

## 摘要

分组密码运行速度快且易于实现,被广泛运用于各种软硬件安全系统。随着分组密码的设计理论不断完善,目前广泛使用的密码算法拥有优秀的理论安全性。然而,在实际工程应用中,差分故障攻击可以在密码设备执行过程中注入故障,并分析故障密文与正确密文之间的关系获得相关的密钥信息,差分故障攻击具有高效的分析效率,能够对加密设备构成严重威胁。因此,研究分组密码算法如何有效检测故障并抵抗差分故障攻击是目前的研究热点之一。

本文主要基于线性结构、线性码及动态秘密 S 盒等思想,针对分组密码算法 DEFAULT 和 Pyjamask 进行差分故障的防护方案设计。主要研究成果如下:

1. 针对 DEFAULT 密码算法无法有效抵抗差分故障攻击的问题,基于横向混淆和线性码的思想,提出一种自动检测所有比特故障的防护方案。方案使用横向混淆实现密码算法的冗余部分,并利用[10, 4, 6]线性码的检错功能对每个 S 盒输入进行防护。研究表明,新的防护方案在 25.08%额外软件实现下,能够有效地检测所有比特故障并纠错半字节的故障,其中检测在 S 盒注入故障的比例为 100%。与已有防护方法相比,新方案在软件实现代价上减少了 31.92%,且具备自动纠错的防护能力。

2. 针对 DEFAULT 算法无法抵抗结合信息差分故障攻击的问题,基于 DEFAULT 算法结构设计和动态秘密 S 盒的思想,提出一种抵抗差分故障攻击的新算法 DEFAULT-DS。算法在 DEFAULT 算法设计的基础之上,利用动态秘密 S 盒的思想改进算法的 S 盒构造。DEFAULT-DS 引入 15 个具有 3 个非零线性结构的秘密 S 盒,并用轮密钥选择 S 盒。实验结果表明,对于经典差分故障攻击和基于结合信息的差分故障攻击,算法提供至少 64 个故障和  $2^{64}$  比特的密钥搜索空间的差分故障防护能力。与已有的防护方案相比较,新提出的算法在不添加冗余的情况下提供有效的差分故障防护能力,相较于 DEFAULT 算法,提高了  $2^{64}$  比特的密钥搜索空间。

3. 针对 Pyjamask 密码算法无法有效抵抗差分故障攻击的问题,基于线性结构和线性码,为 Pyjamask 分组密码算法提供一种差分故障防护方案。方案基于 DEFAULT 算法设计思想,在 Pyjamask 算法前后分别增加 4 轮轮函数,增加的轮函数使用带有 3 个非零线性结构的 S 盒,同时使用一个[10, 4, 6]线性码保护每个 S 盒的输入。实验结果表明,新的防护方案在 39.46%的额外软件实现下,可以为经典差分故障攻击提供 64 个故障和  $2^{64}$  比特密钥搜索空间的防护能力,且方案能提供单比特的纠错能力和全比特的检错能力。相较以往的防护方案,新的方案在实现性能仅增加 2.62%的情况下,提供了单比特自动纠错功能。

**关键词:** 分组密码; 差分故障攻击; 故障检测; 线性结构; 线性码

## Abstract

Block cipher is widely used in hardware and software security systems because of its fast implementation. With the continuous improvement of the design theory of block cipher, the cryptographic ciphers widely used at present have excellent theoretical security. However, in engineering applications, differential fault attack (DFA) can inject faults during the execution of cryptographic devices and analyze the relationship between faulty ciphertext and correct ciphertext to analyze relevant key information. Differential fault attacks have efficient analysis efficiency and can pose a serious threat to cryptographic devices. Therefore, the research on how to effectively detect faults and resist differential fault attack in block ciphers is one of the current research hotspots.

Based on the idea of linear structure, linear code and dynamic secret S-box, this thesis designs a differential fault protection scheme for block cipher algorithms DEFAULT and Pyjamask. The main research results are as follows:

1. Based on the ideas of horizontal confusion and linear code, a protection scheme is proposed for DEFAULT cipher to automatically detect all bit faults to solve the problem that DEFAULT cannot resist differential fault attacks effectively. The scheme uses horizontal obfuscation to implement the redundant parts of the cipher, and utilizes the error detection of [10, 4, 6] linear codes to protect each S-box. The experimental results show that the new protection scheme can detect all bit faults and correct nibble faults with 25.08% additional software implementation, where the proportion of detected faults is 100%. Compared with existing protection methods, the new method reduces software implementation costs by 31.92% and has the ability to automatically correct protection.

2. Based on the idea of DEFAULT cipher design and dynamic secret S-box, a new cipher DEFAULT-DS is proposed to resist differential fault attack to address problem that DEFAULT being unable to resist information-combining differential fault attack. Based on the design of the DEFAULT cipher, DEFAULT-DS utilizes the idea of dynamic secret S-boxes to improve the S-box construction of the cipher. DEFAULT-DS introduces 15 secret S-boxes with 3 non-zero linear structures and selects S-boxes using the round key. The experimental results show that for classical differential fault attacks and Information-combining differential fault attack (IC-DFA), the cipher provides differential fault protection capabilities that require at least 64 faults and  $2^{64}$ -bit key search spaces. Compared with existing protection schemes, the proposed cipher provides effective

differential fault protection capability without adding redundancy, and increases the key search space by  $2^{64}$ -bit compared to DEFAULT.

3. Based on linear structure and linear code, a differential fault protection scheme for Pyjamask block cipher is gifted to solve the problem that Pyjamask can not resist the differential fault attack effectively. The scheme is first based on the design concept of the DEFAULT cipher, adding 4 additional round functions before and after the Pyjamask. The added round functions use S-boxes with 3 non-zero linear structures, and a [10,4,6] linear code is used to protect the input of each S-box. The experimental results show that the new protection scheme can provide protection against 64 faults and  $2^{64}$ -bit key search spaces for classical differential fault attacks with 39.46% additional software implementation, and the scheme can provide the capability of single bit error correction and full bit error detection. Compared to previous protection schemes, the new scheme provides single bit error correction function with only 2.62% increase in performance.

**Keywords:** Block cipher; Differential fault attack; Fault detection; Linear structure; Linear code

# 目录

韦永壮

|                                     |    |
|-------------------------------------|----|
| 摘要 .....                            | I  |
| Abstract.....                       | II |
| 第一章 绪论.....                         | 1  |
| §1.1 研究背景与意义 .....                  | 1  |
| §1.2 研究现状 .....                     | 3  |
| §1.2.1 差分故障攻击研究现状 .....             | 3  |
| §1.2.2 差分故障防护研究现状 .....             | 4  |
| §1.3 论文组织架构 .....                   | 5  |
| 第二章 预备知识.....                       | 7  |
| §2.1 分组密码 .....                     | 7  |
| §2.2 分组密码的故障分析 .....                | 10 |
| §2.2.1 差分故障攻击 .....                 | 11 |
| §2.2.2 差分故障防护方法 .....               | 12 |
| §2.3 本章小结 .....                     | 13 |
| 第三章 针对 DEFAULT 密码算法的差分故障防护方法 .....  | 14 |
| §3.1 DEFAULT 密码算法简介 .....           | 14 |
| §3.2 线性码简介 .....                    | 16 |
| §3.3 横向混淆和纵向隐藏 .....                | 17 |
| §3.4 DEFAULT 算法的防护方案.....           | 18 |
| §3.4.1 基于横向混淆的 DEFAULT 算法实现.....    | 18 |
| §3.4.2 基于线性码的故障检测 .....             | 20 |
| §3.5 结果对比与分析 .....                  | 22 |
| §3.6 本章小结 .....                     | 24 |
| 第四章 抵抗差分故障攻击的分组密码设计 .....           | 25 |
| §4.1 结合信息的差分故障攻击 .....              | 25 |
| §4.2 S 盒的线性结构 .....                 | 28 |
| §4.3 动态秘密 S 盒 .....                 | 29 |
| §4.4 抗差分故障攻击 DEFAULT-DS 算法的设计 ..... | 30 |
| §4.5 结果对比与分析 .....                  | 32 |
| §4.6 本章小结 .....                     | 33 |
| 第五章 Pyjamask 密码算法的差分故障防护方案 .....    | 34 |

|                               |    |
|-------------------------------|----|
| §5.1 Pyjamask 密码算法简介 .....    | 34 |
| §5.2 Pyjamask 密码算法的防护方案 ..... | 37 |
| §5.3 结果对比与分析 .....            | 38 |
| §5.4 本章小结 .....               | 40 |
| 第六章 总结与展望 .....               | 41 |
| §6.1 论文总结 .....               | 41 |
| §6.2 工作展望 .....               | 42 |
| 参考文献 .....                    | 43 |
| 致谢 .....                      | 49 |
| 作者在攻读硕士期间的主要研究成果 .....        | 50 |

## 第一章 绪论

本章将围绕分组密码算法的差分故障攻击及其防护方法进行介绍，首先介绍本课题的研究背景及意义；其次介绍分组密码算法的差分故障攻击及防护方法的研究现状；最后给出论文整体的内容安排。

### § 1.1 研究背景与意义

随着移动通信网络的发展，物联网技术在各行业中得到了广泛的应用。信息安全问题成为物联网时代发展的障碍，近年不断发生的信息安全事件，严重影响了社会的发展，对国家和国民经济造成了严重的影响。人们对信息的安全存储及传输有着越来越高的要求。密码技术是保障信息安全的重要手段，密码学的起源最早可以追溯到古埃及时期古希腊和罗马时期。在公元前 440 年前的古希腊战争中，为了推翻波斯人的统治，奴隶主赫斯坦与爱奥尼亚城统治者采取联合行动，双方通过在奴隶头皮上刺字进行保密通信。这些“古代加密技术”被视为密码学技术的萌芽。密码技术随着历史的发展在不断的改进，20 世纪初到 20 世纪 50 年代由古典密码过渡到近代密码阶段。1949 年香农发表了论文《保密系统的通信理论》，标志着现代密码学的开端。

密码学包括密码编码学和密码分析学两个领域。密码编码学致力于研究如何设计速度快、安全性高的密码体制来保护信息安全，而密码分析学则专注于分析和攻击各种密码编码体制。例如，分析分组密码算法的安全性主要思想是在通信过程中，第三方攻击者在不知道解密密钥的条件下对密文进行分析，并试图获取相应的密钥或者明文。早期的分组密码主要围绕数据加密标准（Data Encryption Standard, DES）展开研究，DES 算法是 70 年代初由 IBM 密码研究项目组设计的分组密码，在 1977 年被美国标准局（National Bureau of Standards, NBS）选为数据加密标准<sup>[1]</sup>。随后在 POS 机、智能卡、加油站等相关领域被广泛应用。由于计算机算力的大幅提升以及针对 DES 的攻击方法层出不穷，DES 的安全性已经不足以满足当前信息时代的安全需求。因此，美国国家标准和技术研究所（The National Institute of Standards and Technology, NIST）在 1997 年开始征集高级加密标准（Advanced Encryption Standard, AES），用于取代原有的 DES 算法<sup>[2]</sup>。经过五年的甄选，2001 年，NIST 宣布将比利时密码学家 John Daemen 和 Vincent Rijmen 设计的 Rijdael 算法作为高级加密标准。相较于 DES 时代存在的安全问题，AES 算法在多个方面得到了改进和提高，以往攻击 DES 的手段对于 AES 不再适用。经过二十多年的研究，AES 算法依旧没有被攻破，目前学术界针对 AES 算法的安全性分析仍然存在局限。在 AES 被公布之后，许多国家和地区

开启密码算法征集活动,公布了各自的商用密码算法标准。如欧洲评选出了 Misty1<sup>[3]</sup>、Canellia<sup>[4]</sup>和 Shacal-2<sup>[5]</sup>算法,韩国将 ARIA 算法作为分组密码算法标准<sup>[6]</sup>。在 2012 年,中国国家密码管理局正式发布并确立 SM4 作为我国的分组密码标准<sup>[7]</sup>。此外,密码学根据加解密密钥是否相同分为对称密码体制和非对称密码体制。对称密码体制包括分组密码、序列密码和消息认证码,非对称密码体制则指公钥密码。其中,分组密码因其高效且安全的特性被广泛应用,是密码学中的核心分支之一。

分组密码首先将数据分割成多个块,然后分别进行加密,保证数据的安全性。由于分组密码的加密效率高,其应用领域十分广泛,包括加密文件、保护数据库、身份验证、安全通信以及支付安全等,涵盖人们日常生活的方方面面。仅仅十年物联网的飞速发展,更多的嵌入式设备如射频识别(RFID)、扫描仪、感应器等不断融入到物联网设备中。但这些物联网环境下所使用的设备不如以往在 PC、服务器等具有较强的计算能力和内存资源等。轻量级分组密码算法应运而生,以解决在资源受限的环境下,物理设备资源不足的问题,同时保障数据加密过程的安全性。

在近几十年,轻量级分组密码的设计与分析逐渐成为密码界研究的热点之一,并已经取得了一定的成果。目前,被广泛应用的轻量级分组密码算法包括 DESL<sup>[8]</sup>、PRESENT<sup>[9]</sup>和 GIFT<sup>[10]</sup>算法等。其中 DESL 在 RFIDSec06 中发布,算法使用轻量化后的 S 盒替代 DES 中原有 S 盒,降低了硬件实现电路的复杂度。CHES 2007, Bogdanov 等人设计了基于比特的轻量级分组密码算法 PRESENT,算法使用的 4 比特 S 盒仅需要 28 个等效门(GE)<sup>[9]</sup>。CHES 2017 中, Banik 等人弥补了 PRESENT 算法线性层的缺陷,设计了 GIFT 轻量级分组密码算法,该算法提高了加解密的运行速度,减少了资源消耗<sup>[10]</sup>。NIST 在 2018 年启动轻量级认证加密算法征集计划,旨在提升物联网的安全性和效率,使物联网产生更加广阔的应用场景,经过多轮的筛选评估,最终于 2023 年 2 月宣布 Ascon 作为最终获胜算法<sup>[11]</sup>。

虽然轻量级分组密码可以一定程度上保证加密设备的安全,但是物理设备在运行时会有种种物理信息的泄漏,这使得侧信道攻击(Side-Channel Analysis, SCA)成为一种威胁。因此一个密码学性质优良的分组密码不仅仅需要抵抗传统的数学分析,同时还要具备抵抗侧信道攻击的能力。侧信道攻击通常需要根据密码算法具体的运行环境来实施相应的攻击。侧信道攻击根据攻击者是否破坏设备正常的运行状态,可以分为主动攻击和被动攻击<sup>[12][13][14]</sup>。其中常见的被动攻击包括能量分析,主动攻击中最常见的则是故障攻击(Fault Attack, FA)<sup>[15]</sup>。

差分故障攻击(Differential Fault Attack, DFA)作为最常见的一种故障攻击,结合了差分攻击和故障攻击的优点,具有注入灵活、计算复杂度低等优点<sup>[16]</sup>。差分故障攻击的主要原理是通过外部的物理干扰改变加密设备的正常执行状态,使得设备输出错误密文,攻击者通过观察正确密文和错误密文的关系,获得相关的密钥信息。与差分攻击不同的是,差分攻击中轮与轮之间的差分传播是连续的,每一轮的输入等于上一

轮的输出,而差分故障攻击可以在加密操作的任意轮和任意时刻注入故障。差分故障攻击具有更好的灵活性,使得攻击者可以在更有利于攻击的位置注入故障,并大幅降低分析的复杂度。差分故障攻击的出现给密码设备带来了严重威胁,因此,设计有效保证密码设备免受差分故障攻击的防护方法是至关重要的。本文主要针对分组密码抵抗差分故障攻击的检测及防护方法进行研究,分别从实现级和算法级的防护方法展开研究。以设计软件实现代价小的防护方案为目标,保证分组密码能在嵌入式设备中高效运行的同时,检测故障注入,抵抗差分故障攻击的威胁。

## § 1.2 研究现状

### § 1.2.1 差分故障攻击研究现状

1996 年, Boneh 等人首次提出了故障攻击,并成功评估了非对称密码 RSA 的安全性<sup>[15]</sup>。1997 年, Biham 等人提出了差分故障攻击,并成功地使用该方法破解了 DES 算法<sup>[16]</sup>。2003 年, Chen 等人提出了一种针对 AES 密钥编排的差分故障攻击,攻击在循环密钥上引入单字节故障,成功用少于 30 对差分密文恢复了 AES 的密钥<sup>[17]</sup>;同年, Piret 等人将故障引入 AES 算法倒数第二和倒数第三轮之间的列混淆,利用 2 个故障密文恢复了算法主密钥<sup>[18]</sup>。2006 年, Zhang 等人采用面向字节的随机故障模型,对 SM4 密码算法使用差分故障攻击,大约只需要 47 个故障密文即可恢复算法主密钥<sup>[19]</sup>。2008 年, Li 等人在 SM4 算法的密钥编排函数中导入故障,仅 8 个错误密文即可恢复 SM4 算法的主密钥<sup>[20]</sup>。2012 年, Zhao 等人通过预测故障位置和传播路径,对 PRESENT 和 PRINT 算法进行差分故障攻击,有效降低了密钥搜索空间<sup>[21]</sup>。2013 年, Bagheri 等人在 PRESENT 算法中间状态引入半字节故障,平均 18 个错误密文恢复算法主密钥<sup>[22]</sup>。2015 年, Xu 等人提出了针对 TWINE 密码算法的差分故障攻击,平均需要 13.15 个故障可恢复算法的 80 比特主密钥<sup>[23]</sup>。2018 年, Zhang 等人提出了持续性故障攻击,在设备进行加密前注入故障,能够有效降低故障攻击中高度耦合的时间同步限制<sup>[24][25]</sup>。2019 年, Khairallah 等人通过在 SPN 算法最后一轮的非线性层注入非均匀故障,有效降低密钥搜索空间,并成功对 PRESENT、GIFT 等一系列 SPN 结构密码算法实施差分故障攻击<sup>[26]</sup>;2020 年, Aikata 等人研究了 NIST 候选算法 SIV-Rijndael256 三轮密码的差分特征,并将差分故障攻击用于密钥编排,成功分析算法主密钥<sup>[27]</sup>;2021 年, Xie 等人提出一种基于随机半字节的差分故障攻击,分别通过 20.24 和 44.96 个密文攻击了 GIFT-64 和 GIFT-128<sup>[28]</sup>;同年, Jiang 等人通过分析 AES 两个 S 盒和列混淆的差分特征,用 188.5 个密文在算法第 8 轮注入故障并分析出密钥信息<sup>[29]</sup>。2022 年, Nageler 等人基于 DEFAULT 算法<sup>[30]</sup>的结构,提出了多种攻击方法,降低了

DEFAULT 算法设计者声称的理论攻击复杂度<sup>[31]</sup>；同年，Anand 等人针对 Rocca 算法，在 8 个内部状态寄存器中的 3 个注入  $4 \times 48$  个故障，导致内部状态完全恢复<sup>[32]</sup>；同年，Bagheri 等人提出统计无效持久故障攻击，并在各种场景有效应用于 Feistel 结构的密码，利用单个位置故障，在最高  $2^{50}$  的密钥搜索空间成功分析 DES、3DES 等密码算法<sup>[33]</sup>；2023 年，Zang 等人基于持久故障和碰撞攻击，成功分析了 OpenSSL 中在不同加密工作模式下的 AES 密码算法<sup>[34]</sup>；同年，Lim 等人提出一种基于单比特翻转的差分故障攻击，通过 64 个错误密文，以 98.8% 的概率恢复了 PIPO64/128 的正确密钥<sup>[35]</sup>；另外在 CHES2023，Zhang 等人提出基于选择明文的持久故障攻击，只需要 256 个错误密文就恢复出 AES 的密钥<sup>[36]</sup>。

### § 1.2.2 差分故障防护研究现状

为保护密码设备，国内外也针对差分故障攻击提出了许多针对硬件、软件的各种防护方案。2010 年，Li 研究了差分故障攻击对国际上流行的分组密码的威胁，证明了许多密码算法并不安全，适当的防护措施对于密码算法是有必要的<sup>[37]</sup>。2012 年，Gierlichs 等人基于传染计算的思想，提出了几种差分故障攻击的应对措施，措施确保注入到密码、伪循环或冗余循环中的错误会感染密文，从而使攻击者无法获得相关的密钥信息<sup>[38]</sup>。2014 年，Tupsamudre 等人改进文献[38]中提出的感染思想，提出了一种更有效地利用随机性来防止针对 AES 差分故障攻击的对策<sup>[39]</sup>。2015 年，Guo 等人提出用故障熵(FE)和故障差分熵(FDE)来评估并发错误检测方案抗差分故障攻击的能力，研究表明均匀分布的故障覆盖率无法用于评估并发错误检测针对差分故障攻击的安全性指标<sup>[40]</sup>；同年，Zhang 等人通过比较同一输入在不同层级运算结果是否相同来抵抗故障攻击<sup>[41]</sup>。2016 年，Schneider 等人提出了一种针对加密硬件实现的对策，该对策将可证明安全的屏蔽方案与错误检测方法结合，成功使 LED 分组密码算法实现抵抗侧信道分析的同时，具备抵抗差分故障攻击的能力<sup>[42]</sup>。2017 年，Punit 等人提出了针对单字节故障作用于 S 盒的攻击的评估框架 XFA，框架可自动预测差分故障攻击能否成功<sup>[43]</sup>；同年，Ghosh 等人基于故障随机化和形式化感染的思想提出一种新的感染对策，并将方案应用于 AES 算法，为算法提供了抵抗故障攻击的能力<sup>[44]</sup>。2018 年，Patranabis 等人介绍了确定性和随机性的感染对策，修复已知对策的一些漏洞并提出了一个新的对策，将新对策应用于 AES 算法，使其能够更好的抵抗差分故障攻击<sup>[45]</sup>；同年，Baksi 等人在所谓的“在明文中调整”，确保将不受控制的值(“weak-in”)插入到块密码明文的某些部分，从而有效地使差分故障攻击更难执行<sup>[46]</sup>。2019 年，Arribas 等人提出了能够评估防护效果的框架 VerFI，VerFI 可以快速检查给定实现所需要的故障检测及纠错能力<sup>[47]</sup>；同年，Benhadjyoussef 等人提出了一种基于奇偶校验的错误检测方案，方案根据 AES 轮函数输出的正确奇偶校验值与预测奇偶校验值进

行比较,来判断是否存在故障的注入,从而抵抗差分故障攻击<sup>[48]</sup>;同年,Beierle等人直接从设计方面考虑,设计了一种可调分组密码算法 CRAFT,算法整体结构采用可调密钥来提升其抗差分故障攻击的能力<sup>[49]</sup>。2020年,Keerthi结合以往多种自动评估框架,提出了一种针对硬件实现方案的自动故障攻击评估方案 FEDS,框架综合考虑多重故障攻击和故障模型,对故障攻击的可利用性进行综合评估<sup>[50]</sup>;同年,Feng等人将感染函数与无保护密码分离,提出了一个通用的评估框架,该框架适用于各种感染对策和攻击场景,相较之前的工作,可以分析出更多的感染漏洞<sup>[51]</sup>;Potestad-Ordonez等人提出了一种使用汉明码生成内部状态的签名来覆盖更多的故障的防护方案,并将该方案用于使用 T 盒实现的 AES 算法,有效提高了故障覆盖率<sup>[52]</sup>;同年,Zhang等人提出使用一些新随机值对密文的差异和感染函数进行干扰,从而无法导出加密信息的防护方案,新方案不仅能抵抗双重故障攻击,还能快速确定目标加密算法的准确故障注入位置<sup>[53]</sup>。2021年,Richter-Brockmann等人提出一个名为 FIVER 的故障验证框架,框架利用有向无环图,结合二元决策树,对依赖于软件实现的故障防护方案进行评估<sup>[54]</sup>;同年,Baksi等人同样从设计的角度考虑提出了 DEFAULT 算法,该算法使用具有线性结构的 S 盒,能够有效抵御差分故障攻击,设计者声称 DEFAULT 算法能保证故障攻击的复杂度不低于  $2^{64}$  比特<sup>[30]</sup>。2022年,Nasahl介绍了 SYNFI 的故障验证框架,用于分析故障对于电路输入输出关系的一般影响和故障对策,使硬件设计者能以系统和半自动的方式评估和验证嵌入式对策的有效性<sup>[55]</sup>;同年,Ghosal等人提出一种保护 AES 免受差分故障攻击的防护方案,方案在算法每一轮添加一个新的扩散层,通过生成最小数量的方程扩大穷举的密钥搜索空间,最终为 AES 提供  $2^{84}$  的密钥搜索空间免受差分故障攻击<sup>[56]</sup>。2023年,Keerthi等人提出一个名为 FaultMeter 的框架,该框架建立与现有技术之上,不仅能识别分组密码软件中易受故障影响的位置,还为每个容易受故障的位置提供了量化,并且框架考虑了不同的密码使用场景,为多种硬件平台自动提供故障对策<sup>[57]</sup>。

由于物联网设备的算力限制和抵抗差分故障攻击的安全需求,保证密码设备在高效运行的同时,免受差分故障攻击的防护方法是值得研究的。本文针对分组密码抵抗差分故障攻击的检测及防护方法进行研究,根据 DEFAULT 和 Pyjamask 分组密码算法的结构设计,利用线性结构、线性码等手段,从实现层或算法层展开防护方法的研究。设计的方案确保分组密码能在嵌入式设备中高效运行,检测故障注入,抵抗差分故障攻击的威胁,同时控制额外的软件消耗。

### § 1.3 论文组织架构

本文共包括六个章节,各章节内容主要安排如下:

第一章 绪论。介绍了分组密码的发展历史和差分故障攻击及其防护手段的研究意

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/645123111341011302>