

DOI:10.3969/j.issn.1671-0673. 2026. 04. 007

一种融合多尺度卷积网络 and 自注意力结构的神经区分器

任文欢, 刘天源, 王林元, 陈 健, 闫 宾

(信息工程大学, 河南 郑州 450001)

摘要: 针对传统卷积结构的神经区分器对密文数据分类精度较低的问题, 提出一种融合卷积网络 and 自注意力结构的神经区分器。首先, 通过设计一种多尺度卷积网络, 以学习密文序列的局部特征; 其次, 在多尺度卷积网络后面引入自注意力机制, 用来增强神经区分器捕捉密文序列中长距离依赖的能力; 最后, 在多种密文数据集上训练该神经区分器。实验结果表明, 该神经区分器在 8 种密文数据集上的分类精度都超越了之前性能较优的神经区分器 SE-ResNet, 特别是在 13 轮的 SIMON64 上, 该神经区分器的分类精度比 SE-ResNet 提高了 3.92%, 证明了该神经区分器具有更加强大的密文特征提取能力。

关键词: 多尺度卷积网络; 自注意力机制; 神经区分器; 密文序列; 差分密码分析

中图分类号: TP183

文献标识码: A

文章编号: 1671-0673(2026)04-0430-06

A Neural Distinguisher Integrating Multi-Scale Convolutional Network and Self-Attention Structure

REN Wenhuan, LIU Tianyuan, WANG Linyuan, CHEN Jian, YAN Bin

(Information Engineering University, Zhengzhou 450001, China)

Abstract: To address the low classification accuracy of traditional convolutional neural distinguishers on ciphertext data, neural distinguisher based on convolutional network and self-attention structure is proposed. Firstly, a multi-scale convolutional network is designed to learn local features of ciphertext sequences. Secondly, the self-attention mechanism is introduced after the multi-scale convolutional network to enhance the ability of the neural distinguisher to capture long-range dependencies in ciphertext sequences. Finally, the neural distinguisher is trained on multiple ciphertext datasets. Experimental results show that the proposed neural distinguisher achieves higher classification accuracy than the previously superior neural distinguisher SE-ResNet on all eight ciphertext datasets. In particular, on 13-round SIMON64, the classification accuracy of the neural distinguisher is improved by 3.92% compared with that of SE-ResNet, demonstrating its more powerful ciphertext feature extraction capability.

Key words: multi-scale convolutional network; self-attention mechanism; neural distinguisher; ciphertext sequence; differential cryptanalysis

2019 年, 在差分密码分析^[1-2]领域, Gohr 针对 6 轮和 7 轮 SPECK32 设计了基于卷积网络的神经区

分器 (Neural Distinguisher, ND)^[3], Gohr 神经区分器的分类精度超过了传统的差分区分器。而且, 基

收稿日期: 2026-03-30; 修回日期: 2026-06-01

基金项目: 国家自然科学基金 (62271504)

作者简介: 任文欢 (1996—), 男, 硕士生, 主要研究方向为智能信息处理。E-mail: rwh1581@163.com

于神经区分器,Gohr在11轮和12轮SPECK32上成功实现了密钥恢复攻击。在差分密码分析领域,这是深度学习技术^[4-6]的首次应用。神经区分器通过学习输入的密文差分,来判断输入的差分是真实的差分还是随机数据,并给出分类结果。

后续学者们对Gohr的神经区分器进行了一系列改进。在Gohr区分器的基础上,Chen等^[7]使用多个密文对作为输入,这种改进的ND在SPECK32^[8]、PRESENT^[9]、DES^[10]、CHASKEY^[11]、SHA3-256^[12]上取得了更高的分类精度。2023年,Liu等^[13]使用深度可分离卷积^[14]改进了Gohr区分器中的标准卷积层。通过将标准卷积分解为逐点卷积和深度卷积,极大减少了神经区分器的参数量。同年,Yue等^[15]引入Inception模块改进了Gohr区分器中的残差结构,这种使用并行卷积网络的残差结构进一步提高了神经区分器在7轮SPECK32上的分类精度。2023年,Bellini等^[16]使用扩张卷积优化了Gohr区分器中的标准卷积层,从而得到了一种适用于多种密码的神经区分器DBitNet。此外,还改进了明文差分的搜索算法,并实现了明文差分搜索、密文数据集构建和神经区分器训练的自动化流程。2024年,Wang等^[17]使用SE-ResNet结构进一步改进了Gohr神经区分器中的残差结构,SE-ResNet通过在经典的残差网络中嵌入挤压-激励(Squeeze-and-Excitation, SE)模块,从而动态调整通道间的特征响应。2025年,Hou等^[18]提出了一种基于多尺度卷积网络和密集型残差连接的神经区分器,并且结合密文和密钥间的差异改进了密文数据集。但是传统卷积结构的神经区分器对密文序列中的微弱特征学习能力有限,这限制了神经区分器的分类精度。

为了更好地处理时间序列数据,Zhao等^[19]提出了一种多尺度卷积网络,它能够有效捕获时间序列的多尺度特征。Transformer^[20]结构同样在处理序列数据中表现优异,它是一种基于自注意力机制的神经网络。Transformer主要由编码器和解码器组成。其中,编码器网络在分类任务中应用广泛,它通过对输入序列进行编码来进行特征提取,然后通过位置编码为输入序列中的每个数据添加位置信息。每层编码网络通常包含一个多头自注意力机制和一个前馈神经网络,每个子层后面接有残差连接和层归一化。自注意力机制能够通过多头注意力有效捕捉全局依赖关系,并且能够并行地处理数据。受上述多尺度卷积网络和自注意力机制的启发,设计了一种融合多尺度卷积网络

和自注意力结构的神经区分器(A Neural Distinguisher Integrating Multi-scale Convolutional Network and Self-Attention Structure, ND-MCSA)。通过整合卷积网络和自注意力机制提高神经区分器对密文数据的分类精度。参考Gohr的神经区分器,设计一种多尺度卷积网络,以捕捉密文序列的局部特征。在多尺度卷积网络后面引入了自注意力机制,以增强神经区分器对密文序列中长距离依赖关系的学习能力。实验结果表明,ND-MCSA在SPECK32、SPECK64、SIMON128、SIMON32、SIMON64、SPECK128、LEA和XTEA这8种密文数据集上的分类精度均超越了之前性能较优的神经区分器SE-ResNet。其中,在13轮SIMON64上,ND-MCSA的分类精度比SE-ResNet提高了3.92%。

1 神经区分器设计方法

针对传统卷积结构的神经区分器对密文数据分类精度低的问题,提出了一种结合多尺度卷积网络和自注意力机制的神经区分器。首先,参考Gohr的神经区分器,设计了一种多尺度卷积网络,以学习密文序列的局部特征;其次,在多尺度卷积网络后面引入了自注意力机制,以增强神经区分器捕捉密文序列中长距离依赖的能力;最后,在不同的密文数据集上训练该神经区分器。

1.1 神经区分器ND-MCSA

多尺度卷积网络能够有效捕获序列数据在不同时间尺度下的空间特征^[19]。考虑到Gohr区分器的结构被广泛借鉴,首先以Gohr的神经区分器为参考设计了一种多尺度卷积网络,以捕捉不同时间尺度下的密文序列特征;然后,在多尺度卷积网络后面引入了自注意力机制,以提高神经区分器对密文序列长距离依赖关系的学习能力。该神经区分器如图1所示。神经区分器共包括7个部分:一个可以接受多密文对的输入层、变形层、多尺度卷积层、位置编码层、自注意力层、全局池化层、包含两个全连接层的输出层。为了更好地发挥区分器的性能,引用文献[7]的8组密文对输入。最后,在不同的密文数据集上训练该神经区分器。此外,该神经区分器所有网络层的正则化系数均为 10^{-5} ,网络训练的批量大小为1 000,训练轮数为30,学习率采用周期性学习率,在0.000 1~0.005之间按训练轮数周期变化,优化器为Adam,损失函数基于均方误差(Mean Squared Error, MSE)。

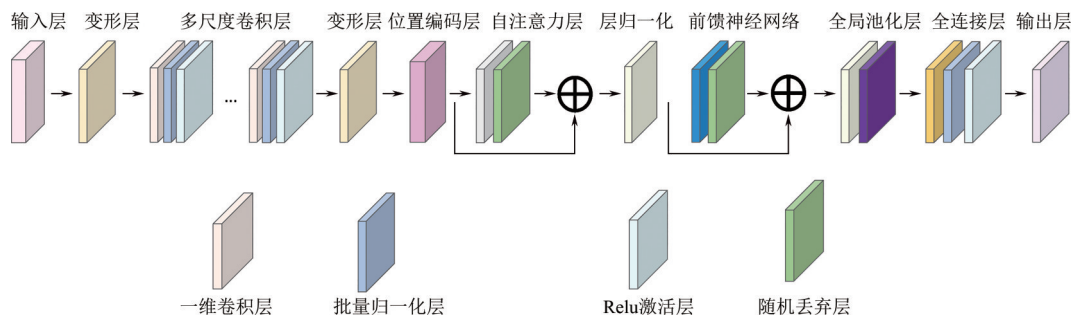


图1 神经区分器ND-MCSA的结构

1.1.1 多尺度卷积网络

以Gohr的神经区分器为参考,设计了多尺度卷积网络,如图2所示。该网络包括输入层、变形层和多尺度卷积层。

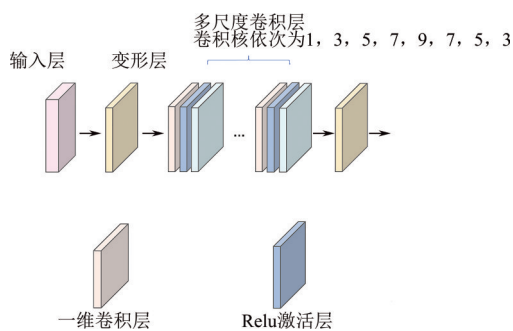


图2 多尺度卷积网络

对于SPECK32,密文长度为64的输入数据被变形为 4×16 ,其中4为通道数。多尺度卷积层由8个结构相同的一维卷积层堆叠构成,卷积核的大小分别为1、3、5、7、9、7、5、3,通道数均为120。此外,每个卷积层后均进行批量归一化(Batch Normalization, BN)层,并使用ReLU激活函数以提取不同感受野下的局部特征。

1.1.2 自注意力机制

多头注意力机制能够有效捕捉序列数据的全局依赖关系,并且能够并行处理数据^[20]。为了进一步提高神经区分器捕获差分序列中长距离依赖关系的能力,多尺度卷积网络后面引入了图3所示的自注意力机制。

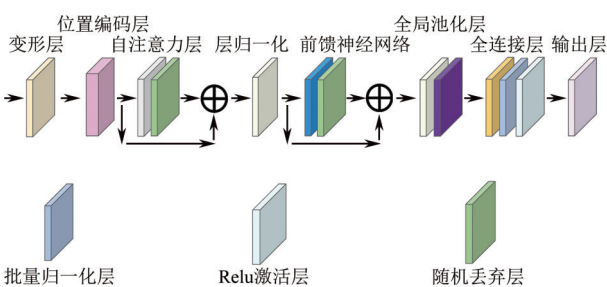


图3 自注意力机制

为了衔接位置编码层,首先对多尺度卷积层的输出进行变形处理。接下来是位置编码层,它能够添加序列数据的位置信息,确保后续的注意力机制能够感知特征的顺序关系。随后是注意力层,数据通过 Q (Query)、 K (Key)和 V (Value)这3个维度相同的权重矩阵生成注意力矩阵 O ,如式(1)所示:

$$O = \text{Attention}(Q, K, V) = \text{Softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (1)$$

式中, d_k 表示权重矩阵 K 的维度。

$$H_i = \text{Attention}(QW_i^Q, KW_i^K, VW_i^V) \quad (2)$$

$$\text{MultiHead}(Q, K, V) = (H_1 \parallel \dots \parallel H_h)W^O \quad (3)$$

式中: $i=1, 2, \dots, h$; h 是注意力头的数量。注意力头的输出 H_i 被拼接成一个长向量,然后与输出权重矩阵 W^O 相乘,得到最终的多头注意力输出^[20]。这一步融合了不同注意力头的信息,使模型能够捕捉密文序列中的多种依赖关系。 W^O 、 W_i^Q 、 W_i^K 和 W_i^V 是可训练参数,分别与 O 、 Q 、 K 和 V 相关联。

注意力层通过掩码确保每个位置仅能关注自身和前面的序列数据。接下来,注意力层的输出经过随机丢弃层(Random Dropout)随机丢弃部分神经元,以防止过拟合。然后,随机丢弃层的输出与位置编码层的输出进行残差连接,这有助于缓解深层网络中的梯度消失问题^[21]。残差网络的输出通过层归一化稳定激活值的分布。归一化后的数据进入前馈神经网络(Feedforward Neural Network, FFN),该网络由一个包含GELU激活函数的两层全连接层构成。全连接层能够对每个位置的特征表示进行非线性变换,从而增强模型的表达能力。前馈网络的输出同样经过随机丢弃层,并与前面层归一化部分的输出进行残差连接,并进行层归一化。最后,层归一化的输出通过全局平均池化和全连接层生成预测输出。其中,每个全连接层含有64个神经元,后面接有批量归一化和ReLU激活层。

从表3可以看出,8种密文数据集上,ND-MCSA的分类精度均高于DBitNet和SE-ResNet,说明ND-MCSA具有更强的差分特征提取能力。

此外,ND-MCSA在6轮、7轮和8轮SPECK32上的分类精度分别为0.9822、0.7880和0.5343。可视化结果分别展示在图4~图6中,从这3个图中可以看出,对于一种密码,加密轮数越高,神经区分器越难以将真实密文和随机数据分开,而且分类后两类数据的聚类中心距离越近。

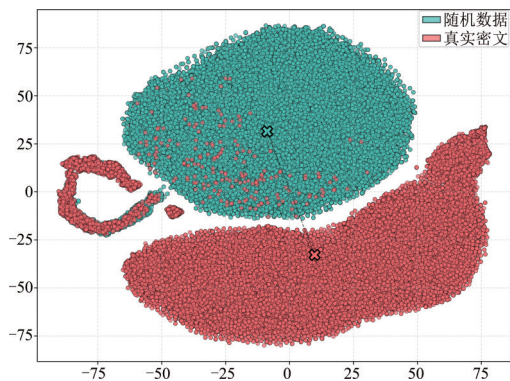


图4 ND-MCSA在6轮SPECK32上的分类可视化

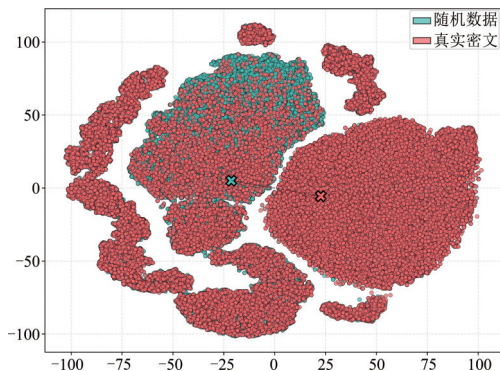


图5 ND-MCSA在7轮SPECK32上的分类可视化

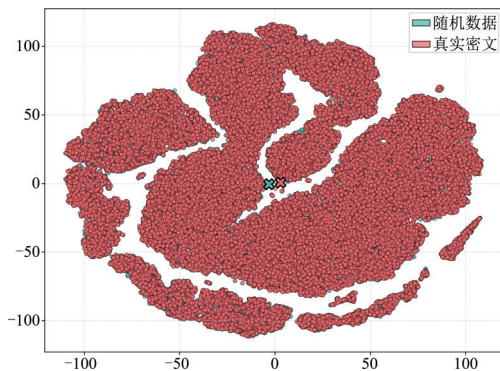


图6 ND-MCSA在8轮SPECK32上的分类可视化

2.2.2 在先验相同SPECK32上的实验

在先验相同的SPECK32上,为了测试ND-MCSA学习派生差分特征的能力,采用文献[7]的实验设置。明文差分 $\alpha=(0x0040,0)$,通过明文差分生成相同标签的 n 个密文对和随机密钥;对于Gohr

的神经区分器^[3],输入为 n 个单密文对,预测标签取 n 个输出的中位数;对于MCND^[7]和ND-MCSA,从 n 个密文对中抽样 m 个密文组作为输入,预测标签为 n 个输出结果的中位数;重复以上步骤 10^6 次。ND-MCSA、Gohr的神经区分器和MCND这3种神经区分器在先验相同SPECK32上的分类精度如表4所示, k 为输入密文对数。

表4 ND-MCSA、Gohr的神经区分器和MCND在先验相同的6轮SPECK32上的分类精度

密钥数量	$k=1$		$k=2$		$k=4$	
	Gohr	ND-MCSA	MCND	ND-MCSA	MCND	ND-MCSA
8	0.9573	0.9617	0.9767	0.9780	0.9823	0.9877
16	0.9860	0.9879	0.9918	0.9945	0.9867	0.9975
32	0.9978	0.9984	0.9991	0.9995	0.9980	0.9999

在6轮SPECK32上,当单个密文对由8个密钥产生时,相比Gohr的区分器和MCND,ND-MCSA取得了更高的分类精度。此外,ND-MCSA的分类精度都会随着输入密文对数的增加而增加。其中,当输入为4个密文对时,ND-MCSA取得了最高的分类精度0.9877。当单个密文对由16或者32个密钥产生时,ND-MCSA仍然能够取得最高的分类精度。而且随着输入密文对数的增加,ND-MCSA的精度会继续提高。当单个密文对由32个密钥产生,输入为4个密文对时,ND-MCSA取得了最高的分类精度0.9999。从表4的结果可以看出,在先验相同的6轮SPECK32上,在使用不同数量的输入密文对和密钥的情况下,ND-MCSA均表现出了最高的分类精度,说明了ND-MCSA具有强大的派生特征提取能力。

2.2.3 ND-MCSA在NASA中的数据复杂度

当汉明距离为2和1,输入密文对 k 分别为1、2和4时,在5轮和6轮的SPECK32上,ND-MCSA、Gohr的神经区分器和MCND在NASA中的数据复杂度如表5所示。

由表5可知,汉明距离为2时,在5轮SPECK32上,当输入单个密文对时,ND-MCSA的数据复杂度为14.203,Gohr为14.212。ND-MCSA随着输入密文对数的增加,数据复杂度会有所下降。其中,当输入4个密文对时,ND-MCSA取得了最低的复杂度10.499。此外,当输入密文对数为2时,ND-MCSA也取得了最低的数据复杂度。

在6轮的SPECK32上,当输入单个密文对时,ND-MCSA的数据复杂度为16.849,Gohr为16.911,

随着输入密文对数的增加,数据复杂度会有所下降;当输入密文对数为 2 和 4 时,ND-MCSA 也取得了最低的数据复杂度。由此可见,当汉明距离为 2 和 1 时,在特定的 5 轮和 6 轮 SPECK32 上,即使输入不同数量的密文对,ND-MCSA 都能够取得最低的数据复杂度。

表 5 汉明距离为 2 和 1 时,ND-MCSA、Gohr 的区分器和 MCND 在 NASA 中 SPECK32 上的数据复杂度

汉明距离	加密轮数	k=1		k=2		k=4	
		Gohr	ND-MCSA	MCND	ND-MCSA	MCND	ND-MCSA
2	5	14.212	14.203	13.165	12.591	12.901	10.499
2	6	16.911	16.849	15.821	15.421	14.764	13.537
1	5	14.720	14.719	13.979	13.275	14.187	11.491
1	6	17.456	17.367	16.484	16.026	15.606	14.225

3 结束语

针对传统卷积结构的神经区分器对密文数据分类精度较低的问题,设计了一种融合多尺度卷积网络和自注意力结构的神经区分器。首先,通过参考 Gohr 的神经区分器,设计一种多尺度卷积网络,以捕捉密文序列的局部特征;随后在多尺度卷积网络后面引入自注意力机制,以增强神经区分器对密文序列中长距离依赖关系的捕获能力。实验结果表明,在 8 种密文数据集上的分类精度超越了之前较优的神经区分器 SE-ResNet。其中,在 13 轮 SIMON64 上,ND-MCSA 的分类精度比 SE-ResNet 提高了 3.92%。这表明融合了自注意力机制和多尺度卷积结构的神经区分器能够更好地学习到密文序列中的微弱特征。

参考文献:

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991,4(1): 3-72.

[2] 王念平,倪亮.一种新的类 CLEFIA 密码结构抵抗差分分析的安全性评估[J].信息工程大学学报,2025,26(1):70-75.

[3] Gohr A. Improving attacks on round-reduced Speck32/64 using deep learning[C]//Advances in cryptology-CRYPTO 2019. Cham, Switzerlang: Springer, 2019:150-179.

[4] 赵未辰,刘天源,闫镔.融合多区域信息的 fMRI 低级视觉区编码模型[J].信息工程大学学报,2025,26(6): 646-651.

[5] 武浩莹,陈杰,刘君.改进 Simon32/64 和 Simeck32/64 神经网络差分区分离器[J].信息安全,2025,25(2): 249-259.

[6] 秦广雪,李丽莎.基于量子卷积神经网络的 ARX 分组

密码区分器[J].信息安全,2025,25(3):467-477.

[7] Chen Y, Shen Y T, Yu H B, et al. A new neural distinguisher considering features derived from multiple ciphertext pairs[J]. The Computer Journal, 2023,66(6):1419-1433.

[8] Beaulieu R, Treatman-Clark S, Shors D, et al. The SIMON and SPECK lightweight block ciphers [C]//Proceedings of the 2015 52nd ACM/EDAC/IEEE design automation conference. Piscataway, USA: IEEE, 2015:1-6.

[9] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: an ultra-lightweight block cipher [C]//Proceedings of the cryptographic hardware and embedded systems-CHES 2007. Berlin, Germany: Springer, 2007:450-466.

[10] Selent D. Advanced encryption standard [J]. Rivier Academic Journal, 2010,6(2):1-14.

[11] Mouha N, Mennink B, Van Herrewege A, et al. Chaskey: an efficient MAC algorithm for 32-bit microcontrollers [C]//Proceedings of the selected areas in cryptography-SAC 2014. Cham, Switzerland: Springer, 2014: 306-323.

[12] Huang S Y, Wang X Y, Xu G W, et al. Conditional cube attack on reduced-round keccak sponge function [C]//Advances in cryptology-EUROCRYPT 2017. Cham, Switzerland: Springer, 2017:259-288.

[13] Liu J S, Ren J J, Chen S Z. A deep learning aided differential distinguisher improvement framework with more lightweight and universality [J]. Cybersecurity, 2023, 6(1):47.

[14] Chollet F. Xception: deep learning with depthwise separable convolutions [C] //Proceedings of the 2017 IEEE conference on computer vision and pattern recognition. Piscataway, USA: IEEE, 2017:1800-1807.

[15] Yue X T, Wu W Q. Improved neural differential distinguisher model for lightweight cipher speck [J]. Applied Sciences, 2023,13(12):6994.