□联合项目 □重点项目

■一般项目

2024年湖南省研究生科研创新项目

申 请 书

|  |  |
| --- | --- |
| **项目名称：** | 面向轻量级分组密码的软件优化实现 |
| **主持人：** | 向嘉豪 |
| **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：** | 13087286239 |
| **传真电话：** | 62661700 |
| **电子信箱：** | simple.xjh@qq.com |
| **申请日期：** | 2024年5月 日 |

**湖南省教育厅**

**2024年**

一、简表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **项目**  **名称** | 面向轻量级分组密码的软件优化实现 | | | | | | | 研究  类别 | | 基础研究 | |  |
| 应用研究 | | √ |
| 试验发展 | |  |
| **研究**  **年限** | 2022 年至 2024 年 | | | | | 申请经费（万元） | | | | 1 | | |
| **项目**  **主持**  **人** | 姓名 | 黄现彤 | 性别 | | 女 | | 身份证号 | | | 432503199809123160 | | |
| 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 | | | 一年级 | | |
| **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： 8 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 | |
| 宋庆玲 | 430124200105074966 | | 无 | 电子信息 | | | | 衡阳师范学院 | |  | |
| 胡敏桦 | 431021199909236546 | | 无 | 电子信息 | | | | 衡阳师范学院 | |  | |
| 孙薇 | 430621200012180020 | | 无 | 电子信息 | | | | 衡阳师范学院 | |  | |
| 杨金玲 | 432402199702050481 | | 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**

|  |
| --- |
| （项目的研究目的、意义；国内外研究现状分析和发展趋势；项目应用前景和学术价值；现有研究基础、条件、手段以及指导教师情况等）   1. 项目的研究目的、意义   1.1项目的研究目的  分组密码主要用于在数据传输和存储中提供机密性保护，随着各国标准化的进展，分组密码在工业和商用领域得到了广泛应用，已成为构建安全信息系统的核心基础。近年来，随着移动互联网和工业智能化的快速发展, 汽车产业不断向智能化和网联化快速转变，车联网中的汽车配备了数百个连接在CAN总线中的电子控制单元（ECU）。这些ECU用于执行驾驶功能，如加速器、制动器、方向盘等的运动。然而，由于ECU之间通信没有进行加密，其数据传输过程中极有可能受到攻击遭到篡改，数据的保密性、完整性和真实性受到了考验。因此，车辆网上数据安全等问题引起了国内外人们的广泛关注，2021年第11届中国汽车论坛上提到“在过去5年时间里，智能汽车被黑客攻击的次数增长了20倍，其中有27.6%的攻击涉及车辆控制。”。据《证券日报》记者不完全统计，2019年，黑客通过入侵共享汽车App、改写程序和数据的方式，盗走包含奔驰CLA、GLA小型SUV、Smartfortwo微型车在内的100多辆汽车。知名汽车网络安全公司Upstream Security发布的2020年《汽车网络安全报告》显示，自2016年至2020年1月份，汽车网络安全事件增长了605%，仅2019年一年就增长1倍以上。2015 年，两名白帽黑客远程入侵了一辆正在路上行驶的切诺基(自由光)，并对其做出减速、关闭引擎、突然制动或者制动失灵等操控。2021年，特斯拉再度因摄像头记录驾驶员面部特征及车内大部分空间而陷入“隐私门”，其中的监控录像就是一名黑客入侵特斯拉汽车后曝出来的信息。 除了网络、程序技术带来的安全风险外，自动驾驶、人工智能等数字化技术的应用也让汽车的安全风险相应增加。在有关数字化应用的攻击中，黑客越来越多地瞄准大数据、人工智能和自动驾驶系统。为此，国家高度重视密码的安全保障作用，鼓励商用密码技术应用。2017 年 6 月《网络安全法》明确了网络安全事故的责任主体，在汽车信息安全方面对整车制造商、车载信息系统提供商及网络服务运营商提出了法律层面的要求，使得汽车行业在汽车信息安全功能产品的生产和运营实现了“有法可依”。然而，传统的加密算法AES在这种情况下不是最佳选择，因为它的操作复杂，如果在硬件中实现，会导致长的执行延迟和大的芯片面积。因此，研究专门适用于这类环境下轻量级分组密码引起了国内外学者的广泛关注，是目前国际密码学研究的热点问题。  1.2项目的研究意义  不同于传统分组密码加密标准，轻量级密码由于应用环境的限制，使得其实现代价、成本将和安全性占据同等重要的地位。因此对算法设计原理和评价准则，以及密码结构、密码部件等关键环节的设计提出了新的挑战。此外，由于侧重密码算法的实现代价，有可能导致算法设计过于简单且安全冗余不够。因此研究改进轻量级分组密码的安全性分析方法将有助于更全面、更准确地评估其安全性，避免可能存在的安全隐患。由于我国目前可用的专门适用于资源受限环境的加密方案很少，特别是针对车联网中的专用安全需求，因此设计适用于车联网节点、公开的、经过详细安全性分析评估的轻量级分组密码有迫切的需求，在理论研究及实际应用中都有着非常重要的意义，将具有巨大的应用需求和广阔的市场应用前景。   1. 国内外研究现状分析和发展趋势   当前，汽车的信息化、智能化不断普及，车联网技术已经在各大车厂的量产车型实现了较为广泛的应用，但随之而来的车联网技术相关安全问题已经日益凸显。车联网体系可归纳为端、管、云三层架构，汽车中CAN总线上的ECU包含于“端”系统。它主要存在以下三方面安全风险：（1） 车载终端架构的安全威胁。随着智能网联汽车的功能越来越多，使得整车的结构越来越复杂，其每个ECU之间交互的复杂度以及处理接受外部数据的需求都对车载体系架构的安全保障能力提出了极高的要求。（2） CAN总线自身的脆弱性。由于ECU在设计之初并没有考虑到对CAN总线上传的数据进行校验的功能， CAN的广播传输允许攻击者进入车内网络，然后窃听CAN传输并识别合法的CAN帧[1]中的模式。针对智能网联汽车来说，其接受的数据不仅包含从云端下载的内容，还有可能接收到通过重放攻击等手段植入的恶意软件发出的指令等信息。（3）车内网络之间的数据传输机制存在安全风险。汽车内部的网络环境存在很多可被攻击的安全缺口，如胎压监测系统、蓝牙模块等。并且车内的网络通信协议安全措施较为薄弱，如CAN除了简单的校验外，不能抵抗攻击者针对OBD-II 端口、受损的 ECU 或信息娱乐和远程信息处理系统等通信节点信息采集、报文收集、重放等攻击。为此，北京交通大学的李聪聪指出，车联网对信息安全的需求主要集中在两方面：身份认证和数据加密。  对于车联网中的身份认证方面的研究。2018 年，华中科技大学的鲁赵骏提出了一种基于区块链的匿名认证方法，通过区块链技术提出一种新型公钥基础设施（Public Key Infrastructure，PKI）架构，改善了匿名认证效率低下和可扩展性差的表现[2]。2020 年，陈葳葳等提出一种高效匿名认证方案[3]。在网联车上路运行时，车辆生成临时密钥并向路边单元（Road Side Unit, RSU）申请入网，区块链系统中的智能合约会记录网联车每次入网的过程并将其打包成区块发布，各用户通过检索区块获取彼此的身份信息。但是随着时间推移，系统中的区块数量和数据量将变得非常庞大，对存储系统是一个严峻挑战。2021 年，Suaib Akhter 等提出一种可以向车联网用户提供隐私保护的身份认证协议，该协议基于多层级的区块链框架实现，通过区块链对公钥证书进行公证，还能提供基于RSA-1024 密码的消息加密服务[4]。综上所述，在现有的车联网身份认证方法中存在以下弊端：不可信的证书会让用户被欺骗，额外的硬件设备（如智能卡）会带来更高昂的成本，多方交互可能会引入额外的时延。  对于数据加密方面的研究，由于传统的加密算法AES在这种情况下不是最佳选择，因为它的操作复杂，如果在硬件中实现，会导致长的执行延迟和大的芯片面积。为了满足这种新计算模式的实时要求，一个合适的轻量级分组密码是至关重要的。轻量级分组密码算法与传统密码算法相比有以下几个特点：（1）在资源严格受限的硬件设备上处理的数据规模比较小且对吞吐率的要求不高，因此，分组长度通常选用64比特，密钥长度选择64比特或80比特；（2）算法大多采用硬件实现，面积是最重要的衡量参数，也是决定成本和功耗的重要指标，一般要求在2000门以内实现；（3）近年的一些应用需求还提出了低延迟，低能量等新指标。因此结合以上特点，目前, 轻量级块密码面临以下挑战：（1）低成本智能设备需要开销最小（例如门数、内存占用）（2）功率和延迟最小（3）足够的安全性性能。因此，针对车联网中的数据安全问题，从理论与实现上提出高安全、高效率、低延迟、低功耗的轻量级密码算法有着重要意义，同时，这种安全也只能依靠独立自主研发。  对于轻量级分组密码的分析与研究，轻量级密分组码结构是密码学者的研究重点之一。近几年国际上先后推出了一系列专门适用于资源受限环境的轻量级分组密码。有使用矩阵表示的扩展广义 Feistel 网络 (EGFN)的LILLIPUT算法[5]。该密码有 30 轮，轮函数由具有 4 位 S-box 的非线性层、具有 XOR 运算的线性层和置换层组成。30 个子密钥是通过密钥函数从 80 位主密钥中获得30 个子密钥是通过密钥调度函数从 80 位主密钥中获得的每轮的子密钥。采用广义Feistel结构(GFS)的超轻量级分组密码µ2[6]。GFN 和 EGFN 之间的区别是遵循混淆阶段的线性层。该密码一种基于4轮16位超轻量级SPN的分组密码和Even-Mansour结构，为了加密和密钥生成，µ2使用4位S-Box。该密码的性能优于PRESENT，安全性评估表明该密码能够抵抗众所周知的攻击。除此之外，最新的采用广义Feistel 结构算法还有SCENERY [7]、 QTL[8]、Liarx[9]、Shadow[10]和CHAM[11]等；借鉴传统分组密码如AES等的设计思想采用SPN结构设计的LED[12]算法，其每一轮包括常数加、S 盒替换、行移位、列混合，每四轮组成一步，进行一次密钥加。可认为其不存在密钥扩展算法，128 比特密钥分为两个 64 比特长度的子密钥轮流与每一步的状态进行异或；有采用SP结构设计的PRESENT算法[13]，该算法还被列入了ISO国际标准。之后，PRESENT的设计者提出了GIFT[14], 其通过结合S盒的差分分布表（DDT）/线性近似表（LAT）引入置换来改进PRESENT,使S盒消耗的资源更少。还有采用SPN结构且结构对合的Loong算法[15]，这种结构非常适合轻量级加密，因为它的对合特性使它能够使用相同的过程进行加密和解密。它的块大小为64位，有三个版本供选择，分别是64位、80位和128位。与密钥大小对应，迭代次数分别为16、20和32轮。它在硬件和软件上都被证明是非常有效的，因为它可以实现代码的重用。这种密码在对抗差分和线性攻击时表现得非常好，而且还能抵抗中间相遇攻击、相关密钥攻击和其他已知攻击。除此之外，SAND[16]、DoT[17]、PriPresent[18]和 SFN[19]等是一些最新基于SPN结构的算法;近年来，针对新的应用需求，又陆续提出了一些可同时兼顾硬件面积和其它指标的算法，典型的如同时兼顾硬件和8位微处理器甚至32/64位服务器端软件实现性能的LBlock[20]算法，其中LBlock算法采用 4 比特 S 盒，线性操作包括 32 比特字的循环左移 8 位以及按 4 比特 nibble 的置换;基于低延迟理念设计的可以在一个时钟周期内完成一次加密的PRINCE[21]和MANTIS[22]算法，其中PRINCE算法前 5轮与后 5 轮的轮常数具有简单的代数关系，除此之外是互逆的操作。该算法无密钥扩展算法，一部分用作白化密钥，另一部分作为子密钥直接与轮常数和轮状态进行异或，具有α—反射性；专注低能量指标设计的Midori[23]算法等；面向资源极度受限的超轻量级密码LRBC[24]和SLIM[25]等；特别的，美国国家安全局也公布了他们设计的轻量级分组密码SIMON和SPECK[26],它们分别采用逻辑运算和模加运算作为非线性部件结合类似于Feistel的结构，可灵活支持32/48/64/80/96/128比特的分组长度，设计独特新颖。  此外，对于轻量级分组密码部件研究也受到了广泛关注。在轻量级密码部件方面，考虑到硬件实现代价，目前大部分轻量级分组密码都采用了4比特S盒，对其密码学性质的研究已经比较充分。通过定义线性等价和仿射等价，已完成对4比特S盒的分类并给出了16类差分/线性性质达到最优的4比特S盒的代表元，Saarinen[27]又进步定义了置换-异或等价，同一等价类中的S盒不但具有相同的差分和线性性质，而且具有相同的代数性质、电路复杂度等。在线性变换方面，很多轻量级分组密码都使用了比特或字节换位等适宜硬件实现的操作，后续的设计中为了增强扩散性，陆续提出了利用迭代的方式构造分支数达到最优的线性变换,如LED算法中利用有限域矩阵迭代4次构造的MDS矩阵。类似的，Li等人[28]研究了利用扩展的 L-M 结构构建扩散层以获得大尺寸的二元矩阵。  另一方面，对轻量级分组密码的安全性分析也是至关重要的研究内容，由于设计时通常较多的考虑了实现效率的影响，普遍对安全性评估不够，更容易导致安全漏洞。尤其是部分厂商设计使用的简单密码系统如KeeLoq、E0、A5/1、Hitag2等，这些设计普遍过于简单，导致已被成功破解并给出实际攻击。此外，对于近年来提出的某些轻量级分组密码，由于采用了过于简单的轮函数或者特殊的密码结构，导致算法在提出不久就出现安全问题，主要包括： Eichlseder等人[29]通过半截断特征方法对全轮MANTIS的实际密钥恢复攻击等; 张等人[30]通过将持久性故障分析应用于倒数第二轮，可以恢复 80 位的完整 PRESENT 密钥;郝等人[31]分析了TWINE密码的排列规律，提出了一种利用其差分特性的差分故障攻击方法等。上述攻击结果表明现有的都分轻量级分组密码没有提供足够的安全冗余，尤其部分采用特殊结构的密码算法，有可能存在致命的安全缺陷，导致理论破解甚至实际攻击的存在，将对实际应用带来安全隐患。此外还有部分算法的设计原理不明，如美国国家安全局提出的SIMON和SPECK算法，由于缺乏足够的安全性说明和评估，导致对其可能存在安全漏洞或后门的质疑始终存在。研究针对利用在传统密码算法分析领域取得重大进展的新型密码分析方法，特别是近年来飞速发展且取得大量突破成果的自动分析技术，对现有轻量级分组密码安全性的进一步分析和评估是至关重要的。  随着普适计算、物联网技术的发展，轻量级密码会被应用在越来越多的场合。但是不同的轻量级密码的应用场景并不相同，大部分并不能满足车联网的要求。2017年，Santosh Ghosh等人[32] 针对车联网中CAN总线以及ECU的特点，在众多轻量级密码中选取PRINCE, SIMON, SPECK 和PRESENT这四个轻量级密码算法进行了硬件优化实现以及分析。2020年，Castiglione Arcangelo等人[33]评估了用于在车辆上引入轻量级密码的有效性。在实验阶段，使用了汽车级Linux 1 (AGL) 实现PRESENT、SIMON和SPECK，评估它们对系统性能的影响。2021年，Gao Runchen等人[34]针对自动驾驶的图像传输安全问题提出了一种轻量级分组密码。该方法结合了Feistel架构和基于滑动窗口(SCESW)的短加密，在保证其安全性的同时显著降低了计算开销。由于智能网联汽车的热潮，车联网的安全问题是密码学者们目前研究的热点，但是据我们查找文献所知，在这一特殊应用需求下专门设计的轻量级分组密码算法还未发现。因此，面向车联网节点的轻量级分组密码的设计、实现、安全分析还需大量研究，针对面向车联网节点之间的安防密码系统的研究与实现刻不容缓。  参考文献  [1] Liu J, Zhang S, Sun W, et al. In-vehicle network attacks and countermeasures: Challenges and future directions[J]. IEEE Network,2017, 31(5): 50-58.  [2] 鲁赵骏. 车联网隐私保护方案研究[D]. 华中科技大学, 2018.11.  [3] 陈葳葳,曹利,邵长虹.基于区块链技术的车联网高效匿名认证方案[J].计算机应用,2020,40（10）:2992-2999.  [4] A F Suaib Akhter, Mohiuddin Ahmed, et al. A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET[J]. Sustainability, 2021, 13(400):400.  [5] Berger T P, Francq J, Minier M, et al. Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput [J]. IEEE Transactions on Computers, 2016, 65 (7) :2074-2089.  [6] Yeoh W Z, Teh J S, Sazali M I S B M. μ2: A Lightweight Block Cipher[J]. Computational Science and Technology, 2019, 603: 281-290.  [7] Feng J, Li L. SCENERY: a lightweight block cipher based on Feistel structure[J]. Frontiers of Computer Science, 2022, 16(3): 1-10.  [8] Lang L, Botao L, Hui W. QTL: A New Ultra-Lightweight Block Cipher [J]. Microprocessors and Microsystems, 2016,45:45-55.  [9] Mishra S, Sadhya D. Liarx: A lightweight cipher based on the lts design strategy of arx[C]. International Conference on Information Systems Security. Springer-Verlag, 2020. 185-197.  [10] 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.  [11] Kwon H, An S W, Kim Y B, et al. Designing a CHAM block cipher on low-end microcontrollers for internet of things[J]. Electronics, 2020, 9(9): 1548.  [12] Al-Shatari M, Hussin F A, Abd Aziz A, et al. An efficient implementation of LED block cipher on FPGA[C].2019 First International Conference of Intelligent Computing and Engineering (ICOICE). Springer-Verlag ,2019. 1-5.  [13] Tezcan C. Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT [J]. Journal of Systems Architecture, 2022: 102402.  [14] Li W, Cao S, Gu D, et al. Ciphertext-only fault analysis of GIFT lightweight cryptosystem[J]. Science China Information Sciences, 2022, 65(3): 1-3.  [15] Liu B T, Li L, Wu R X, et al. Loong: a family of involutional lightweight block cipher based on SPN structure[J]. IEEE Access, 2019, 7: 136023-136035.  [16] Chen S, Fan Y, Sun L, et al. SAND: an AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations[J]. Designs, Codes and Cryptography, 2021: 1-44.  [17] Patil J, Bansod G, Kumar S K. DoT: A New Ultra-Lightweight SP Network Encryption Design for Resource-Constrained Environment [C]. International Conference on Data Engineering and Communication Technology. Springer-Verlag, 2019.249-257.  [18] Girija M, Manickam P, Ramaswami M. PriPresent: an embedded prime LightWeight block cipher for smart devices [J]. Peer-to-Peer Networking and Applications, 2020,13(5): 1-11.  [19] Lang L, Botao L, Zhou Y. SFN: A New Lightweight Block Cipher [J]. Microprocessors & Microsystems, 2018,60:138-150.  [20] Cui Y, Xu H, Qi W. Improved integral attacks on 24-round LBlock and LBlock-s[J]. IET Information Security, 2020, 14(5): 505-512.  [21] Rashidi B. Low‐cost and two‐cycle hardware structures of PRINCE lightweight block cipher[J]. International Journal of Circuit Theory and Applications, 2020, 48(8): 1227-1243.  [22] Hua J, Liu T, Cui Y, et al. Low-Data Cryptanalysis On SKINNY Block Cipher[J]. The Computer Journal, 2022.  [23] Guo H, Zhang Z, Yang Q, et al. A New Method To Find All The High-Probability Word-Oriented Truncated Differentials: Application To Midori, SKINNY And CRAFT[J]. The Computer Journal, 2022.  [24] Biswas A, Majumdar A, Nath S, et al. LRBC: a lightweight block cipher design for resource constrained IoT devices [J]. Journal of Ambient Intelligence and Humanized Computing, 2020,11(1): 1-15.  [25] Aboushosha B, Ramadan R A, Dwivedi A D, et al. SLIM: A Lightweight Block Cipher for Internet of Health Things [J]. IEEE Access, 2020, 8: 203747-203757.  [26] Beaulieu R, Treatman-Clark S, Shors D, et al. The SIMON and SPECK lightweight block ciphers [C]. Annual Design Automation Conference. IEEE Computer Society, 2015.1–6.  [27] Rafiq A, Khan M. Construction of new S-boxes based on triangle groups and its applications in copyright protection[J]. Multimedia Tools and Applications, 2019, 78(11): 15527-15544.  [28] Li X, Wu W. Constructing Binary Matrices with Good Implementation Properties for Low-Latency Block Ciphers based on Lai-Massey Structure[J]. The Computer Journal, 2021.  [29] Eichlseder M, Kales D. Clustering related-tweak characteristics: application to MANTIS-6[J]. IACR Transactions on Symmetric Cryptology, 2018: 111-132.  [30] Zhang F, Zhang Y, Jiang H, et al. Persistent fault attack in practice[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020: 172-195.  [31] Luo H, Wu Y, Chen W. Differential fault attack on TWINE block cipher with nibble[C].2020 IEEE 20th International Conference on Communication Technology (ICCT). Springer-Verlag, 2020. 1151-1155.  [32] Ghosh S, Misoczki R, Zhao L, et al. Lightweight block cipher circuits for automotive and iot sensor devices[C]. Advanced architectures and algorithms for internet delivery and applications. Association for Computing Machinery, 2017. 1-7.  [33] Castiglione A, Palmieri F, Colace F, et al. Securing the internet of vehicles through lightweight block ciphers[J]. Pattern Recognition Letters, 2020, 135: 264-270.  [34] Gao R, Li S, Gao Y, et al. A lightweight cryptographic algorithm for the transmission of images from road environments in self-driving[J]. Cybersecurity, 2021, 4(1): 1-11. |
| 1. 项目应用前景和学术价值   首先，轻量级分组密码的研究是由实际的应用需求促成的，特别是针对车联网等具体应用领域的专用安全需求。智能网联汽车对时效性要求高，因此我国国密算法应用在车联网体系中存在较多困难。目前可用的专门适用于车联网节点环境的加密方案很少，因此设计公开的、经过详细安全性分析评估的轻量级分组密码有迫切的现实需求，是解决隐私保护、数据保密等安全问题现实可行的解决方案和技术手段。  其次，对于车联网来说，通过数据通信的不光是车内，更大一部分是车外的通信，因此车联网节点的密码算法接口需要统一，对轻量级分组密码安全性的研究，将有助于提高分析效率，有效降低可能的安全隐患，实现更快速、更准确、更公平的安全性评估，推动我国车联网相关的轻量级分组密码标准的征集和制定等。  最后，车联网与人的出行息息相关，车联网的安全严重影响着人民的财产和生命安全。对轻量级分组密码的分析研究能够有效提高我国智能网联汽车的安全性，在理论研究及实际应用中都有着非常重要的意义，无论从战略意义还是安全角度考虑都至关重要，将具有巨大的应用需求和广阔的市场应用前景。   1. 现有研究基础、条件、手段   4.1现有研究基础  本项目组主要成员中，有研究生 4 人（包括申请人黄现彤）。本项目组一直从事轻量级分组密码算法的分析与设计研究，在该领域取得一定的研究成果，目前取得的成果有发明专利3项，发表论文2篇，担任并已结题的国家级、省级、校级项目4项,获得挑战杯等奖项3项。因此，本项目组对轻量级方向形成了一定的研究基础，对研发面向车联网新型低延迟的轻量级分组密码算法有着重要意义。  4.2现有研究条件  项目组所依托的 “嵌入式计算与信息安全研究所” 湖南省重点实验室，目前占地面积80平米，相应重要的实验研发设备均已购置,能提供项目良好的研究开发和工作环境，学校对科研工作很重视，也能提供足够的科研工作时间。该研究所有一支稳定的队伍（在职在岗的教师 2 人，博士、硕士研究生20多人）长期从事轻量级密码算法构造及应用、轻量级密码算法优化、轻量级密码算法安全性分析、密码算法攻击的研究，目前发表多篇SCI论文、申请了多项专利，特别在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，有产学研项目研究经历，在面向产业化应用研发方面具有较好成果。  4.3现有研究手段  本项目组针对目前国内外车联网节点的安全事件以及解决方案，利用各种多媒体、三大数据库、欧洲密码会议、亚洲密码会议、美国密码会议等渠道持续关注与学习。本项目组针对轻量级分组密码算法的结构设计，结合目前主流结构SPN与Feistel以及NIST报告中建议的结构设计规范，本项目组目前采用混合方式构造密码算法结构；针对轻量级密码算法的S盒设计，本项目组有使用位片技术、小盒构造大盒方法、元胞自助机、遗传算法等方法构造S盒的研究与实现；针对轻量级密码算法的P置换设计，本项目组提出了一类自反P置换构造方法，该方法利用二维平面图以及合理的数学定理构造了高扩散且自反的P置换；针对轻量级密码算法的性能评估，本项目组在Xilinx Virtex-5 FPGA以及ASIC上进行硬件评估，评估的指标主要为面积、延迟、功耗、吞吐量等。在8/32位微处理器平台上进行软件评估，评估指标主要为速度、ROM、RAM等。本项目组通过差分分析、线性分析、积分分析、侧信道分析、立方攻击等攻击方法进行安全性评估。   1. 指导教师情况   1）主持与参与的主要项目列表如下：  [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省市联合基金: 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] 湖南省教育厅资助科研重点项目: 轻量级分组密码系统设计关键技术研究 (No.19A072)，2020.1-2022.12.  2）近年发表的相关论文列表如下：  [1] Lang Li, Jingya Feng, Botao Liu, 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)  [2] Lang Li, Botao Liu, Hui Wang. QTL: A New Ultra-Lightweight Block Cipher. Microprocessors and Microsystems, 45 (2016) pp.45-55. (SCI、ESI高引）  [3] Botao Liu, Lang Li\*, Ruixue Wu, Mingming Xie, Qiuping Li. Loong: A family of Involutional Lightweight Block Cipher Based on SPN Structure, IEEE Access, vol.7, pp.136023–136036, 2019. (SCI 3区)  [4] Yu Ou, Lang Li\*. Research on a High-order AES Mask Anti-Power Attack. IET Information Security, 2020-4-14 accepted. (SCI 4区,密码学会推荐B类期刊)  [5] Lang Li, Yi Zou, Ge Jiao. FPGA Implementation of AES Algorithm Resistant Power Analysis attacks. CENet2017, Shanghai, China, Proceedings of Science, 2017, 357-363.  [6] Ying Guo, Lang Li \*, Botao Liu, Shadow: A Lightweight Block Cipher for IoT Nodes, in IEEE Internet of Things Journal [J]. IEEE Internet of Things Journal, 2021, 8(16): 13014-13023. (SCI 1区）  [7] Yu Ou, Lang Li\*. Side-Channel Analysis Attacks based on Deep Learning Network. Frontiers of Computer Science，2020.8 accepted. [https://doi.org/10.1007 /s11704-020- 0209-4](https://doi.org/10.1007%20/s11704-020-%200209-4). (SCI 3区)  [8] Lang Li, Jinggen Liu, Ying Guo, 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)  [9] Di Li, Lang Li\*, Yu Ou. CKGS: A Way Of Compressed Key Guessing Space to Reduce Ghost Peaks[J]. KSII Transactions on Internet and Information Systems (TIIS), 2022, 16(3): 1047-1062. (SCI 4区)  [10] Jingya Feng, Lang Li. SCENERY: a lightweight block cipher based on Feistel structure[J]. Frontiers of Computer Science, 2022, 16(3): 1-10.  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  [2] 指导老师：李浪，学生：郭影，刘景根，曹夏薇，谢玄兰，黄现彤。HBcipher:一种高效的轻量级分组密码，湖南省第十三届“挑战杯”湖南省大学生课外学术科技作品竞赛三等奖.2019.6  [3] 指导老师:李浪，学生：梁琪琦，柴萌。基于轻量级密码的安卓手机图片隐私保护软件，湖南省第15届大学生应用软件作品开发大赛三等奖.2019.8  [4] 指导老师：李浪，学生：郭影、李迪、陈文、杨金玲、刘嘉辉。安全芯伙伴—AI侧信道分析平台，湖南省第十四届“挑战杯”湖南省大学生课外学术科技作品竞赛一等奖.2021.5   1. 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 |

1. **研究方案**

|  |
| --- |
| 1. 研究目标、研究内容和拟解决的关键问题   1.1研究目标  针对车联网架构中，车辆中一些配置较低、面积较小的ECU之间相互通信的过程中，为了数据的安全性、完整性，研发一种专用的轻量级分组密码有着重要意义。因此，本项目将研发一种面向车联网节点的轻量级分组密码算法，为了达到这一目标，需要以下三方面的子目标研究。  （1）针对车联网节点下实际应用的机密性保护需求，设计一种新型低面积、低延迟、低功耗和高安全的轻量级分组密码。  （2）针对车联网对延迟的要求，在密码结构、密码部件等关键环节提出低延迟的设计理论。  （3）针对轻量级密码算法在车联网环境中的可移植性，考虑将轻量级密码算法与车联网节点ECU芯片结合，做到既能快速对明文加密，又不会让ECU因移植算法和加密运算带来过多开销。  1.2研究内容  本次研究项目的内容是针对车联网节点的受限环境下，遵循2017年NIST给出轻量级密码设计准则，研究轻量级分组密码设计与分析方面的理论基础和关键技术，具体研究内容包括：  （1）针对目前车联网环境的安全通信问题以及解决方案进行研究  首先，针对汽车内部通信环境，研究目前车联网中的通信方式；其次，根据现有的智能网联汽车安全事件，研究车联网通信中CAN总线协议存在的安全风险；再次，考虑目前CAN总线协议中已有的安全方案，分析与评估其方案在车联网中的优势与劣势，重点考察低延迟、高效率、高安全的评估标准。最后，针对目前车联网存在的安全风险，考虑已有的研究中存在的不足，确立面向车联网节点的轻量级分组密码的设计目标，其中设计目标重点考虑低延迟指标。  （2）针对现有轻量级分组密码算法的结构进行研究  密码结构通常需要灵活支持32/48/64/80/96比特等多种长度规模，针对车联网中低延迟等应用需求以及特点，研究适用其通信长度的参数的密码结构以及合理的轮数。目前，轻量级分组密码的迭代方法主要有两种：SPN结构、Feistel结构，在结合两种结构的优点的同时，研究具有良好的扩散性和混淆性特点的密码算法。同时，研究对通用密码结构的安全性评估方法，利用差分、线性等攻击方法考察不同结构参数对安全性的影响。  （3）针对轻量级密码算法部件进行设计及安全性评估  首先，针对车联网环境中低延迟的需求，研究直接利用逻辑电路构造轻量级密码组件的方法，以基本逻辑运算的门数、延迟作为权重，研究具有较小硬件实现代价且达到最优密码学性质的非线性和线性组件的设计。其次，针对ECU之间的通信方式，在结合CAN总线协议中的CAN ID特性，以不同的ECU不同加密过程为设计目的，研究轮函数与CAN ID的相关性设计理论。再次，研究基于小规模低深度部件，利用密码结构、迭代多次等方式构造具有低延迟且较优密码学性质的S盒和扩散层的设计理论。最后，针对利用密码结构迭代多次构造的非线性置换，研究其实际差分概率、线性偏差、代数次数等密码特性的精确计算方法。  （4）针对车联网环境对轻量级分组密码进行设计与优化  在上述研究基础上，针对车联网节点下的CAN总线以及ECU的特点，设计一个轻量级分组密码算法来保护通信安全，研究对其安全性的全面精确评估，重点解决在安全冗余和低延迟、低功耗的折中平衡。同时，研究硬件优化实现技术，提出降低延迟的实现方法。  1.3拟解决的关键问题  （1）研究的轻量级密码部件需与部件之间和整体密算法结构之间相互关联，从而设计有混淆原则与扩散原则特性的轻量级密码算法。  （2）研究轻量级密码算法在低复杂性易于实现的同时，还需具有强大的体系结构保证安全性。  （3）设计一个在车联网节点的CAN总线以及ECU的环境限制下低功耗、低延迟且可以抵抗线性和差分等攻击的轻量级分组密码。   1. 拟采取的研究方法及可行性分析   2.1拟采取的研究方法  鉴于本项目的研究内容以及项目组在相关领域的工作积累，拟采取如下详细研究方案和技术路线:   1. 研究轻量级分组密码的在车辆网中应用可行性。   首先，考察现有车联网节点产品使用技术，了解车联网节点之间传输数据完成的业务行为。其次，充分考查节点设备中CAN总线以及ECU的应用，如防抱死制动系统、四轮驱动系统、电控自动变速器、主动悬架系统、安全气囊系统、多向可调电控座椅等，针对CAN总线以及ECU在车联网节点下承担的作用，分析其存在的安全风险。再次，考察车联网节点下使用轻量级密码算法，总结轻量级分组密码在其环境中面临的挑战。最后，结合图1和图2，研究构造一种适用于该场景下小型设备的轻量级分组密码，重点考虑在低资源的情况下，保证其效率和安全性。其中，图1是通过总线通讯协议将 ECU节点连接起来的车内总线网络架构，图2为ECU各节点向CAN总线发送数据的数据帧格式。    图1车联网平台架构示意图  图2 CAN总线报文结构  （2）研究及构建轻量级分组密码算法结构模型  首先，针对密码结构的最新设计趋势，尤其是现有轻量级分组密码，将轮函数和轮数合理搭配是影响密码算法延迟和安全性的重要部分之一。因此，对于通用的密码算法解构，如Feistel结构、各类型广义Feistel结构、SPN结构，考虑将轮数以及CAN ID细化为轮函数内部具体信息，提取出其中的共性指标，对密码算法的结构进一步建立。其次，针对算法加密过程中需抵抗一些常见的攻击方法，重点研究加密算法的加密轮函数与密钥扩展，从而提供良好的安全性；除此之外，为使轻量级密码算法具有低延迟的特性，通过密码算法结构特征，研究构造出适用于车联网节点下的轻量级密码算法。图3为项目组按照上述思路构造的技术示例图。图4 面向车联网节点的轻量级密码算法设计结构模型    图3 轻量级密码算法技术示例图    图4轻量级密码算法设计的结构模型  （3）研究及设计轻量级密码部件。  首先，总结现有轻量级密码算法设计的特点和可能存在的安全性风险，特别是总结轻量级分组密码存在的安全共性问题。其次，研究基于非线性不变量、可分性质等新型密码分析思想对轻量级分组密码的应用。再次，针对PRESENT、PICCOLO、 TWIN等基于传统密码和P置换设计结构轻量级分组密码，结合置换表、线性变换矩阵、代数式、方程组、逻辑结构图等相关的扩散层构造方法，重点研究其结构特殊性质并进行优化，构造具有自反性、扩散快的P置换。最后系统研究S盒的密码性质，考虑车联网中低延迟需求，结合对轮函数经过多轮迭代后的线性变换矩阵秩、整体代数次数、子密钥相关性等密码特性的分析，着重解决具有低延迟性能且达到最优/较优密码性质的S盒和线性变换的设计方法和实现技术。最后图5为项目组按照上述思路构造的技术示例图。    图 5 一种44的S盒构造结构图  （4）研究轻量级分组密码的攻击方法。  考察目前攻击者对车联网中常用的攻击手法，结合现有轻量级分组密码的设计特点和可能存在的安全弱点，利用对传统分组密码安全性分析的研究成果和工作积累，研究安全性高的密码算法。针对现有的典型轻量级分组密码，采用MILP求解技术，研究差分攻击、线性攻击、相关密钥攻击、代数攻击、整数攻击、中间相遇攻击、不可能差、立方攻击等主要分析方法，特别是由于轻量级分组密码在车联网中开放环境使用特点，还需研究其抗旁路攻击能力。  （5）研究车联网环境下的轻量级分组密码算法设计  结合上述的研究基础上，充分调研车联网节点下特殊应用的安全性需求，确定算法的设计需求及软硬件实现模型、延迟和安全性等指标要求，研发一个资源环境限制下低延迟、高安全、低能耗的轻量级密码算法。针对密码算法在安全冗余与实现性能间的合理平衡，研究的轻量级密码算法具有分组规模小、轮函数简单、密码算法轮函数与轮数合理搭配等主要特点。轻量级分组密码算法研究设计出来后，在此基础上，对算法进行整体实测，以及对密码算法进行差分、线性等安全性分析。图6为本项目设计的轻量级分组密码算法的F1函数加密结构图，其中右边为F1函数端口结构图，左边为F1函数具体加密结构图。    图 6 轻量级密码算法F1函数加密结构图  2.2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）目前可用的专门适用于车联网节点环境的加密方案很少，研究适用于该环境的专用轻量级密码算法是本项目的特色。  （2）在轻量级分组密码设计中考虑低延迟等新指标是本项目的设计特色，兼顾硬件实现面积、低延迟、低功耗和高安全具有自反性的密码部件构造是本项目的创新之一。  （3）结合CAN总线下ECU数据传输的特征，构造一种加密过程不重复的轻量级分组密码算法是本项目的创新之一。   1. 预期研究进展   1）2022年6月—2022年11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，研究和学习轻量级密码算法设计原理以及车联网节点架构，为本项目算法设计打下基础。  2）2022年12月—2023年6月  研究轻量级密码部件的精确密码特性的计算方法，并应用到对具体轻量级分组密码的实际攻击研究。  轻量级S盒、行移位与列混合、各密码组件函数的研究与低延迟性能优化。  3）2023年7月—2023年11月  对典型的轻量级分组密码结构进行深入研究。同时，研究密码结构与密钥、轮函数与轮数、低延迟与轮函数、低延迟与轮数的相关性，结合各种攻击方法来研究密码结构的安全性评估。  4）2023年12月—2024年6月  基于轻量级密码部件和通用密码结构研究的研究结果，针对车联网节点的特性，完成轻量级分组密码的设计，并对新算法进行全面的安全性评估和软硬件优化实现及性能测试。  对项目研究工作进行总结，准备项目结题，撰写总结报告，参加结题答辩。   1. 预期成果 2. 发表SCI论文一篇以上。 |

**四、研究基础**

|  |
| --- |
| 与本项目有关的研究工作积累和已取得的研究工作成绩及目前承担项目的情况（项目负责人和其它成员情况分开填写并且项目、成果及奖励等须注明承担或完成人姓名等相关信息）   1. 与本项目有关的研究工作积累和已取得的成绩   本项目组一直从事分组密码的分析与设计研究，对最近几年的一些轻量级分组密码算法的结构以及组件特点进行了研究与分析，阅读了相关的最新轻量级密码算法论文并对论文中提出的算法进行了实现，对轻量级密码算法已取得一定的成果和经验，并且本项目组对于面向车联网节点的轻量级密码算法也已经有了初步的研究，与轻量级密码算法有关的论文、专利、获得的奖以及完成的项目如下。  项目负责人：  [1] **Xiantong Huang**，Lang Li，Ying Guo. The optimal implementation of Khudra Lightweight Block Cipher.CENet2019, Changsha, China, Springer,2019.  [2] 冯景亚，李浪，郭影，**黄现彤**. Midori密码算法FPGA优化研究.衡阳师院学院学报, 2020, 41(3):133-138.  [3] 李浪，**黄现彤**.一种轻量级AEROGEL分组密码的加密实现方法.申请号：202010244240.1  [4] 国家级大学生创新创业训练计划项目（S201910546006），一种轻量级分组密码构造的研究与实现，研究年限：2019.5-2020.5,已结题,主持.  [5] 衡阳师范学院大学生课外学术科技创新基金重点项目（校科字【2021】2号-31）,一种S盒构造方法实现与研究, 研究年限：2018.11-2019.11,已结题,参与.  [6] 郭影,刘景根,曹夏薇,谢玄兰,**黄现彤** (指导教师：李浪). HBcipher:一种高效的轻量级分组密码,第十三届“挑战杯“湖南省大学生课外学术科技作品竞赛三等奖,湖南省教育厅,2019.  [7] 刘景根,**黄现彤**,谢玄兰,杨紫荆,曹夏薇(指导教师：李浪). 衡阳师范学院第十九届大学生课外学术科技作品竞赛一等奖,衡阳师范学院,2019.4.  [8] **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.  项目其他成员：  [1] 李浪，**宋庆玲**，杨金玲，李永超. 一种轻量级可调分组密码实现方法、系统、电子设备以及可读存储介质. 申请号：202011301394.6.  [2] 郭影, **宋庆玲**, 李浪. 深度学习模型的权重矩阵加密软件V1.0, 登记号: 2020SR1092477.   1. 目前承担项目情况   [1] 衡阳师范学院第二十二届大学生课外学术科技作品竞赛, 自主知识产权的车联网终端安防密码系统，衡阳师范学院,2021.9. |

**五、经费预算**

|  |  |  |
| --- | --- | --- |
| 支 出 科 目 | 金 额  （万元） | 计 算 根 据 及 理 由 |
| 合 计 | 1 |  |
| 科研业务费 | 0.5 | 参加相关会议、调研学习交流等差旅费用 |
| 论文发表、专利申请等费用 |
| 实验材料费 | 0.5 | 所需易耗芯片、测试板等 |
| 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。项目内容主要是面向车联网节点的环境限制下，研究一种低延迟、低功耗且可以抵抗线性和差分等攻击的轻量级分组密码。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 |