Software Engineering and Applications 软件工程与应用, 2023, 12(1), 45-50
Published Online February 2023 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2023.121005

Hans汉斯

基于差分分布表的密码分析方法研究

罗　昊，王心怡，李　晶

哈尔滨师范大学计算机科学与信息工程学院，黑龙江 哈尔滨

收稿日期：2023年1月9日；录用日期：2023年2月9日；发布日期：2023年2月16日

摘　要

随着5G、边缘计算、雾计算等前沿技术的快速发展，大量的敏感信息由物联网设备存储、处理和发送，数据传输安全性由此面临巨大的挑战。而实现安全可靠的传输必须有一套优良的分组密码算法作为基础，差分分布表(Differential Distribution Table, DDT)因其在设计、修改和攻击轻量级分组密码等方面的优势，逐渐成为研究的热点。本文首先介绍了差分分布表的理论构建基础。然后，根据应用场景不同分别从Feistel、SPN、ARX三种结构进行细致的划分，讨论了差分分布表在密码算法安全性分析中的重要性。最后，展望差分分布表DDT在未来的研究方向，为后续研究提供参考借鉴。

关键词

分组密码，差分分布表，安全性分析

Research on Cryptanalysis Method Based on Differential Distribution Table

Hao Luo, Xinyi Wang, Jing Li

College of Computer Science and Information Engineering, Harbin Normal University, Harbin Heilongjiang

Received: Jan. 9th, 2023; accepted: Feb. 9th, 2023; published: Feb. 16th, 2023

Abstract

With the rapid development of cutting-edge technologies such as 5G, edge computing, and fog computing, a large amount of sensitive information is stored, processed, and sent by IoT devices, and data transmission security is therefore facing huge challenges. To achieve safe and reliable transmission, a set of excellent block cipher algorithms must be used as the basis. Differential Distribution Table (DDT) has gradually become a research hotspot due to its advantages in designing, modifying and attacking lightweight block ciphers. This paper analyzes the common attack methods of block ciphers based on differential distribution table DDT. First, the theoretical founda-

文章引用: 罗昊, 王心怡, 李晶. 基于差分分布表的密码分析方法研究[J]. 软件工程与应用, 2023, 12(1): 45-50.
DOI: 10.12677/sea.2023.121005

tion of the differential distribution table is introduced. Secondly, according to different application scenarios, the three structures of Feistel, SPN, and ARX are carefully divided, and the importance of differential distribution tables in the security analysis of cryptographic algorithms is discussed. Finally, the future research direction of differential distribution table DDT is prospected, which provides reference for follow-up research.

Keywords

Block Cipher, Differential Distribution Table, Security Analysis

1. 引言

随着无线传感器和物联网技术的普及和发展，数据安全问题应运而生。分组密码算法作为保护数据安全的一种重要手段，广泛应用在数据加密、消息认证和数字签名等领域，如保护个人、政府和军队之间的通信数据安全，免遭黑客窃听、篡改、伪造、抵赖[1]等。近年来，分组密码算法的安全性分析更是科研人员比较感兴趣的研究方向，攻击者可以通过改进现有的攻击方法破解这些分组密码，而研究人员的目标则是如何提高数据传输中实现加密算法的稳定性[2]。评估轻量级分组密码算法安全性能的方法有很多，最常见的是差分分析和线性分析，在大多数的差分密码分析中，构建差分分布表 DDT 是必不可少的一步。因此，在研究分组密码算法的安全性分析时，通常使用差分分布表来检测所构建的分组密码 S 盒的状态，以提高密码算法安全性分析的效率[3]。与此同时，也有很多研究提出了基于不同的方式来提高抵抗差分攻击的能力，以达到更快地恢复分组密码密钥的目的[4]。

差分分布表的首次出现是由以色列密码学家 Biham 和 Shamir 在 1990 年提出的 DES 类密码的差分密码分析方法[5]。随后，我国学者来学嘉和外国学者 James L. Massey、Sean Murphy 在 1991 年共同提出了马尔可夫密码的思想[6]，对 Biham 和 Shamir 的差分分布表作了新的补充。1997 年，自从美国国家安全局(NIST)在全球范围内公开征集 AES 算法[7]以来，有关差分分析的文献层出不穷，差分分布表作为研究迭代型分组密码安全性的最有效的方法之一，在差分分析中起到了重要作用。相比于传统方法，差分分布表在研究 S 盒差分分布的不均衡性上有优势，能够更快速地得到高概率的高轮差分特征及差分特征概率，因此分组密码差分分析的研究大多是以差分分布表为基础展开。

本文首先介绍了差分分布表的理论构建基础，然后分别介绍了差分分布表在分组密码常见的三种结构 Feistel、SPN 和 ARX 上的应用。最后，给出了差分分布表的研究热点和未来发展方向。

2. 差分分布表的构建

差分分布表 DDT 主要适用于基于差分分析原理的密码算法安全性分析中，具体细分的话，可分别适用于：差分分析、高阶差分分析、截断差分分析、不可能差分分析和飞去来器攻击等。而后者都是差分分析的变体，所以要想了解差分分布表 DDT 的构建，首先要介绍最基本的差分分析原理。

2.1. 差分分析原理

差分分析是一种选择明文攻击，由 Biham 与 Shamir 在密码学顶会 CRYPTO 1990 会议上首次提出[5]，

是分组密码最常用的分析方法之一。

差分分析具体实现原理如图 1 所示，对于给定的一组输入明文$\left(X,X^*\right)$，其中$X,X^*\in\{0,1\}^n$，二者的输入差分值记为$\Delta_1=X\oplus X^*$。经过加密后所对应的输出密文记为$\left(Y,Y^*\right)$，二者的输出差分值记为$\Delta_2=Y\oplus Y^*$，其中$Y,Y^*\in\{0,1\}^n$。差分分析的基本思想可以理解为：通过分析特定的明文差分值Δ_1与对应的密文差分值Δ_2之间的关系来获得概率最高的密钥。

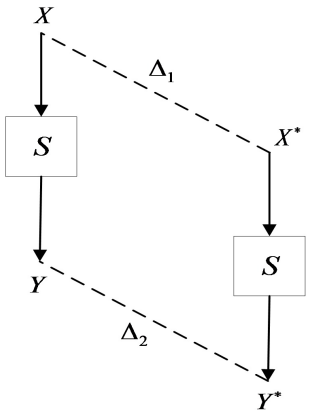

Figure 1. Principle of differential analysis
图 1. 差分分析原理

2.2. 差分分布表的理论基础

对于给定的分组密码执行差分攻击，攻击者需从明文和密文中寻找每一个可能提取的差分特征，用于描述明文和密文之间的关系。假设S是属于有限域$\mathbb{F}_2^n$的一种映射，对于任一给定结构的输入差分Δ_1和输出差分Δ_2，其中$\Delta_1,\Delta_2\in\mathbb{F}_2^n$，根据异或运算的特殊性质，满足：

$$DDT\left(\Delta_1,\Delta_2\right)=\#\left\{x\in\mathbb{F}_2^n:S\left(x\right)\oplus S\left(x\oplus\Delta_1\right)=\Delta_2\right\} \tag{1}$$

则可生成一个差分分布表 DDT [8]。该表包含经过 S 盒后的所有输入差分与输出差分的可能。其中表中每一列表示输入差分，每一行表示输出差分。表中的交汇处的数值表示给定输入差分，对应的输出差分所出现的次数。表中的最大值用于计算在作为密钥恢复阶段的加密过程中使用的预期密钥的概率。因此，差分分布表 DDT 可用于恢复加密密钥或者可以通过降低概率值来提升分组密码抵抗差分攻击的能力。

3. 差分分布表 DDT 的适用场景

在最近几年的文献中，有许多关于差分分布表 DDT 在密码算法安全性分析上应用的研究。2018 年 Sehrawat [9]等人发表了一篇关于轻量级分组密码应用在物联网(IoT)等资源受限设备上的综述，主要介绍了一些常见的评估分组密码算法性能的安全性分析方法，其中有一些涉及到 DDT 在密码安全性分析和重构分组密码等方面的应用。同年，Dey [10]等人提出了两种方法来分析 S 盒之间的关系，其中一种方法是基于差分分布表 DDT 的差分分析。2020 年，Tentu [11]等人总结了最近出现的一些密码分析技术和攻击方法，其中一些图解所描述的攻击，正是基于差分分布表 DDT 的差分分析。本章主要从差分分布表 DDT 在轻量级分组密码算法最常用的三种结构 Feistel 结构、SPN 结构、ARX 结构上的应用进行研究。

3.1. Feistal 结构中差分分布表的研究

2018 年，Dehnavi [12]等人给出了一种确定轻量级分组密码 SIMON 和 SPECK 的差分－线性特征的

方法。通过修改差分－线性特征，提高这两种算法的安全性。同时，作者利用差分分布表 DDT 对两种算法进行差分特征识别和概率计算。结果表明，该方法能有效地提高 SIMON 和 SPECK 算法抵抗差分攻击和线性攻击的能力。2019 年，Dunkelman [13]等人发现，根据原始密钥 E 分离出的两个子密钥 E_0 和 E_1 之间存在显著相关性的特点，通过使用傅里叶变换可以快速构建差分－线性连接表(DLCT)，并以 DLCT 表结果为标准选择 E_0 中的差分特征和 E_1 中的线性近似，最终提出了一种差分－线性攻击的混合攻击方法。此外，通过将 DLCT 与 DDT 结合，改进了之前的攻击方法，实现了对 ICEPOLE 算法和 8 轮 DES 算法的差分－线性攻击。

2022 年，Fan [14]等人提出了一种对 ANU-II 算法的改进，ANU-II 是一种具有 Feistel 结构的超轻量级的分组密码，作者从差分分布表 DDT 中列出所有可能的差分传播特征，并结合混合整数线性规划 MILP 的内容，最终仅使用几对明文和 $2^{62.4}$ 个全轮加密就完成了密钥恢复，证明了标准的 ANU-II 算法是不安全的。同年，Teh [15]等人使用差分分布表 DDT 来提取 WARP 算法的特征，成功建立一个有效的区分器，最终实现了基于高概率差分特征的飞去来器攻击，提高了恢复密钥的能力。同年，Zhang [16]等人利用不可能差分攻击评估了轻量级分组密码 μ^2 的安全性，通过差分分布表 DDT 来计算密码的差分特征概率，选取最高概率差分并与中间相错技术相结合，构造了最长至 7 轮的不可能差分区分器，并实现了 μ^2 算法的 10 轮不可能差分攻击。实验结果表明，μ^2 算法若想抵抗不可能差分分析，迭代轮数至少要大于 10 轮。

3.2. SPN 结构中差分分布表的研究

2018 年，Zhang [17]等人给出了对 SKINNY 算法的差分密码分析，首先通过建立 DDT 表，使用混合线性整数规划 MILP 确定了不同轮数中活跃的 S 盒数目。最后根据差分特征结果表明，轻量级分组密码算法 SKINNY-64/192 能抵抗 11 轮差分攻击。2019 年，Cao [18]等人提出了一种密码分析方法来评估不同分组大小的 GIFT 算法的性能，使用差分分布表 DDT 方法提取了 GIFT-64 和 GIFT-128 的差分特征概率，并用 MILP 进行分析。实验结果表明，与其他密码分析方法相比，引入差分分布表 DDT 可以更好地提升密钥恢复概率。2020 年，Ji [19]等人使用飞去来器攻击和矩形攻击来评估 GIFT 算法在恢复单个密钥和相关密钥方面的性能。而差分分布表 DDT 在该文献中主要用于从提取的密码特征中确定概率。结果表明，这两种攻击的复杂性和轮数的增加都减少了两种 GIFT 算法攻击所需猜测的密钥数量。

2021 年，Kousalya [20]等人根据 S 盒结构设计的差分特性，对现有密码进行了差分密码分析，提出了一种动态 S 盒设计，并通过实现差分分布表 DDT，对现有结构的活跃 S 盒数目进行了评估。实验结果表明，活跃的 S 盒数目增加有效提高了 PRESENT 算法的安全性。2022 年，Hu [21]等人给出了一种通过实现 DDT 求所有不可能差分的方法。该方法的基本思想是找出给定的基于 SPN 的 64 bit 分组密码的输入和输出之间的差分。利用混合整数线性规划 MILP 模型，将差分对分成若干小组，产生一个可能的差集。通过剔除不存在的不可能差分组，减小了搜索空间，并成功实现在 SKINNY-64 算法上。实验结果表明，对于 CRAFT、GIFT 等分组长度比较大的算法，该方法具有较高的性能。

3.3. ARX 结构中差分分布表的研究

2018 年，Dwivedi [22]等人用嵌套蒙特卡罗方法实现了部分 DDT 的概率(PDDT)，进而寻找合理的路径，并评估 ARX 结构中 LEA 算法的性能。具体做法是将一条较长的差分特征分割为两个短的差分特征，从而减少搜索空间。实验结果表明，差分分布表 DDT 可以减少 LEA 算法在 9 轮后的搜索空间。

2020 年，Liu [23]等人提出了移位相关差分分布表(CDDT)的概念，给出了一种寻找所有可能的输出差分的方法，可以在 ARX 密码中找到最优的差分轨迹。实验结果表明，所提出的差分分布表方法可以将 HIGHT 算法的最佳差分轨迹提高到 10 轮，并分别找到了 10 轮 SPECK32 算法、12 轮 SPECK48 算法、

16 轮 SPECK64 算法、8 轮 SPECK96 算法和 8 轮 SPECK128 算法的最佳差分轨迹。

2021 年，Benamira [24]等人提供了一种基于机器学习的寻找区分器方法，研究发现神经区分器通常依赖于密文对的差分分布，通过在学习阶段内在地构建一个非常好的差分分布表(DDT)的近似值，并使用该信息直接对密文对进行分类。最终，在保障区分器精度和效率的同时，成功构建了一个基于纯密码分析的 SPECK 算法区分器。

2022 年，Pal [25]等人提出了一种基于差分特征的深度学习模型，获得了以 ARX 为基础结构的 HIGHT、LEA 和 SPARX 算法的深度学习区分器。在模型训练阶段，使用 DNN 模型实现了差分分布表，该模型的目标是提高所寻找区分器的轮数。结果表明，该模型将 HIGHT 算法区分器轮数提高到 14 轮，LEA 算法提高到 13 轮，SPARX 算法提高到 11 轮。

4. 结论与展望

差分分布表是评估轻量级分组密码算法安全性的重要模块之一，在 Feistel、SPN、ARX 等分组密码结构中均有所应用。同时，差分分布表 DDT 在提高分组密码算法抵抗差分攻击的稳定性、提升所构建区分器的轮数、改进现有攻击方法和实现新提出的攻击方法等方面均有较好的理论基础支撑。此外，差分分布表 DDT 所提供的差分特性，不仅可以允许密码设计者通过修改 S 盒结构或增加循环轮数来提高其密码的安全性，还有助于寻找最短差分路径和活跃的 S 盒数目，而这些活跃 S 盒数我们可以建议密码设计者对其进行修改和重新设计。

展望差分分布表 DDT 在未来研究方向，主要可以归为以下 3 个方面。

第一，由于差分分布表 DDT 提供的差分特性是密码设计的基础。那么设计者是否可以通过 DDT 预估新密码所需的循环轮数以达到足够安全，或者是否可用于重新评估并修改算法的设计规范，提高与新国际标准的兼容性。

第二，差分分布表 DDT 能否可以与其他函数模型一起使用，并构建可以恢复密钥的随机性的区分器，以实现更佳的差分攻击。

第三，差分分布表 DDT 如何与深度学习等机器算法更好地融合，实现密码算法的自动化破译。

基金项目

哈尔滨师范大学研究生培养质量提升工程“新工科背景下创新创业型研究生多维培养模式的研究——以网络安全方向研究生培养为例”和哈尔滨师范大学本科专业人才培养方案研究改革专项(XJGRYK2022012)。

参考文献

[1] 罗守山. 密码学与信息安全技术[M]. 北京: 北京邮电大学出版社, 2009: 45-50.

[2] Lee, T.R., *et al*. (2021) Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes. *IEEE Access*, **9**, 134052-134064. https://doi.org/10.1109/ACCESS.2021.3116468

[3] Bagane, P.A. and Sirbi, K. (2020) Bibliometric Survey for Cryptanalysis of Block Ciphers towards Cyber Security. *Library Philosophy and Practice*, 1-18.

[4] Guo, H., Sun, S., Shi, D., Sun, L., Sun, Y., Hu, L. and Wang, M. (2020) Differential Attacks on CRAFT Exploiting the Involutory s-Boxes and Tweak Additions. *IACR Transactions on Symmetric Cryptology*, **2020**, 119-151. https://doi.org/10.46586/tosc.v2020.i3.119-151

[5] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of DES-Like Cryptosystems. *Journal of Cryptology*, **4**, 3-72. https://doi.org/10.1007/BF00630563

[6] Lai, X., Massey, J.L. and Murphy, S. (1991) Markov Ciphers and Differential Cryptanalysis. In: *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, 17-38.

https://doi.org/10.1007/3-540-46416-6_2

[7] Daemen, J. and Rijmen, V. (2002) The Design of Rijndeal. AES—The Advanced Encryption. Springer-Verlag, Berlin.

[8] Hadipour, H., Bagheri, N. and Song, L. (2021) Improved Rectangle Attacks on SKINNY and CRAFT. *IACR Transactions on Symmetric Cryptology*, **2021**, 140-198. https://doi.org/10.46586/tosc.v2021.i2.140-198

[9] Sehrawat, D. and Gill, N.S. (2018) Lightweight Block Ciphers for IoT Based Applications: A Review. *International Journal of Applied Engineering Research*, **13**, 2258-2270.

[10] Dey, S. and Ghosh, R. (2018) A Review of Existing 4-bit Crypto S-Box Cryptanalysis Techniques and Two New Techniques with 4-bit Boolean Functions for Cryptanalysis of 4-bit Crypto S-Boxes. *Advances in Pure Mathematics*, **8**, 272. https://doi.org/10.4236/apm.2018.83015

[11] Tentu, A.N. (2020) A Review on Evolution of Symmetric Key Block Ciphers and Their Applications. *IETE Journal of Education*, **61**, 34-46. https://doi.org/10.1080/09747338.2020.1769508

[12] Dehnavi, S.M. (2018) Further Observations on SIMON and SPECK Block Cipher Families. *Cryptography*, **3**, 1. https://doi.org/10.3390/cryptography3010001

[13] Bar-On, A., Dunkelman, O., Keller, N. and Weizman, A. (2019) DLCT: A New Tool for Differential-Linear Cryptanalysis. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (*EUROCRYPT*), Springer, Berlin, 313-342. https://doi.org/10.1007/978-3-030-17653-2_11

[14] Fan, T., Li, L., Wei, Y. and Pasalic, E. (2022) Differential Cryptanalysis of Full-Round ANU-II Ultra-Lightweight Block Cipher. *International Journal of Distributed Sensor Networks*, **18**, 15501329221119398-15501329221119398. https://doi.org/10.1177/15501329221119398

[15] Teh, J.S. and Biryukov, A. (2022) Differential Cryptanalysis of WARP. *Journal of Information Security and Applications*, **70**, Article ID: 103316. https://doi.org/10.1016/j.jisa.2022.103316

[16] Zhang, K., Lai, X., Guan, J. and Hu, B. (2022) Research on the Security Level of μ^2 against Impossible Differential Cryptanalysis. *KSII Transactions on Internet and Information Systems* (*TIIS*), **16**, 972-985. https://doi.org/10.3837/tiis.2022.03.012

[17] Zhang, P. and Zhang, W. (2018) Differential Cryptanalysis on Block Cipher Skinny with MILP Program. *Security and Communication Networks*, **2018**, Article ID: 3780407. https://doi.org/10.1155/2018/3780407

[18] Cao, M. and Zhang, W. (2019) Related-Key Differential Cryptanalysis of the Reduced-Round Block Cipher GIFT. *IEEE Access*, **7**, 175769-175778. https://doi.org/10.1109/ACCESS.2019.2957581

[19] Ji, F., Zhang, W., Zhou, C. and Ding, T. (2020) Improved (Related-Key) Differential Cryptanalysis on GIFT. In: *International Conference on Selected Areas in Cryptography* (*ICSAC*), Springer, Berlin, 198-228. https://doi.org/10.1007/978-3-030-81652-0_8

[20] Kousalya, R. (2021) Security Analysis against Differential Cryptanalysis Using Active S-Boxes. *Turkish Journal of Computer and Mathematics Education* (*TURCOMAT*), **12**, 701-709.

[21] Hu, K., Peyrin, T. and Wang, M. (2022) Finding All Impossible Differentials When Considering the DDT. Cryptology ePrint Archive.

[22] Dwivedi, A.D. and Srivastava, G. (2018) Differential Cryptanalysis of Round-Reduced LEA. *IEEE Access*, **6**, 79105-79113. https://doi.org/10.1109/ACCESS.2018.2881130

[23] Liu, Z., Li, Y., Jiao, L. and Wang, M. (2020) A New Method for Searching Optimal Differential and Linear Trails in ARX Ciphers. *IEEE Transactions on Information Theory*, **67**, 1054-1068. https://doi.org/10.1109/TIT.2020.3040543

[24] Benamira, A., Gerault, D., Peyrin, T. and Tan, Q.Q. (2021) A Deeper Look at Machine Learning-Based Cryptanalysis. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (*EUROCRYPT*), Springer, Berlin, 805-835. https://doi.org/10.1007/978-3-030-77870-5_28

[25] Pal, D., Mandal, U., Chaudhury, M., Das, A. and Chowdhury, D.R. (2022) A Deep Neural Differential Distinguisher for ARX Based Block Cipher. Cryptology ePrint Archive.