项目申请书

向嘉豪

2024 年 4 月 17 日

1 立项依据

1.1 项目的研究目的、意义

1.1.1 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。

1.1.2 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 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。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设计。在确保算法实现的灵活性的前提下，这将最大程度地提高算法实现的性能。

1.2 国内外研究现状分析和发展趋势

1.3 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).

2 研究方案