

# 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

## 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.

1.4 项目应用前景和学术价值

1.5 现有研究基础、条件、手段

1.5.1 现有研究基础

1.5.2 现有研究条件

1.5.3 现有研究手段

## 2 研究方案

2.1 研究目标、研究内容和拟解决的关键问题

2.1.1 研究目标

2.1.2 研究内容

2.1.3 拟解决的关键问题

2.2 拟采取的研究方法及可行性分析

2.2.1 拟采取的研究方法

2.2.2 可行性分析

2.3 本项目的创新之处

2.4 预期研究进展