□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优化实现 | | | | | | | 研究  类别 | | 基础研究 | |  |
| 应用研究 | | √ |
| 试验发展 | |  |
| **研究**  **年限** | 2024 年至 2026 年 | | | | | 申请经费（万元） | | | | 1 | | |
| **项目**  **主持**  **人** | 姓名 | 向嘉豪 | 性别 | | 男 | | 身份证号 | | | 430525200011025117 | | |
| 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： 23 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 | |
| 邓联瑞 | 430503200101071514 | | 无 | 电子信息 | | | | 衡阳师范学院 | |  | |
| 夏生成 | 43042219980524379X | | 无 | 电子信息 | | | | 衡阳师范学院 | |  | |
| 岳兴起 | 430502200202175519 | | 无 | 网络空间安全 | | | | 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项目负责人在长沙学院学习本科专业。  2023.9~2026.6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  随着基础通信设施的不断完善，如5G网络的普及，人们对通信的需求逐渐增加。这种需求的增长催生了大量基于通信的应用，如工业互联网、车联网、物联网等。然而，随着这些网络中传输的数据量的增加，安全问题变得越来越严重。这主要是由网络数据中数据包传输机制引起的。幸运的是，对称加密算法提供了一种解决方案，只需双方协商好密钥，就能确保数据在公共信道下的安全传输，而无需调整传输机制。  对称加密算法中，最广泛使用的是2001年的AES[1]国际算法。它在WEB、WIFI等领域，以及服务器与个人计算机上都得到了广泛的应用。然而，为了避免AES算法存在的未知门陷，我国在2006年提出了SM4[2] 对称加密算法来替代AES算法。值得一提的是，SM4在2021年正式成为ISO标准并得到了国际认可。这些传统的对称算法在计算资源充足的场景下，能够提供较高的安全性。但在计算资源受限的场景下，由于这些算法的计算复杂度较高，因此需要一种更加轻量级的对称加密算法来满足这种场景的需求。  美国国家标准局NIST于2019年启动了轻量级密码算法LWC的征召。在56个轻量级密码算法的竞争中，ASCON[3]算法经过三轮筛选，最终脱颖而出。到了2023年，ASCON算法已经成为NIST的轻量级加密标准。由于ASCON算法在资源受限的场景下表现出较高的性能，因此在物联网、车联网等场景中具有广泛的应用前景。  相较而言，我国在轻量级加密算法上的起步较晚，暂时还没有自己的轻量级加密算法标准。然而，在2019年由中国密码学会组织的全国密码算法设计竞赛中，一等奖获得者是一种名为uBlock[4]的轻量级加密算法。这种算法在计算资源充足的环境下表现优秀，同时在资源受限的场景下，也展现出了高性能。尽管如此，uBlock算法并未像ASCON算法那样得到广泛的学者关注，这使得我国在轻量级加密算法上与国际顶尖水平存在较大的差距。  这种差距不仅体现在轻量级加密算法的设计上，也同样存在于其实现上。这包括硬件和软件实现。具体来说，需要考虑如何高效设计硬件加密的IP核，并将其集成入芯片，以实现硬件级别的安全。同时，也需要考虑如何将加密算法高效实现于8-bit或32-bit的微控制器中，以确保应用的软件级别安全。我国在这个领域的研究相对较少。因此，本项目的目标是研究轻量级加密算法的实现，以推动我国在轻量级加密算法领域的研究进展。  1.2项目的研究意义  在上世纪的算法设计中，对称加密算法的设计主要考虑了安全性。然而，这些设计往往较少考虑其在资源受限的场景下的性能。例如，DES[5]的实现部分提及其在软件与硬件的实现，但并未给出具体的参考实现方案与实现性能。  在NIST的LWC竞赛中，轻量级加密算法的设计不仅考虑了安全性，还考虑了其在资源受限的场景下的实现性能[6]。这无疑对算法的设计提出了更高的要求。实现算法设计与实现性能之间的桥梁，是本项目研究的出发点。在考虑最新的软硬件平台技术下，将加密算法的组件转化为相应的电路或程序，是本项目研究的手段。更具体来说，本项目的研究意义体现在以下几个方面：  1. 研究轻量级加密算法在专用集成电路(ASCI)和现场可编程门阵列(FPGA)上的硬件实现。这将提高算法实现的性能，同时确保其硬件级别的安全。  2. 研究轻量级加密算法在8-bit或32-bit的微控制器上的软件实现。这将提高算法实现的性能，同时确保其软件级别的安全。  3. 研究轻量级加密算法的软硬件协同实现。在确保算法实现的灵活性的前提下，最大程度地提高算法实现的性能。   1. 国内外研究现状分析和发展趋势   网络数据传输量的增加使得网络安全问题日益严重。对称加密算法是一种能够确保数据在公共信道下安全传输的解决方案。然而，传统的对称加密算法在计算资源受限的场景下计算复杂度较高。因此，需要一种轻量级的对称加密算法来满足这种场景的需求。  在2011年之前，轻量级加密算法的研究主要集中在硬件实现上。这是因为硬件实现能够提供更高的性能，如ISO的轻量级加密标准PRESENT[7]。同时，硬件实现也能确保算法的安全性。然而，随着应用场景的增加，性能需求也在变化。现在，不仅关注硬件的电路面积，也开始关注软件加密的执行时间，如美国国家安全局(NSA)2013年提出的SIMON[8]。此外，还关注硬件加密的功耗，如2015年亚密会提出的Midori[9]，以及硬件加密的时延，如2016年美密会提出的SKINNY[10]。因此，轻量级加密算法的内涵正在不断扩展。  2.1轻量级加密算法硬件实现  轻量级加密算法的设计和实现都在不断发展和完善。早期的轻量级加密算法主要集中在硬件实现上。例如，Arich等人对DES算法的硬件实现[11]，他们将DES的加密速率提高到了1 Gbits/s。随着硬件实现的进步，性能指标也从电路面积和加密吞吐量扩展到了功耗和时延等方面。为了实现这些性能指标，提出了一些全新的硬件实现技术。其中，串行、展开、迭代、流水线等技术得到了广泛应用。  串行实现的核心思想是降低加密时的数据带宽。这种方法可以实现对加密组件的重复使用，并减少电路中的寄存器使用数量，以实现更低的电路面积。Good等人提出了AES算法的串行实现[12]。他们在Xilinx Spartan-II FPGA (XC2S15)上实现了面积资源174 slices和两个内存块。在这种实现中，最小的数据带宽为一个字节。为了进一步降低数据带宽，Leong等人提供了IDEA算法的比特级数据带宽的串行实现[13]。然而，对于以S盒作为基本加密组件的加密算法，实现一比特级的数据带宽是困难的。为了解决这个问题，Jean等人为类SPN结构的加密算法提出了比特滑动技术[14]。这种技术可以实现比特级的数据带宽。  展开实现的核心思想是在同一周期内计算加密算法的多轮函数。这种方法可以降低加密所需的延迟，并在引入更多面积的情况下获取更高的吞吐量。Elbirt等人在AES算法竞选的最终轮中使用了展开实现[15]。他们的2轮展开实现Rijndael算法实现了最高的吞吐量，这在对比基于轮的迭代实现时尤为明显。Gupta等人将展开实现与流水线结合[16]，这极大地提高了RC4[17]算法的吞吐量。  迭代实现的核心思想是在同一周期内运算加密算法的一轮函数。通过反馈机制，可以实现多轮函数的计算。这种方法可以减少加密所需的面积，但会增加加密所需的延迟。值得注意的是，迭代实现在面积与吞吐量之间实现了较好的平衡。在AES算法竞选的最终轮中，Elbirt等人的迭代实现的Rijndael获得了最高的吞吐量与面积比[15]。类似的情况也出现在LWC竞赛中。ASCON算法的迭代实现在面积与吞吐量上取得了较好的平衡[6]。  流水线实现的核心思想是将加密算法的一轮函数分解为多个阶段。这样，每个阶段的计算可以并行进行，实现多个分组同时加密。这种方法可以显著提高加密所需的吞吐量，但会增加实现的面积。Kryjak等人运用了这种流水线技术[18]。他们对CLEFIA[19]算法进行了实现，极大地提高了加密的吞吐量。然而，考虑到所需的资源，这种实现主要适用于超性能计算场景。  总的来说，对于传统的性能指标，如面积和吞吐量，轻量级加密算法的硬件实现已经有了较好的解决方案。然而，对于新的性能指标，如功耗和时延，还需要进一步的研究。未来的研究重点是如何提出新的硬件实现技术，以适应这些新的性能指标。  2.2轻量级加密算法软件实现  轻量级加密算法的软件实现主要集中在微控制器上。这与硬件实现有所不同。微控制器提供了更高的灵活性。例如，可以在不同的应用场景下调整加密算法的参数，或者使用不同的加密算法。同时，微控制器也提供了更高的可移植性。例如，可以在不同的硬件平台上运行加密算法。然而，相比硬件实现，软件实现的性能指标通常较低。  早期的轻量级加密算法的软件实现主要集中在8-bit微控制器上。这些微控制器常用于RFID和传感器等设备。在1991年，Merkle尝试将Khufu算法进行软件实现。这为算法在其他不同场景下的应用打开了新的可能性[20]。后来，Osvik将AES算法实现在8-bit的AVR微控制器上，刷新了当时的最快加密记录[21]。  随着微控制器的发展，32-bit微控制器成为主流。软件实现的侧重也发生了改变。Rogaway开始在32-bit的现代微控制器上，对SEAL算法进行了软件实现[22]。Bertoni首次将AES算法实现在32-bit的微控制器上，并通过多种架构的仿真器对优化实现进行验证[23]。Schwabe在结合ARM平台在Cortex-M3和M4上实现了AES算法，扩展了AES算法的用途[24]。  在软件实现中，存在一些特殊的情况需要注意。例如，抵抗侧信道攻击通常需要添加额外的操作。如何更高效地实现这些抗攻击的操作，成为了一个重要的研究方向。例如，Rivain提出了一种高阶掩码技术[25]。这种技术可以有效地抵抗设备在侧信道攻击中的相关功耗攻击。另一方面，轻量级加密算法在某些场景下具有优势。例如，在区块链等对加密算法吞吐量要求较高的场景下，轻量级加密算法可以发挥重要作用。利用SIMD指令集可以提高加密算法的吞吐量[26]。此外，也可以利用GPU来实现加密[21]。这些都是软件实现的重要方向。  总的来说，软件实现的技术比硬件实现更为丰富。因此，许多研究都集中在如何将加密算法高效地实现在更先进的平台上。未来的研究重点将是开发新的软件实现技术，以适应这些新的平台。同时，也需要考虑如何预防新的攻击方式。  2.2轻量级加密算法软硬件协同实现  相比硬件实现和软件实现，软硬件协同实现的研究相对较少。这主要是因为软硬件协同实现需要同时考虑硬件和软件的特性。然而，软硬件协同实现在保证算法性能的同时，也能提高算法的灵活性。例如，当加密算法的标准发生变化时，软硬件协同实现能够更快地适应这些变化。值得注意的是，与硬件实现和软件实现相比，软硬件协同实现起步较晚。  在早期的实现中，加密算法的硬件实现和软件实现通常是分开的。例如，加密算法作为IP核心，以片上外设的形式挂载在数据总线上，如Usselmann实现的AES算法[27]。由于外设与CPU之间的通信开销较大，这种实现方式的性能较低。为了提高性能，一些研究开始尝试将加密算法的硬件实现与软件实现集成在一起。这种实现方式可以减少外设与CPU之间的通信开销，从而提高性能。然而，由于各家厂商的CPU架构不同且闭源，这种实现方式的研究较少。  开源硬件的发展为软硬件协同实现的研究带来了新的机遇。例如，RISC-V是一种开源的CPU架构，可以自由使用。这种架构的出现，为软硬件协同实现提供了新的研究方向。Marshall设计了一套轻量级扩展指令集，将ChaCha算法实现在RISC-V上[28]。基于扩展指令集，Chen在2023年提出了一组通用扩展指令集在RISC-V之上，并将其运用到了LWC最终轮的10个算法上[29]。这种方式将加密的硬件电路集成入了CPU的执行流水线中，保证了加密操作的速度。同时，加密算法中的通用操作被设计为对应的指令，这样即使加密标准更新，也能保持对加密算法的加速效果。  总的来说，软硬件协同实现为轻量级加密算法的实现开辟了新的研究方向。这种实现方式将不利于软件实现的部分转化为硬件实现，并以此作为基础操作。然后，利用软件指令来构建整体算法，从而在加密算法的性能与灵活性之间取得平衡。这也为算法设计提供了一条全新的思路。未来的研究重点是将轻量级加密算法中的通用操作设计为扩展指令集或通用加密IP核。。  参考文献  [1] Daemen, Joan, and Vincent Rijmen. "AES proposal: Rijndael." (1999).  [2] Diffie, Whitfield, and George Ledin. "SMS4 encryption algorithm for wireless networks." Cryptology ePrint Archive (2008).  [3] Dobraunig, Christoph, et al. "Ascon v1. 2: Lightweight authenticated encryption and hashing." Journal of Cryptology 34 (2021): 1-42.  [4] Wen-Ling, Wu, et al. "The block cipher uBlock." Journal of Cryptologic Research 6.06 (2019): 690-703.  [5] Pub, F. I. P. S. "Data encryption standard (des)." FIPS PUB (1999): 46-3.  [6] Mohajerani, Kamyar, et al. "FPGA benchmarking of round 2 candidates in the NIST lightweight cryptography standardization process: Methodology, metrics, tools, and results." Cryptology ePrint Archive (2020).  [7] Bogdanov, Andrey, et al. "PRESENT: An ultra-lightweight block cipher." Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. Springer Berlin Heidelberg, 2007.  [8] Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers." Proceedings of the 52nd annual design automation conference. 2015.  [9] Banik, Subhadeep, et al. "Midori: A block cipher for low energy." Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29--December 3, 2015, Proceedings, Part II 21. Springer Berlin Heidelberg, 2015.  [10] Beierle, Christof, et al. "The SKINNY family of block ciphers and its low-latency variant MANTIS." Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36. Springer Berlin Heidelberg, 2016.  [11] Arich, Touria, and Mohssine Eleuldj. "Hardware implementations of the data encryption standard." The 14th International Conference on Microelectronics,. IEEE, 2002.  [12] Good, Tim, and Mohammed Benaissa. "AES as stream cipher on a small FPGA." 2006 IEEE International Symposium on Circuits and Systems. IEEE, 2006.  [13] Leong, Monk-Ping, et al. "A bit-serial implementation of the international data encryption algorithm IDEA." Proceedings 2000 IEEE Symposium on Field-Programmable Custom Computing Machines (Cat. No. PR00871). IEEE, 2000.  [14] Jean, Jérémy, et al. "Bit-Sliding: A Generic Technique for Bit-Serial Implementations of SPN-based Primitives: Applications to AES, PRESENT and SKINNY." Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. Springer International Publishing, 2017.  [15] Elbirt, Adam J., et al. "An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 9.4 (2001): 545-557.  [16] Gupta, Sourav Sen, et al. "High-performance hardware implementation for RC4 stream cipher." IEEE Transactions on Computers 62.4 (2012): 730-743.  [17] Paul, Goutam, and Subhamoy Maitra. RC4 stream cipher and its variants. CRC press, 2011.  [18] Kryjak, Tomasz, and Marek Gorgon. "Pipeline implementation of the 128-bit block cipher CLEFIA in FPGA." 2009 International Conference on Field Programmable Logic and Applications. IEEE, 2009.  [19] Shirai, Taizo, et al. "The 128-bit blockcipher CLEFIA." Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14. Springer Berlin Heidelberg, 2007.  [20] Merkle, Ralph C. "Fast software encryption functions." Advances in Cryptology-CRYPTO’90: Proceedings 10. Springer Berlin Heidelberg, 1991.  [21] Osvik, Dag Arne, et al. "Fast software AES encryption." Fast Software Encryption: 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers 17. Springer Berlin Heidelberg, 2010.  [22] Rogaway, Phillip, and Don Coppersmith. "A software-optimized encryption algorithm." Journal of Cryptology 11 (1998): 273-287.  [23] Bertoni, Guido, et al. "Efficient software implementation of AES on 32-bit platforms." Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4. Springer Berlin Heidelberg, 2003.  [24] Schwabe, Peter, and Ko Stoffelen. "All the AES you need on Cortex-M3 and M4." International Conference on Selected Areas in Cryptography. Springer International Publishing, 2016.  [25] Rivain, Matthieu, Emmanuel Prouff, and Julien Doget. "Higher-order masking and shuffling for software implementations of block ciphers." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2009.  [26] Xu, Runqing, et al. "High-throughput block cipher implementations with SIMD." Journal of Information Security and Applications 70 (2022): 103333.  [27] Usselmann, Rudolf. "Advanced encryption standard/rijndael ip core." 2007-08-20. https://opencores.org/projects/aes\\_core (2002).  [28] Marshall, Ben, Daniel Page, and Thinh Hung Pham. "A lightweight ise for chacha on risc-v." 2021 IEEE 32nd International Conference on Application-specific Systems, Architectures and Processors (ASAP). IEEE, 2021.  [29] Cheng, Hao, et al. "RISC-V instruction set extensions for lightweight symmetric cryptography." IACR Transactions on Cryptographic Hardware and Embedded Systems (2023): 193-237. |
| 1. 项目应用前景和学术价值   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 |