Modeling and Simulation 建模与仿真, 2025, 14(4), 471-485
Published Online April 2025 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2025.144302

Hans汉斯

Simon32/64神经网络差分区分器的优化

潘俊龙[1]，刘　亚[1,2]，赵逢禹[3]，曲　博[4]，刘先蓓[5]

[1]上海理工大学光电信息与计算机工程学院，上海
[2]香港狮子山网络安全实验室，香港
[3]上海出版印刷高等专科学校信息与智能工程系，上海
[4]港专学院网络空间科技学院，香港
[5]安徽财经大学统计与应用数学学院，安徽 蚌埠

收稿日期：2025年3月16日；录用日期：2025年4月9日；发布日期：2025年4月17日

摘　要

Simon32/64是美国国安局推荐的轻量级分组密码，现有基于深度学习的差分分析研究多采用单一数据格式和网络模型，未充分挖掘其优化潜力。本文探讨五种输入数据格式与三种神经网络模型的协同效应对Simon32/64神经差分区分器性能的影响。首先，提出倒数第二轮的多三面体输出差分数据格式M3PODPR，并结合四种已有数据格式，与ResNet、带Inception模块的ResNet、SENet进行全组合实验，构建15种数据－模型组合架构，并分别在相同训练集大小和相同明文数据量下，构造神经区分器并进行性能测试。实验表明：在SENet和M3PODPR架构下，9到11轮Simon32/64神经差分区分器均取得最高准确率，优于所有其它组合架构，也优于现有Simon32/64神经区分器的其它结果。因此M3PODPR可有效提升神经区分器的准确率，为密码分析提供新的优化方向。

关键词

Simon32/64，差分分析，神经区分器，倒数第二轮的多三面体输出差分，SENet

Optimization of Neural Differential Distinguishers for Simon32/64

Junlong Pan[1], Ya Liu[1,2], Fengyu Zhao[3], Bo Qu[4], Xianbei Liu[5]

[1]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai
[2]Hong Kong Lion Rock Labs of Cyberspace Security, Hong Kong
[3]Department of Information and Intelligent Engineering, Shanghai Publishing and Printing College, Shanghai
[4]Institute of Cyberspace Technology, Hong Kong College of Technology, Hong Kong
[5]School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu Anhui

Received: Mar. 16th, 2025; accepted: Apr. 9th, 2025; published: Apr. 17th, 2025

文章引用: 潘俊龙, 刘亚, 赵逢禹, 曲博, 刘先蓓. Simon32/64 神经网络差分区分器的优化[J]. 建模与仿真, 2025, 14(4): 471-485. DOI: 10.12677/mos.2025.144302

Abstract

Simon32/64 is a lightweight block cipher recommended by the National Security Agency (NSA). Existing studies on it against deep learning-based differential cryptanalysis primarily adopt a single data format and a network model, failing to fully exploit optimization potential. This paper investigates the synergistic effects of five input data formats and three neural network models on the performance of neural differential distinguishers for Simon32/64. Specifically, we propose the M3PODPR (Multiple 3-Polytope Output Difference Data Format in the Penultimate Round), evaluating the performance of M3PODPR and four existing data formats with ResNet, ResNet with Inception modules and SENet. A total of 15 data-model combinations are constructed and tested under identical training set sizes and plaintexts. Experimental results show that the SENet with M3PODPR architecture achieves the highest accuracy for 9 to 11 rounds of neural differential distinguishers for Simon32/64, outperforming all other combinations and existing results. Therefore, M3PODPR effectively enhances the accuracy of neural distinguishers, providing a new optimization direction for cryptanalysis.

Keywords

Simon32/64, Differential Analysis, Neural Distinguishers, Multiple 3-Polytope Output Difference Data Format in the Penultimate Round, SENet

Copyright © 2025 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

随着物联网(IoT)和嵌入式设备的快速发展，轻量级分组密码因其低资源消耗和高软硬件实现成为保障数据安全的核心技术之一。Simon32/64 [1]是美国国家安全局(NSA)推选的轻量级加密算法，在资源受限环境中得到了广泛应用。然而它采用较短的 32 比特分组长度且相对简单的轮函数，研究者对其安全性保持持续关注[2] [3]。传统的密码分析方法，如差分分析[4]、线性分析[5]，在面对 Simon32/64 算法中模乘运算时，难以构造有效的区分器，导致分析效果受限[6]。因此，需要探索新的分析手段以评估 Simon32/64 的安全性，为 Simon32/64 的安全性评估提供新的思路。

近年来，深度学习与差分分析的融合为密码分析提供了新的研究思路。2019 年，Gohr [7]基于残差神经网络首次构造了 Speck32/64 的差分区分器，成功攻击了简化轮次的 Speck32/64 [1]，证明了深度学习在捕捉密码算法非线性特征方面的潜力。随后，研究者们主要从输入数据格式和神经网络架构两个方面对神经网络差分区分器进行优化。例如：2020 年，Su 等[8]提出多面体密文对作为输入数据格式，将 8 轮 Simon32/64 的神经网络差分区分器准确率提升至 92%。2021 年，Hou 等[9]采用多输出差分对作为输入，提高了 7~8 轮 Speck32/64 和 9~10 轮 Simon32/64 的区分器准确率。2022 年，Bao 等[10]用挤压激励网络替代残差网络，优化 Simon32/64 的神经网络差分区分器，提高了分类精度。2023 年，Chen 等[11]采用多密文对作为输入，并应用于五种不同的密码算法，实验表明该方法能有效提升神经网络差分区分器的准确率。Zhang 等[12]结合初始模块和残差网络，提出 9~11 轮 Simon32/64 的神经网络差分区分器。

尽管上述研究在 Simon32/64 的神经网络差分分析上取得了重要进展，但仍存在两大局限性。第一，输入数据格式与模型架构的优化缺乏系统性，现有研究往往孤立地结合单一数据格式与单一模型，例如多面体密文对[8]仅与残差网络结合，缺乏对多种数据格式与多种模型的系统性配对实验；第二，对加密

过程中间轮次特征的挖掘不足，现有方法普遍依赖最终轮密文作为输入，难以有效捕捉算法内部的非线性传播规律。

针对上述问题，本文提出多维协同优化框架，系统探索输入数据格式与神经网络模型的组合效应对Simon32/64差分区分器性能的影响，提升了Simon32/64神经网络差分区分器的性能，为基于深度学习的密码分析方法提供了新的优化思路。主要贡献包括：

1) 本研究优化Simon32/64的输入数据格式，并探讨其与神经网络模型的协同作用。在现有输入数据格式的基础上，提出M3PODPR数据格式，以增强对Simon32/64非线性结构的表征能力。结合三种神经网络模型与五种数据格式，构建15种神经区分器进行系统分析。实验结果表明，该数据格式在所有模型中均优于现有格式，并在挤压激励网络下取得最佳表现，8~11轮Simon32/64任务的最高准确率分别达到100.00%、98.20%、79.55%和60.29%，展现出更强的泛化能力。

2) 明文均衡策略下的公平性分析：为确保实验公平性，本文采用2×10^7个明文样本进行训练，以消除不同数据格式间的固有偏差。实验结果表明，M3PODPR结合SENet仍能在8~11轮任务中取得最高准确率，分别为99.99%、96.14%、73.55%、51.37%，进一步验证了该方案的有效性。

3) 本研究将SENet与M3PODPR相结合，并与现有方法进行对比。实验结果表明，该方案在9~11轮Simon32/64任务中均取得最优性能，显著优于传统数据格式。

2. 预备知识

本章主要介绍Simon32/64轻量级分组密码的基本原理、不同输入数据格式的构造方法、用于密码分析的神经网络模型，以及Gohr提出的神经网络差分区分器。

2.1. 符号说明

本文的符号说明如表1所示。

Table 1. Symbol description
表1. 符号说明

符号	含义
$\gg/\ll$	循环右移/循环左移
$\oplus$	按位异或运算
$\odot$	按位与运算
k_g	最后一轮子密钥

2.2. 加密算法Simon简介

Simon是美国国家安全局(NSA)于2013年提出的一类轻量级分组密码算法族，专为资源受限的嵌入式设备设计，其结构简洁，易于硬件实现。Simon家族包含多个版本，本文研究对象为Simon32/64，即分组长度为32位，密钥长度为64位，加密轮数为32轮。

Simon32/64采用Feistel网络结构，将32位明文分为左右两个16位分组，记为L_0和R_0，通过多轮迭代逐步混淆与扩散。每轮加密流程如下：

$$L_{i+1}=R_i\oplus\left(L_i\ll1\right)\odot\left(L_i\ll8\right)\oplus\left(L_i\ll2\right)\oplus k_i$$

$$R_{i=1}=L_i$$

Simon32/64 的密钥扩展算法以及其他详细信息可参考文[1]。

2.3. 不同输入数据格式

在 Gohr 提出的经典数据生成方法中，明文对$\left(M^1,M^2\right)$被加密为密文对$\left(C^1,C^2\right)$作为训练样本。其中正样本(标签 1)是由满足输入差分$M^1\oplus M^2=\Delta_{\text{in}}$的明文对加密生成。负样本(标签 0)是由随机明文对加密生成。在此基础上，研究人员提出了多种扩展的数据格式，以增强神经网络区分器的训练效果：

1) 多密文对(MCP: Multiple Ciphertext Pairs)：采用 t 组明文对$\left\{\left(M^{1,1},M^{1,2}\right),\cdots,\left(M^{t,1},M^{t,2}\right)\right\}$，通过同一随机密钥加密生成$t$组密文对$\left\{\left(C^{1,1},C^{1,2}\right),\cdots,\left(C^{t,1},C^{t,2}\right)\right\}$作为训练样本。

2) 多输出差分对(MOD: Multiple Output Differences)：在多密文对的基础上，进一步计算 t 组密文对的差分$\left\{\left(C^{1,1}\oplus C^{1,2}\right),\cdots,\left(C^{t,1}\oplus C^{t,2}\right)\right\}$作为训练样本。

3) 单三面体密文对(S3PCP: Single 3-polytope ciphertext pair)：在 Gohr 的数据生成方法上，将明文对扩展为三个明文$\left(M^1,M^2,M^3\right)$，并满足：$M^1\oplus M^2=\Delta_{\text{in1}}$和$M^1\oplus M^3=\Delta_{\text{in2}}$。

4) 单四面体密文对(S4PCP: Single 4-polytope ciphertext pair)：在单三面体密文对的基础上，进一步扩展为四个明文$\left(M^1,M^2,M^3,M^4\right)$，并满足：$M^1\oplus M^2=\Delta_{\text{in1}}$、$M^1\oplus M^3=\Delta_{\text{in2}}$和$M^1\oplus M^4=\Delta_{\text{in3}}$。

这些扩展数据格式通过增加明文对数量或引入多面体结构，丰富了训练样本的统计特征，使神经网络区分器能够更有效地捕捉密码算法的非线性特征。图 1 展示了多密文对和多输出差分对的生成过程。

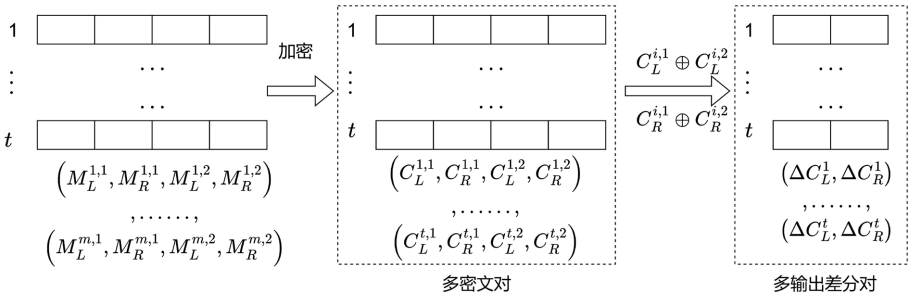

Figure 1. Generation process of multiple ciphertext pairs and multiple output differences
图 1. 多密文对和多输出差分对的生成过程

2.4. 神经网络模型架构

近年来，深度学习在密码分析领域的应用不断深入，神经网络架构的优化显著提升了差分区分器的性能。本文主要介绍三类适用于 Simon32/64 神经网络分析的经典模型。

1) 残差网络(ResNet: Residual Network)：He 等[13]于 2016 年提出 ResNet，其核心通过残差连接缓解深层网络的梯度消失问题。残差块的数学定义如下：

$$y=F\left(x,\{W_i\}\right)+x$$

其中，x 为输入，F 为卷积层和非线性激活函数的组合，W_i为权重矩阵。残差连接允许网络直接传递原始输入，使得深层网络训练更加稳定。在密码分析中，ResNet 因其强大的特征传递能力被广泛采用。

2) 初始模块和残差网络的混合网络(Inception + ResNet: Inception Module and Residual Network)：Szegedy 等[14]提出的初始(Inception)模块采用并行多尺度卷积，增强了特征空间的多样性。Inception + ResNet 结合了 Inception 的多尺度特征提取能力和 ResNet 的稳定梯度传递特性。

3) 挤压激励网络(SENet: Squeeze-and-Excitation Network)：Hu 等[15]于 2018 年提出 SENet，其核心思想是通道注意力机制，通过挤压和激励两步操作动态调整特征通道的重要性。挤压操作对特征图进行

全局平均池化，生成通道描述向量。激励操作通过全连接层学习通道间依赖关系，输出通道权重。在密码分析中，SENet 能够聚焦于关键差分特征，抑制噪声干扰，提升区分器性能。

2.5. Gohr 的神经网络差分区分器

Gohr 针对 Speck32/64 设计了一种基于深度学习的神经网络区分器[7]，该方法采用单一密文对(SCP: Single Ciphertext Pairs)的数据格式仅需约束单一明文差分 Δ_{in} 即可实现有效分类。对于给定的密码算法 E，区分器的目标是判定密文对 $\left(C^1, C^2\right)$ 是否来源于满足特定差分条件的明文对 $\left(M^1, M^2\right)$，其标签函数定义为：

$$Y\left(C^1, C^2\right)=\begin{cases}1, & \text{if } \cdot M^0 \oplus M^1=\Delta_{\text{in}} \\ 0, & \text{if } \cdot M^0 \oplus M^1 \neq \Delta_{\text{in}}\end{cases}$$

Gohr 采用单输出神经元的残差网络作为基础架构，最终输出样本属于正类的概率，当预测概率大于 0.5 时，判定样本标签为 1，否则为 0。

3. M3PODPR 数据格式

本节提出了一种新的输入数据格式 M3PODPR (Multiple 3-Polytope Output Differences in Penultimate Round)，用于增强神经网络区分器对 Simon32/64 倒数第二轮非线性特征的捕捉能力。该格式基于多面体密文对的输出差分，结合数据增强技术，以提升分类器的识别精度。接下来介绍其生成流程，并分析其在 Simon32/64 区分任务中的优势。

3.1. 设计动机

Benamira 等[16]研究表明，神经网络差分区分器能够有效捕捉加密算法倒数第二轮和倒数第三轮的中间状态特征。受此启发，本文提出一种新的输入数据格式，旨在提 Simon32/64 倒数第二轮的输出差分信息，以增强神经网络区分器对中间轮次的非线性特征的捕捉能力。

3.2. Simon32/64 算法的特性

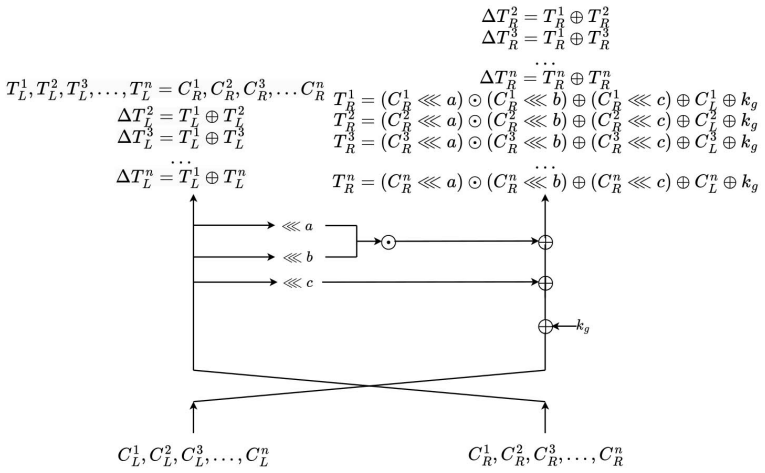

Figure 2. Output information of the penultimate round in Simon32/64
图 2. Simon32/64 倒数第二轮输出的信息

给定 n 面体密文对 $\left(C^1, C^2, C^3, \cdots, C^n\right)$，根据 Simon32/64 的加密特性，可以从密文逆向推导出倒数第

二轮的部分输出信息，具体过程如图 2 所示。若已$\left(C^1,C^2,C^3,\cdots,C^n\right)$及最后一轮子密钥$k_g$，可计算倒数第二轮的输出$\left(C^1,C^2,C^3,\cdots,C^n\right)$，即使未知$k_g$，仍可直接获得右半部分的差分信息$\Delta T_R$。因此基于多面体密文对，可以构造出倒数第二轮的多面体输出差分：$\left(\Delta T_L^2,\Delta T_R^2,\Delta T_L^3,\Delta T_R^3,\cdots,\Delta T_L^n,\Delta T_R^n\right)$。这种数据格式可用于训练神经网络区分器，以更深入地捕捉 Simon32/64 的中间轮次非线性特征。

3.3. M3PODPR 数据生成过程

本文采用三面体密文对的格式，在生成倒数第二轮的三面体输出差分后，进一步采用数据增强技术，即：在倒数第二轮，应用多个三面体输出差分，增强数据集的统计特征。具体实现如图 3 所示：

1) 使用任意主密钥，加密 t 组三面体明文对：

$$\left\{\left(M^{1,1},M^{1,2},M^{1,3}\right),\cdots,\left(M^{t,1},M^{t,2},M^{t,3}\right)\right\}$$

2) 得到 t 组三面体密文对：

$$\left\{\left(C^{1,1},C^{1,2},C^{1,3}\right),\cdots,\left(C^{t,1},C^{t,2},C^{t,3}\right)\right\}$$

3) 进一步计算倒数第二轮的输出差分：

$$\left\{\left(\Delta T^{1,2},\Delta T^{1,3}\right),\cdots,\left(\Delta T^{t,2},\Delta T^{t,3}\right)\right\}$$

4) 以此构造新的输入数据格式，定义为倒数第二轮的多三面体输出差分(M3PODPR: Multiple 3-Polytope Output Differences in Penultimate Round)。

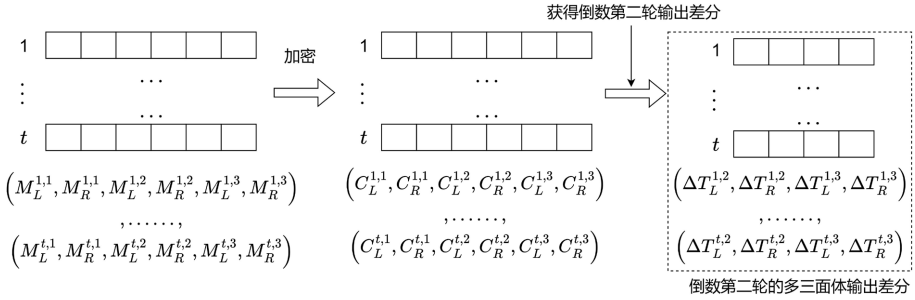

Figure 3. Generation process of M3PODPR
图 3. 倒数第二轮的多三面体输出差分的生成过程

4. 基于多数据－多模型 Simon32/64 区分器的协同优化实验

针对 Simon32/64 神经区分任务，研究了不同数据格式与神经网络模型的组合对区分器性能的影响。首先，在固定训练集 10^7 下，评估五种数据格式与三种深度学习模型的组合性能，以寻找准确率最高的区分器。随后，为确保不同数据格式在相同明文消耗量 2×10^7 下进行公平对比，进一步开展公平性实验。

4.1. 实验环境

本文在 Linux 平台上使用 Python 3.6.15 进行实验，服务器配置如下：AMD EPYC 7542 处理器(32 核)、667GB 内存、NVIDIA GeForce RTX 3090 (24GB 显存)，实验存储为 50GB NVMe SSD，并使用 CUDA 12.2 和 TensorFlow 2.5.0 实现模型。

4.2. 生成输入数据格式

本实验基于 Gohr 提出的神经网络区分器训练范式，采用二元交叉熵损失函数及动态学习率调整策

略，通过替换输入数据格式与模型架构，系统评估不同组合对 Simon32/64 区分器性能的影响。相较于 Gohr 提出的单一数据格式(单密文对)和单一模型(残差网络)，本文扩展至五类数据格式，具体如下：

1) 多密文对(MCP: Multiple Ciphertext Pairs)

采用随机密钥加密多个明文对 $\left\{\left(M^{1,1},M^{1,2}\right),\cdots,\left(M^{t,1},M^{t,2}\right)\right\}$ $(t=16)$，生成多密文对 $\left\{\left(C^{1,1},C^{1,2}\right),\cdots,\left(C^{16,1},C^{16,2}\right)\right\}$，明文对的输入差分为 $\Delta_{\text{in}}=(0,0040)$。

2) 多输出差分对(MOD: Multiple Output Differences)

采用随机密钥加密多个明文对 $\left\{\left(M^{1,1},M^{1,2}\right),\cdots,\left(M^{t,1},M^{t,2}\right)\right\}$ $(t=16)$，生成多输出对 $\left\{\left(C^{1,1}\oplus C^{1,2}\right),\cdots,\left(C^{16,1}\oplus C^{16,2}\right)\right\}$，明文对的输入差分为 $\Delta_{\text{in}}=(0,0040)$。

3) 单三面体密文对(S3PCP: Single 3-Polytope Ciphertext Pair)

采用三明文 $\left(M^1,M^2,M^3\right)$ 构造三面体密文 $\left(C^1,C^2,C^3\right)$ 对。并满足输入差分 $M^1\oplus M^2=(0,0080)$ 和 $M^1\oplus M^3=(0,0040)$。

4) 单四面体密文对(S4PCP: Single 4-Polytope Ciphertext Pair)

采用四明文 $\left(M^1,M^2,M^3,M^4\right)$ 构造四面体密文 $\left(C^1,C^2,C^3,C^4\right)$ 对。并满足输入差分 $M^1\oplus M^2=(0,0080)$、$M^1\oplus M^3=(0,0040)$ 和 $M^1\oplus M^4=(0,0020)$。

5) 倒数第二轮多三面体输出差分对(M3PODPR: Multiple 3-Polytope Output Differences in Penultimate Round)

采用多三面体明文对 $\left\{\left(M^{1,1},M^{1,2},M^{1,3}\right),\cdots,\left(M^{t,1},M^{t,2},M^{t,3}\right)\right\}$ $(t=16)$，通过逆向计算倒数第二轮的输出差分：征 $\left\{\left(\Delta T^{1,2},\Delta T^{1,3}\right),\cdots,\left(\Delta T^{16,2},\Delta T^{16,3}\right)\right\}$。并满足输入差分 $M^{i,1}\oplus M^{i,2}=(0,0080)$、$M^{i,1}\oplus M^{i,3}=(0,0040)$。

4.3. 神经网络模型设计与架构

为了提升神经网络对 Simon32/64 差分特征的学习能力，本文采用三种深度学习模型进行实验分析，包括 ResNet、Inception + ResNet 和 SENet。以下分别介绍这三种模型的具体架构。

ResNet：继承 Gohr 的基线架构。图 4 详细展示了本文所采用的残差网络的具体结构。其中，在模块 1 中，包含一个一维卷积神经网络(1D-CNN)，其卷积核大小(Kernel Size)为 1，滤波器数量(Filters)为 32。在模块 2 中，网络由两个 1D-CNN 组成，每个卷积层的核大小均为 3，滤波器数量同样设定为 32，以提取更深层次的特征信息。最后，在模块 3 中，网络采用了三层全连接层(Fully Connected Layers)，其输出维度依次为 64、64 和 1，以进一步整合前面提取的特征并完成最终的分类。

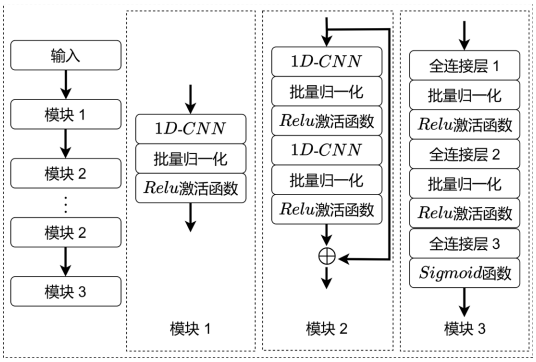

Figure 4. Residual network model structure
图 4. 残差网络模型结构

Inception + ResNet：结合多尺度卷积与残差连接，结构如图 5 所示。初始模块通过 1 × 1、2 × 2 和 8 × 8 不同尺寸的卷积核并行提取多尺度局部特征，增强模型对不同粒度信息的感知能力。残差模块进一步筛选重要通道，强化关键信息的传递。在模块 1 中，包含三个 1D-CNN，卷积核大小分别为 1、2 和 8，滤波器数量均为 32。模块 2 由两个 1D-CNN 组成，初始卷积核大小为 3，滤波器数量增加至 96，并在每个残差块后逐步增大 2，以扩展感受野，提升长距离依赖建模能力。该架构兼具特征提取的多样性与关键信息增强能力，有效提升模型性能。

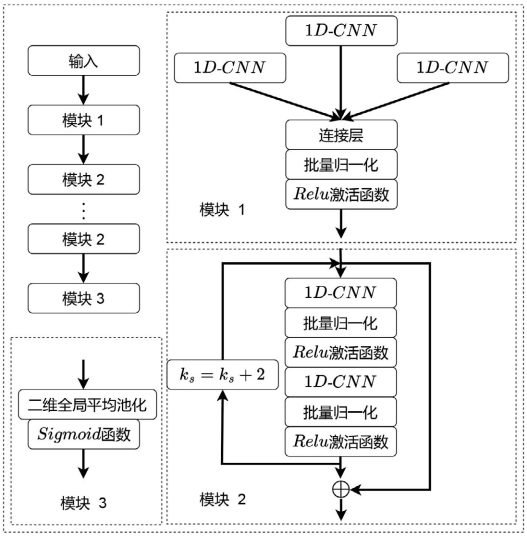

Figure 5. Hybrid network model of the inception module and residual network
图 5. 初始模块和残差网络的混合网络模型

SENet：引入通道注意力机制优化特征权重。图 6 展示了本文使用的挤压激励网络的结构，模块 1 采用 1D-CNN 进行初步特征提取，卷积核大小为 1，滤波器数量 64，并通过两个全连接层(输出维度均为 64)进一步处理。模块 2 由两个 1D-CNN 组成，卷积核大小均为 3，滤波器数量 64，同时包含两个全连接层(输出维度 64)。模块 3 由三层全连接层组成，输出维度依次为 128、128、1，用于整合特征并完成最终预测。该架构通过注意力机制自适应调整特征权重，有效提升模型的特征表达能力和关键信息捕获能力。

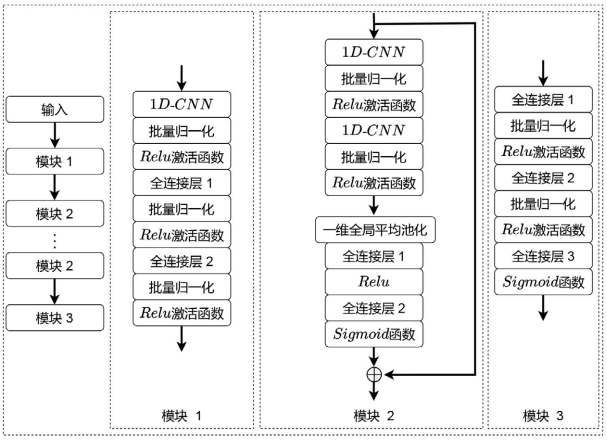

Figure 6. Squeeze-and-Excitation network model structure
图 6. 挤压激励网络模型结构

4.4. 基于 10^7 训练集的神经网络区分器性能评估

为了全面评估不同数据格式与模型架构的组合性能，实验采用五种数据格式与三种神经网络模型，共构建 15 种神经网络区分器。训练集、验证集和测试集的规模分别为 107、106 和 106。在区分器训练 100 个 epoch 后，8~11 轮 Simon32/64 的测试集准确率如表 2 和图 7 所示。实验中，仅当准确率超过 51% 时，区分器被视为有效。

从实验结果可以看出，不同数据格式在各类神经网络模型中的表现存在显著差异，同时数据格式对明文的消耗量也影响了区分器的性能，表明数据输入方式对神经网络的学习能力至关重要。

MCP、S3PCP 和 S4PCP 在 Inception + ResNet 结构下表现最佳。例如，当输入数据格式为 S4PCP 时，基于 Inception + ResNet 的区分器在 9 轮 Simon32/64 任务中的测试集准确率达到 71.26%，显著优于基于 ResNet 下 63.64%和 SENet 下 65.43%的准确率。从数据特性来看，MCP、S3PCP 和 S4PCP 直接由密文对构成，完整保留了密文的全局分布模式和局部比特的关联性，使得数据维度较高，要求模型同时捕捉局部细节与宏观统计特征。而 Inception + ResNet 通过多尺度特征提取与深层残差连接，能够更有效地学习这类高维数据。其中，Inception 模块采用 1×1、2×2 和 8×8 卷积核的并行结构，2×2 卷积关注邻近比特的局部关联性，而 8×8 卷积则识别更大范围的统计偏差，实现不同尺度的特征提取。同时，ResNet 结构通过残差连接缓解梯度消失问题，提升模型的稳定性，使其在处理高维密文数据时仍能保持良好的学习能力。

此外，从明文消耗量的角度来看，S3PCP 和 S4PCP 相较于 MCP 具有更低的明文消耗量，分别为 3×10^7 和 4×10^7，而 MCP 的明文消耗量为 32×10^7。尽管 S3PCP 和 S4PCP 明文消耗量较少，但其在 Inception + ResNet 结构下的 9 轮区分任务中仍能保持较高准确率(S3PCP 为 69.47%, S4PCP 为 71.26%)，表明在一定范围内，通过优化数据格式，可以在降低明文消耗量的同时保持较好的区分能力。然而，当轮数增加至 10 轮及以上，S3PCP 和 S4PCP 的准确率均下降至 51%以下，表现出失效现象，说明在深轮次任务中，低明文消耗的数据格式难以提供足够的可学习特征，导致区分器的有效性降低。

相比之下，MOD 和 M3PODPR 在 SENet 结构下表现最佳。例如，当输入数据格式为 M3PODPR 时，基于 SENet 的区分器在 10 轮 Simon32/64 任务中的测试集准确率达到 79.55%，相比基于 Inception + ResNet 结构下 75.41%的准确率提高 4.14%。从数据特性来看，MOD 和 M3PODPR 主要基于输出差分(异或结果)，相比直接使用密文对，这类数据的关键信息密度较低，数据分布较为稀疏，且关键特征信号较弱，容易受到噪声干扰。而 SENet 采用通道注意力机制，通过“挤压–激励”操作自动学习各通道的重要性权重，能够动态调整特征通道的权重，强化关键差分信息，同时抑制无关噪声干扰。相比 Inception + ResNet 的静态多尺度卷积，SENet 能够根据输入数据的特征自适应调整权重，因此在处理 MOD 和 M3PODPR 这类非均匀分布的数据格式时表现更优。

值得注意的是，尽管 MOD 和 M3PODPR 在数据结构上相比 MCP、S3PCP 和 S4PCP 具有更低的信息密度，但 M3PODPR 通过引入更复杂的差分信息，提供了更丰富的可学习特征。在明文消耗量上，M3PODPR 明文数量为 48×10^7，明显高于 MCP、MOD、S3PCP 和 S4PCP。实验结果表明，尽管 M3PODPR 需要消耗更多的明文进行训练，但其提供的高质量特征能够有效提升区分器的性能，使其在 10 轮及以上任务中仍能保持较高的准确率(10 轮任务中，基于 SENet 结构的区分器测试集准确率达到 79.55%，11 轮任务中仍能保持 60.29%)。相比之下，其他四种数据格式(MCP, MOD, S3PCP 和 S4PCP)在 10 轮及以上完全失效，准确率均低于 51%。这一结果表明，在深轮次任务中，增加明文消耗量有助于增强区分器的稳定性和泛化能力，尤其是当数据格式能够提供更具区分性的特征时，额外的明文消耗可以转化为显著的性能增益。

综合来看，M3PODPR 在三种神经网络模型 ResNet、Inception + ResNet 和 SENet 中均取得最优表现，

Table 2. Test accuracy of Simon32/64 neural distinguishers in rounds 8~11 with the 10^7 training set sizes
表 2. 基于 10^7 训练集 8~11 轮 Simon32/64 神经区分器的测试集准确率

网络模型	数据格式	训练明文数据量	测试准确率(%)			
			8 轮	9 轮	10 轮	11 轮
ResNet	MCP	32×10^7	95.12	71.34	无效	无效
	MOD	32×10^7	81.23	60.23	无效	无效
	S3PCP	3×10^7	90.86	61.33	无效	无效
	S4PCP	4×10^7	92.13	63.64	无效	无效
	M3PODPR	48×10^7	99.99	90.25	70.16	53.95
Inception + ResNet	MCP	32×10^7	100.00	88.70	无效	无效
	MOD	32×10^7	83.34	64.76	无效	无效
	S3PCP	3×10^7	93.68	69.47	无效	无效
	S4PCP	4×10^7	95.47	71.26	无效	无效
	M3PODPR	48×10^7	100.00	93.20	75.41	55.29
SENet	MCP	32×10^7	93.70	75.41	无效	无效
	MOD	32×10^7	85.47	69.35	无效	无效
	S3PCP	3×10^7	75.34	64.76	无效	无效
	S4PCP	4×10^7	82.20	65.43	无效	无效
	M3PODPR	48×10^7	**100.00**	**98.20**	**79.55**	**60.29**

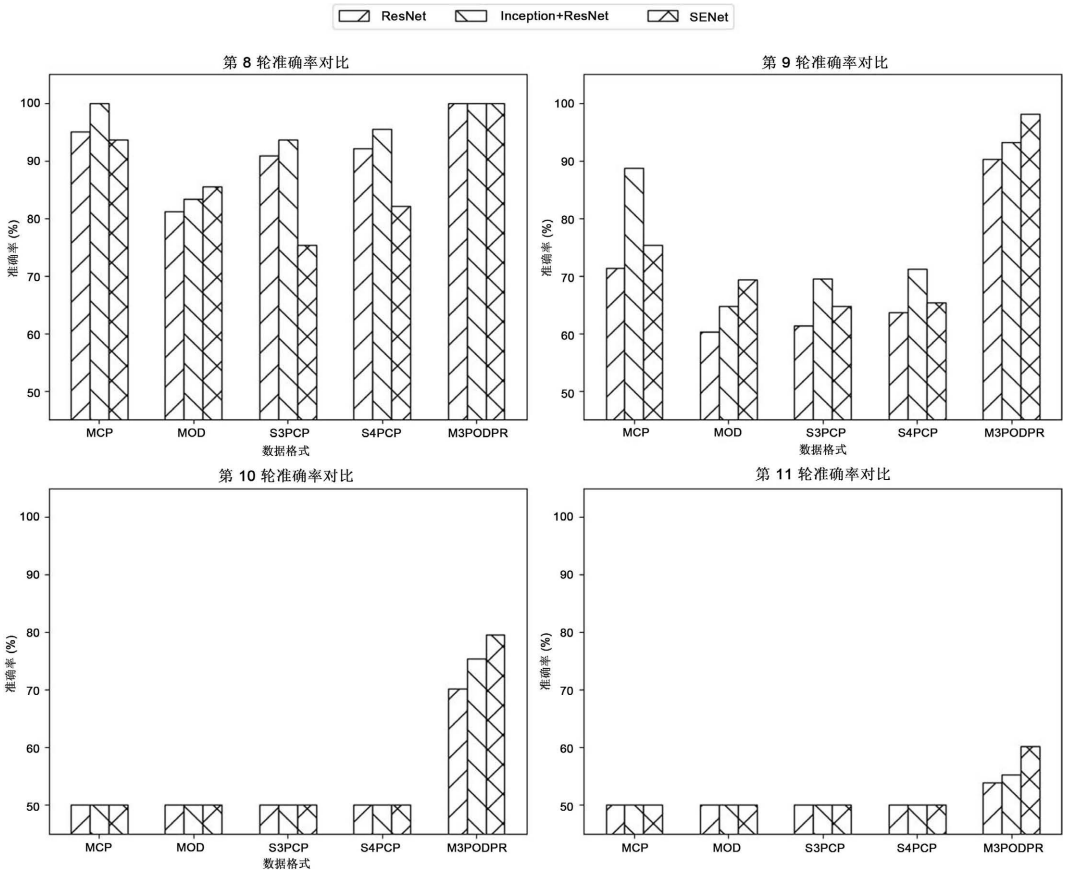

Figure 7. Test accuracy of Simon32/64 neural distinguishers in rounds 8~11
图 7. 8~11 轮 Simon32/64 神经区分器的测试集准确率

且在 SENet 结构下达到全局最优，成为 15 种神经网络区分器中的最佳方案。实验结果显示，仅当输入数据格式为 M3PODPR 时，基于 ResNet、Inception + ResNet 和 SENet 的区分器才能在 10 轮和 11 轮 Simon32/64 任务中保持有效性。相比之下，其他四种数据格式 MCP、MOD、S3PCP 和 S4PCP 在 10 轮及以上完全失效，准确率均低于 51%。这一结果表明，M3PODPR 格式不仅能够规避最终轮密钥混淆的影响，同时结合适当的明文消耗量优化了区分器的训练过程，在深轮次任务中展现出更强的区分能力和稳定性。

4.5. 基于 2×10^7 个明文的神经网络区分器性能评估

Table 3. Number of single-sample plaintexts for five data formats
表 3. 五类数据格式的单样本明文的数量

数据格式	单样本明文的数量
MCP	32
MOD	32
S3PCP	3
S4PCP	4
M3PODPR	48

在初步实验中，由于五类数据格式的单样本明文数量不同(见表 3)，导致在相同训练集规模(10^7 个样本)下，总明文量存在显著差异。这一不均衡性可能会影响不同数据格式的神经区分器训练效果，使得某些数据格式在训练过程中受益于更丰富的明文信息，从而影响实验结果的公平性。

为消除明文总量差异对性能评估的影响，本节增设公平性实验组，强制所有数据格式的总明文量固定为 2×10^7，并通过调整训练集规模实现数据均衡。具体调整方案如下：

训练集大小的计算方式：

$$\text{训练集大小} = \frac{2\times10^7}{\text{单样本的明文数量}}$$

验证集和测试集大小的计算方式：

$$\text{验证集和测试集大小} = \frac{2\times10^7}{\text{单样本的明文数量}}$$

这一调整方案能够有效消除不同数据格式在明文利用率上的差异，确保实验对比的公平性，使得不同数据格式的神经区分器性能可以在相同明文总量的前提下进行客观评估。实验结果如表 4 所示。

实验结果表明 SENet 结合 M3PODPR 结构在 8~10 轮的准确率最高分别是 99.99%、96.14%和 73.55%，显著优于 ResNet 和 Inception + ResNet，进一步验证了 SENet 的通道注意力机制能够有效增强差分特征的学习能力。相比之下，其他四种数据格式 MCP、MOD、S3PCP、S4PCP 在 10 轮及以上完全失效，说明仅依赖最终轮密文对难以提供有效的区分信息，而 MOD 格式在所有轮次均无效，表明单独使用输出差分不足以训练出有效的神经区分器。此外，Inception + ResNet 结合 M3PODPR 发生过拟合，可能是由于该模型结构复杂，所需训练样本较多，但公平性实验减少了训练集大小，导致泛化能力下降，需要进一步调整正则化策略或优化模型参数。

Table 4. Test accuracy of Simon32/64 neural distinguishers in rounds 8~11 with 2×10^7 plaintexts
表 4. 基于 2×10^7 个明文 8~11 轮 Simon32/64 神经区分器的测试集准确率

网络模型	数据格式	训练集大小	测试准确率(%)			
			8 轮	9 轮	10 轮	11 轮
ResNet	MCP	$2 \times 10^7/32$	76.54	50.61	无效	无效
	MOD	$2 \times 10^7/32$	无效	无效	无效	无效
	S3PCP	$2 \times 10^7/3$	82.70	64.43	无效	无效
	S4PCP	$2 \times 10^7/4$	83.30	65.76	无效	无效
	M3PODPR	$2 \times 10^7/2$	99.10	85.60	62.76	无效
Inception + ResNet	MCP	$2 \times 10^7/32$	过拟合			
	MOD	$2 \times 10^7/32$	无效	无效	无效	无效
	S3PCP	$2 \times 10^7/3$	91.20	65.43	无效	无效
	S4PCP	$2 \times 10^7/4$	91.32	65.87	无效	无效
	M3PODPR	$2 \times 10^7/2$	过拟合			
SENet	MCP	$2 \times 10^7/32$	88.43	58.75	无效	无效
	MOD	$2 \times 10^7/32$	无效	无效	无效	无效
	S3PCP	$2 \times 10^7/3$	69.03	53.60	无效	无效
	S4PCP	$2 \times 10^7/4$	68.74	53.47	无效	无效
	M3PODPR	$2 \times 10^7/2$	**99.99**	**96.14**	**73.55**	**51.37**

4.6. 与现有研究的实验结果对比

本节将本文最佳实验结果(SENet 结合 M3PODPR 构造的区分器)与现有研究的实验结果进行对比分析，以评估本研究方法在神经区分任务中的改进效果。本对比主要针对 9~11 轮 Simon32/64 任务的区分器准确率，同时，为了确保公平性，现有研究的实验结果中也取其最优结果进行比较。通过分析不同方法在这些轮次上的测试集准确率，可以直观地验证 M3PODPR 数据格式的有效性以及 SENet 结构在特征提取方面的优势。

Table 5. Comparison of experimental results between this study and related works
表 5. 本研究与相关工作的实验结果对比

网络模型	数据格式	轮数	准确率%	来源
ResNet	S4PCP	9	63.73	文献[8]
SENet	SCP	9	65.15	文献[10]
ResNet	MOD	9	82.27	文献[9]
Inception + ResNet	MCP	9	96.30	文献[12]
SENet	**M3PODPR**	**9**	**98.20**	**本文 4.1 节**
ResNet	S4PCP	10	50.14	文献[8]
SENet	SCP	10	56.10	文献[10]
ResNet	MOD	10	61.09	文献[9]

续表

Inception + ResNet	MCP	10	72.30	文献[12]
SENet	**M3PODPR**	**10**	**79.55**	**本文 4.1 节**
ResNet	S4PCP	11	-	文献[8]
SENet	SCP	11	51.74	文献[10]
ResNet	MOD	11	-	文献[9]
Inception + ResNet	MCP	11	58.78	文献[12]
SENet	**M3PODPR**	**11**	**60.29**	**本文 4.1 节**

如表 5 所示，根据实验结果，我们对不同方法的优缺点进行了深入分析，并通过实验数据进行了详细对比。Su 等[8]提出的 S4PCP (单四面体密文对)结合 ResNet 结构在 9 轮上实现了 63.73%的准确率，虽然通过多面体密文对增强了特征信息，但仍然依赖最终轮密文，在深轮次任务(10 轮及以上)中失效(准确率降至 50.14%或更低)。Bao 等[10]提出的 SCP (单密文对)数据格式结合 ResNet 进行分类，具有训练速度快、计算成本低的优势，但仅使用单一密文对，导致区分能力受限，9 轮准确率仅为 65.15%，且在 10 轮及以上下降至 56.10%，无法有效识别深轮次的密码特征。Hou 等[9]采用 MOD (多输出差分)数据格式，在 9 轮 Simon32/64 任务中的准确率达到 82.27%，但在 11 轮时仍然存在信息丢失问题，无法维持有效的区分能力。Zhang 等[12]结合 MCP (多密文对)数据格式与 Inception + ResNet 结构，在 9 轮任务中取得了 96.30%的准确率，相比 ResNet 和 SCP 具有更强的特征提取能力，但在 10 轮任务中准确率下降至 72.30%，11 轮进一步降至 58.78%，表明该方法的泛化能力仍然有限。相比之下，本文提出的 M3PODPR 数据格式结合 SENet，在 9 轮任务中实现了 98.20%的最高准确率，并在 10 轮和 11 轮任务中分别达到 79.55%和 60.29%，均显著优于现有方法，证明了倒数第二轮特征增强的有效性，同时展现出更强的泛化能力。然而，该方法相较于其他方法对明文的消耗量较大，是未来优化的一个方向。

从理论上来看，M3PODPR 数据格式能够取得优异结果的主要原因在于 Simon32/64 采用 Feistel 结构，每轮加密过程中，密钥混合操作会不断引入新的非线性特征。相比最终轮密文，倒数第二轮的输出仍然保留了部分未被最终轮密钥完全混淆的状态信息，使得神经网络在学习过程中能够更有效地捕捉和利用这些特征。此外，信息熵分析表明，倒数第二轮的输出差分携带了更高的信息量，从而增强了数据的区分性，使 M3PODPR 格式能够提取更丰富的密码学特征，进一步提升神经区分器的分类能力。然而，将该数据格式构造的神经区分器应用于密钥恢复攻击时，仍需消耗大量选择明文，这在实际应用中可能带来一定的开销，因此如何优化明文利用效率将是未来研究的重要方向。

5. 总结与展望

5.1. 总结

本研究围绕神经区分任务，对五种不同的数据格式 MCP、MOD、S3PCP、S4PCP、M3PODPR 和三种不同的神经网络架构 ResNet、Inception + ResNet、SENet 进行了系统的对比实验，共构建了 15 种不同的神经区分器，并在 8~11 轮 Simon32/64 算法上进行了测试分析。实验结果表明，数据格式的选择对于神经区分器的性能具有重要影响，其中 M3PODPR 格式在所有轮次下均表现最佳，显著优于传统的 MCP、MOD、S3PCP 和 S4PCP 格式，证明了引入多轮次密文信息可以有效提升神经区分器的准确率。同时，在不同的网络架构对比中，SENet 由于其通道注意力机制，在所有数据格式下均表现优于 ResNet 和 Inception + ResNet，展现了更强的特征提取能力。最终，SENet 结合 M3PODPR 的组合在 9~11 轮任务中均取得最

优结果，其中 9 轮(98.20%)和 10 轮(79.55%)的准确率远超现有研究，11 轮(60.29%)的准确率也保持领先，展现了较好的泛化能力。然而，随着轮次的增加，所有方法的准确率均有所下降，在 11 轮任务中，大部分传统数据格式准确率都接近 50%，表明神经区分器在更高轮次任务中的能力受限。本研究的实验结果充分证明了 M3PODPR 数据格式的有效性以及 SENet 在神经区分任务中的优势，为后续研究提供了新的优化方向。

5.2. 未来展望

尽管本研究取得了较好的实验结果，但仍存在一些值得进一步探讨的问题。首先，如何进一步提升神经区分器在高轮次任务(如 11 轮及以上)的准确率，仍然是一个重要挑战，可以考虑引入更深层次的特征表示或优化训练策略来增强模型的泛化能力。其次，本研究主要基于 Simon32/64 进行实验，未来可以扩展至其他轻量级密码(如 Speck、PRESENT)，验证 M3PODPR 格式的通用性。最后，随着神经密码分析技术的发展，还可以探索如何结合传统密码分析方法(如差分路径搜索)与神经网络，提高攻击的可解释性和效率。

基金项目

本研究得到了国家自然科学基金资助项目(62002184)、安徽省高校自然科学重点项目(2024AH050011)和香港狮子山网络安全实验室研究课题资助(LRL24017)的资助。

参考文献

[1] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L. (2015) The SIMON and SPECK Lightweight Block Ciphers. *Proceedings of the* 52*nd Annual Design Automation Conference*, San Francisco, 7-11 June 2015, 1-6. https://doi.org/10.1145/2744769.2747946

[2] 赵彦杰, 刘伟, 王伟, 等. 轻量级分组密码 SIMON 和 SPECK 的安全性分析[J]. 密码学报, 2017, 4(2): 75-85.

[3] 王旭姿. SIMON 类型轻量级分组密码算法的安全性分析研究[D]: [博士学位论文]. 北京: 中国科学院大学, 2021.

[4] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of Des-Like Cryptosystems. *Journal of Cryptology*, **4**, 3-72. https://doi.org/10.1007/bf00630563

[5] Matsui, M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T., Ed., *Advances in Cryptology—EUROCRYPT*'93, Springer, 386-397. https://doi.org/10.1007/3-540-48285-7_33

[6] 胡禹佳, 代政一, 孙兵. SIMON 算法的差分-线性密码分析[J]. 信息网络安全, 2022, 22(9): 63-75.

[7] Gohr, A. (2019) Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning. In: Boldyreva, A. and Micciancio, D., Eds., *Advances in Cryptology—CRYPTO* 2019, Springer, 150-179. https://doi.org/10.1007/978-3-030-26951-7_6

[8] Su, H., Zhu, X. and Ming, D. (2021) Polytopic Attack on Round-Reduced Simon32/64 Using Deep Learning. In: Wu, Y. and Yung, M., Eds., *Information Security and Cryptology*, Springer, 3-20. https://doi.org/10.1007/978-3-030-71852-7_1

[9] Hou, Z., Ren, J. and Chen, S. (2021) Improve Neural Distinguishers of SIMON and Speck. *Security and Communication Networks*, **2021**, Article ID: 9288229. https://doi.org/10.1155/2021/9288229

[10] Bao, Z., Guo, J., Liu, M., Ma, L. and Tu, Y. (2022) Enhancing Differential-Neural Cryptanalysis. In: Agrawal, S. and Lin, D., Eds., *Advances in Cryptology—ASIACRYPT* 2022, Springer, 318-347. https://doi.org/10.1007/978-3-031-22963-3_11

[11] Chen, Y., Shen, Y., Yu, H. and Yuan, S. (2022) A New Neural Distinguisher Considering Features Derived from Multiple Ciphertext Pairs. *The Computer Journal*, **66**, 1419-1433. https://doi.org/10.1093/comjnl/bxac019

[12] Zhang, L., Wang, Z. and Wang, B. (2024) Improving Differential-Neural Cryptanalysis. *IACR Communications in Cryptology*, **1**. https://doi.org/10.62056/ay11wa3y6

[13] He, K., Zhang, X., Ren, S. and Sun, J. (2016) Deep Residual Learning for Image Recognition. 2016 *IEEE Conference on Computer Vision and Pattern Recognition* (*CVPR*), Las Vegas, 27-30 June 2016, 770-778. https://doi.org/10.1109/cvpr.2016.90

[14] Szegedy, C., Liu, W., Jia, Y.Q., Sermanet, P., Reed, S., Anguelov, D., *et al*. (2015) Going Deeper with Convolutions. 2015 *IEEE Conference on Computer Vision and Pattern Recognition* (*CVPR*), Boston, 7-12 June 2015, 1-9. https://doi.org/10.1109/cvpr.2015.7298594

[15] Hu, J., Shen, L. and Sun, G. (2018) Squeeze-and-Excitation Networks. 2018 *IEEE*/*CVF Conference on Computer Vision and Pattern Recognition*, Salt Lake City, 18-23 June 2018, 7132-7141. https://doi.org/10.1109/cvpr.2018.00745

[16] Benamira, A., Gerault, D., Peyrin, T. and Tan, Q.Q. (2021) A Deeper Look at Machine Learning-Based Cryptanalysis. In: Canteaut, A. and Standaert, F.X., Eds., *Advances in Cryptology—EUROCRYPT* 2021, Springer, 805-835. https://doi.org/10.1007/978-3-030-77870-5_28