计算机科学
COMPUTER SCIENCE

# 基于深度学习的GIFT-128与ASCON算法神经差分区分器研究

苏睿韬，任炯炯，陈少真

引用本文

苏睿韬，任炯炯，陈少真. 基于深度学习的GIFT-128与ASCON算法神经差分区分器研究[J]. 计算机科学, 2026, 53(3): 453-458.

SU Ruitao, REN Jiongjiong, CHEN Shaozhen. Deep Learning-based Neural Differential Distinguishers for GIFT-128 and ASCON [J]. Computer Science, 2026, 53(3): 453-458.

---

**相似文章推荐（请使用火狐或 IE 浏览器查看文章）**

**Similar articles recommended (Please use Firefox or IE to view the article)**

基于多任务学习的眼科视频特征融合与多维画像

Multi-task Learning-based Ophthalmic Video Feature Fusion and Multi-dimensional Profiling

计算机科学, 2026, 53(3): 383-391. https://doi.org/10.11896/jsjkx.260200058

基于Transformer架构的RNA二级结构预测方法

Prediction Method of RNA Secondary Structure Based on Transformer Architecture

计算机科学, 2026, 53(3): 375-382. https://doi.org/10.11896/jsjkx.250100005

基于少量目标数据和深度学习的行人重识别方法

Pedestrian Re-identification Methods Based on Limited Target Data and Deep Learning

计算机科学, 2026, 53(3): 287-294. https://doi.org/10.11896/jsjkx.260100073

基于双分支融合与分段域适应迁移学习的疲劳驾驶检测

Fatigue Driving Detection Based on Dual-branch Fusion and Segmented Domain AdaptationTransfer Learning

计算机科学, 2026, 53(3): 78-87. https://doi.org/10.11896/jsjkx.250500025

聚焦边界和多尺度特征融合的脑卒中病灶分割

Boundary-focused Multi-scale Feature Fusion Network for Stroke Lesion Segmentation

计算机科学, 2026, 53(2): 264-272. https://doi.org/10.11896/jsjkx.250300137

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250600176

# 基于深度学习的 GIFT-128 与 ASCON 算法神经差分区分器研究

**苏睿韬　任炯炯　陈少真**
信息工程大学　郑州 450001
(suruitao01@163.com)

**摘　要**　差分分析是评估分组密码安全性的关键方法,通过追踪明文差分的传播以区分密码与随机置换。传统分析方法应对复杂算法时存在局限,而深度学习的特征提取优势为密码分析开辟了新路径。为实现分组密码的安全性评估,提出了一种融合传统差分分析与深度学习方法的神经差分区分器构造方法。在数据集构造方面,采用多密文对三元组输入格式,保留差分特征并捕捉跨密文对相关性。网络架构基于卷积神经网络并融合残差收缩网络,构建深度扩张结构及多尺度特征融合机制。在 GIFT-128 和 ASCON-PERMUTATION 算法上的实验表明:对于 GIFT-128 算法,其 6 轮、7 轮区分器的准确率最高可达 99.70%和 95.47%,分别提升了 9.30%和 13.09%;在 ASCON 的 4 轮分析中,准确率最高达到 53.54%。这证明了深度学习方法在密码安全性分析上的有效性。

**关键词**:深度学习;差分分析;分组密码;神经区分器; GIFT-128;ASCON
**中图分类号**　TN918

## Deep Learning-based Neural Differential Distinguishers for GIFT-128 and ASCON

SU Ruitao,REN Jiongjiong and CHEN Shaozhen
Information Engineering University,Zhengzhou 450001,China

**Abstract**　As a critical method for block cipher security evaluation,differential cryptanalysis distinguishes ciphers from random permutations by analyzing plaintext difference propagation during encryption. Traditional approaches struggle with complex cryptographic algorithms,while deep learning offers new cryptanalysis perspectives increasingly applied in recent years. To enhance the security evaluation of block ciphers,this paper proposes a neural differential distinguisher construction method that integrates traditional differential analysis with deep learning. For dataset construction,a triplet input format comprising multiple ciphertext pairs is adopted to preserve differential characteristics and capture cross-ciphertext-pair correlations. The network architecture builds upon Convolutional Neural Networks(CNNs) and incorporates residual shrinkage networks to form a deep expansion structure with a multi-scale feature fusion mechanism. Experiments on GIFT-128 and ASCON-PERMUTATION demonstrate significant improvements:For GIFT-128,the highest accuracy of 6-round and 7-round distinguishers reaches 99.70%(an improvement of 9.30%) and 95.47%(an improvement of 13.09%),respectively. For the 4-round analysis of ASCON,the highest accuracy achieves 53.54%. These results validate the effectiveness of the deep learning approach in cryptographic security analysis.

**Keywords**　Deep learning,Differential cryptanalysis,Block cipher,Neutral distinguisher,GIFT-128,ASCON

## 1　引言

随着大数据与人工智能技术的飞速发展,信息安全问题日益重要。作为保障信息安全的核心技术,密码学通过加密、认证和完整性保护等功能,为信息安全提供核心保障,确保数据在传输和存储中的机密性和可信度。分组密码因其高效性、可实现性和广泛适用性成为现代密码学的重要组成部分,在信息安全领域发挥重要作用。

差分分析[1]是对分组密码算法进行安全性分析的重要方法,其核心思想是通过分析明文差分(即两个明文的异或结果)在加密过程中的传播和变化,来寻找算法的潜在弱点。基于这种分析方法,推广得到了高阶差分分析[2]、不可能差分分析[3]、相关密钥差分分析[4]等多种分析方法,在算法分析中取得了许多重要的理论成果。

深度学习通过层次化信息处理从数据中提取特征进行决策。2019 年,Gohr[5]在 CRYPTO 上首次将深度学习与传统差分密码分析融合,针对 SPECK32/64 设计了深度残差网络(ResNet),构建了 8 轮神经差分区分器,其精度优于传统方法。这证明了深度学习应用于差分密码分析的价值,为该领域的研究开辟了新方向。与传统差分分析相同,基于深度

到稿日期:2025-06-24　返修日期:2025-10-25
基金项目:国家自然科学基金(62206312)
This work was supported by the National Natural Science Foundation of China(62206312).
通信作者:任炯炯(jiongjiong_fun@163.com)

学习的差分分析重点在于区分器的构造，区分器的精度越高，轮数越多，恢复密钥的复杂度越低，算法分析的结果越好。

2021 年，Chen 等[6]通过采用多组密文对作为神经网络训练样本，显著提升了 SPECK32/64 算法 5－7 轮神经差分区分器的精度。次年，Hou 等[7]将多输出差分纳入训练样本，进一步优化了 SPECK 与 SIMON 算法的神经差分区分器精度。2023 年，Lu 等[8]基于前两轮推断信息，成功构建了单密钥及相关密钥条件下的 SIMON 神经差分区分器，其准确率获得明显提升；同年，Bao 等[9]通过将神经网络输入设置为前轮输出的线性组合，有效提升了 SIMON32/64 算法区分器的精度。2024 年，Shen 等[10]提出了一种新模型，显著提升了针对 GIFT 与 ASCON 算法的神经区分器精度。Zhang 等[11]受 GoogleNet 架构启发，通过多尺度特征融合进一步增强了 SPECK 算法的区分器性能，凸显了该结构在密码分析中的有效性。Wang 等[12]基于差分分析和样本特征分析，通过用固定差分替代随机差分来生成负样本，有效提高了 SPECK 和 SIMON 算法网络区分器的准确率。此外，Seok 等[13]利用机器学习技术优化输入差分的选择，进一步提升了 SIMON 和 SPECK 算法的精准度。

尽管上述研究在特定算法上取得了显著进展，但其方法仍存在局限性——难以迁移至新型密码算法，且特征提取机制未充分挖掘密文间关联性。为突破这些限制并进一步提升区分器精度，本文融合传统差分分析与深度学习方法，提出新型神经差分区分器构造框架，对区分器的输入结构进行探究，针对两种结构算法提出了适配的数据集构造方法与专用网络架构设计，提取密文对深层相关特征，实现跨算法的高精度区分能力，增强方法的可解释性和对密码分析本质的观察。本文提出的神经差分区分器在 GIFT-128 与 ASCON 算法上实现全面性能突破，对于 GIFT-128 算法，6 轮 8 对密文区分器精度达 99.70%，7 轮 32 对密文精度达 95.47%，较文献[10]中最优值提升 28.85%。对于 ASCON 算法，4 轮 32 对密文精度提升至 53.54%，且在 8/16/32 对规模下实现稳定增长。这些结果验证了多密文对输入结构与残差收缩模块在深层特征提取中的有效性。

本文第 2 章概述 GIFT-128，ASCON-PERMUTATION 算法及相关基础知识；第 3 章提出一种神经差分区分器的构造方法；第 4 章和第 5 章基于上述方法分别构造 GIFT-128 算法和 ASCON-PERMUTATION 算法的神经差分区分器；最后总结全文并展望未来。

## 2 预备知识

### 2.1 GIFT-128 算法

GIFT-128 是由 Banik 等[14]设计的一种基于替换-置换网络(SPN)结构的轻量级分组密码，广泛应用于物联网(IoT)设备安全、嵌入式系统数据保护等场景。作为轻量级密码领域的代表算法，其设计被公认为是现代轻量级密码设计的典范。该算法提供 128 位分组长度与 128 位密钥长度，共迭代 40 轮加密操作。轮函数包含 3 个有序操作，即 SubCells，PermBits 和 AddRoundKey。

SubCells：通过可逆 4×4 S 盒实现非线性代换，对状态数据的每个 4 位进行混淆。

PermBits：对 32 位状态字实施不同的比特置换。

AddRoundKey：将轮密钥与状态进行异或，其中轮密钥由密钥状态中提取的两个 32 位段($U \| V$)构成。

### 2.2 ASCON-PERMUTATION 算法

Ascon 是由 Dobraunig 等[15]设计的基于置换的轻量级认证加密算法，采用海绵结构(Sponge Construction)实现数据加密与完整性保护的统一框架。作为 CAESAR 竞赛胜出算法及 NIST 轻量密码标准化项目最终候选方案，其设计被公认为是现代轻量密码安全性与效率平衡的标杆。Ascon 操作的状态大小为 320 位(由 5 个 64 位的字 $x_0,\cdots,x_4$ 组成)，状态寄存器为 $S=x_0 \| x_1 \| x_2 \| x_3 \| x_4$，其主要组成部分是一个 320 位的置换，通过不同的常量和轮数来实现。

与文献[10]相同，本文只考虑 320 位的置换，置换 $p$ 的每一轮包括常量加法 $pC$、替换层 $pS$ 和线性扩散层 $pL$ 这 3 个步骤。

常量加法 $pC$：在每一轮中，将轮常量 $cr$ 添加到状态寄存器字 $x_2$ 中，增加的常数根据轮数而变化。

替换层 $pS$：替换层 $pS$ 用一个 5 比特的 S 盒并行应用 64 次来更新状态。具体对应规则是：对于算法内部的 5 个 64 比特字 $x_0,x_1,x_2,x_3,x_4$，每个 S 盒独立处理这 5 个字在同一比特位置上的值，即第 $j$ 个 S 盒($0 \leqslant j < 64$)的输入比特为 $x_0[j],x_1[j],x_2[j],x_3[j],x_4[j]$，其中 $x_0$ 是最高有效位。

线性扩散层 $pL$：每个 64 比特寄存器字 $x_i$ 通过线性函数 $\sum_i(x_i)$ 进行扩散，即 $x_i \leftarrow \sum_i(x_i)$，$i=0,\cdots,4$。

$$x_0 \leftarrow \sum_0(x_0)=x_0 \oplus (x_0 ggg 19) \oplus (x_0 ggg 28)$$

$$x_1 \leftarrow \sum_1(x_1)=x_1 \oplus (x_1 ggg 61) \oplus (x_1 ggg 39)$$

$$x_2 \leftarrow \sum_2(x_2)=x_2 \oplus (x_2 ggg 1) \oplus (x_2 ggg 6)$$

$$x_3 \leftarrow \sum_3(x_3)=x_3 \oplus (x_3 ggg 10) \oplus (x_3 ggg 17)$$

$$x_4 \leftarrow \sum_4(x_4)=x_4 \oplus (x_4 ggg 7) \oplus (x_4 ggg 41)$$

其中，$x ggg i$ 表示将 64 比特字 $x$ 向右循环移位 $i$ 位。

### 2.3 差分分析

差分密码分析由 Biham 与 Shamir 提出，是一种基于选择明文攻击的密码分析方法。其核心在于研究迭代密码系统中，特定输入差分 $\Delta in$ 对输出差分 $\Delta out$ 的传播规律。该方法现已成为评估分组密码安全性的基准指标之一，其有效性依赖于高效的差分区分器构建。

**定义 1**(差分特征) 迭代分组密码的一条 $i$ 轮差分特征 $\Omega=(\beta_0,\beta_1,\cdots,\beta_{i-1},\beta_i)$ 是指，当输入对 $(X,X^*)$ 的差分值满足 $X \oplus X^*=\beta_0$，在 $i$ 轮加密过程中，中间状态 $(Y_j,Y_j^*)$ 的差分值满足 $Y_j \oplus Y_j^*=\beta_j$ ($1 \leqslant j \leqslant i$)，其中，$1 \leqslant i \leqslant i$。

**定义 2**(差分概率) 迭代分组密码的一条 $i$ 轮差分 $(\alpha,\beta)$ 所对应的概率 $DP(\alpha,\beta)$ 是指，在输入 $X$、轮密钥 $K_1,K_2,\cdots,K_i$ 取值独立且均匀分布的情形下，当输入对 $(X,X^*)$ 的差分值满足 $X \oplus X^*=\alpha$，经过 $i$ 轮加密后，输出对 $(Y_i,Y_i^*)$ 的差分值满足 $Y_i \oplus Y_i^*=\beta$ 的概率。

当发现 $r-1$ 轮差分特征的概率显著超过随机置换概率 $1/2^n$ 时，便构造一个 $r-1$ 轮的差分区分器。该区分器通过分析 $(\Delta in,\Delta out)$ 的联合分布模式实现两类判别：真实的 $r-1$ 轮加密与随机置换。随后利用该区分器，可以逐步恢复部分密

钥信息。差分区分器的概率越高,恢复密钥所需的数据量就越少;区分器覆盖的路径越长,攻击所需的计算资源就越少。

### 2.4 神经差分区分器

神经差分区分器通过深度学习实现密码数据的高效分类,其本质与图像识别、语音处理等领域的分类任务具有内在相似性。神经差分区分器[5]通过训练神经网络模型,精准区分真实密文对(由固定输入差分的明文对加密生成)与随机密文对(随机明文对加密产生),训练完成的区分器可用于密钥恢复攻击,其在区分准确率与攻击复杂度方面均优于传统方法。

训练数据集的构建遵循以下流程:

1)随机生成主密钥 $K$;

2)构造满足输入差分为 $\Delta in$ 的明文对($P$,$P^*$);

3)加密明文对($P$,$P^*$)生成密文对($C$,$C^*$)作为训练样本。

在神经网络的训练过程中,每个样本都被赋予一个标签 $Y$,取值为 0 或 1。值 1 表示数据是由输入差分为 $\Delta in$ 的明文对($P$,$P^*$)加密后所生成的,而值 0 表示数据是由随机对加密生成的。

区分器对输入的密文进行判断,如果认为密文是由固定差分生成,则输出 1,否则输出 0。

区分器的性能是指区分器正确识别正负样本的能力,以准确率为评价指标。当验证准确率大于 50% 的随机猜测概率时,该模型即被认定为是有效的神经差分区分器。高精度的区分器模型不仅能提升密钥恢复效率,还可显著降低攻击复杂度。Gohr 基于此方法成功恢复了 11 轮 SPECK32/64 算法的轮密钥,实证了该技术在密钥恢复攻击中的优越性。

## 3 神经差分区分器构造方法

深度学习模型在密码分析领域展现出显著优势,通过深度神经网络对密文数据进行特征学习和模式识别,可以更精准地捕捉输入差分所呈现的特定规律,从而构建出更完备的差分路径特征库。本章研究神经差分区分器的构造方法,其基本框架包括数据集构造、网络结构设置以及模型训练 3 个部分。

### 3.1 数据集构造

有监督学习是深度学习的一个重要分支,其核心是利用带有标签的训练数据集。在这个数据集中,每个样本都与一个标签相对应,而这个标签则代表了深度学习模型所期望的输出,对于优化神经网络参数起着至关重要的作用。因此,在构建神经差分区分器时,应充分考虑所选数据格式的多样性,并确保其能够全面涵盖所有潜在情况,从而有效提升区分器的性能。

在数据集构造阶段,选择采用多密文对差分结构的输入格式,即多密文输入下的($C\oplus C^*$,$C$,$C^*$)格式,具体构造方法如下。

首先,确定固定差分 $\Delta in$ 作为神经差分区分器的输入差分,设每个样本包含 $S$ 个密文对,对于每个样本,随机生成 $S$ 个与目标算法分组长度 $m$ 对齐的明文 $P$,共生成 $n$ 个样本。对于每个样本,将明文 $P$ 与 $\Delta in$ 进行异或,得到 $P^*$。随后,创建一个长度为 $n$ 的二元标签集合 $Y$,其中 $Y=1$ 表示有效差分对,$Y=0$ 表示随机噪声对。随后将 $Y$ 中元素与集合 $P^*$ 中的每组元素进行匹配,对于负样本($Y=0$ 的情况),将对应的 $P^*$ 替换为随机明文 $P^{**}$。

然后,使用目标加密算法加密明文对,得到密文对($C$,$C^*$),具体加密过程为:

$$\begin{cases} C=Encrypt(K,P) \\ C^*=Encrypt(K,P^*), & Y=1 \\ C^*=Encrypt(K,P^{**}), & Y=0 \end{cases}$$

最后,将每个密文对转化为三元组($C\oplus C^*$,$C$,$C^*$),其中 $C\oplus C^*$ 显式地保留差分特征。对于包含 $S$ 个密文对的样本,沿特征维度拼接 $S$ 个三元组,形成最终输入张量。

详细的数据集构造流程如图 1 所示。

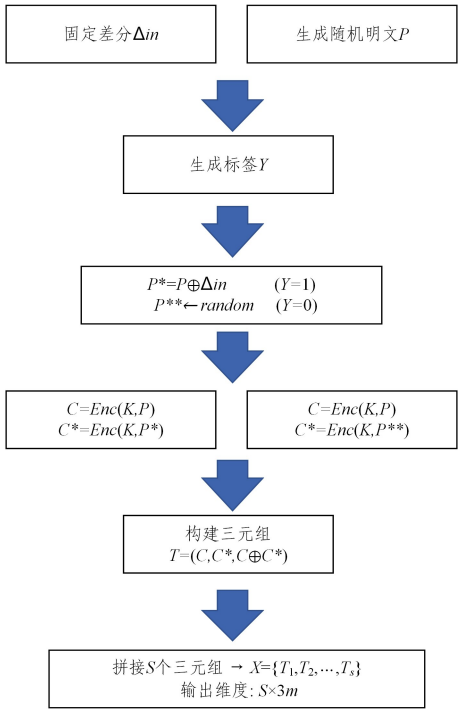



图 1 数据集构造流程

Fig. 1 Process of dataset construction

图 1 中包含 6 个主要模块,分别是样本初始化、标签生成、负样本处理、加密与数据生成、输入结构构造和最终输入张量形成。在样本初始化模块中,确定固定差分 $\Delta in$ 并生成随机明文 $P$;标签分配模块创建二元标签集合 $Y$;负样本处理模块将 $Y=0$ 的样本替换为随机明文 $P^{**}$;加密与数据生成模块根据标签 $Y$ 的值,使用目标算法加密得到密文对($C$,$C^*$);输入结构构造模块将密文对转化为三元组($C\oplus C^*$,$C$,$C^*$)。最后,沿特征维度拼接多个三元组形成最终输入张量,为神经差分区分器的训练提供高质量的数据基础。

数据集的具体结构如图 2 所示。

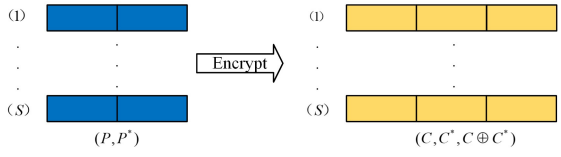



图 2 数据集结构

Fig. 2 Dataset format

通过该方法构造数据集，使得输入的样本不仅包含密文本身所具有的特征，还进一步体现出密文对之间的差分关系，增强模型对差分特征的敏感性。根据文献[16]中的结论，神经差分区分器的决策机制本质上依赖于密文对的差分分布特征，神经差分区分器本质上是在学习阶段构建密码差分分布表的高精度近似，并直接基于该信息分类密文对。这一结论揭示了在数据集构造中，显式加入密文差分信息的必要性。进一步，多对密文的拼接设计使模型能够捕捉密文对之间的相关性，使用多密文对输入的情况下，由于多个密文对对应同一标签，进一步聚合多个密文对的统计特征，降低了随机噪声的影响。因此，相较于单密文对的情况，多密文对输入的方差更小，达到了提升差分区分器精度的目的。

### 3.2 网络结构设置

Gohr 开创性地采用残差网络(ResNet)作为核心模型来构造神经差分区分器[5]。ResNet 通过残差连接机制有效缓解深层卷积神经网络中的梯度消失问题，显著提升了模型训练的稳定性与计算效率，最终实现分类准确度的提升。

本文采用改进的残差网络架构，其核心创新在于自适应阈值机制。该结构以输入数据维度为起点，经重塑层调整数据形状，形成适合后续卷积操作的特征序列。初始卷积层使用小尺寸卷积核对输入特征进行初步特征提取，并使用批量归一化(Batch Normalization)和 ReLU 激活函数增强特征表达能力。接着，网络通过两个额外的全连接层对初始卷积特征进行非线性映射，以提高模型的特征适应性，形成初始特征表示。

网络主体部分由多个残差收缩模块 RSB(Residual Shrinkage Block)构成，每个 RSB 模块包含两个卷积层、批量归一化和 ReLU 激活函数，用于深度特征提取。模块内部引入了软阈值化机制，通过计算残差路径的绝对值并结合全局平均池化、全连接层和缩放因子生成网络，动态调整特征权重，实现特征选择和噪声抑制。为了避免维度不匹配，当输入和输出通道数不一致时，网络采用 $1\times1$ 卷积对输入进行调整，确保残差连接的有效性。相较于针对图像处理领域的残差收缩网络，参数设定针对密码分析任务进行了适配，将输出通道数等关键维度统一调整为密码算法分组长度的整数倍，使网络结构与密码算法的输出长度精确对齐，增强了块内关联特征的学习能力。同时，完成了二维到一维的转换，形成面向密文数据流的块序列处理范式，不仅顺应了密文数据结构的特性，更大幅降低了参数量。

在模块堆叠后，网络通过展平层将多维特征映射转换为一维特征向量，随后利用全连接层逐步降低特征维度，最终输出预测结果。网络整体设计结合了残差学习和注意力机制的优势，既能有效缓解深层网络的梯度消失问题，又可通过软阈值化动态聚焦于重要特征，提升模型的表达能力和泛化性能。RSB-ResNet 的具体网络结构如图 3 所示。

训练参数设置方法如下：随机生成 $1\times10^7$ 个训练集样本和 $1\times10^6$ 个验证集样本。验证集仅用于评估模型泛化能力，不参与参数优化过程。通过预处理将原始数据转换为神经网络输入格式，数据集以 $1\times10^4$ 的批量大小进行分批训练，共执行 120 个训练周期。采用循环学习率策略，设置步长为 30 个周期，基础学习率为 $1\times10^{-4}$，最大学习率为 $2\times10^{-3}$。损失函数选用均方误差(MSE)，优化器采用 Adam 算法，并引入 L2 正则化(系数 $\lambda=1\times10^{-4}$)以控制模型复杂度。

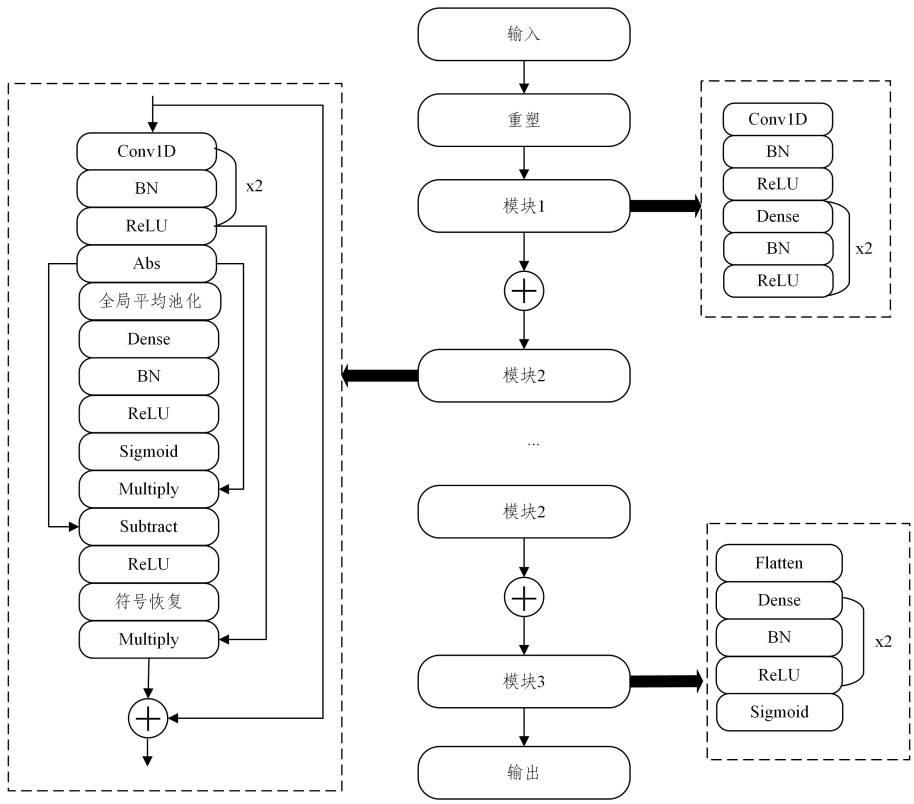



图 3 RSB-ResNet 网络结构

Fig. 3 Network structure of RSB-ResNet

为了进一步验证该网络结构的有效性，以 6 轮 GIFT-128 算法为例，选取文献［8］中所采用的 SE-ResNet 网络结构，将其作为对比模型与本文所提网络结构开展对照实验，在相同训练参数设置下的实验结果如表 1 所列。

表 1　6 轮 GIFT-128 不同网络结构下神经差分区分器的精度对比

Table 1　Accuracy comparison of neural differential distinguishers for 6-round GIFT-128 under different network architectures

| 密文对数 | $Acc/\%$ | |
|---|---|---|
| | RSB-ResNet | SE-ResNet |
| 1 | 86.36 | 78.83 |
| 2 | 93.88 | 87.61 |
| 4 | 97.93 | 95.04 |
| 8 | 99.70 | 98.90 |

实验表明，在相同密文对条件下，本文采用的 RSB-ResNet 网络结构有效提升了神经差分区分器的精度，验证了该网络结构的有效性。

## 4　GIFT-128 神经差分区分器应用

本章从数据集构造与网络结构选择两个方面，基于第 3 章的神经差分区分器构造方法，构造 GIFT-128 算法的神经差分区分器。

GIFT-128 算法基于 SPN 结构，其轮函数依次执行替换-置换操作并输出 128 比特密文，采用"密文对＋密文差分"的数据构造模式精准捕捉 S 盒非线性与比特置换规律。

针对 6 轮和 7 轮 GIFT-128 算法，结合算法的结构特征，算法的输入差分优先考虑低汉明重量的固定差分，在差分传播中可以减少非线性操作导致的不必要的活跃比特出现，这样有利于以更高的概率传播，分析更多的算法轮次。

综合上述原因，同时结合文献[10]中数据集构造方法，使用汉明重量为 1 的固定差分(0x00000000800000000000000000000000)进行实验。为探究密文对数量对模型性能的影响，进一步构建了包含不同规模密文对的数据集，并利用这些数据集训练神经差分区分器。

实验对比结果如表 2、表 3 和图 4 所示。

表 2　6 轮 GIFT-128 神经差分区分器精度对比

Table 2　Accuracy comparison of neural differential distinguishers for 6-round GIFT-128

| 密文对数 | $Acc/\%$ | | |
|---|---|---|---|
| | 本文算法 | 文献[10] | 文献[10] |
| 1 | **86.36** | 78.36 | 77.06 |
| 2 | **93.88** | 84.77 | 85.84 |
| 4 | 97.93 | 88.00 | 93.87 |
| 8 | 99.70 | 87.12 | 98.59 |

表 3　7 轮 GIFT-128 神经差分区分器精度对比

Table 3　Accuracy comparison of neural differential distinguishers for 7-round GIFT-128

| 密文对数 | $Acc/\%$ | | |
|---|---|---|---|
| | 本文算法 | 文献[10] | 文献[10] |
| 1 | 60.85 | 56.06 | 55.42 |
| 2 | **63.60** | 55.64 | 58.04 |
| 4 | **70.54** | 50.17 | 61.73 |
| 8 | **79.71** | 50.06 | 66.62 |
| 16 | **88.31** | | |
| 32 | **95.47** | | |

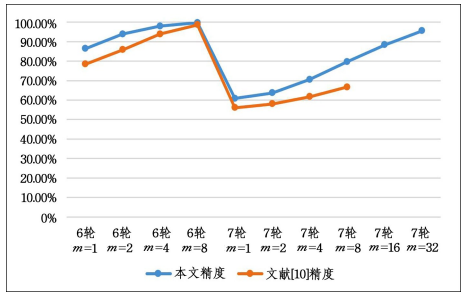



图 4　GIFT-128 神经差分区分器对比结果

Fig. 4　Comparative results of neural differential distinguishers for GIFT-128

综合分析表明，本文提出的神经差分区分器在 GIFT-128 算法的 6 轮与 7 轮分析中均实现全面性能突破，可以发现随着密文对数的增加，区分器的准确率也相应提升，且在相同密文对规模下，实验结果均优于文献[10]的结果。6 轮 8 对密文时，提出的区分器的准确率达到 99.70%，为当前轮数下最高，7 轮 8 对密文时，区分器准确率较文献[10]提升最大，达 13.09%。同时，本文首次在 7 轮算法中探索 16/32 对密文规模并取得有效区分。结合两种区分器构造架构的分析表明，新构造的数据格式能够更好地提取密文对间包含的特征，使得网络模型学习到更多隐形特征，进一步提升了区分器的准确率。

## 5　ASCON-PERMUTATION 神经差分区分器应用

针对 4 轮 ASCON-PERMUTATION 算法，考虑到算法独特的置换结构，算法输出为 320 比特的密文。为了更好地提取密文间的相关特征，采取密文对结合密文差分的模式。为了减少不必要的活跃比特出现，使得差分能够以较高的概率传递更多轮数，使用汉明重量低的输入差分。因此，在数据集构造阶段，通过对 64 位的寄存器 $x_0$ 使用差分(0x00000001)进行异或，构造汉明重量为 1 的固定差分，并分别构建了包含不同规模密文对的数据集。应用第 4 章中提出的网络结构，训练得到对应的神经差分区分器。具体对比结果如表 4 和图 5 所示。

表 4　ASCON-PERMUTATION 神经差分区分器精度对比

Table 4　Accuracy comparison of neural differential distinguishers for ASCON-PERMUTATION

| 密文对数 | $Acc/\%$ | | |
|---|---|---|---|
| | 本文算法 | 文献[10] | 文献[10] |
| 1 | 50.45 | 50.56 | 50.69 |
| 2 | 50.81 | 50.54 | 50.91 |
| 4 | 51.07 | 50.18 | 51.21 |
| 8 | 51.81 | 50.09 | 51.56 |
| 16 | 52.66 | 50.27 | 52.12 |
| 32 | 53.54 | 50.02 | 52.63 |

分析表 4 和图 5 的验结果可知，本文方法在 4 轮 ASCON-PERMUTATION 算法分析中实现了系统性性能优化。实验显示：随着密文对数增加，区分器精度呈现稳定上升趋势。在相同数据规模下，本文区分器获得的结果在 8 对及以上密文规模中均超越文献[10]的最高值。以 32 对密文为例，本文方法的准确率达 53.54%，提升 0.91%，且在 16 与 32 对

规模下创造了当前区分器最高准确率的记录。在密文对数低的情况下，本文方法的准确率与文献[10]基准相当，这表明本文方法在有限数据下的特征提取能力仍有提升空间。结合区分器架构分析，新数据格式在高数据规模下稳定增长，在8/16/32对输入密文的情况下，分别提升了0.25%/0.54%/0.91%，验证了其对深层特征捕捉的有效性。

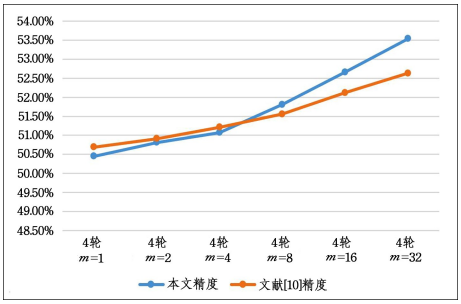



图5 ASCON-PERMUTATION神经差分区分器对比结果

Fig. 5 Comparative results of neural differential distinguishers for ASCON-PERMUTATION

**结束语** 本文提出一种融合多密文对输入结构与残差收缩网络的神经差分区分器构造方法，在GIFT-128和ASCON-PERMUTATION算法上实现了神经差分区分器的精度提升。通过采用$(C \oplus C^*, C, C^*)$多密文对输入格式，显式保留差分特征并捕捉跨密文对相关性；结合自适应残差收缩网络，提升了特征提取能力。

本文构建了一种集“数据构造-网络架构-训练策略”于一体的神经差分分析框架，为轻量级密码安全性评估提供了新范式，证实了深度学习在密码分析中的巨大潜力。当前工作仍存在一些局限性：深度学习模型的“黑盒”特性导致决策过程缺乏密码学机理层面的可解释性，框架的跨算法迁移能力尚未得到系统验证。未来工作将聚焦动态特征融合机制、跨算法迁移学习及可解释性增强，进一步拓展神经差分分析的应用深度与广度。

## 参 考 文 献

[1] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4: 3-72.

[2] LAI X J. Higher order derivatives and differential cryptanalysis [C]// Proceeding of the Symposium on Communication, Coding and Cryptography. Springer, 1994: 10-13.

[3] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]// Advances in Cryptology—EUROCRYPT'99. Berlin: Springer, 1999: 12-23.

[4] BIHAM E. New types of cryptanalytic attacks using related keys[J]. Journal of Cryptology, 1994, 7: 229-246.

[5] GOHR A. Improving attacks on round-reduced speck32/64 using deep learning [C] // Advances in Cryptology-CRYPTO 2019. 2019: 150-179.

[6] CHEN Y, YU H. A New Neural Distinguisher Model Considering Derived Features from Multiple Ciphertext Pairs[J]. The Computer Journal, 2023, 66(6): 1419-1433.

[7] HOU Z, REN J, CHEN S. Improve neural distinguisher for cryptanalysis[EB/OL]. https://eprint.iacr.org/2021/1017.

[8] LU J, LIU G, SUN B, et al. Improved(related-key) differential-based neural distinguishers for SIMON and SIMECK block ciphers[J]. The Computer Journal, 2024, 67(2): 537-547.

[9] BAO Z, LU J, YAO Y, et al. More insight on deep learning-aided cryptanalysis[C]// Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer, 2023: 436-467.

[10] SHEN D, SONG Y, LU Y, et al. Neural differential distinguishers for GIFT-128 and ASCON[J]. Journal of Information Secu-rity and Applications, 2024, 82: 103758.

[11] ZHANG L, WANG Z L, WANG B C. Improving Differential-Neural Cryptanalysis [J]. IACR Communications in Cryptology, 2024, 1(3): 13.

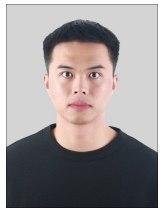
[12] WANG G, WANG G, SUN S. Investigating and enhancing the neural distinguisher for differential cryptanalysis [J]. IEICE Transactions on Information and Systems, 2024, 107: 1016-1028.

[13] SEOK B, LEE C. A novel approach to construct a good dataset for differential-neural cryptanalysis [J]. IEEE Transactions on Dependable and Secure Computing, 2024, 22: 246-262.

[14] BANIK S, PANDEY S K, PEYRIN T, et al. GIFT: A small present: Towards reaching the limit of lightweight encryption [C]// Proceedings of Cryptographic Hardware and Embedded Systems. Springer, 2017: 321-345.

[15] DOBRUNIG C, EICHLSEDER M, MENDEL F, et al. Ascon v1. 2: lightweight authenticated encryption and hashing [J]. Journal of Cryptology, 2021, 34: 1-42.

[16] BENAMIRA A, GERAULT D, PEYRIN T, et al. A Deeper Look at Machine Learning-Based Cryptanalysis[C]// Advances in Cryptology—EUROCRYPT 2021. Cham: Springer, 2021: 436-467.



**SU Ruitao**, born in 2001, postgraduate. His main research interest is analysis of block ciphers.

**REN Jiongjiong**, born in 1995, Ph.D. His main research interest is analysis of block ciphers.

（责任编辑：何杨）