convolutional layer with residual connection, which allow effective extraction of local bit-level pattern. Residual learning has shown to improve the training stability and performance of deep network [25]. The Transformer model replace convolutional operation with self-attention mechanism, allowing the network to capture long-range dependencies across different bit position [26]. The hybrid architecture combine both method.

Table 2: Neural Network Architecture Comparison

Component	ResNet	Transformer	ResNet–Transformer
Input	64-bit difference	64-bit difference	64-bit difference
Input format	(1×64)	(64×1)	(1×64)
Initial layer	Conv1D	Linear embedding	Conv1D
Residual connections	Yes	No	Yes
Global dependency	No	Self-attention	Transformer encoder
Attention heads	—	4	4
Feed-forward dim	—	128	128
Output	Binary probability	Binary probability	Binary probability
Training objective	BCE	BCE	BCE

2.4. Training Procedure

All neural models are trained using binary cross-entropy loss,

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^{N} \left[y_i \log f_\theta(\Delta C_i) + (1 - y_i) \log(1 - f_\theta(\Delta C_i)) \right],$$

ResNet–Transformer Hybrid Architecture for Cryptographic Analysis

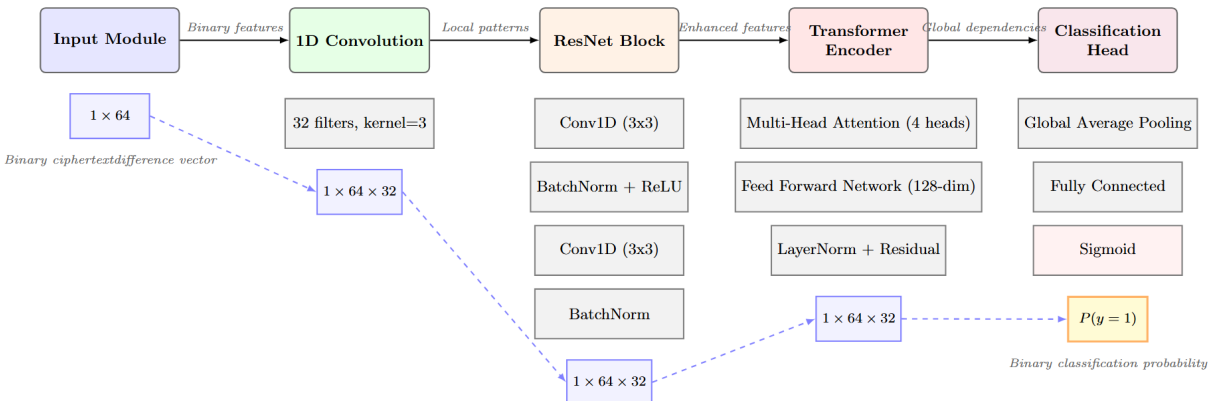

Figure 1: Overview of the proposed ResNet–Transformer hybrid network for binary cryptographic classification.

where N denote the batch size. The optimization is done using Adam optimizer with a fixed learning rate. The training is carried out for a fixed number of epochs, and the model performance is evaluated on the held-out test set after every few epochs. The main evaluation metric is the classification accuracy on the test set. An accuracy that is significantly higher than 0.5 indicates a successful distinguishing capability, while values close to 0.5 suggest a behavior that cannot be distinguished from a random permutation.

2.5. Experimental Scope and Assumptions

The experiments focus exclusively on round-reduced versions of the ciphers. Full-round analysis is not taken into account because neural distinguishers are mainly designed for exploratory assessment rather than direct key recovery. In addition, only fixed input differences are investigated, leaving adaptive or multi-difference techniques for future research. These limitations restrict the results' direct relevance to actual assault scenarios, but they do provide controlled comparison across cipher architecture.All experiments were conducted using fixed random seeds to ensure reproducibility.

3. Experimental Results

This section describes the experimental results of neural differential distinguishers applied to four lightweight block ciphers with varying round topologies. The evaluation looks at test accuracy, which is a way to see how well the neural network can tell the difference between cipher outputs and random permutations. All of the results were gotten using the same dataset construction method, training protocol, and evaluation factors that were discussed in Section 3.

3.1. Overall Performance Across Architectures

The main processing flow of the combination of ResNet-Transformer architecture is shown in Figure 1, and Table 2 lists the architectural elements of every model that was assessed. These architectures are evaluated in identical experimental conditions to enable a fair comparison. It is observed that neural model gives good distinguisher for the initial rounds and its ability decreases as the number of rounds increases. This is inline with the classical cryptanalysis where diffusion strengthen with every extra round. Among the three constructed architectures, the hybrid ResNet–Transformer model gives the highest test accuracy, specially for ARX and Feistel-based ciphers. This shows that combining convolutional feature extraction together with self-attention improves the accuracy. But the performance difference between the architectures is not same and depend more on the cipher structure.

3.2. Results on PRESENT

For PRESENT, which follow a substitution–permutation network design, the neural distinguishability decrease very fast when the number of rounds are increased. In lower rounds, both ResNet and Transformer model reach moderate accuracy, which indicate there is exploitable statistical pattern. As the rounds go higher, the distinguisher accuracy become close to random guessing baseline. For PRESENT, hybrid architecture could not bring a signficant improvement when compared to that of single-architecture. This behavior can be explained by the strong diffusion property of SPN design, where local patterns are quickly spread out. Because of this, neither local convolutional filter nor global attention mechanism can keep meaningful distinguishing information after small number of rounds.

Table 3: PRESENT Test Accuracy

Rounds	ResNet	Transformer	ResNet + Transformer
5	0.6936	0.6994	0.6967
6	0.5537	0.5604	0.5371
7	0.5046	0.5090	0.4965

3.3. Results on HIGHT

In contrast, HIGHT show higher distinguishability for more number of rounds. Both ResNet and Transformer models keep accuracy above random guessing for more rounds compared to PRESENT. From the below table 4 it follows that the hybrid model consistently achieve the best performance. This improvement establishes that ARX-based construction keep both local and long-range dependency that can be captured effectively by a neural model. Convolutional layers seems well suited for modeling modular addition and bitwise operation, while the Transformer part help by capturing interaction across distant bit position. These result highlight that ARX cipher give more favorable structure for neural distinguisher.

Table 4: HIGHT Test Accuracy

Rounds	ResNet	Transformer	ResNet + Transformer
9	0.7061	0.7188	0.8429
10	0.6366	0.6409	0.6295
11	0.5212	0.5227	0.5754

3.4. Results on PRINCE

For PRINCE, special care is needed because of its involutive structure. After applying random input whitening, the neural models shows gradual decrease in accuracy when the number of rounds increase. In lower rounds, the distinguishability stay relatively high, but the accuracy reduce steadily with more rounds. The ResNet and Transformer models show similar performance on PRINCE, with minute differences. The hybrid architecture do not give strong advantage in this case. This observation in tabe 5 suggest that global symmetry play dominant role in PRINCE, which limits the benefit of combining local and global feature extraction once trivial symmetry leakage is removed.

Table 5: PRINCE Test Accuracy

Rounds	ResNet	Transformer	ResNet + Transformer
6	0.8665	0.8718	0.8550
7	0.7722	0.7796	0.7384
8	0.6795	0.6898	0.6357
9	0.6250	0.6297	0.5767

3.5. Results on TWINE

TWINE show a different behavior compared to that of the other cipher. In lower rounds, all models reach very high accuracy, which indicate strong structural leakage. However, the change from high distinguishability to near-random behavior happen very suddenly as the number of rounds increase. The ResNet model perform especially well in low rounds, which may be due to the Feistel structure producing strong local correlation. In higher rounds, the performance of all architectures become close to random guessing. The hybrid model show limited advantage in this situation we can see table 6, reflecting the sharp diffusion transition that is inherent in TWINE design.

Table 6: TWINE Test Accuracy

Rounds	ResNet	Transformer	ResNet + Transformer
7	0.9912	0.9676	0.9898
8	0.7298	0.5913	0.7470
9	0.5069	0.5049	0.5017

3.6. Comparative Observations

From the experiments it follows that

- The cipher structure is the main factor that influences neural distinguishability.
- SPN design diffuse very fast, ARX design keep exploitable pattern for longer time, Feistel design show sudden transition, and involutive design require careful handling of dataset.
- The choice of architecture is primay, its effect is secondary compared to the structural property of the cipher.
- hybrid architectures are most useful when both local and global dependency exist together in the cipher structure (This explain their effectiveness on HIGHT and, to some extent, on TWINE in lower rounds)
- In cases where diffusion is too fast or too symmetric, increasing architectural complexity give diminishing return.

4. Discussion

The results show that the cipher structure have more influence on neural distinguishability than the selection of neural architecture. SPN-based PRESENT lose distinguishability very quickly when the number of rounds increase, which is consistent with its fast diffusion property. In this scenario, neither convolution-based nor attention-based model give a clear advantage. ARX-based HIGHT stay distinguishable for more number of rounds. The hybrid ResNet Transformer model perform well for HIGHT, since ARX construction keep both local and long-range dependencies that neural model can exploit. TWINE show different behavior, with very high distinguishability at low rounds followed by a sudden change to near-random behavior as diffusion become stronger. For PRINCE, input whitening is required to avoid trivial distinguisher caused by its involutive structure. After this mitigation, all architectures show gradual decrease in accuracy. Overall, hybrid model is most effective when cipher structure expose the complementary local and global pattern, but their advantage is limited when diffusion is too fast or too symmetric.

5. Limitations

This study is restricted to round-reduced cipher and considered only distinguishing attack. The full-round security and key recovery attack are not included in this study. The analysis depend on fixed input difference, which may not represent all possible cryptanalytic behavior. Furthermore, only limited number of neural architectures and training configurations are evaluated. While these limitation allow controlled comparison, they reduce the direct applicability to real-world attack scenario.

6. Conclusion

This paper investigates neural differential distinguisher for lightweight block cipher with different structural designs. In a unified experimental framework, SPN-, ARX-, Feistel-, and involutive-based cipher are evaluated using ResNet, Transformer, and hybrid architecture. The results show that the cipher structure have strong influence on neural distinguishability, often more important than the choice of architecture. PRESENT lose distinguishability very quickly, while HIGHT remain vulnerable for more rounds. TWINE show strong leakage in early rounds followed by fast transition to random behavior, and PRINCE need careful dataset handling because of involutive symmetry. The hybrid ResNet Transformer model give the most consistent performance across different cipher families, although its advantage depends on the presence of both local and global dependency. Overall, these finding confirm that neural cryptanalysis should be viewed as a complementary analysis tool for reduced-round evaluation. Future work will explore adaptive differential cryptanalysis with deeper neural model towards pragmatic cryptanalysis by key-recovery.

Acknowledgments

This work is supported by the RUSA project letter No. RUSA-ANURU/Research Project-02/Sanction Order/2024 dt:01-06-2024 and the authors would like to thank RUSA.

References

1. Shannon, C.E. A Mathematical Theory of Communication. Bell Syst. Tech. J. 27, 379–423 (1948). doi:10.1002/j.1538-7305.1948.tb01338.x
2. Biham, E.; Shamir, A. Differential Cryptanalysis of the Data Encryption Standard. Springer (1993).
3. Matsui, M. Linear Cryptanalysis Method for DES Cipher. EUROCRYPT'93, Springer (1993). doi:10.1007/3-540-48285-7_33
4. Daemen, J.; Knudsen, L.; Rijmen, V. The Block Cipher Square. FSE'97, Springer (1997). doi:10.1007/BFb0052343
5. Knudsen, L.; Wagner, D. Integral Cryptanalysis. FSE 2002, Springer (2002). doi:10.1007/3-540-45661-9_9
6. Lucks, S. The Saturation Attack – A Bait for Twofish. FSE 2001, Springer (2001). doi:10.1007/3-540-45473-X_1
7. Bogdanov, A. et al. PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007, Springer (2007). doi:10.1007/978-3-540-74735-2_31
8. Beaulieu, R. et al. The SIMON and SPECK Lightweight Block Ciphers. DAC 2015 (2015). https://eprint.iacr.org/2013/404
9. Leander, G. Small Scale Variants of the Block Cipher PRESENT. Cryptology ePrint Archive (2010). https://eprint.iacr.org/2010/143
10. Cho, J.Y. Linear Cryptanalysis of Reduced-Round PRESENT. CT-RSA 2010, Springer (2010). doi:10.1007/978-3-642-11925-5_21
11. Wang, M. Differential Cryptanalysis of Reduced-Round PRESENT. CANS 2008, Springer (2008). doi:10.1007/978-3-540-89641-8_6
12. Collard, B.; Standaert, F.-X. A Statistical Saturation Attack Against PRESENT. CT-RSA 2009, Springer (2009). doi:10.1007/978-3-642-00862-7_10
13. Wu, S.; Wang, M. Integral Attacks on Reduced-Round PRESENT. FSE 2013, Springer (2013). doi:10.1007/978-3-662-43933-3_10
14. Xiang, Z. et al. Applying MILP Method to Searching Integral Distinguishers. ASIACRYPT 2016, Springer (2016). doi:10.1007/978-3-662-53887-6_24
15. Gohr, A. Improving Attacks on Round-Reduced SPECK Using Deep Learning. CRYPTO 2019, Springer (2019). doi:10.1007/978-3-030-26948-7_22
16. Hou, B. et al. Linear Attack on Round-Reduced DES Using Deep Learning. ToSC 2020. doi:10.13154/tosc.v2020.i1.73-96
17. Tian, W.; Hu, B. Deep Learning Assisted Differential Cryptanalysis for SIMON. KSII Trans. Internet Inf. Syst. 15(2), 600–616 (2021). doi:10.3837/tiis.2021.02.003
18. Benamira, A. et al. A Deeper Look at Machine Learning-Based Cryptanalysis. EUROCRYPT 2021, Springer (2021). doi:10.1007/978-3-030-77870-5_7
19. Chen, Y.; Yu, H. A New Neural Distinguisher Model Considering Derived Features. IACR ePrint 2021/310. https://eprint.iacr.org/2021/310

20. Hou, Z.; Ren, J.; Chen, S. Improve Neural Distinguisher for Cryptanalysis. IACR ePrint 2021/1014. https://eprint.iacr.org/2021/1014

21. Bao, Z. et al. Enhancing Differential-Neural Cryptanalysis. ASIACRYPT 2022, Springer (2022). doi:10.1007/978-3-031-22966-4_4

22. Kim, H. et al. Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited. Entropy 25, 986 (2023). doi:10.3390/e25070986

23. Gohr, A.; Leander, G.; Neumann, P. An Assessment of Differential-Neural Distinguishers. IACR ePrint 2022/654. https://eprint.iacr.org/2022/654

24. Liu, J.S. et al. Improved Neural Distinguishers with Multi-Round Construction. J. Inform. Secur. Appl. 74, 103461 (2023). doi:10.1016/j.jisa.2023.103461

25. He, K. et al. Deep Residual Learning for Image Recognition. CVPR 2016, IEEE (2016). doi:10.1109/CVPR.2016.90

26. Raffel, C. et al. Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer. J. Mach. Learn. Res. 21, 1–67 (2020).

27. Chollet, F. Xception: Deep Learning with Depthwise Separable Convolutions. CVPR 2017. doi:10.1109/CVPR.2017.195

28. So, J. Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers. Secur. Commun. Netw. (2020). doi:10.1155/2020/8853740

29. Sikdar, S.; Kule, M. Recent Trends in Cryptanalysis Techniques: A Review. Springer (2022).

30. Xiao, Y.; Hao, Q.; Yao, D.D. Neural Cryptanalysis: Metrics, Methodology, and Applications. IEEE DSC (2019). doi:10.1109/DSC.2019.00058

31. Gundaram, P.K.; Naidu, T.A.; Guntupalli, N.; Yerukala, N. Design and Analysis of a New Stream Cipher Based on Ring FCSR Automaton. *International Journal of Computing and Digital Systems*, (2023).

32. Gundaram, P.K.; Naidu, T.A.; Allu, S.N. State Transition Analysis of GSM Encryption Algorithm A5/1. *Journal of Communications Software and Systems* **18**(1), 36–41 (2022).

33. Gundaram, P.K. Cryptanalysis of Selected ARX-Based Block Ciphers. *Cryptology ePrint Archive*, Report 2024/XXX (2024).

34. Naidu, T.A.; Gundaram, P.K. Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained Devices. *International Journal of Information Security and Privacy*, (2021).

Department of Mathematics, Rayalaseema University,
Kurnool, 518007, Andhra Pradesh, India.
E-mail address: [1]praveenumkumar5@gmail.com
E-mail address: [2]anand.putcha@yahoo.com