

基于机器学习的分组密码结构识别

夏锐琪, 李曼曼, 陈少真

(信息工程大学网络空间安全学院, 河南 郑州 450001)

摘要: 加密算法的识别与区分是密码分析领域的重要组成部分, 是密钥恢复技术的前提条件之一, 随着人工智能技术的不断发展, 利用机器学习、神经网络等技术研究密码分析问题日趋成熟, 这为实现以加密算法为代表的密码体制识别技术提供了有效的思路与启发。通过研究机器学习的基本原理, 从理论和实验两个角度对 Feistel 和 SPN 结构的多种常见分组密码算法进行了识别实验, 解决了随机密钥条件下利用未知密文识别分组密码加密结构的问题。引入游程分布指标、特征分布函数和 KL 散度等概念, 通过分析两种分组密码结构加密后的密文特征分布, 推导随机密钥条件下两种结构密文游程分布表达式, 利用 KL 散度计算分布的差异性, 证明两种结构密文间存在差异性, 论证了实验的可行性; 根据理论结果, 建立了随机森林和 Adaboosting2 种机器学习模型, 对 12 种分组密码算法在随机密钥条件下全轮加密后的密文提取密文游程分布指标, 按照同种结构单一算法和同种结构混合算法两种标准对不同结构分组密码算法进行了识别。实验结果显示, 两组实验中对各个具体算法的结构识别准确率高于 80%, 较已有工作提高 40% 左右, 有效解决了随机密钥情况下分组密码结构识别问题, 严格证明了两种分组密码结构之间在密文扩散性、分布关系上确实存在可区分的差异性, 也为密码算法设计和安全性评估提供一定的参考。

关键词: 分组密码; 机器学习; 特征指标; 概率统计; 密数据识别

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023040

Identification on the structures of block ciphers using machine learning

XIA Ruiqi, LI Manman, CHEN Shaozhen

Institute of Cyberspace Security, Information Engineering University, Zhengzhou 450001, China

Abstract: Cryptographic identification is a critical aspect of cryptanalysis and a fundamental premise for key recovery. With the advancement of artificial intelligence, cryptanalysis based on machine learning has become increasingly mature, providing more effective methods and valuable insights for cryptographic identification. The distinguishability experiments were performed based on the Machine Learning to identify the structures of block

收稿日期: 2022-01-20; 修回日期: 2022-06-09

通信作者: 李曼曼, limanman15@163.com

基金项目: 河南省自然科学基金 (232300421394)

Foundation Item: The Natural Science Foundation of Henan Province (232300421394)

引用格式: 夏锐琪, 李曼曼, 陈少真. 基于机器学习的分组密码结构识别[J]. 网络与信息安全学报, 2023, 9(3): 79-89.

Citation Format: XIA R Q, LI M M, CHEN S Z. Identification on the structures of block ciphers using machine learning[J]. Chinese Journal of Network and Information Security, 2023, 9(3): 79-89.

ciphers in conditions of random keys. The identification of two structures of block ciphers from theoretical and experimental angles was studied. The differences of features in two structures' cipher texts have been deduced by introducing the runs distribution index, feature distribution functions, KL-divergence, etc. After completing the feasibility research, experiments to identify the structures of two block ciphers using two Machine Learning models and the runs distribution index were conducted. The experiments were divided into two groups: single algorithm group and mixture algorithms group. It is found that the accuracy of both groups are more than 80%, which is around 40% higher than former work. The problem of identifying the structures of Block Ciphers in the conditions of random keys is solved in detail. Meanwhile, differences between the two structures of block ciphers are verified, which can serve as a reference for the design of cryptography algorithms.

Keywords: block ciphers, machine learning, feature indices, probabilities and statistic, cryptography identification

0 引言

随着计算机和网络技术的发展,密码学在信息安全保护方面呈现重要的作用。实际工作中,恢复密钥和破解密文是密码分析者的主要工作目标,大数据时代数据量剧增,传统的分析方法已无法满足实际需求。得益于人工智能技术的发展,利用人工智能解决密码学问题取得了显著成效,受到广泛关注^[1]。

基于人工智能的密码分析工作分为密钥恢复、密码算法识别、模拟加密等多个方面。在密码分析中,分析者往往仅掌握密文信息,而如何恢复密钥也取决于具体加密算法,只有获得密文加密信息才能展开相关工作,因此识别密文加密算法是恢复密钥的前提。目前,利用机器学习识别密码算法是一种有效的分析手段,相关成果层出不穷。

1998年,Ramzan等^[2]使用一种初等的神经网络对几种标准密码算法进行尝试性识别实验,初步建立了密码算法识别的工作方法。随后,Pooja等^[3]通过比较自然语言的语素频率,对4种古典密码算法进行了区分。随机性指标公布后,Dileep等^[4]通过建立词包模型提取密文特征,对DES、Blowfish、AES等算法利用支持向量机和 K 近邻算法进行识别对比,但在非固定密钥条件下效果较差。Manjula等^[5]对包括公钥密码算法在内的多个密码算法利用C4.5模型在固定密钥下进行识别。通过提取8种不同的密文特征,实验准确率高于70%。随后,Mishra^[6]、Barbosa^[7]、Chou^[8]等进一步研究了多种机器学习密码算法识别问题,对各种类型的密码算法建立不同机器学习

模型进行实验,将识别准确率提高到接近100%。赵志诚^[9]、李洪超^[10]等在此基础上,将实验方案予以补充完善,改进识别模型,使得这项工作更加成熟。

随着深度学习的发展,利用深度神经网络技术对更复杂情况下的密码算法识别也取得了一定成果。Souza等^[11]通过建立一种神经网络模型,对小批量密文的AES算法进行了区分攻击,结果优于已知相关成果。Sandeep使用卷积神经网络等常用神经网络模型对Blowfish、AES等分组密码算法进行多种分段长度下的识别,取得较理想的实验结果^[12]。曹莉茹^[13]使用前馈神经网络、卷积神经网络等对包括公钥密码、古典密码在内的多种算法提取随机性指标特征进行识别,其识别查准率达到100%。

实际情况中,加密算法使用的密钥通常是不固定的,而随机密钥条件下的密码识别缺乏充足的实验分析,且识别效果较固定密钥条件差。因此,本文考查随机密钥条件下,利用机器学习识别两种常见的分组密码加密结构:代换-置换网络(SPN, substitution-permutation network)结构与Feistel结构。一方面,将研究对象适当推广,克服了识别一类给定范围密码算法的局限性与特殊性;另一方面,准确识别分组密码结构可为密码分析工作提供有力的支持,缩小实际分析中密文识别的范围,提高恢复密钥的效率等,具体工作思路描述如下。

引入密文游程分布指标、特征分布函数、相对熵等概念,推导两种结构密文的特征值分布函数,证明两种分组密码结构的密文存在差异性,从机器学习底层工作原理角度论证该工作的可行

性。基于可行性理论，在随机密钥条件下，建立两种机器学习算法（随机森林与 Adaboosting 模型），选择 12 种不同结构的分组密码算法进行识别。实验的准确率总体高于 80%，较已知工作提高 40% 左右。

1 相关工作

1.1 基本概念

基于机器学习的密码识别流程如图 1 所示。

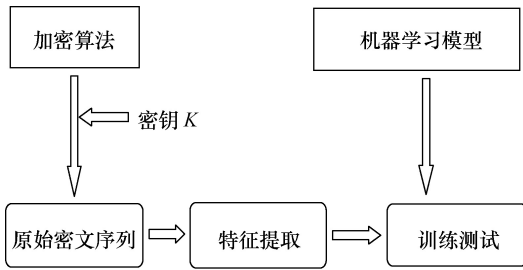


图 1 密码算法识别流程
Figure 1 The workflow of cryptography identification

特征提取与模型训练测试是密码识别实验中关键的步骤。随机性检测指标^[14]是一组由国家标准技术研究所（NIST, National Institute of Standard and Technology）公布用于检测密文序列随机性程度的测试指标，共 15 种，该指标常被用于提取待识别密文的特征值。为了区分两种分组密码结构在密文特征值分布上的差异性，给出简洁高效的实验方案，通过分析比较 15 种指标的定义等，发现游程分布指标能够较好地实现这一目标。

定义 1 （游程分布指标）^[14]。若长度为 n 的比特序列中连续出现 l 个 1 时，则称该序列有 l 长 1 游程。统计各个长度的游程个数 $x_i, i=1, 2, \dots, n$ ，形成游程分布指标 $(x_1, x_2, x_3, \dots, x_n)$ 。

当分析大量密文数据时，游程分布可用分布函数表示，密文序列游程分布函数定义如下。

定义 2 设密文序列 X 中长度为 i 的游程出现的概率为 $p_i, i=1, 2, \dots, n$ ，则 $F(i \leq l) = \sum_{i=1}^l p_i$ 为该密文序列游程分布函数。

汉明重量是密码学中的重要概念，被广泛用于研究密码算法的性质等。

定义 3 （汉明重量）^[15]。在比特序列 X 中，1 的个数记为 $w_H(X)$ ，称为 X 的汉明重量。

为保证安全性，要求分组密码结构的非线性组件等具有良好的密码学性质，无偏性（平衡性）保证非线性组件具有较强的扩散性和混淆性，定义如下。

定义 4 （无偏性）^[16]。对于非线性变换 $Y = S(X)$ ，若 Y 中 0,1 比特出现概率相同，则称非线性变换 S 是无偏的，也称为平衡性。

在信息编码学及机器学习原理中，KL (kullback-leibler) 散度能够较好地刻画训练数据的分布差异性，是区分两种分组密码结构密文特征的关键。若待分类数据集特征分布间 KL 散度有差距，机器学习模型就能很好地将不同分布区分开，分类效果就越好。KL 散度定义如下。

定义 5 （KL 散度）^[17]。设两个不同的随机变量分布函数为 $P(x)$ ， $Q(x)$ ，则它们的 KL 散度为

$$D(P \parallel Q) = \sum_{i=1}^n P(i) \log \frac{P(i)}{Q(i)} \quad (1)$$

当 $Q(i) = 0$ 时，该项取 0。KL 散度用于度量两种分布之间的差异性，散度值越大，则二者差异性越大。

1.2 机器学习模型简介

机器学习被广泛用于回归、分类等数据分析问题中，通过对数据集的训练和测试后，可以自动处理类似的问题。目前，以集成学习为代表的多学习器模型具有较强的工作能力，应用十分广泛。本文使用两种典型集成学习算法——随机森林算法^[18]与 Adaboosting 算法。

随机森林算法^[18]将多个决策树单元按照层级排列连接。每个决策树单元都是独立的，与前后层之间的单元相互连接。对输入的数据进行判断后传递给下一个单元，当判别信息传递到输出层时，随机森林将收集所有输出层单元的结果进行投票，取结果数值中的众数作为模型输出的判别结果。随机森林算法对大规模多维数据集的处理能力较好，具有很好的泛化性。随机森林模型如图 2 所示。

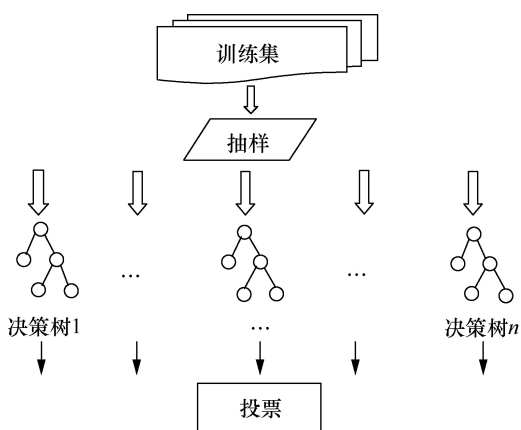


图 2 随机森林模型
Figure 2 Random forest model

Adaboosting 算法^[19]是另一种集成学习模型。与随机森林相比,二者结构上具有一定相似性,但 Adaboosting 算法侧重于对误分类数据的修正。每一次判断后,模型将对错结果,增大错误数据集的权重后再进行分类,直至完全正确或达到设定阈值的限度。同时,对分类能力较好的分类器将增加其分类工作量,而表现一般的则适当减少。Adaboosting 模型对多分类任务的效果较为理想,其工作稳定性较好,不易受异常数据的干扰,如图 3 所示。

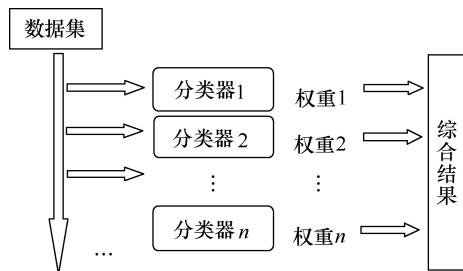


图 3 Adaboosting 模型
Figure 3 Adaboosting model

1.3 分组密码的结构及典型算法介绍

分组密码属于对称加密算法,其结构主要分为 SPN 结构与 Feistel 结构两种。SPN 结构含有非线性变换与线性置换层以及密钥混合等,非线性变换通常由 S 盒实现,线性置换层(P 置换层)由一个变换矩阵实现,如图 4 所示。Feistel 结构包含两个分支,包括密钥混合、非线性变换等操作,如图 5 所示。考虑到安全性,要求两种结构的非线性变换均满足无偏性。

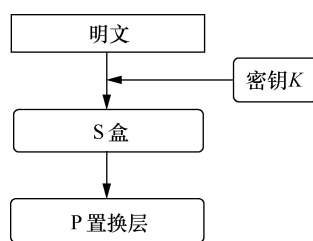


图 4 SPN 结构
Figure 4 The SPN structure

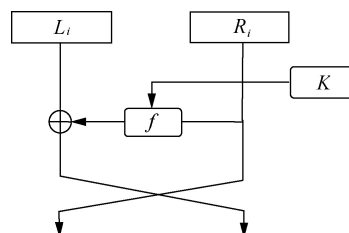


图 5 Feistel 结构
Figure 5 The Feistel structure

本文实验使用 12 种不同结构的分组密码^[20-30],包括 6 种国际标准分组密码和 6 种轻量级分组密码,具体如表 1 所示。

表 1 分组密码
Table 1 The block ciphers

SPN 结构	Feistel 结构
AES-128 ^[20]	DES ^[30]
Serpent-128 ^[21]	SIMON-64 ^[27]
SKINNY-64 ^[22]	Speck-32 ^[27]
PRESENT ^[23]	KASUMI ^[28]
Midori-64 ^[24]	Twofish ^[26]
ARIA-128 ^[25]	TWINE ^[29]

1.4 符号说明

文中使用的相关符号说明如下。

$\oplus$: 异或符号。

K_i : 第 i 轮子密钥。

k_{ij} : K_i 的第 i 比特。

$P(x|y)$: 事件 x, y 的条件概率。

$\binom{n}{m}$: n, m 的组合数。

$d(P, Q)$: 分布 $P(x)$ 与 $Q(x)$ 的 KL 散度。

2 分组密码结构识别可行性分析

由图 1 和机器学习原理可知,基于机器学习的算法结构识别实验可行性关键在于探究两种结

构算法的密文在特征分布上是否具有差异性。通过分析 15 种随机性指标，得到在游程分布指标下，两种分组密码结构的密文特征分布之间存在可区分性，具体分析过程如下。

令 A 为 SPN 结构的分组密码类， n_A 为分组长度， l_A 为密钥长度，加密轮数为 r_A ；令 B 为 Feistel 结构分组密码类， n_B 为分组长度， l_B 为密钥长度，加密轮数为 r_B ，密钥为随机选取；令 $n = \min\{n_A, n_B\}$ ， $l_K = \min\{l_A, l_B\}$ ，不要求 $n_A = n_B$ ， $l_A = l_B$ 或 $r_A = r_B$ ，即这种条件下结构差异性与分组长度或加密轮数等无关。

2.1 SPN 结构密文游程分布函数

定理 1 (SPN 结构密文游程分布)。随机密钥下 A 算法类密文游程分布函数为

$$F_A(i \leq l) = \sum_{j=1}^n \lambda_{ij} p_j \quad (2)$$

其中， $\lambda_{ij} > 0$ ， $p_j = \binom{n}{j} \left(\frac{1}{2}\right)^n$ 。

证明 设 A 算法明文为 X 。不妨先考虑首轮迭代，设明文与密钥 K_1 异或混合后状态为 X' ，则

$$X' = X \oplus K_1 \quad (3)$$

随机密钥 K 每比特 k_i 满足

$$P(k_i = 0) = P(k_i = 1) = \frac{1}{2} \quad (4)$$

故首轮子密钥 K_1 每比特满足

$$P(k_{1i} = 0) = P(k_{1i} = 1) = \frac{1}{2} \quad (5)$$

因此， X' 每比特 x'_i 满足

$$P(x'_i = 1) = P(x'_i = 0) = \frac{1}{2} \quad (6)$$

随后，进入非线性层 S 盒时，由 S 盒无偏性

$$P(S(x'_i) = 1 | x'_i = 0, 1) = P(S(x'_i) = 0 | x'_i = 0, 1) = \frac{1}{2} \quad (7)$$

$S(X')$ 中 l 长游程的概率为

$$P(i = l) = \binom{n}{l} \left(\frac{1}{2}\right)^n \quad (8)$$

简记为 p_l 。

进入线性变换层 θ 后，设 $\theta(S(X'))$ 为变换后

的状态，设其中 i 长游程概率为 p'_i ，由于 θ 为线性可逆的，线性变换前后各长度游程存在转移概率关系。

$$p'_i = \lambda_{ij} p_j \quad (9)$$

其中， $\lambda_{ij} > 0$ 。进一步地， $\theta(S(X'))$ 中各长度游程可被线性表示为

$$\begin{pmatrix} p'_1 \\ p'_2 \\ \dots \\ p'_{n-1} \\ p'_n \end{pmatrix} = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \dots & \lambda_{1n} \\ \lambda_{21} & \dots & \dots & \lambda_{2n} \\ \dots & \dots & \dots & \dots \\ \lambda_{n1} & \lambda_{n2} & \dots & \lambda_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ \dots \\ p_{n-1} \\ p_n \end{pmatrix} \quad (10)$$

其中， $\lambda_{ij} > 0$ ， $1 \leq i \leq n$ ， $1 \leq j \leq n$ 。

经过首轮加密， A 算法密文的游程分布特征函数可表示为

$$F(i \leq l) = \sum_{i=1}^l p'_i = \sum_{i=1}^l \sum_{j=1}^n \lambda_{ij} p_j \quad (11)$$

其中， $p_l = P(i = l) = \binom{n}{l} \left(\frac{1}{2}\right)^n$ ， $\lambda_{ij} > 0$ 。再由 SPN

结构迭代的重复性以及每轮随机子密钥混合，每轮密文游程分布函数与首轮相同，即

$$F_i = F(1 \leq i \leq r_A) \quad (12)$$

故 SPN 结构分组密码密文的游程分布函数为

$$F(i \leq l) = \sum_{i=1}^l p'_i = \sum_{i=1}^l \sum_{j=1}^n \lambda_{ij} p_j \quad (13)$$

其中， $p_j = P(i = j) = \binom{n}{j} \left(\frac{1}{2}\right)^n$ ， $\lambda_{ij} > 0$ 。

2.2 Feistel 结构密文游程分布函数

定理 2 (Feistel 结构密文游程分布)。随机密钥下 B 算法类密文游程分布函数为

$$F_B(i \leq l) = \sum_{i=1}^l p_i \quad (14)$$

其中， $p_i = \binom{n}{i} \left(\frac{1}{2}\right)^n$ 。

证明 Feistel 结构每轮加密分为两个分支，设每轮迭代前状态为 $X = (L_{i-1}, R_{i-1})$ ， $i \geq 1$ ，则连续

两轮迭代后

$$\begin{aligned} L_{i+1} &= L_{i-1} \oplus f(K_{i-1}, R_{i-1}) \\ R_{i+1} &= R_{i-1} \oplus f(K_i, R_i) = \\ R_{i-1} \oplus f(K_i, L_{i-1} \oplus f(K_i, R_{i-1})) \end{aligned} \quad (15)$$

其中, f 为非线性函数, K_i 为第 i 轮子密钥, f 可分为两种变换。

1) $f = f(R_i \oplus K_i)$, 则

$$P(x_i \oplus k_{ii} = 0) = P(x_i \oplus k_{ii} = 1) = \frac{1}{2} \quad (16)$$

由于 f 具有无偏性, 故

$$P(f(X, K) = 0) = P(f(X, K) = 1) = \frac{1}{2} \quad (17)$$

2) $f = f(R_i) \oplus K_i$, 则同理

$$P(f(R_i) \oplus K_i = 0) = P(f(R_i) \oplus K_i = 1) = \frac{1}{2} \quad (18)$$

综上, X 经过非线性变换 f 后每位取 0,1 的概率均为 $\frac{1}{2}$ 。

与左侧 L_i 异或后, 每比特取值概率保持不变。

$$P(f(R_i, K_i) \oplus L_i = 0) = P(f(R_i, K_i) \oplus L_i = 1) = \frac{1}{2} \quad (19)$$

故经过两轮连续迭代后, 输出状态中各长度游程的概率为

$$P(i = l) = \binom{n}{l} \left(\frac{1}{2}\right)^n \quad (20)$$

同理, 由 Feistel 结构的迭代重复性, $2r$ ($r=1, 2, \dots$) 轮迭代 Feistel 结构算法密文各长度游程概率不变。

因此, 全轮 Feistel 结构分组密码密文游程分布函数为

$$F_B(i \leq l) = \sum_{i=1}^l p_i \quad (21)$$

其中, $p_i = P(i = j) = \binom{n}{j} \left(\frac{1}{2}\right)^n$ 。

分析前两部分推导的随机密钥条件下 SPN 结构与 Feistel 结构分组密码的密文游程分布函数表达式。在此基础上, 研究二者之间是否存在 KL 散度上的差异性, 从而完成分组密码结构识别实验的可行性分析。

注: 定理 1 与定理 2 从理论角度得到两种不同结构分组密码在随机密钥条件下密文游程分布的一般形式。以 AES-128、DES、SIMON-32 这 3 种不同分组长度和结构的算法为例, 拟合它们在随机密钥条件下密文游程分布函数具体分布并计算其表达式。

图 6~图 8 为 3 种分组密码在随机密钥条件下 2^{20} 量级密文的游程分布 (为方便比较, 统一规定横坐标游程长度范围为 1~64)。

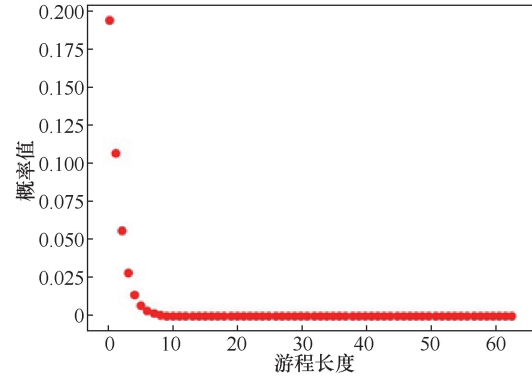


图 6 AES-128 游程分布
Figure 6 The runs' distribution of AES-128

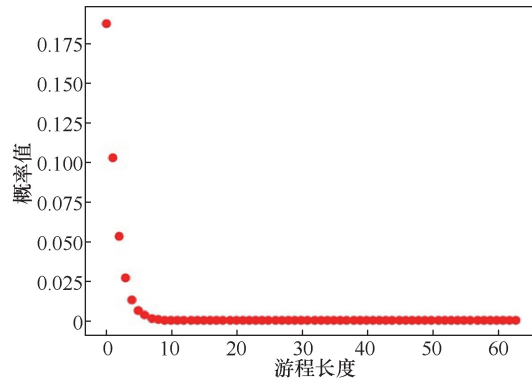


图 7 DES 游程分布
Figure 7 The runs' distribution of DES

根据分布图像使用插值法近似计算得到 AES-128 游程分布的表达式为

$$F_{\text{AES}} \approx \sum_{i=1}^{11} a_i n^i \quad (22)$$

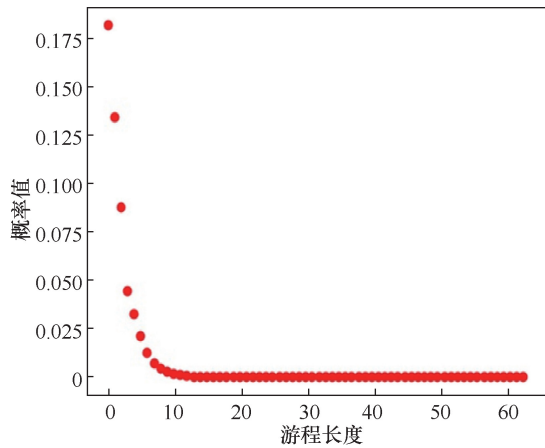


图8 SIMON-32 游程分布

Figure 8 The runs' distribution of SIMON-32

$(a_1, a_2, \dots, a_{12})^T = (0.485, -0.167, -0.333, 9.52 \times 10^{-2}, 0.337, -0.344, 0.156, -4.10 \times 10^{-2}, 6.73 \times 10^{-3}, -7.04 \times 10^{-4}, 4.5 \times 10^{-5})$ 。同理，DES 与 SIMON-32 的游程分布函数为

$$F_{\text{DES}} \approx \sum_{i=1}^{10} a_i n^i \quad (23)$$

$(a_1, a_2, \dots, a_{12})^T = (0.212, 2.87 \times 10^{-2}, -6.82 \times 10^{-2}, -2.33 \times 10^{-2}, 5.10 \times 10^{-2}, -2.92 \times 10^{-2}, 9.44 \times 10^{-3}, -1.95 \times 10^{-3}, 2.68 \times 10^{-4}, -2.43 \times 10^{-5})$

$$F_{\text{SIMON}} \approx \sum_{i=1}^{12} a_i n^i \quad (24)$$

$(a_1, a_2, \dots, a_{12})^T = (0.202, 2.39 \times 10^{-2}, -6.42 \times 10^{-2}, -1.22 \times 10^{-2}, 5.54 \times 10^{-2}, -4.00 \times 10^{-2}, 1.50 \times 10^{-2}, -3.44 \times 10^{-3}, 5.03 \times 10^{-4}, -4.74 \times 10^{-5}, 2.79 \times 10^{-6}, -9.37 \times 10^{-8})$

2.3 两种结构游程分布函数差异性

定理 3 任取分组密码算法 $A_1, A_2 \in A$, $B_0 \in B$, 则在随机密钥下, A_1, A_2, B_0 密文游程分布函数的 KL 散度满足

$$d(A_1, A_2) < d(A_1, B_0), d(A_1, A_2) < d(A_2, B_0) \quad (25)$$

证明 以 $d(A_1, A_2) < d(A_1, B_0)$ 为例, 等价于证明

$$|d(A_1, B_0) - d(A_1, A_2)| > 0 \quad (26)$$

由 KL 散度定义, $F_{A_1} = F_{A_2}$, 故

$$d(A_1, A_2) = 0 \quad (27)$$

$$|d(A_1, B_0) - d(A_1, A_2)| = |d(A_1, B_0)| = \left| \sum_{i=1}^l \sum_{j=1}^n \lambda_{ij} \binom{n}{j} \left(\frac{1}{2}\right)^n \log \frac{\sum_{j=1}^n \lambda_{ij} \binom{n}{j} \left(\frac{1}{2}\right)^n}{\binom{n}{j} \left(\frac{1}{2}\right)^n} \right| \quad (28)$$

由于 $\lambda_{ij} > 0$, 即存在某些 $i \in \{1, 2, \dots, n\}$ 使

$$\frac{\sum_{j=1}^n \lambda_{ij} \binom{n}{j} \left(\frac{1}{2}\right)^n}{\binom{n}{j} \left(\frac{1}{2}\right)^n} \neq 1 \quad (29)$$

即

$$\left| \sum_{i=1}^l \sum_{j=1}^n \lambda_{ij} \binom{n}{j} \left(\frac{1}{2}\right)^n \log \frac{\sum_{j=1}^n \lambda_{ij} \binom{n}{j} \left(\frac{1}{2}\right)^n}{\binom{n}{j} \left(\frac{1}{2}\right)^n} \right| > 0 \quad (30)$$

因此

$$|d(A_1, B_0) - d(A_1, A_2)| = |d(A_1, B_0)| > 0 \quad (31)$$

另一部分则同理可得。

因此, 在 KL 散度度量关系下, 两种结构的密文游程分布函数存在差异性, 具有可区分性。

通过推导 SPN 结构与 Feistel 结构两种算法在随机密钥条件下的密文游程分布函数表达式, 利用 KL 散度证明二者存在差异性。KL 散度是机器学习识别分类数据的重要依据, 待分类数据分布之间存在 KL 散度上的差距, 是利用机器学习算法进行识别的前提。

3 分组密码结构识别实验

由可行性分析结果可知, SPN 结构与 Feistel 结构算法在随机密钥条件下, 密文游程分布指标的分布存在区分性。因此, 通过提取游程分布特征使用机器学习训练识别两种结构算法是可行的。

实验建立两种机器学习模型 (随机森林算法与 Adaboosting 算法), 对 12 种不同结构的标准分组密码进行识别, 实验条件为随机密钥加密, 工作模式统一为 ECB (electronic codebook) 模式。

实验环境为：硬件配置 Intel Core i7，软件配置 Python3.7 程序设计语言，Scikit-learn 0.23.1。数据量为每个算法密文与密钥为 2^{21} 量级。

3.1 实验步骤

基于机器学习的分组密码结构识别按照图 1 中工作流程进行。为保证严谨性与一般性，实验总体分为两部分：单个算法结构识别和全部算法结构识别。

1) 随机生成密钥 K ，给定一组明文序列，对 12 种分组密码算法加密，得到原始密文数据 C ，任取长度 L ，对 C 进行分割，得到待提取特征的密文子序列 $\lfloor C/L \rfloor$ 个。

2) 对密文子序列中含有的游程进行统计，得到全部密文 C 中最长游程的长度，设为 r ，因此提取游程分布指标的维度为 r 。

3) 对每个密文子序列按照统一的维度 r ，提取游程分布特征，长度为 i 的游程个数为 x_i ，若该长度游程不存在则填 0。以此得到对应特征 $(x_1, x_2, \dots, x_r)$ 。在特征 $r+1$ 维标记其对应的数据标签，如表 2 所示。

表 2 数据标签
Table 2 The label of data

密文特征算法	标签
AES-128	S1
Serpent-128	S2
SKINNY-64	S3
PRESENT	S4
Midori-64	S5
ARIA-128	S6
DES	F1
SIMON-64	F2
Speck-32	F3
KASUMI	F4
Twofish	F5
TWINE	F6

4) 按任意两种结构算法为一组(如 S1 与 F3)将特征输入两种机器学习模型进行训练测试，通过调整模型参数，以 10 折交叉验证实验得到第一部分实验结果。即每组实验以 9:1 的比例轮流划定训练集与验证集，每组实验次数为 10 次，取 10 次实验结果的均值作为对模型精度的估计。

5) 将全部算法密文特征数据按结构划分为 2 类，SPN 结构算法(S1~S6)密文特征标签统一记为 S，Feistel 结构算法(F1~F6)统一记为 F。重复步骤 4)得到第二部分实验结果。

实验流程如图 9 所示。

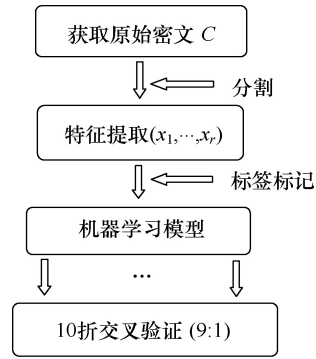


图 9 实验流程

Figure 9 The process of experiment

3.2 实验结果

由实验流程可知，第一部分取 12 种算法中任意 2 个不同结构算法特征为一组(如 S1 与 F2)，输入随机森林与 Adaboosting 算法进行训练测试，故每个模型共 36 组识别实验，输出结果取 2 种结构识别 10 次实验的平均准确率；实验第二部分将 12 种算法按结构分为 2 类，作为一组加密结构类型输入模型实验，输出结果也取平均准确率。实验输出结果可表示为

$$\text{Accuracy} = \frac{1}{10} \sum_{i=1}^{10} \text{accuracy}_i \quad (32)$$

其中，Accuracy 为输出准确率， accuracy_i 为每组每次实验结果准确率。

3.2.1 随机森林模型结果

随机森林模型准确率如表 3 所示。

表 3 随机森林模型准确率
Table 3 The accuracy of Random Forest model

—	F1	F2	F3	F4	F5	F6
S1	88.2%	96.7%	95.6%	91.2%	90.7%	92.3%
S2	93.4%	97.8%	98.9%	98.9%	99.0%	92.7%
S3	99.3%	97.8%	97.0%	94.5%	91.3%	90.8%
S4	91%	81.4%	86.2%	93.7%	95.7%	97.6%
S5	91.2%	97.3%	97.3%	88.5%	96.4%	95.9%
S6	91.1%	91.0%	89.2%	89.3%	92.7%	93.8%

由表3可知,随机密钥条件下,利用随机森林算法,识别两种不同结构分组密码准确率均高于80%,且大部分实验组的结果高于90%,说明利用游程分布特征作为识别对象,区分2种分组密码结构能够取得显著成果。

3.2.2 Adaboosting 模型结果

Adaboosting 模型准确率如表4所示。

表4 Adaboosting 模型准确率
Table 4 The accuracy of Adaboosting model

—	F1	F2	F3	F4	F5	F6
S1	92.2%	96.7%	95.6%	99%	99.7%	92.3%
S2	97.8%	97.8%	98.9%	98.9%	99.0%	92.7%
S3	99.3%	97.8%	97.0%	94.5%	91.3%	99.8%
S4	91%	95.2%	99.5%	93.7%	95.7%	97.6%
S5	91.2%	97.3%	97.3%	96.2%	96.4%	95.9%
S6	99.1%	88.9%	97.0%	99.3%	99.7%	99.8%

由表4可知,Adaboosting 模型整体效果优于随机森林模型。相同条件下,识别两种结构算法准确率总体高于90%,且大部分实验组结果接近100%。该模型识别效果理想,且稳定性较好。

3.2.3 整体结构识别结果

整体结构识别准确率如表5所示。

表5 整体结构识别准确率
Table 5 The accuracy of the whole structures

模型	准确率
随机森林模型	90.1%
Adaboosting 模型	92.9%

由表5可知,将同种结构算法密文特征作为整体的一组进行识别实验时,其区分效果依旧十分理想,平均准确率大于90%。具有同一种结构的不同分组密码,通过识别其密文游程分布能够统一地实现较好的区分效果。

3.3 实验分析

由3.2节实验结果可知,利用游程分布特征,在随机密钥下能够较理想地区分两种不同分组密码结构。第一部分实验中,在每个模型36组实验中,每组实验准确率均能超过80%,最高准确率达99.8%;第二部分实验中,将具有同种结构的全部算法作为一类进行识别,其准确率依然超过90%。与先前的相关工作^[4,5,9]相比,准确率

提高约40%,有效改进了复杂条件下区分分组密码密文的效果。

可行性分析中已证明两种结构的特征分布间存在KL散度上的差距,机器学习模型通过拟合待分类数据分布间的KL散度值,对数据集进行分类。因此,在KL散度上具有分布差异性的数据集能够更好地被机器学习模型处理并分类,实验很好地验证了这一结论。

另外,实验选取的分组密码较为广泛,除6种标准分组密码外,还包括PRESENT在内的6种轻量级分组密码,通过两部分实验前后对比,排除了因算法类型造成的结果特殊性。这进一步说明本文结论存在普遍性,适用范围较广。

从机器学习模型的角度分析,以集成学习为代表的多学习器算法(如随机森林、Adaboosting等)对分析多维数据具有良好的工作性能,拟合并区分数据特征分布能力强。针对在KL散度量下具有差异性的两种分组密码结构密文特征数据,其工作效果十分理想。

本文实验能够较好地识别SPN结构与Feistel结构两种较常见的加密结构。针对如广义Feistel结构、HPC结构等其他结构,将密码算法识别技术和本文的结构识别方法相结合,可以对未知密文给出更全面的识别结果,进而获取更全面的结构信息。关于识别更多类型密码算法结构的问题,将在下一步的工作中重点关注并尝试给出更加详细的解决方案。

4 结束语

本文研究了随机密钥条件下,基于密文游程分布特征的SPN结构与Feistel结构识别问题,主要工作可分为两个部分:①引入游程分布指标、特征分布函数以及KL散度等概念,从机器学习工作原理角度,推导两种结构密文特征分布函数表达式,利用KL散度证明两种结构密文特征存在差异性,给出详细的可行性分析;②利用随机森林与Adaboosting两种模型,对12种不同结构分组密码提取密文序列中的游程分布指标,通过识别密文游程分布指标区分两种分组密码结构。实验结果的识别准确率高于80%,与已知工作相

比,显著改进了实验的效果。本文工作为实际情况下密码分析者恢复密钥提供帮助,有效获取未知密文加密算法的结构信息,缩小密码算法识别范围,也为提高复杂条件下的密码算法识别效果提供了指导。

参考文献:

- [1] RIVEST R L. Cryptography and machine learning[C]//The International Conference on the Theory and Application of Cryptology. 1991: 427-439.
- [2] RAMZAN Z. On using neural networks to break cryptosystems[J]. Manuscript, 1998.
- [3] POOJA M. Classification of ciphers[R]. Indian Institute of Technology, Kanpur, 2001.
- [4] DILEEP A D, SEKHAR C C. Identification of block ciphers using support vector machines[C]//The 2006 IEEE International Joint Conference on Neural Network Proceedings. 2006: 2696-2701.
- [5] MANJULA R, ANITHA R. Identification of encryption algorithm using decision tree[C]//International Conference on Computer Science and Information Technology. 2011: 237-246.
- [6] MISHRA S, BHATTACHARJYA A. Pattern analysis of cipher text: a combined approach[C]//2013 International Conference on Recent Trends in Information Technology (ICRTIT). 2013: 393-398.
- [7] BARBOSA F, VIDAL A, MELLO F. Machine learning for cryptographic algorithm identification[J]. Journal of Information Security and Cryptography (Enigma), 2016, 3(1): 3-8.
- [8] CHOU J W, LIN S D, CHENG C M. On the effectiveness of using state-of-the-art machine learning techniques to launch cryptographic distinguishing attacks[C]//Proceedings of the 5th ACM Workshop on Security and Artificial Intelligence. 2012: 105-110.
- [9] 赵志诚. 基于机器学习的密码体制识别研究[D]. 郑州: 信息工程大学, 2018.
ZHAO Z C. The Research of Cryptosystem Recognition Scheme Based on Machine Learning[D]. Zhengzhou: Information Engineering University, 2018.
- [10] 李洪超. 基于密文特征的密码算法识别研究[D]. 西安: 西安电子科技大学, 2018.
LI H C. Cipher-text features based cipher system recognition[D]. Xi'an: Xidian University, 2018.
- [11] SOUZA W A R, TOMLINSON A. A distinguishing attack with a neural network[C]//2013 IEEE 13th International Conference on Data Mining Workshops. 2013: 154-161.
- [12] PAMIDIPARTHI S, VELAMPALLI S. Cryptographic algorithm identification using deep learning techniques[M]//Evolution in Computational Intelligence. 2021: 785-793.
- [13] 曹莉茹. 基于深度学习的密码算法识别研究[D]. 成都: 电子科技大学, 2021.
- CAO L R. A research of cryptographic algorithm recognition scheme based on machine learning[D]. Chengdu: University of Electronic Science and Technology of China, 2021.
- [14] ZAMAN J, GHOSH R. Review on fifteen statistical tests proposed by NIST[J]. Journal of Theoretical Physics and Cryptography, 2012, 1: 18-31.
- [15] HOFFSTEIN J, SILVERMAN J H. Random small hamming weight products with applications to cryptography[J]. Discrete Applied Mathematics, 2003, 130(1): 37-49.
- [16] WU C K, FENG D. Boolean function representation of S-boxes and boolean permutations[M]//Boolean Functions and Their Applications in Cryptography. 2016: 217-241.
- [17] COVER T M, THOMAS J A. Entropy, relative entropy and mutual information[J]. Elements of Information Theory, 1991, 2(1): 12-13.
- [18] BIAU G, SCORNET E. A random forest guided tour[J]. Test, 2016, 25(2): 197-227.
- [19] YING C, QI GUANG M, JIA Chen L, et al. Advance and prospects of AdaBoost algorithm[J]. Acta Automatica Sinica, 2013, 39(6): 745-758.
- [20] AKKAR M L, GIRAUD C. An implementation of DES and AES, secure against some attacks[C]//International Workshop on Cryptographic Hardware and Embedded Systems. 2001: 309-318.
- [21] BIHAM E, ANDERSON R, KNUDSEN L. Serpent: a new block cipher proposal[C]//International Workshop on Fast Software Encryption. 1998: 222-238.
- [22] LIU G, GHOSH M, SONG L. Security analysis of SKINNY under related-tweakey settings[J]. Cryptology ePrint Archive, 2016.
- [23] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: an ultra-lightweight block cipher[C]//International Workshop on Cryptographic Hardware and Embedded Systems. 2007: 450-466.
- [24] BANIK S, BOGDANOV A, ISOBE T, et al. Midori: a block cipher for low energy[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2015: 411-436.
- [25] PARK J, YUN Y, KIM Y D, et al. Design and implementation of ARIA cryptic algorithm[J]. Journal of the Institute of Electronics Engineers of Korea SD, 2005, 42(4): 29-36.
- [26] SCHNEIER B. The Twofish encryption algorithm[J]. Dr. Dobbs's Journal: Software Tools for the Professional Programmer, 1998, 23(12): 30-34.
- [27] BEAULIEU R, SHORS D, SMITH J, et al. The SIMON and SPECK lightweight block ciphers[C]//Proceedings of the 52nd Annual Design Automation Conference. 2015: 1-6.
- [28] HALAGALI B P, DESAI V V. Implementation of chaos based cryptography in kasumi block cipher[C]//2018 International Conference on Communication and Signal Processing (ICCSPP). 2018: 165-169.
- [29] SUZAKI T, MINEMATSU K, MORIOKA S, et al. Twine: a

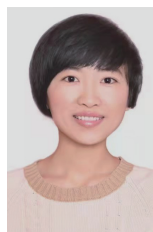
lightweight, versatile block cipher[C]//ECRYPT Workshop on Lightweight Cryptography. 2011, 2011.

- [30] THAKUR J, KUMAR N. DES, AES and blowfish: symmetric key cryptography algorithms simulation based performance analysis[J]. International Journal of Emerging Technology and Advanced Engineering, 2011, 1(2): 6-12.

[作者简介]



夏锐琪（1997-），男，江苏宝应人，信息工程大学硕士生，主要研究方向为分组密码安全性分析。



李曼曼（1986-），女，河南开封人，信息工程大学讲师，主要研究方向为分组密码安全性分析。



陈少真（1967-），女，江苏无锡人，信息工程大学教授、博士生导师，主要研究方向为分组密码安全性分析。