□联合项目 □重点项目

◾一般项目

2023年湖南省研究生科研创新项目

申 请 书

|  |  |
| --- | --- |
| **项目名称：** | 基于深度学习的AI密码分析研究 |
| **主持人：** | 黄莹 |
| **所在单位：** | 衡阳师范学院 |
| **联合企业：** |  |
| **所属学科：** | 电子信息 |
| **联系电话：** | 13469454580 |
| **传真电话：** | 62661700 |
| **电子信箱：** | 1160239682@qq.com |
| **申请日期：** | 2023年4月26日 |

**湖南省教育厅**

**2023年**

一、简表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **项目**  **名称** | 基于深度学习的AI密码分析研究 | | | | | | | 研究  类别 | | 基础研究 | |  |
| 应用研究 | | **√** |
| 试验发展 | |  |
| **研究**  **年限** | 2023年5月至2024年5月 | | | | | 申请经费（万元） | | | | 1.0 | | |
| **项目**  **主持**  **人** | 姓名 | 黄莹 | 性别 | | 女 | | 身份证号 | | | 430105200003256129 | | |
| 在读层次 | 硕士 | 学科专业及研究方向 | | 电子信息及嵌入式计算与信息安全研究方向 | | 在读学年 | | | 二年级 | | |
| **指**  **导**  **教**  **师** | 姓名 | 李浪 | | 性别 | 男 | | 学历学位 | | | 研究生、博士 | | |
| 技术职称 | 教授 | | 学科专业及研究方向 | 计算机专业 | | | | | 嵌入式计算与信息安全 | | |
| 目前指导学生数 | 博士：0名，硕士：16名 | | | 联系电话 | | 15873438955 | | |  | | |
| **主**  **要**  **研**  **究**  **人**  **员** | 姓 名 | 身份证号码 | | 技术职务 | 专业 | | | | 所在单位 | | 本人签名 | |
| 黄现彤 | 432503199809123160 | | 无 | 电子信息 | | | | 衡阳师范学院 | |  | |
| 朱思琦 | 510704199904132423 | | 无 | 电子信息 | | | | 衡阳师范学院 | |  | |
|  |  | |  |  | | | |  | |  | |
|  |  | |  |  | | | |  | |  | |
|  |  | |  |  | | | |  | |  | |
| **项目负责人主要学习和工作经历（从上大学开始）** | 2017.9~2021.6项目负责人在衡阳师范学院学习本科专业。  2021.9~2024.6项目负责人在衡阳师范学院学习硕士专业。 | | | | | | | | | | | |

二、立项依据

|  |
| --- |
| 1. 项目的研究目的、意义   习近平总书记曾指出，网络安全与国家安全、经济社会稳定以及人民利益息息相关。随着物联网技术的广泛应用，保护物联网设备上的隐私数据与安全已成为国家和人民关注的热点。在这种背景下，保护这些设备上的数据隐私和安全变得至关重要。因此，轻量级分组密码作为一种加密算法应运而生，以实现在资源受限的设备上高效和安全的数据保护。轻量级密码算法应用于物联网资源受限环境的数据隐私保护，实现成本、安全性和实现代价同等重要。然而，为了追求低消耗和高效率，算法的设计可能会导致安全性降低，因此对轻量级分组密码的安全性分析变得至关重要。评估其安全性主要看抵抗已知攻击方法的能力，而设计者通常采用差分分析和积分分析等方法进行安全评估。  随着科技的发展，深度学习已经在医疗、智能驾驶等领域得到广泛应用。在密码学领域，深度学习主要应用于侧信道攻击，而在传统密码分析方面如差分分析和积分分析等领域，深度学习技术的研究成果相对较少。因此，本项目旨在利用深度学习这一工具对传统密码分析进行改进，研究一种基于AI的密码分析模型。这项研究能够在一定程度上促进密码设计学的发展，并有助于国家在密码安全领域争取主动权。 |
| 1. 国内外研究现状分析和发展趋势   随着物联网资源受限设备的增加，保护敏感数据的安全性变得更加重要[1]。物联网设备追求低能耗和高效率，这也导致其存在安全风险。为维护敏感数据安全，轻量级分组密码至关重要。轻量级分组密码的安全性取决于对已知攻击的抵抗能力[2]。  深度学习是目前最先进的技术之一，在医疗、智能驾驶等领域都发挥着关键作用[3]。其能够学习到庞大数据集隐含的规律。在密码学领域中，深度学习广泛用于侧信道攻击[4]和密码组件设计[5]，鲜少有人利用深度学习改进密码分析。然而，2019年Gohr利用深度学习开辟了传统密码分析的全新方向[6]。深度学习在传统密码分析领域也取得了一定的进展，目前可以分为三个方向。  深度学习在密码算法分析领域的第一个方向是将密码算法看作黑盒，让模型学习特定密码算法的明文对和密文对，从而掌握算法的内在规律（即算法结构）。没有具体的密码算法信息，攻击者只能通过输入输出猜测密钥，这种方法被称为黑盒攻击。该模型学习明文对和密文对的模式，尽可能准确地还原密钥，从而对密码算法攻击和破解。Jaewoo So设计了一种密钥范围在64ASCII字符的区分器模型[7]。该模型在密码算法未知的条件下，猜测所使用的密钥。该模型应用于S-DES、SIMON和SPECK[8]密码算法，成功攻破了全轮的SIMON32/64和SPECK32/64密码，但未能攻破S-DES算法。Hyunji Kim等人在Jaewoo So的基础上进一步的改进和扩展[9]，其成功地突破了密钥限制在64ASCII字符的条件，攻破全轮S-AES、SPECK和SIMON算法。在任意密钥的条件下，成功破解全轮S-DES算法。这表明他们的深度学习模型具有更广泛的适用性，可以攻击更多类型的密码算法。这些结果表明深度学习在密码算法分析领域的应用具有很大的潜力，可以为密码学的安全性提供更加有效的保障。  深度学习在密码算法分析领域的第二个方向，即利用神经网络模拟密码算法，并用神经网络的评价参数来评估密码算法的安全强度。Ya Xiao等人提出了一个新的评估密码算法安全性的思路，即利用神经网络的评价参数来公平地评估分组密码的安全性[10]。他们将对称密码算法看作黑盒，在不了解具体密码算法组件的条件下，利用神经网络来完成对密码算法安全强度的评估。基于这种测量标准，他们发现保护车载系统安全的Hitag2算法的安全性要弱于3轮的DES算法。这表明利用神经网络评估密码算法的安全性是一种有效的方法，可以为密码算法的设计和分析提供重要的参考依据。  深度学习在密码算法分析领域的第三个方向是将深度学习用于改善传统密码分析。Gohr最早将深度学习引入传统密码分析，构建了一种耗时较少、成本较低的神经区分器。神经网络将随机序列和密文序列的区分问题表达为深度学习中的分类问题，随后的研究也在此基础上扩展。Benamira等人全面解释了Gohr等人的神经网络区分器[11]。实验结果表明，神经网络区分器比传统差分区分器的准确率更高的原因是学习到了差分分布表以外的差分信息。这些信息包括算法在倒数第二轮或倒数第三轮上能够推导得到的差分条件。Baksi的研究视角放在更大的分组大小的非马尔科夫链密码算法[12]，使用MLP(多层感知机)模型[13]构建适合的差分区分器。Jain[14]使用MLP模型构建PRESENT[15]的差分区分器。该研究证明了较少隐藏层的网络同样也可以构建分组密码区分器。Tian等人针对SIMON算法设计了11轮、12轮和13轮的神经网络区分器[16]。同时也研究了ResNet[17]网络的变体会对网络模型的训练收敛速率有影响。Hou等人在轮数减少SIMON32算法上构建区分器的同时，探究了输入差分模式对区分器准确度的影响[18]。实验结果证实，汉明重量为1的输入差分对9轮区分器准确率的影响更大。Behnam等人首次将神经网络应用于积分分析方法[19]。该研究利用深度学习构建了能够适用于SPN、Festiel和ARX三种经典结构的积分区分器，并利用生成的积分区分器对SPECK32/64进行密钥恢复攻击。这些研究表明深度学习通过在传统密码分析的应用来提高密码算法安全性，从而改进传统密码分析方法。  在密码分析领域中，深度学习技术被视为一种新的工具，可以用于快速、高效地评估算法安全性，以及帮助攻击者破解密码算法。深度学习技术能够从差分轨迹或积分轨迹所生成的数据集中学习其背后规律，将区分器转换为分类问题，从而更好的改进传统密码分析方法。这种结合方式还处于初步阶段，目前仍存在许多理论和实际问题需要研究与完善。因此，如何解释深度学习在传统密码分析方法中的适用性、评估神经网络在区分器任务中学习到的密码算法特征的合理性、利用丰富的神经网络模型提高区分器的准确率以及对不同结构的密码算法的适用性。这些问题都是值得探索的。在未来，我们可以继续研究如何更好地结合深度学习技术和传统密码分析方法，以提高密码算法的安全性和可靠性。  参考文献：   1. Salimitari M, Chatterjee M, Fallah Y P. A survey on consensus methods in blockchain for resource-constrained IoT networks[J]. Internet of Things, 2020, 11:100212. 2. Praveen R, Pabitha P. Improved Gentry–Halevi's fully homomorphic encryption‐based lightweight privacy preserving scheme for securing medical Internet of Things[J]. Transactions on Emerging Telecommunications Technologies, 2023:e4732. 3. Din I U, Guizani M, Rodrigues J J P C, et al. Machine learning in the Internet of Things: Designed techniques for smart cities[J]. Future Generation Computer Systems, 2019, 100:826-843. 4. Benadjila R, Prouff E, Strullu R, et al. Deep learning for side-channel analysis and introduction to ASCAD database[J]. Journal of Cryptographic Engineering, 2020, 10(2):163-188. 5. Bolufé-Röhler A, Tamayo-Vera D. Machine learning based metaheuristic hybrids for S-box optimization[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(11):5139-5152. 6. Gohr A. Improving attacks on round-reduced speck32/64 using deep learning[C]. Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2019:150-179. 7. So J. Deep learning-based cryptanalysis of lightweight block ciphers[J]. Security and Communication Networks, 2020, 2020. 8. Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK lightweight block ciphers[C]. Proceedings of the 52nd annual design automation conference. Springer, Berlin, Heidelberg, 2015:1-6. 9. Kim H, Lim S, Kang Y, et al. Deep Learning based Cryptanalysis of Lightweight Block Ciphers, Revisited[J]. Cryptology ePrint Archive, 2022. 10. Xiao Y, Hao Q, Yao D D. Neural cryptanalysis: Metrics, methodology, and applications in cps ciphers[C]. 2019 IEEE Conference on Dependable and Secure Computing (DSC). IEEE, Piscataway, NJ, 2019:1-8. 11. Benamira A, Gerault D, Peyrin T, et al. A deeper look at machine learning-based cryptanalysis[C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2021:805-835. 12. Baksi A. Machine learning-assisted differential distinguishers for lightweight ciphers[M]. Classical and Physical Security of Symmetric Key Cryptographic Algorithms. Springer, Berlin, Heidelberg, 2022:141-162. 13. Jordan M I, Mitchell T M. Machine learning: Trends, perspectives, and prospects[J]. Science, 2015, 349(6245):255-260. 14. Jain A, Kohli V, Mishra G. Deep learning based differential distinguisher for lightweight cipher PRESENT[J]. Cryptology ePrint Archive, 2020. 15. Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An ultra-lightweight block cipher[C]. Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop. Springer, Berlin, Heidelberg, 2007:450-466. 16. Tian W, Hu B. Deep learning assisted differential cryptanalysis for the lightweight cipher simon[J]. KSII Transactions on Internet and Information Systems (TIIS), 2021, 15(2):600-616. 17. He K, Zhang X, Ren S, et al. Deep residual learning for image recognition[C]. Proceedings of the IEEE conference on computer vision and pattern recognition. IEEE, Piscataway, NJ, 2016:770-778. 18. Hou Z, Ren J, Chen S. Cryptanalysis of round-reduced SIMON32 based on deep learning[J]. Cryptology ePrint Archive, 2021. 19. Zahednejad B, Lyu L. An improved integral distinguisher scheme based on neural networks[J]. International Journal of Intelligent Systems, 2022, 37(10):7584-7613. |
| 1. 项目应用前景和学术价值   在物联网等资源受限环境中，轻量级密码算法的使用已经广泛普及。然而，为了保证网络安全和信息安全，对于密码算法的安全性分析至关重要。轻量级密码算法追求低消耗和高效率的同时，也不可避免地降低了安全性。现在已经有了一些公认的轻量级密码算法标准，如ISO/IEC 29192和NIST SP 800-185等。这些标准提供了一些设计准则和安全标准。然而，仍然需要进一步研究先进的密码分析模型，以解决安全问题并保障隐私保护和数据保密，这对于我国在密码学领域的国际地位提高非常重要，具有广泛的应用前景和重要的实际意义。这种研究对于我国在密码学领域的国际地位提高非常重要，无论从理论研究还是实际应用的角度，都具有重要意义。 |
| 1. 现有的研究基础、条件、手段   1) 研究基础  本项目组一直致力于分组密码算法的安全性分析研究，并在该领域取得了一定的研究成果。我们对深度学习在密码分析领域有着独特的理解。项目组所在的嵌入式计算与信息安全实验室在分组密码研究领域拥有丰富的研究工作积累和项目组织实施经验，同时具备先进完备的基础设施和科学完善的管理体系，能够为本项目的顺利实施提供保障。  2) 研究条件  项目组所依托的“嵌入式计算与信息安全研究所”是湖南省重点实验室，占地面积80平米，配备了相应的实验研发设备，为项目提供了良好的研究开发和工作环境。学校非常重视科研工作，并能提供足够的科研工作条件。我们的研究团队由在职在岗的2名教师和20多名博士、硕士研究生组成，长期从事密码算法的安全性分析与攻击、轻量级密码算法优化、轻量级密码算法设计的研究。目前发表了多篇SCI论文，并申请了多项专利。特别是在SoC芯片、FPGA实现研究与设计方面积累了宝贵的经验与教训，有着良好的软硬件开发团队作风和项目经验，有专业资深的老师指导，并具有产学研项目研究经历。在面向产业化应用研发方面，我们已经取得了较好的成果。  3) 研究手段  项目组利用多种渠道（如多媒体、三大数据库、欧洲密码会议、亚洲密码会议、美国密码会议等）持续关注和学习基于深度学习与密码分析方法结合的领域。我们从传统密码分析方法出发，建立相应的神经网络区分器模型。我们研究了深度学习在传统密码分析方法中的适用性，以及深度学习评估在这一特定任务中学习到的密码算法特征的合理性，探讨了如何利用丰富的神经网络模型来提高区分器模型的准确率以及神经网络模型对不同结构密码算法的适用性。针对不同类型的深度学习模型，我们选取不同的监督训练方式，并对模型进行训练。 |
| 1. 指导教师情况   1) 主持代表性项目：   1. 国家自然科学基金面上项目：抗功耗攻击的新型轻量级分组密码及其并行验证（No.61572174）,2016.1-2019.12. 2. 湖南省自然科学基金项目：自主知识产权的轻量级分组密码技术及产业化（No.2019JJ60004）,2019.1-2021.12. 3. 湖南省教育厅科研重点项目：轻量级分组密码系统设计关键技术研究 (No.19A072)，2020.1-2022.12. 4. 湖南省自然科学基金面上项目：于深度学习的密码芯片侧信道安全分析理论及技术研究（2022JJ30103）,2022.1-2024.12.   2) 发表的代表性论文：   1. Guo Y, Li L, Liu B. Shadow: A lightweight block cipher for IoT nodes[J]. IEEE Internet of Things Journal, 2021,8(16): 13014-13023. (SCI 1区, ESI) 2. Huang X, Li L, Yang J. IVLBC: An Involutive Lightweight Block Cipher for Internet of Things[J]. IEEE Systems Journal, 2022,12:1-12. (SCI 2区, ESI) 3. 李浪,李肯立,贺位位,邹祎,刘波涛.Magpie:一种高安全的轻量级分组密码算法[J].电子学报, 2017, 45(10):2521-2527. 4. Feng J, Li L. SCENERY: a lightweight block cipher based on Feistel structure[J]. Frontiers of Computer Science, 2022, 16(3):1-10. (SCI 2区, ESI) 5. Yan L, Li L, Guo Y. DBST: a lightweight block cipher based on dynamic S-box[J]. Frontiers of Computer Science, 2023, 17(3):1-9. (SCI 2区, ESI) 6. Ou Y, Li L. Side-channel analysis attacks based on deep learning network[J]. Frontiers of Computer Science, 2022, 16(2):1-11. (SCI 2区, ESI) 7. Li L, Liu J, Guo Y, et al. A new S-box construction method meeting strict avalanche criterion[J]. Journal of Information Security and Applications, 2022, 66:103135. (SCI 3区, ESI) 8. Li L, Feng J, Liu B, et al. Implementation of PRINCE with resource-efficient structures based on FPGAs[J]. Frontiers of Information Technology & Electronic Engineering, 2021, 22(11): 1505-1516. (SCI 3区, ESI) 9. Ou Y, Li L, Li D, et al. ESRM: an efficient regression model based on random kernels for side channel analysis[J]. International Journal of Machine Learning and Cybernetics,2022,13 (2022):3199–3209.(SCI 3区, ESI) 10. Li D, Li L, Ou Y. CKGS: A Way of Compressed Key Guessing Space to Reduce Ghost Peaks[J]. KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 2022, 16(3):1047-1062. (SCI 4区, ESI) 11. Yang J, Li L, Guo Y, et al. DULBC: A dynamic ultra-lightweight block cipher with high-throughput[J]. Integration, 2022, 87:221-230. (SCI 4区, ESI) 12. Ou Y, Li L. Research on a high-order AES mask anti-power attack[J]. IET Information Security, 2020,14(5):580-586. (SCI 4区, 密码学会推荐B类期刊) 13. Kuang J, Guo Y, Li L. IIoTBC: A Lightweight Block Cipher for Industrial IoT Security[J]. KSII Transactions on Internet and Information Systems, 2023,17(1):97-119.(SCI 4区, ESI) 14. 李浪,欧雨,邹祎.一种AES随机变换掩码方案及抗DPA分析[J].密码学报,2018,5(4):442-454. 15. 李浪,郭影,刘波涛,欧雨.HBcipher：一种高效的轻量级分组密码[J].密码学报,2019, 6(3):336–352. 16. Chen W, Li L, Guo Y. DABC: A dynamic ARX-based lightweight block cipher with high diffusion[J]. KSII Transactions on Internet and Information Systems, 2023,17(1):165-184.(SCI 4区, ESI) 17. Huang Y, Li L, Guo Y, et al. An efficient differential analysis method based on deep learning[J]. Computer Networks, 2023, 224:109622. (SCI 3区, ESI) 18. Chen W, Li L, Guo Y, et al. SAND-2: An optimized implementation of lightweight block cipher[J]. Integration, 2023.   3) 近年的主要获奖：   1. 李浪, 焦铬, 邹祎, 刘波涛. 新型轻量级分组密码关键技术及其应用, 湖南省技术发明三等奖, 2019.12 2. 李浪、焦铬、李秋萍、欧雨、刘波涛、郭影. 面向物联网环境的自主知识产权密码技术及应用.湖南省计算机学会科学技术二等奖, 2022.7   4) 近年来已授权的发明专利：   1. 一种轻量级分组密码SCS的实现方法与装置.专利号: ZL201711428178.6. 2. 一种轻量级密码算法HBcipher实现方法与装置.专利号: ZL201810025266.X. 3. 一种完全雪崩4 × 4的 S 盒实现方法.专利号: ZL201910310953.0. 4. 一种基于d+1阶掩码的抗功耗攻击方法.专利号:ZL201910285584.4. 5. 一种轻量级分组密码算法的实现方法.专利号:ZL201910250703.2. 6. 轻量级密码算法SCENERY实现方法、装置及存储介质.专利号: ZL201911070 142.4. 7. 基于轻量级分组密码算法Shadow的加密方法、装置及计算机可读介质. 专利号:ZL201910916368.5. 8. 一种轻量级AEROGEL分组密码的实现方法. 专利号: ZL202010244240.1. 9. 一种新型分组密码CORL的实现方法. 专利号: ZL202010247023.8. 10. 基于深度学习的侧信道分析方法. 专利号: ZL202010368459.2. 11. 一种基于遗传算法的功耗攻击高效筛选方法. 专利号: ZL202110548000.5. 12. 一种压缩密钥猜测空间的侧信道攻击方法. 专利号: ZL202110596380.X. 13. 基于广义二维猫映射的轻量级分组密码算法GCM实现. 专利号: ZL202110746280.0. |

1. 研究方案

|  |
| --- |
| 1. 研究目标、研究内容和拟解决的关键问题   1) 研究目标  本研究的研究对象为深度学习技术在密码分析方法中的应用，研究目标如下：  (1) 探究深度学习模型在传统密码分析方法中的适用性，包括分析深度学习在不同密码分析方法的适用性，如差分分析、积分分析等。  (2) 评估深度学习模型在密码分析任务中密码算法特征的合理性，包括对深度学习模型学习到的密码算法特征进行量化评估和进行可解释性分析，以及比较不同特征提取方法的效果等。  (3) 研究利用不同的神经网络模型提高区分器的准确率，包括设计和优化神经网络结构、选择合适的损失函数、采用数据增强技术等方法，提高算法区分器的准确率和鲁棒性。  (4) 研究深度学习模型对不同结构的密码算法的适用性，包括分析深度学习模型在不同分组密码算法结构下的适用性和性能表现，如Feistel结构、SPN结构、ARX结构等。  2) 研究内容  (1) 深度学习模型在不同类型密码分析方法中的适用性分析及评估  研究内容包括分析深度学习模型在不同类型的传统密码分析方法的适用性，如差分分析、积分分析等。这需要首先研究不同类型的密码分析方法，深入理解其原理和特点，并进一步分析如何利用深度学习技术来改进这些方法的效果和性能。同时，还需要制作相应的数据集和评估指标，以评估深度学习模型在不同密码分析方法的适用性和性能。    图1 差分密码分析中分类模型理论转化  (2) 深度学习模型在密码分析任务中的特征学习和分析  本研究旨在探究深度学习模型在密码分析任务中学习到的密码算法特征的合理性，并围绕这一目标展开研究。首先，设计合适的深度学习模型，以学习和提取密码算法的特征；然后，量化评估深度学习模型学习到的密码算法特征的合理性和有效性；接着，比较不同特征提取方法的效果，并分析其优缺点；最后，对学习到的密码算法特征进行可解释性分析，以了解深度学习模型在密码分析方法中的工作原理。  (3) 利用神经网络优化区分器模型的准确率和鲁棒性  本研究旨在提高密码学中区分器模型的准确率和鲁棒性。首先，我们将选择合适的特征提取方法来区分密码算法。其次，采用数据增强技术来扩充训练集，提高区分器模型的泛化能力和鲁棒性。接着，我们将评估算法区分器的性能和效果，包括准确率、召回率、精确率、F1分数等指标，以比较不同方法的优劣。最后，将区分器模型应用到具体的密码算法分析中，提高区分器的区分准确性和效率。本研究旨在为密码学中区分器模型的性能优化和应用提供理论和实践支持。    图2 深度学习基础部件  (4) 深度学习模型在不同密码算法结构中的适用性与性能评估  本研究旨在评估深度学习模型在不同结构密码算法的适用性和性能表现。首先，分析深度学习模型在Feistel、SPN、ARX结构密码等不同算法结构下的表现，探究不同算法结构对深度学习模型的影响。接着，选择合适的特征提取和模型设计方法，以提高深度学习模型的性能和鲁棒性。然后，我们将采用数据增强技术来扩充训练集，提高模型的泛化能力和鲁棒性。最后，我们将评估各种深度学习模型在不同密码算法结构下的表现，并比较不同模型的优劣，以为密码分析方法的研究和应用提供参考。该研究将为密码学算法的优化和加密技术的发展提供有益的指导和促进作用。  3) 拟解决的关键问题  (1) 深度学习在轻量级密码分析中的适用性及寻找最适合的模型  拟解决的关键性问题包括如何评估深度学习在不同密码分析方法的适用性，以及如何找到最适合密码分析的深度学习模型。这需要深入研究不同类型的密码分析技术，了解其特点和局限性，并探索使用深度学习技术来解决这些问题的方法。同时，还需要开发适用于特定密码分析任务的数据集和评估指标，以保证深度学习模型的可靠性和可比性。通过综合分析和评估，寻找最适合特定密码分析任务的深度学习模型，以提高密码分析的效率和准确性。  (2) 深度学习在密码分析中的特征学习和分析问题的进一步研究  拟解决的关键问题包括设计合适的深度学习模型以学习和提取密码算法的特征；量化评估其特征的合理性和有效性；比较不同特征提取方法的效果并分析其优缺点、对学习到的密码算法特征进行可解释性分析以了解深度学习模型在传统密码分析中的工作原理；探究深度学习模型在密码分析中的适用性和性能；以及结合传统密码分析方法和深度学习方法以提高密码分析任务的效率和准确性。  (3) 深度学习在密码分析任务中的模型选择与适用性评估  拟解决的关键问题包括利用丰富的神经网络模型来提高区分器模型的准确率。具体而言，设计和优化神经网络结构，选择合适的损失函数，采用数据增强技术等方法来提高区分器模型的性能。接着，选择合适的特征提取方法来区分不同的密码学算法，以进一步提高区分器模型的准确率和鲁棒性。然后，采用数据增强技术来扩充训练集，提高区分器模型的泛化能力和鲁棒性。然后，我们将评估算法区分器的性能和效果，包括准确率、召回率、精确率、F1分数等指标，以比较不同方法的优劣。最后，我们将应用算法区分器在实际场景中，提高密码识别和鉴别的准确性和效率。  (4) 深度学习模型在不同结构密码算法中的适用性和性能评估  本研究旨在评估深度学习模型在不同结构的密码算法中的适用性和性能表现。为此，我们需要解决以下关键问题。首先，需要分析深度学习模型在Feistel、SPN、ARX结构密码等不同算法结构下的表现，以探究不同算法结构对深度学习模型的影响。其次，需要选择合适的特征提取和模型设计方法，以提高深度学习模型的性能和鲁棒性。为提高模型的泛化能力和鲁棒性，需要利用数据增强技术来扩充训练集，从而更好地适应不同的密码算法结构和应用场景。最后，需要评估各种深度学习模型在不同密码算法结构下的表现，并比较不同模型的优劣，以为密码学算法的研究和应用提供参考和指导。 |
| 1. 拟采取的研究方法及可行性分析   1) 拟采取的研究方法  本项目聚焦于传统密码分析与人工智能领域，探讨深度学习在传统密码分析中的应用，研究优化深度学习模型的设计，以提高深度学习在密码分析中的精度与泛化能力。为此，本项目将采取如下研究方法：  (1) 深入分析不同类型密码分析技术，探究深度学习技术应用的可行性  研究深度学习在不同密码分析方法的适用性，并探究如何利用深度学习技术来增强不同类型的密码分析技术的效果和性能。为此，我们将开发相应的数据集和评估指标，以评估深度学习模型在不同密码分析方法的适用性和性能。同时，探讨深度学习模型在密码保护和加密的应用，以提高数据安全性和隐私保护水平，为密码学领域的发展做出贡献。  (2) 基于深度学习的密码算法特征提取及应用研究  通过设计合适的深度学习模型，量化评估模型学习到的密码算法特征的合理性和有效性，并进行可解释性分析，以了解深度学习模型在密码分析中的工作原理。同时，探究深度学习模型在密码分析任务中的适用性和性能，并结合传统密码分析方法和深度学习方法，提高密码分析任务的效率和准确性。  (3) 基于深度学习的密码分析区分器模型研究  首先，设计并优化深度学习模型的结构，包括卷积神经网络、循环神经网络等，以学习和提取密码算法的特征。其次，选择合适的损失函数，比较交叉熵、对抗性损失等不同损失函数的效果，并通过反向传播算法进行模型训练和参数优化。接着，采用数据增强技术，如翻转、旋转、缩放等，扩充训练集，提高区分器模型的泛化能力和鲁棒性。最后，将区分器模型应用在具体密码算法中，评估区分器模型的性能和效果。  (4) 基于深度学习的不同结构密码算法区分器的性能比较  研究不同结构的密码算法的适用性和性能表现，包括Feistel结构、SPN结构、ARX结构密码等不同分组密码算法结构。首先，收集相关数据集，并将其转换为可供深度学习模型训练的格式。然后，设计和实现不同的深度学习模型，包括卷积神经网络、循环神经网络和注意力机制等模型，并采用不同的特征提取方法，以提高模型的性能和鲁棒性。为提高模型的泛化能力和鲁棒性，采用数据增强技术来扩充训练集，从而更好地适应不同的密码算法结构和应用场景。最后，对各种深度学习模型在不同密码算法结构下的表现进行评估和比较，并分析其优缺点。  2) 可行性分析  首先，针对本项目的主要研究内容和研究目标，项目组做了充分的准备并制定了详细的研究方案和细致的研究计划。同时，针对本项目的各项主要研究内容，本项目组在理论和技术方面均已具备大量的研究基础和工作积累，这将会积极促进本项目的顺利的启动和研究深入。  其次，在研究内容的描述中，我们尽可能细化，明确研究对象，具体研究方法。尤其是在研究方案的阐述中，我们明确了需解决的问题，初步拟定了采取的技术方法等，研究计划清楚且现实可行。  最后，项目的研究目标和预期成果制定合理适度，能够保证研究的广度和深度。  综上所述，我们认为完成本项目的研究是切实可行的。 |
| 1. 本项目的创新之处   1) 本项目将探究深度学习在传统密码分析方法中的适用性，包括分析深度学习在不同分析方法中的适用性，如差分分析、积分分析等。传统密码分析方法通常依赖于数学模型和算法，而深度学习技术则是一种基于数据驱动的方法，通过学习大量的数据来发现规律和特征，为传统密码分析领域提供新的思路。  2) 本项目将评估深度学习在密码分析任务中的密码算法特征的合理性，包括对深度学习模型学习到的密码算法特征进行量化评估、比较不同特征提取方法的效果，并对学习到的特征进行可解释性分析，有助于深入理解深度学习模型在密码分析中的作用。  3) 本项目将研究如何利用丰富的神经网络模型提高算法区分器的准确率，包括设计和优化神经网络结构、选择合适的损失函数、采用数据增强技术等方法，提高算法区分器的准确率和鲁棒性，为密码分析的效率和准确性提供支持。  4) 本项目将研究深度学习模型对不同结构的密码算法的适用性，包括分析深度学习模型在不同分组密码算法结构下的表现，如Feistel结构、SPN结构、ARX结构密码等，评估其在不同密码结构的适用性和性能表现，以提供创新的解决方案。 |
| 1. 预期研究进展   1) 2023年6月—2023年9月  确定总体方案，对项目实施做出具体安排：文献、资料的跟踪及收集，研究和学习差分密码分析与深度学习结合理论与方法，为本项目的模型设计打下基础。  2) 2023年10月—2023年12月  阅读前沿技术论文，总结目前差分密码分析与深度学习的结合方法，对比不同结合方法的优劣，并确认本项目的差分密码分析与深度学习技术结合方式。  3) 2024年1月—2024年2月  对经典的差分密码分析模型进行深入研究，掌握不同网络在模型训练中充当的职能，选取合适的组件搭建适用于本项目的深度学习模型，并收集模型训练的差分分析数据集，确立模型的评估方法。  4) 2024年3月—2024年5月  对上一阶段设计好的差分密码分析模型进行python实现，对该模型进行评估，并调试模型的超参数，收集实验数据，从实验数据中选取评估结果最好的模型作为项目的最终模型。最后总结各项工作，做好项目结题工作，撰写总结报告、参加结题答辩。 |
| 1. 预期成果   发表SCI论文一篇以上。 |

四、研究基础

|  |
| --- |
| 1. 与本项目有关的研究工作积累和已取得的成绩   本项目所在的嵌入式计算与信息安全实验室在分组密码算法分析研究领域有着丰富的研究工作积累和项目组织实施经验，配备了先进完备的基础设施和科学完善的管理体系，可保障本项目的顺利实施。申请人及其团队一直从事密码算法分析、设计与实现研究，在高性能计算集群服务器的支持下，能够有效地训练深度学习模型。项目组拥有较好的软硬件研发环境，并在前期进行了充分的理论与技术研究，为本项目的开展奠定了良好的基础。本项目研究目标明确、内容具体、重点突出，方案切实可行。  项目主要研究人员：  [1] Huang Y(**黄莹**), Li L, Guo Y, et al. An efficient differential analysis method based on deep learning[J]. Computer Networks, 2023, 224:109622. (SCI三区, ESI)  [2] Chen W, Li L, Guo Y, Huang Y(**黄莹**). SAND-2: An optimized implementation of lightweight block cipher[J]. Integration, 2023. (SCI四区)  [3] Jinling Yang, Lang Li, Ying Guo, Xiantong Huang(**黄现彤**). DULBC: A dynamic ultra-lightweight block cipher with high-throughput[J]. Integration, 2022, 87: 221-230.( SCI四区)  [4] Xiantong Huang(**黄现彤**), Lang Li, Jinling Yang. IVLBC: An Involutive Lightweight Block Cipher for Internet of Things. IEEE Systems Journal, 2022,12:1-12. ( SCI二区)  [5] **黄现彤,黄莹**等. 一种适用于车联网终端的轻量级分组密码IoVCipher实现方法及其系统. 申请号：202111402291.3.（公开进入实质审查阶段）  [6] **黄现彤**,李遇缘,张洪,李迪,陈文,**黄莹**等. 车安“芯”——智能网联汽车信息安全守护者，第十届“挑战杯”湖南省大学生创业计划竞赛二等奖.2022.6.  [7] **黄现彤**,**黄莹**,宋庆玲,陈诗蓉,李臣(指导教师：李浪). 衡阳师范学院第二十届大学生课外学术科技作品竞赛特等奖,衡阳师范学院,2020.4.   1. 目前承担项目情况   无 |

五、经费预算

|  |  |  |
| --- | --- | --- |
| 支 出 科 目 | 金 额  （万元） | 计 算 根 据 及 理 由 |
| 合 计 | 1.0 |  |
| 科研业务费 | 0.5 | 参加相关会议、调研学习交流等差旅费用 |
|  | 0.5 | 论文发表、专利申请等费用 |
| 实验材料费 |  |  |
| 仪器设备费 |  |  |
| 相关经费 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 指  导  教  师  意  见 | （就项目研究目标、内容、创新性、研究方案的可行性、预计创新成果等写出具体意见）  项目组成员均为实验室成员，有非常严格的管理制度，有一定的前期研究基础，均有较好的科研创新意识与自学能力。项目内容主要是研究基于深度学习的AI密码分析模型。针对差分分析和积分分析两类，搭建特定的深度学习网络模型。项目方案切实可行，易操作，可执行，预期成果有很高的应用价值，同意推荐申报。  签名： 年 月 日 | |
| 指  导  教  师  承  诺 | 我承诺：如果项目获得专项，我将依照《湖南省研究生科研创新项目管理办法》的有关章则和学校的有关规定对项目进行切实指导和监管。  承诺人： 年 月 日 | |
| 研究生院处审查以及经费保障意见 | 负责人： 年 月 日  （公章） | |
|  | 专家评审意见 | 省教育厅审定意见 |
| 专家签名： 年 月 日 | 年 月 日 |