计算机科学
COMPUTER SCIENCE

轻量级分组密码算法综述

钟悦，谷杰铭，曹洪林

引用本文

钟悦，谷杰铭，曹洪林. 轻量级分组密码算法综述[J]. 计算机科学，2023，50(9)：3-15.

ZHONG Yue, GU Jieming, CAO Honglin. Survey of Lightweight Block Cipher[J]. Computer Science, 2023, 50(9): 3-15.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230500190

轻量级分组密码算法综述

钟 悦[1] 谷杰铭[2,3] 曹洪林[1]
1 中国政法大学证据科学研究院 北京 100088
2 国家计算机网络应急技术处理协调中心 北京 100029
3 哈尔滨工业大学网络空间安全学院 哈尔滨 150001

摘 要 随着信息技术的快速发展,人类将进入万物互联时代,数以亿计的物联网设备接入网络,针对用户隐私、网络环境等的网络攻击持续增长。因此,保障物联网设备的信息安全至关重要。由于物联网设备的计算能力、电池容量和内存等资源十分受限,传统的分组密码算法不适用于具有低时延、低功耗等要求的物联网设备,轻量级分组密码算法应运而生。文中概述了轻量级分组密码算法的研究现状及进展,并根据算法结构将其分成6类进行详细阐述;依据多维度评价指标分别对轻量级分组密码算法的软硬件实现进行综合对比与分析,并从安全性、资源开销和性能3方面进行深入探讨;最后展望了轻量级分组密码算法的未来研究方向。

关键词:轻量级分组密码;物联网;数据安全;密码算法;隐私保护
中图法分类号 TP309

Survey of Lightweight Block Cipher

ZHONG Yue[1],GU Jieming[2,3] and CAO Honglin[1]
1 Institute of Evidence Law and Forensic Science,China University of Political Science and Law,Beijing 100088,China
2 National Computer Network Emergency Response Technical Team/Coordination Center of China,Beijing 100029,China
3 School of Cyberspace Science,Harbin Institute of Technology,Harbin 150001,China

Abstract With the rapid development of information technology,human beings are entering the era of ubiquitous connectivity,where billions of Internet of Things(IoT) devices are connected to the network. The continuous growth of network attacks targeting user privacy and the network environment has made it crucial to ensure the information security of IoT devices. Due to the limited computational capabilities,battery capacity,and memory resources of IoT devices,conventional block cipher algorithms are not suitable for IoT devices that require low latency and low power consumption,lightweight block cipher algorithms have emerged to address these challenges. This paper provides an overview of the research status and progress of lightweight block cipher algorithms,and categorizes them into six types according to their structure. It comprehensively compares and analyzes the hardware and software implementations of lightweight block cipher algorithms based on multidimensional evaluation criteria. Furthermore,it explores the security,resource consumption,and performance aspects in-depth. Finally,this paper discusses the future research directions of lightweight block cipher algorithms.

Keywords Lightweight block cipher,Internet of Things,Data security,Cipher algorithm,Privacy protection

1 引言

随着物联网技术在智能家居、智慧城市、环境保护等领域的快速发展和物联网设备的普及,人们的生活变得更加智能化和自动化。人类进入了万物互联的新时代,但是随之而来的安全问题不容忽视。

与常见的网络设备(如服务器、智能手机等)相比,物联网设备(如无线传感器、植入式医疗设备等)的资源十分有限[1],表现在内存较小、计算能力较低、电池功率有限、物理空间较小、易受攻击[2]等方面。此外,物联网设备大多需要实时处理数据,并且设备之间的数据交换频率较高[3]。当物联网设备联网后进行数据传输时,面临较大的信息安全风险[4]。在此情况下,使用密码算法是保护物联网设备网络通信安全最合适的方法之一。密码算法可以防止数据遭受未授权访问、破译、篡改等,从而确保数据传输的安全。

然而,如图1所示,在资源受限设备上部署传统的密码算法面临诸多挑战。因此,研究者们提出了轻量级密码算法来

到稿日期:2023-05-26 返修日期:2023-06-22
基金项目:中央高校基本科研业务费专项资金
This work was supported by the Fundamental Research Funds for the Central Universities.
通信作者:钟悦(zhongyue@cupl.edu.cn)

保障资源受限设备的信息安全。通过引入轻量级特性，如更小的存储空间、更低的能耗和更快的计算速度等，可以在资源受限设备上实现密码算法的实时响应，满足相关设备的安全性需求。

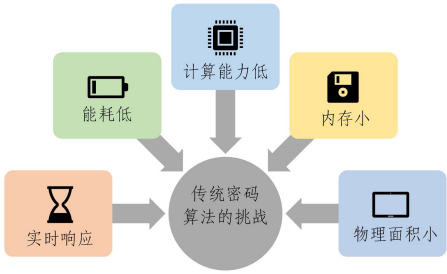

图 1 传统密码算法在资源受限设备上面临的挑战

Fig. 1 Key challenges of conventional cryptography on resource-constrained device

轻量级分组密码算法是轻量级密码算法的重要研究分支和密码分析的研究热点之一，被广泛应用于各类物联网设备。近年来，许多轻量级分组密码算法相继被提出，研究人员对相关密码算法在不同平台上的硬件或软件实现性能进行了评估[2,5-15]。然而，相关研究更多地关注适用于特定领域或应用程序的算法，较少涉及对轻量级分组密码算法的整体性讨论。Hosseinzadeh 等[13]分析了经典的轻量级分组密码算法的硬件实现性能，但是该项研究仅考虑了算法间的单项指标对比，并且缺少对软件实现性能的讨论。Dar 等[14]回顾了多种轻量级分组密码算法的特性并分析了它们的逻辑结构和设计原理，但未对比算法的实现性能和资源开销。Mohajerani 等[15]讨论了进入美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)第二轮竞赛的算法，但是该项研究仅考虑了吞吐量和处理速度这两个性能指标，未对相关算法的硬件实现性能和软件实现性能进行综合评估。

本文介绍了轻量级分组密码算法的研究现状，并总结了该领域的最新进展。此外，本文对 39 种先进的轻量级分组密码算法进行了分类、归纳和讨论，并依据多维度评价指标对相关算法的硬件实现和软件实现分别进行了对比和分析。最后，本文从安全性、资源开销和性能 3 个角度对轻量级分组密码算法进行了深入探讨，并对当前该领域亟待研究解决的问题和未来可能的研究方向进行了论述。

2 轻量级分组密码的起源与发展

2.1 发展背景与特性

现代密码学的研究始于 20 世纪 70 年代。在 70 年代初期，IBM 公司设计了数据加密标准(Data Encryption Standard，DES)[16]，并被美国国家标准局确定为第一个联邦数据加密标准。受嵌入式系统的限制[17-18]，早期的轻量级密码算法主要针对特定的应用场景，如适用于远程无钥匙系统的 KeeLoq[19]等。90 年代起，互联网的兴起推动了密码算法的快速发展，国际数据加密算法(International Data Encryption Algorithm，IDEA)[20]、小型加密算法(Tiny Encryptyion Algorithm，TEA)[21]和 Camellia[22]等经典分组密码算法相继被提出。高级加密标准(Advanced Encryption Standard，AES)[23]是美国联邦政府采用的新一代加密标准，在世界上被广泛使用，其安全性高于 DES，但需要更大的物理计算空间。为了进一步满足轻量化的需求，Eisenbarth 等[24]在研究中提出了基于 DES 和 AES 的紧凑型实现方案。

21 世纪初，随着嵌入式系统的快速发展，适当的安全性和较小的物理空间成为轻量级分组密码算法的主要设计目标。PRESENT[25]是物理面积最早达到 1 000 个等效门数(Gate Equivalent，GE)的算法之一，其能耗和运行速度也得到了大幅度优化。众多密码算法的轻量化版本被相继提出：mCrypton[26]是紧凑版的 Crypton[27]，被用于低功耗的电子标签和传感器；PUFFIN-2[28]是 PUFFIN[29]的轻量化版本，基于串行架构设计，占用面积仅为 1 083 GE；DESL[30]和 DESXL[30]分别是 DES 和 DESX[31]的轻量级版本，利用串行硬件技术降低了门电路复杂度。同时，研究者们提出了一些面向特定领域的轻量级分组密码算法，如适用于移动通信系统和通用分组无线服务的 KASUMI[32]、适用于集成电路生产和个性化定制的 PRINTcipher[33]、适用于电子产品代码加密的 EPCBC[34]，以及适用于具有有限指令集的低内存处理器的 SEA[35]。此外，为配合 WAPI 无线局域网标准的推广应用，中国国家密码管理局陆续推出了自主设计的 SM1，SM4[36]和 SM7 3 种分组密码算法。其中，SM1 和 SM7 仍处于未公开阶段。SM4 具有较高的安全性，但其所需的硬件占用面积较大，难以满足轻量化的需求[36-37]。

随着普适计算时代的到来，大量物联网设备被广泛应用于人们的生产和生活中，因此，如何降低延迟和能耗成为了设计分组密码算法的热点问题。RECTANGLE[38]，ITUbee[39]和 SIMON[40]等低能耗、低延迟的轻量级分组密码算法相继被提出，以适应无线传感器网络、电子标签(Radio Frequency Identification，RFID)等资源受限的环境。此外，随着密码分析技术的进步，轻量级密码算法的安全性问题日益显露[41]并受到重视。研究者提出了传统算法的掩码技术[42]和易于掩码的密码算法，如 PICARO[43]，Zorro[44]和 Robin[45]等，以应对边信道攻击；并应用宽轨迹策略等方法设计出了高效、安全的轻量级分组密码算法，如 PRINCE[46]，PRIDE[47]和 HISEC[48]等，以应对差分密码分析和线性密码分析。

轻量级分组密码算法的低能耗、低延迟和低物理空间需求等特性解决了传统密码算法在资源受限设备(如 RFID 标签、传感器网络等)上的困境。此外，轻量级分组密码算法作为众多信息安全协议的核心，也适用于与资源受限设备直接或间接交互的其他资源丰富设备(如智能手机、服务器等)。

2.2 主要结构类型

如图 2 所示，主流的轻量级分组密码算法依据其内部结构，可以分为以下 6 种：代换-置换网络(Substitution-Permutation Network，SPN)结构、Feistel 网络(Feistel Network，FN)结构、广义 Feistel 网络(General Feistel Network，GFN)结构、ARX(Add-Rotate-XOR)结构、非线性反馈移位寄存器(Non-Linear Feedback Shift Register，NLFSR)结构和混合(Hybrid)结构。

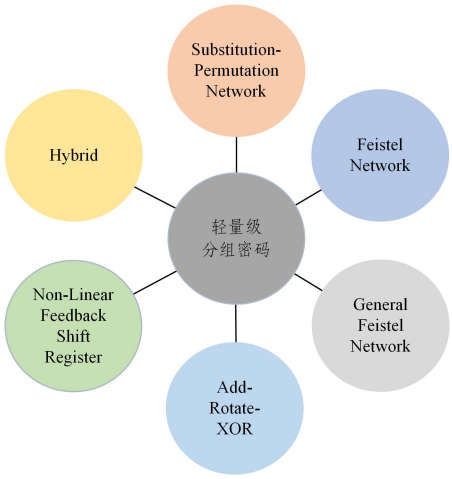

图 2　轻量级分组密码算法的结构类型

Fig. 2　Structure of lightweight block cipher algorithms

SPN 结构是国际上使用最为广泛的分组密码结构之一，其通过一系列的替换盒（Substitution-box，S 盒）和置换盒（Permutation-box，P 盒）运算使得明文的每一位影响密文中多位的值。SPN 结构的混淆扩散速度快，算法实现时吞吐量大，但加解密过程则相反，需要为解密算法付出额外代价。

Feistel 结构将每组明文分为等长的两部分，在每轮迭代运算中，使用轮函数加密一部分，完成迭代后组合成密文分组。Feistel 结构的加解密方式相同，降低了硬件实现成本，但是混淆扩散速度慢，并且需要更多的迭代轮数以保证安全性。

GFN 结构是 Feistel 结构的扩展形式，主要包括 Type-I，Type-II 和 Type-III 型 3 种结构[49]。其中 Type-II 型结构将每组输入拆分成 n 个子块（$n>2$），对每两个子块应用 1 次 Feistel 变换，并对 n 个子块进行循环移位[50]。与 Feistel 结构相比，GFN 混淆扩散速度更快，并具备高并行性的特点。

ARX 结构使用模加、循环移位和异或 3 种运算替换 GFN 结构中的 S 盒，简化了轮函数的结构，其中只有模加运算为非线性运算，具有软件实现效率高、吞吐量大、防护时序攻击代价小等特点。但是与 SPN 和 FN 结构相比，其安全性仍有待进一步研究。

NLFSR 结构利用序列密码的组件完成算法的硬件实现，其当前状态是其前一状态的非线性反馈值[51]。

Hybrid 结构将上述任意 3 种结构组合在一起，实现提升算法性能（如吞吐量、等效门数、能耗等）的目的，以满足特定的应用需求。

3　轻量级分组密码算法

表 1 列出了目前主流的轻量级分组密码算法的结构类型，本章将依据结构分类介绍相关密码算法。本章中所使用的符号含义如下：

1）“Cipher-n/m”表示算法的分组长度为 n 位，密钥长度为 m 位；

2）“Cipher-m”表示算法的密钥长度为 m 位。

表 1　基于结构分类的轻量级分组密码算法

Table 1　Structure-wise of lightweight block cipher algorithms

算法结构	算法
SPN	AES，mCrypton，PRESENT，PUFFIN-2，KLEIN，PRINCE，RECTANGLE，PRIDE，SKINNY，IVL-BC
FN	DESL，DESXL，MIBS，LBlock，SIMON，ITUbee，SLIM，LBC-IoT，SCENERY，LBCCS
GFN	CLEFIA，TWIS，Piccolo，TWINE，HISEC，WARP，DBST
ARX	HIGHT，SPECK，LEA，CHAM，SAND，GFRX
NLFSR	KATAN，KTANTAN，Halka
Hybird	Hummingbird，Hummingbird-2，PRESENT-GRP

3.1　SPN 结构

AES[23] 由 NIST 提出，是现代密码学发展史上重要的里程碑，用来替代 DES[16]。在硬件实现方面，轻量化实现的 AES 需要 2400 GE，比传统实现的最小值减少了约 23%[41]。

mCrypton[26] 的分组长度为 64 位，密钥长度设计为 64 位、96 位和 128 位，迭代轮数为 13 轮，专门用于资源受限的微型设备。mCrypton 被视为 Crypton[27] 的轻量化版，其设计沿用 Crypton 的总体架构，但是对每个组件功能进行了重新设计和简化，降低了能耗等实现代价。

PRESENT[25] 的分组长度为 64 位，密钥长度设计为 80 位和 128 位，迭代轮数为 31 轮，是一种典型的面向硬件设计的超轻量级密码算法，在 2012 年成为 ISO/IEC 国际标准。PRESENT 的特点是使用单个 4×4 的 S 盒，加密过程中在非线性替换层并行使用 16 次 S 盒，在线性扩散层使用比特置换，降低了硬件资源开销。

PUFFIN-2[28] 的分组长度、密钥长度和迭代轮数分别是 64 位、80 位和 34 轮，被视为 PUFFIN[29] 的轻量化版，其基于串行化体系结构实现，同时提供加密和解密功能。在硬件实现方面，PUFFIN-2 的物理面积占用（1083 GE）比序列化实现的 PRESENT-80（1296 GE）减少了约 16%[28]。

KLEIN[52] 的分组长度为 64 位，由 KLEIN-64 和 KLEIN-80 以及 KLEIN-96 组成，其非线性替换使用 1 个具有自反性的 4 位 S 盒，列字节混合设计借鉴了 AES 的列混合变换。KLEIN 在经典传感器平台上具有更好的软件实现性能[52]。

PRINCE[46] 的分组长度、密钥长度和迭代轮数分别是 64 位、128 位和 12 轮，由 64 位的算法 PRINCEcore 和两个白化密钥构成。PRINCE 的加解密过程可以使用相同的电路，节约了硬件资源开销，并且该算法的延迟较低。

RECTANGLE[38] 的分组长度为 64 位，密钥长度设计为 80 位和 128 位，迭代轮数为 25 轮。RECTANGLE 的替换层由 16 个 4×4 的 S 盒并行组成，很好地平衡了安全性和性能；置换层由 3 次循环移位组成，降低了硬件成本。

PRIDE[47] 是面向软件设计的密码算法，分组长度、密钥长度和迭代轮数分别是 64 位、128 位和 30 轮，并针对 8 位微处理器进行了优化，其线性层的出色设计使得算法具有良好的软件实现效能和安全性。

SKINNY[53] 是一种采用可调密钥框架的分组密码算法，根据可调密钥大小和分组长度分为 6 个版本，其延迟较低，并具备较强的安全性。在硬件实现方面，SKINNY 的占用面积

和吞吐量普遍优于 SIMON。

IVLBC[54]的分组长度为 64 位，密钥长度设计为 80 位和 128 位，迭代轮数是 29 轮，具有对合的轻量级 S 盒和 P 置换，解密过程复用加密过程的代码和电路。在相同的加解密电路情况下，IVLBC-128 的软硬件实现开销低于 PRINCE 等。

3.2 Feistel 结构

DESL[30]的分组长度、密钥长度和迭代轮数分别是 64 位、56 位和 16 轮，是 DES 的一种轻量化设计。为降低算法的门电路复杂度，DESL 重复使用 1 个 S 盒 8 次。在硬件实现方面，DESL 和 DES 的吞吐量相同，但前者的占用面积(1 848 GE)比后者(2 309 GE)减少了约 20%[30]。

DESXL[30]的分组长度、密钥长度和迭代轮数分别是 64 位、184 位和 16 轮，是 DES 的另一种轻量化设计。与 DES 相比，为提升算法的安全性，DESXL 对密钥空间进行扩充。

MIBS[55]的分组长度为 64 位，密钥长度设计为 64 位和 80 位，迭代轮数是 24 轮，密钥调度算法借鉴了 PRESENT 的设计思路。MIBS 的轮函数与 PRESENT 相似，均使用 SPN 结构和 1 个 4×4 的 S 盒。在硬件实现方面，MIBS-80 和 PRESENT-80 的吞吐量相同，占用面积相近。

LBlock[56]的分组长度、密钥长度和迭代轮数分别是 64 位、80 位和 32 轮，密钥调度算法借鉴了 PRESENT 的设计，采用 NLFSR 结构，并利用 S 盒变换和循环移位生成轮密钥。在硬件实现方面，LBlock 和 PRESENT-80 的吞吐量相同，但是前者的占用面积(1320 GE)比后者(1570 GE)减少了约 16%。

SIMON[40]由美国国家安全局(National Security Agency，NSA)提出，根据不同的分组长度和密钥长度分为 10 个版本，轮函数由循环左移、按位与和按位异或运算组成，线路实现简单，具有较好的软硬件实现性能。

ITUbee[39]是面向软件设计的密码算法，分组长度、密钥长度和迭代轮数分别是 80 位、80 位和 20 轮，采用无密钥生成的策略，具有低功耗、低内存需求的特点。在软件实现方面，ITUbee 的延迟低于 LBlock，KLEIN-80 等。

SLIM[57]的分组长度、密钥长度和迭代轮数分别是32 位、80 位和 32 轮，是一种超轻量级密码算法，轮函数的替换层使用 4 个相同的 4×4 的 S 盒。在硬件实现方面，SLIM 仅需要 553 GE，低于 SIMON-32/64。

LBC-IoT[58]的分组长度、密钥长度和迭代轮数分别是 32 位、80 位和 32 轮，是一种超轻量级密码算法，使用 4 位的 S 盒、移位和异或运算，降低了硬件实现成本。在硬件实现方面，LBC-IoT 仅需要 548 GE，和 SLIM 接近，同样低于 SIMON-32/64 等。

SCENERY[59]的分组长度、密钥长度和迭代轮数分别是 64 位、80 位和 28 轮，轮函数由 8 个 4×4 的并行 S 盒和 1 个 32×32 的二进制矩阵组成。在硬件实现方面，SCENERY 需要1 438 GE，低于 RECTANGLE-80，PRESENT-80 等。

LBCCS[60]的分组长度、密钥长度和迭代轮数分别是 128 位、128 位和 20 轮，其特点是利用组合混沌系统构造了高安全性的 S 盒和具有良好扩散性的 P 盒，并且通过设计可扩展的轮函数降低了算法的复杂度。在硬件实现方面，LBCCS 需要 2 227 GE，低于 PRESENT-80，CLEFIA 等[60]。

3.3 GFN 结构

CLEFIA[61]采用 4 分支的 GFN 结构，由 CLEFIA-128，CLEFIA-192 和 CLEFIA-256 组成，其中，CLEFIA-128 的数据处理过程可以基于串行化体系结构实现，不需要额外的寄存器[62]。CLEFIA 在 2012 年被 ISO/IEC 确定为标准化的轻量级分组密码之一。

TWIS[63]的设计灵感来源于 CLEFIA，采用 2 分支的 GFN 结构，分组长度、密钥长度和迭代轮数分别是 128 位、128 位和 10 轮。与 CLEFIA 相比，TWIS 具有更高的安全性。

Piccolo[64]的分组长度为 64 位，根据密钥长度分为 Piccolo-80 和 Piccolo-128，是一种超轻量级密码算法，加密过程主要包括密钥白化、F 函数和字节置换操作等。在硬件实现方面，串行实现的 Piccolo-80 需要 683 GE 完成加密，并额外需要 60 GE 完成解密。

TWINE[65]采用 16 分支的 GFN 结构，分组长度为 64 位，密钥长度设计为 80 位和 128 位，迭代轮数是 36 轮。TWINE 与 LBlock 在设计上有相似之处，但前者的轮函数使用单个 S 盒，后者使用 10 个不同的 S 盒；前者的密钥调度算法使用半字节置换，后者使用比特置换。

HISEC[48]的分组长度、密钥长度和迭代轮数分别是 64 位、80 位和 15 轮，其借鉴了 PRESENT 的设计思路，但使用不同的比特置换方式。在硬件实现方面，HISEC 需要 1 695 GE，高于 PRESENT-80，TWINE-80 等。

WARP[66]采用 32 个半字节的改进 Type-II 型结构，分组长度、密钥长度和迭代轮数分别是 128 位、128 位和 41 轮。在硬件实现方面，WARP 的占用面积低于 SKINNY-128/128，SIMON-128/128 等。

DBST[67]采用了 4 分支的 GFN 结构变体，分组长度、密钥长度和迭代轮数分别是 128 位、64 位和 32 轮，该变体在保留 Feistel 结构的一致性的基础上改善了扩散性。DBST 使用了比特切片技术，使得 S 盒与密钥动态关联。在硬件实现方面，DBST 的占用面积和 SKINNY-128/128 接近。

3.4 ARX 结构

HIGHT[68]采用 8 分支的 GFN 结构，分组长度、密钥长度和迭代轮数分别是 64 位、128 位和 32 轮，轮函数的输入和输出都是 8 位。HIGHT 的设计是面向 8 位处理器的，因此在 8 位处理器上的性能表现良好。

SPECK[40]由 NSA 提出，根据不同的分组长度和密钥长度分为 10 个版本。与 SIMON 相比，SPECK 的软件实现性能更佳；但由于模 2^n 运算的硬件开销大于与运算，因此 SIMON 的硬件实现性能更好。

LEA[69]是面向软件设计的密码算法，由 LEA-128，LEA-192，LEA-256 组成。其在通用处理器上实现快速软件加密，特点是代码体积小。在软件实现方面，LEA-128 的 ROM(590 字节)和 RAM(32 字节)占用均低于 AES-128(2 164 字节和 304 字节)。

CHAM[70]采用 4 分支的 GFN 结构，由 CHAM-64/128，CHAM-128/128 和 CHAM-128/256 组成，适用于资源高度受限的设备。在硬件实现方面，CHAM 使用无状态即时密钥

调度算法，不需要维护密钥状态信息，因此占用面积平均比SIMON减少约27%。

SAND[71]由SAND-64/128和SAND-128/128组成，特点是将按位与、循环移位和异或操作限制在半字节内，从而支持基于S盒的安全性分析。在硬件实现方面，SAND-64/128的占用面积仅为1287GE，低于SKINNY-64/128，TWINE-128等[71]。

GFRX[72]采用4分支的GFN结构，根据不同的分组长度和密钥长度分为7个版本，其使用两个不同的轮函数F_{AN}和F_{AD}。GFRX可以根据不同的硬件资源需求实现不同的序列化级别，最高可达到完全序列化。在硬件实现方面，GFRX-128的占用面积和吞吐量均优于HIGHT，DESL等。

3.5 NLFSR结构

KATAN[73]的设计灵感来源于KeeLoq[19]，分组长度设计为32位、48位和64位，密钥长度为80位，迭代轮数为254轮，是一种面向硬件设计的密码算法。KATAN主体使用两个NLFSR，密钥调度算法基于线性反馈移位寄存器(Linear Feedback Shift Register，LFSR)实现。

KTANTAN[73]与KATAN有很多相同的特性，例如两者的分组长度、密钥长度和迭代轮数都相同。为降低门电路复杂度，KTANTAN采用基于NLFSR的轮函数结构。与KATAN相比，KTANTAN使用硬编码加密密钥，每轮加密过程选用其中的两位。

Halka[74]的分组长度、密钥长度和迭代轮数分别为64位、80位和24轮，特点是使用LFSR实现了8位S盒的乘法逆运算。Halka的密钥调度算法与PRESENT相似，但Halka使用8位S盒而非4位S盒。在硬件实现方面，Halka的占用面积(1475 GE)比PRESENT-80(1570 GE)减少了约7%。

3.6 Hybrid结构

Hummingbird[75]的分组长度、密钥长度和迭代轮数为16位、256位和20轮，是一种超轻量级密码算法。Hummingbird采用分组密码和流密码混合的结构，包括4个16位内部状态寄存器和1个16位LFSR。

Hummingbird-2[76]是Hummingbird系列的第二代算法，分组长度是16位，密钥长度是128位，使用64位初始向量初始化寄存器。与Hummingbird相比，Hummingbird-2采用认证机制抵御信息扩展攻击，其安全性得到了提升。

PRESENT-GRP[8]的分组长度、密钥长度和迭代轮数分别是64位、128位和31轮，该算法基于位置换指令组运算(GRP)实现，使用PRESENT的S盒提升了混淆性。在硬件实现方面，PRESENT-GRP的占用面积(2125GE)高于PRESENT-128(1884GE)。

4 轻量级分组密码算法的多维度评估

4.1 性能评价指标

轻量级分组密码算法需要在实现成本和性能间达到平衡，其度量指标中部分仅与硬件实现有关(如等效门数和硬件技术)，部分仅与软件实现有关(如内存)，其余则是通用指标。本文基于以下11个指标综合评价算法性能。

分组长度(Block Size)：分组密码算法将明文分组后加密，每次处理特定长度的一组信息。由于分组长度与加密所需的计算资源和能耗呈正相关，因此物联网设备通常采用较小的分组长度。如表2所列，AES，CLEFIA，LEA和WARP采用的分组长度最大，为128位；Hummingbird-2采用的分组长度最小，仅有16位；其余多数算法的分组长度为64位。

密钥长度(Key Size)：密钥长度指密码算法使用的密钥的比特数。通常情况下，密钥越长，算法安全性越高，但需要更多的计算资源和更高的能耗。如表2所列，Hummingbird使用的密钥长度为256位；DESL仅使用56位密钥。

迭代轮数(Number of Rounds)：与传统密码算法相比，轻量级分组密码算法的结构相对较为简单，通常采用多轮迭代运算以提升安全性。一般情况下，算法的迭代轮数越多，密码分析越困难，但过多的迭代轮数会降低算法性能。因此，选择迭代轮数时应使得密码分析的计算复杂度大于穷举攻击所需的计算复杂度。

等效门(Gate Equivalent)：表示算法硬件实现所需的逻辑门数量，反映了算法在电路上运行时所需的物理空间大小。依据ISO/IEC标准[77]，轻量级密码算法的等效门数应当在1000～2000之间。

硬件技术(Technology Value)：指用于算法实现的CMOS技术，单位是μm。硬件实现的复杂性和使用等效门表示的物理空间的度量取决于算法使用的硬件技术值。当硬件技术值不同时，算法的等效门数也会有所不同。例如，Rolfes等在文献[78]中介绍了PRESENT-80在0.18μm，0.25μm和0.35μm的CMOS技术值的情况下，算法的占用面积分别为1075GE，1169GE和1000GE。

延迟(Latency)：指计算每个明文/密文分组所需的时钟周期数。

内存(Memory)：指算法需要的RAM和ROM的空间大小，通常以字节为单位。其中，RAM用于存储算法计算过程中的值，ROM用于存储算法的代码和密钥等静态数据。

吞吐量(Throughput)：指在特定频率下，算法的加密/解密操作所能实现的每秒转换的比特数。吞吐量T的大小与频率有关，计算式如下：

$$T=\frac{B\times F}{N} \tag{1}$$

其中，B是分组长度(以比特为单位)，F是频率，N是每个分组的时钟周期数。通常情况下，研究轻量级分组密码算法时使用的硬件频率为100KHz，软件频率为4MHz。传统算法的吞吐量较高，相应的所需的能耗和等效门数都较高。轻量级分组密码算法的主要设计目标是在低能耗和低等效门数的情况下提供更高的吞吐量。

效能(Efficiency)：用于评估算法的性能和实施规模间的关系，分为硬件效能和软件效能。通常情况下，效能值越高越好。硬件效能E_{hardware}的计算公式[79]如下：

$$E_{\text{hardware}}=\frac{T}{G} \tag{2}$$

其中，T 是算法的吞吐量(单位为 Kbps)，G 是算法实现所需的等效门数(单位为 KGE)。

类似的，软件效能 $E_{software}$ 的计算公式[79]如下：

$$E_{software}=\frac{T}{S} \tag{3}$$

其中，T 是算法的吞吐量(单位为 Kbps)，S 是算法可执行文件的代码大小(单位为 kB)。

功率(Power Requirement)：指算法实现所需的功率大小，通常以 μW 为单位。对于硬件实现，功率可以依据等效门数和硬件技术值进行粗略估算。对于软件实现，功率一般是指使用 8 位、16 位或 32 位微控制器运行时的功率。

能量消耗(Energy Consumption)：对于硬件和软件实现而言，每比特的能量消耗 C_{bit} 的计算公式如下：

$$C_{bit}=\frac{L\times P}{B} \tag{4}$$

其中，L 是算法的延迟，P 是算法实现所需的功率，B 是算法的分组长度(单位为比特)。

4.2 性能评估

本文对比了 39 个轻量级分组密码算法的 38 种硬件实现和 26 种软件实现，并依据 4.1 小节中的评价指标对算法性能进行评估。表 2 列出了在 0.09 μm，0.13 μm，0.18 μm 和 0.25 μm 的硬件技术值下的密码算法的硬件实现性能，表 3 列出了相应密码算法在 8 位、16 位和 32 位微控制器下的软件实现性能。

表 2 轻量级分组密码算法的硬件性能

Table 2 Hardware implementation performance of lightweight block cipher algorithms

Algorithm	block size	key size	Number of rounds	Technology value	Gate area	Latency	Throughput	Efficiency	Power	Energy
AES[41]	128	128	10	0.13	2400	226	56.64	23.60	2.40	42.38
mCrypton[26]	64	128	12	0.13	2949	13	492.30	166.93	3.00	6.00
PRESENT[25]	64	80	31	0.18	1570	32	200.00	127.38	2.35	11.77
PUFFIN-2(D)[28]	64	80	34	0.18	1083	1240	5.20	4.80	1.62	314.75
KLEIN[52]	64	80	16	0.18	1478	271	23.62	15.98	2.21	93.87
PRINCE[80]	64	128	12	0.13	2953	12	533.30	180.59	2.95	5.53
PRIDE	64	128	20	—	—	—	—	—	—	—
RECTANGLE[38]	64	80	25	0.13	1600	26	246.00	167.68	1.46	5.96
SKINNY[53]	64	128	36	0.18	1696	36	177.78	104.82	2.54	14.29
IVLBC(D)[54]	64	128	29	0.18	1773	29	220.69	124.47	2.66	12.05
DESL[30]	64	56	16	0.18	1848	144	44.40	24.02	2.77	62.37
DESXL[30]	64	184	16	0.18	2168	144	44.40	20.47	3.25	73.17
MIBS[55]	64	80	32	0.18	1530	32	200.00	130.71	2.30	11.47
LBlock[56]	64	80	32	0.18	1320	32	200.00	151.51	2.00	9.90
ITUbee	80	80	20	—	—	—	—	—	—	—
SIMON[40]	64	128	44	0.13	1000	368	17.40	17.40	1.00	57.50
SLIM[57]	32	80	32	0.13	553	—	—	—	0.55	—
LBC-IOT[58]	32	80	32	0.13	548	—	—	—	0.55	—
SCENERY[59]	64	80	28	0.18	1438	28	228.57	158.95	2.16	9.45
LBCCS[60]	128	128	20	0.18	2227	—	—	—	3.34	—
CLEFIA[61]	128	128	18	0.09	4950	36	355.56	71.83	3.45	9.74
Piccolo[64]	64	80	25	0.13	1136	27	237.04	208.66	1.13	4.80
Piccolo(S)[64]	64	80	25	0.13	683	432	14.81	21.68	0.68	46.10
TWINE[65]	64	80	36	0.09	1503	36	178.00	118.42	1.05	5.91
TWINE(S)[65]	64	80	36	0.09	1116	540	11.80	10.57	0.78	65.91
HISEC[48]	64	80	15	0.18	1695	—	—	—	2.54	—
WARP*[66]	128	128	41	0.09	763	8128	75.00	98.30	28.40	—
DBST[67]	128	64	32	0.18	1698	32	400.00	235.57	2.55	6.38
HIGHT[68]	64	128	32	0.25	3048	34	188.20	61.75	5.48	29.14
SPECK[40]	64	128	27	0.13	1127	464	13.80	12.24	1.12	81.20
LEA[69]	128	128	24	0.13	3826	168	76.19	19.91	3.82	50.22
CHAM[70]	64	128	80	0.13	826	80	80.00	96.85	0.83	10.38
CHAM(S)[70]	64	128	80	0.13	665	1280	5.00	7.52	0.67	134.00
SAND*[71]	64	128	48	0.09	1287	48	133.30	103.57	32.97	—
GFRX[72]	64	128	27	0.13	1609	31	206.45	128.31	1.61	7.80
KATAN[73]	64	80	254	0.13	1054	255	25.10	23.81	1.05	42.00
KTANTAN[73]	64	80	254	0.13	688	255	25.10	36.48	0.68	27.41
Halka[74]	64	80	24	0.18	1475	—	—	—	2.21	—
Hummingbird	16	256	20	—	—	—	—	—	—	—
Hummingbird-2[76]	16	128	—	0.18	2159	20	80.00	37.05	3.23	40.48
PRESENT-GRP[8]	64	128	31	0.18	2125	—	—	—	3.18	—

表 3　轻量级分组密码算法的软件性能

Table 3　Software implementation performance of lightweight block cipher algorithms

Algorithm	Microcontroller/bit	ROM	RAM	Latency	Energy	Throughput	Efficiency
AES[81]	8	918	—	4192	16.7	122.000	132.890
mCrypton(D)[82]	16	3108	24	108415	146.3	2.300	0.740
PRESENT[83]	8	1562	83	1937461	7749.8	0.130	0.080
PUFFIN-2	—	—	—	—	—	—	—
KLEIN(D)[24]	8	1268	18	6095	25.1	42.000	33.120
PRINCE[83]	8	4300	63	17207	68.8	14.870	3.450
PRIDE[47]	8	266	0	1514	6.0	169.000	635.330
RECTANGLE	—	—	—	—	—	—	—
SKINNY	—	—	—	—	—	—	—
IVLBC(D)[54]	8	—	74	47816	—	5.350	—
DESL(D)[84]	8	3098	0	8365	33.4	30.600	9.870
DESXL(D)[24]	8	820	48	84602	348.2	3.000	3.650
MIBS(D)[82]	16	3138	16	58688	79.2	4.300	1.370
LBlock[56]	8	—	—	3955	15.8	64.700	—
ITUbee[39]	8	716	0	2607	10.4	122.700	171.360
SIMON[40]	8	246	0	901	3.6	284.000	1154.470
SLIM	—	—	—	—	—	—	—
LBC-IOT	—	—	—	—	—	—	—
SCENERY	—	—	—	—	—	—	—
LBCCS	—	—	—	—	—	—	—
CLEFIA[85]	8	3046	—	28648	114.5	17.800	5.840
Piccolo[83]	8	1178	65	25681	102.7	9.960	8.450
TWINE(D)[65]	8	1304	414	2168	8.6	118.000	90.490
HISEC	—	—	—	—	—	—	—
WARP[66]	8	1038	0	5083	—	100.730	97.040
DBST	—	—	—	—	—	—	—
HIGHT[83]	8	1084	54	11399	45.5	22.450	20.710
SPECK[40]	8	186	0	599	2.3	427.500	2298.380
LEA[69]	32	590	32	5231	—	97.800	165.760
CHAM[70]	8	202	3	1232	—	207.790	1028.660
SAND	—	—	—	—	—	—	—
GFRX	—	—	—	—	—	—	—
KATAN(D)[24]	8	338	18	72063	289.2	3.500	10.350
KTANTAN(D)[82]	16	16252	790	11004783	14856.4	0.023	0.001
Halka	—	—	—	—	—	—	—
Hummingbird(D)[75]	8	2950	1064	2414	9.6	26.500	8.980
Hummingbird-2(D)[76]	16	770	50	1520	2.0	42.100	54.670
PRESENT-GRP[8]	32	2980	1384	—	—	—	—

除非另有说明，表 2 和表 3 中的密码算法的实现仅包含加密过程。此外，符号的说明如下：

1)“(S)”表示算法为串行实现；

2)“(D)”表示算法包含加密和解密过程；

3)“*”表示算法的硬件频率为 10MHz。

4.2.1　硬件实现评估

在硬件实现方面，图 3－图 6 分别依据吞吐量、占用面积、效能和能耗对表 2 中的密码算法进行了排序。为了公平地评估算法性能，我们对不同硬件技术值下的算法进行分类排序，对于超过 10 种实现的类别，仅展示其中的前 10 位。

在吞吐量方面，设定硬件频率为 100 kHz，如图 3 所示，PRINCE，mCrypton 和 DBST 的吞吐量位居前三，超过了 300 Kbps。然而，如表 2 所列，PUFFIN-2(D)，CHAM(S)，TWINE(S)，SPECK，Piccolo(S)和 SIMON 的吞吐量均低于 20 Kbps，表明加解密所需的时间较长。在占用面积方面，如图 4 所示，LBC-IoT，SLIM，CHAM，CHAM(S)，Piccolo(S)，KTANTAN 和 WARP 的等效门数均小于 1 000 GE。其中，LBC-IoT 的等效门数最小，仅需要543 GE。如表 2 所列，CLEFIA，HIGHT 和 LEA 的等效门数都超过了 3 000 GE，表明其轻量化程度较差。

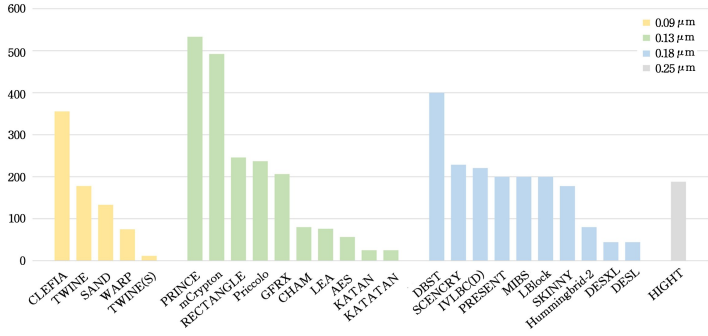

图 3　吞吐量排名(硬件实现)

Fig. 3　Throughput ranking in hardware implementations

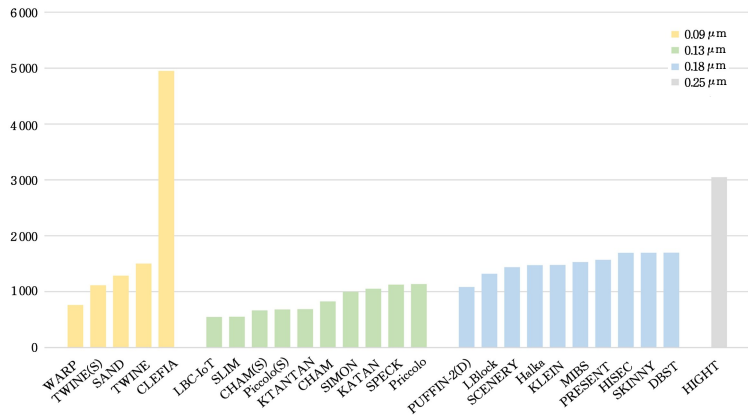

图 4 占用面积排名(硬件实现)

Fig. 4 Physical area ranking in hardware implementations

在效能方面,如图 5 所示,DBST,Piccolo,PRINCE,RECTANGLE,mCrypton,SCENERY 和 LBlock 的数值较高,超过了 150 Kbps/KGE。但由表 2 可知,PRINCE 和 mCrypton 的等效门数超过了 2 900 GE,因此难以适用于资源受限程度较高的环境。在效能超过 100 Kbps/KGE 的算法中,仅有 SCENERY,SAND,Piccolo 和 LBlock 的等效门数低于 1 500 GE。

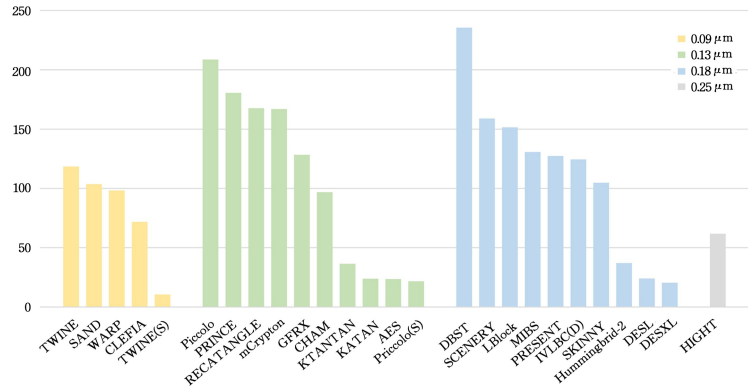

图 5 效能排名(硬件实现)

Fig. 5 Hardware efficiency ranking in hardware implementations

在能耗方面,如图 6 和表 2 所示,RECTANGLE,mCrypton,PRINCE,CLEFIA,Piccolo,TWINE,DBST,SCENERY,LBlock 和 GFRX 的能耗较低,均小于 10 μJ/bit。其中,Piccolo 的能耗最低,仅为 4.8 μJ/bit;而 PUFFIN-2(D)的能耗最高,达到了 314.75 μJ/bit,导致其难以适用于电池容量受限的物联网环境。

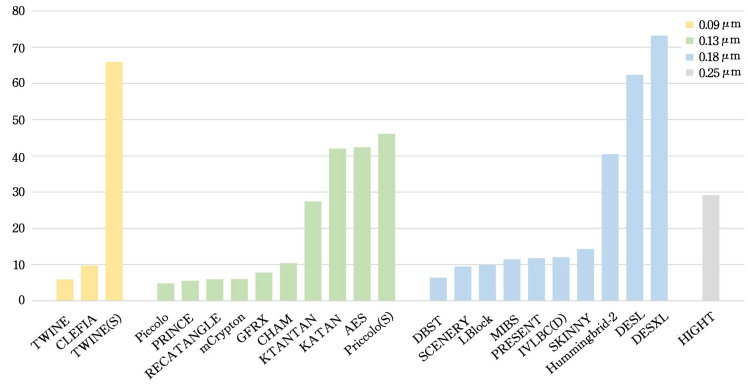

图 6 能耗排名(硬件实现)

Fig. 6 Energy consumption ranking in hardware implementations

表 2 列出了 Piccolo(S),TWINE(S)和 CHAM(S)的各项指标,结果表明采用串行实现的方式可以减少硬件占用面积,但是延迟和能耗会显著增加。

整体而言,如表 2 所列,相较于其他算法,Piccolo 的各项评估指标表现最好。PRESENT,RECTANGLE,TWINE,IVLBC(D),LBlock,MIBS,SCENERY,DBST,SAND 和 GFRX 的效能较高、延迟较低,并且等效门数不超过 2 000 GE,综合性能良好。此外,mCrypton,PRINCE 和 CLEFIA 表现出低延迟、高吞吐量的特性,但它们的占用面积较大。

4.2.2　软件实现评估

在软件实现方面，图 7—图 10 分别依据吞吐量、效能、能耗和内存占用对表 3 中的密码算法进行了排序。为了公平地评估算法性能，我们对不同微控制器环境下的算法进行分类排序，对于超过 10 种实现的类别，仅展示其中的前 10 位。

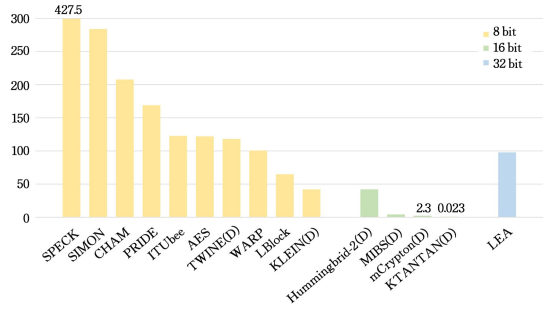

图 7　吞吐量排名(软件实现)

Fig. 7　Throughput ranking in software implementations

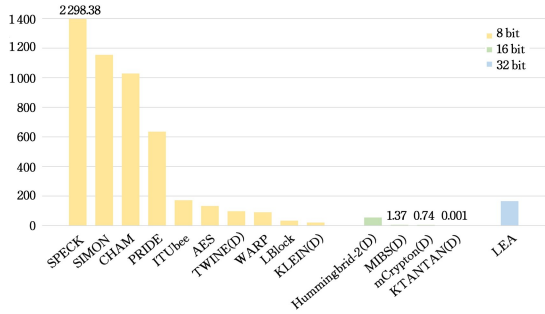

图 8　效能排名(软件实现)

Fig. 8　Software efficiency ranking in software implementations

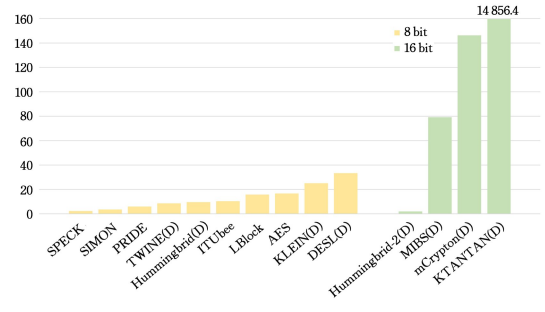

图 9　能耗排名(软件实现)

Fig. 9　Energy consumption ranking in software implementations

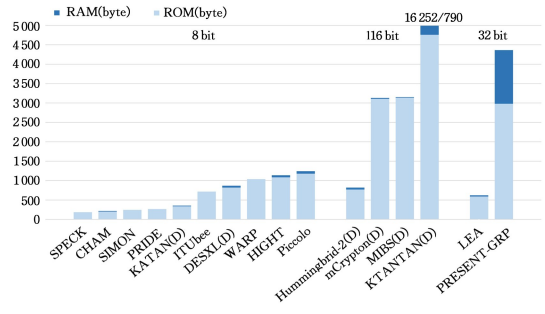

图 10　内存占用排名(软件实现)

Fig. 10　Memory usage ranking in software implementations

在吞吐量方面，设定软件频率为 4 MHz，如图 7 所示，SPECK，SIMON，CHAM 和 PRIDE 的吞吐量较高，超过了 150 Kbps。其中，SPECK 的吞吐量最高，达到了 427.5 Kbps。如表 3 所列，KATAN(D)，KTANTAN(D)，PRESENT，mCrypton(D)，DESXL(D)和 MIBS(D)的吞吐量低于 5 Kbps，表明加解密所需的时间相对较长。

在效能方面，如图 8 和表 3 所示，SPECK，SIMON，CHAM，PRIDE，ITUbee 和 LEA 的数值超过了 150 Kbps/KB。其中，SPECK，SIMON 和 CHAM 均超过 1 000 Kbps/KB。然而，PRESENT，KTANTAN(D)，mCrypton(D)，PRINCE，DESXL(D)和 MIBS(D)的效能低于 5 Kbps/KB。

在能耗方面，如图 9 所示，SPECK，SIMON、PRIDE，TWINE(D)，Hummingbird(D)和 Hummingbird-2(D)的能耗较低，小于 10 μJ/bit。其中，Hummingbird-2(D)的能耗最低，仅为 2 μJ/bit；而 KTANTAN(D)的能耗最高，为 14 856.4 μJ/bit。

在内存占用方面，如图 10 和表 3 所示，SPECK，CHAM，SIMON，PRIDE 和 KATAN(D)的 ROM 和 RAM 占用都较低，总内存占用不超过 500 字节。在 ROM 方面，mCrypton(D)，PRINCE，CLEFIA，DESL(D)，MIBS(D)和 KTANTAN(D)的占用超过 3 000 字节。其中，KTANTAN(D)的 ROM 占用最高，达到 16 252 字节，超过了 4KB ROM 的界限。在 RAM 方面，TWINE(D)，KTANTAN(D)，Hummingbird(D)和 PRESENT-GRP 的占用超过 256 字节，因此它们难以适用于资源极度受限的物联网设备。而 PRIDE，WARP，SIMON，ITUbee，DESL(D)和 SPECK 在运行过程中不占用 RAM，因此其不受限于设备的 RAM 大小。

整体而言，如表 3 所列，SPECK，SIMON 和 PRIDE 的内存占用、延迟和能耗均较低，整体表现良好，而 PRESENT 和 KTANTAN(D)的加解密速度较慢，延迟和能耗较高。

4.3　安全性、资源开销与性能

Kong 等[86]在研究中发现，资源受限设备中所使用的密码算法的安全性、资源开销和性能之间存在重要联系，并应当保持适当的平衡。如图 11 所示，同时优化三者中的任意两个目标相对容易实现，但是同时优化这 3 个目标是一项非常具有挑战性的工作[11]。在安全性方面，通常情况下，密钥长度越长、迭代轮数越多，密码的破解难度越高。在算法性能方面，更多的迭代轮数意味着更高的计算需求和延迟[86]。此外，处理平台的架构也会影响算法性能，与串行化体系结构相比，并行处理机制可以提升性能、降低延迟，但在资源开销方面，串行化体系结构的硬件成本更低。同时，密钥长度的增加会加大算法对存储的需求。因此，实现低延迟、安全性强的轻量级分组密码算法需要耗费更多的资源[87]。为了满足轻量化加解密需求，需要找到安全性和算法性能之间的平衡点。

在算法结构方面，与 SPN 结构相比，Feistel 结构的加解密过程一致，避免了额外的解密设计，能够降低硬件资源开销。然而，SPN 结构具有更高的安全性，其轮函数在每轮迭代中修改所有的分组信息，因此具有更好的混淆性和扩散性。

研究者们已经提出了许多轻量级分组密码算法，相关算法各有侧重，但存在各自的问题。例如，CHAM-64/128 和 Piccolo-80 的等效门数较低(665 GE 和 683 GE)，处于超轻量级范围，但它们的延迟较高；DESL 使用的密钥长度(56 位)较短，但它的等效门数(1 848 GE)较高。也有部分算法仅适用

于特定的领域，例如 G-TBSA[88] 能耗较低、资源开销较小，仅适用于无线传感器网络。因此，轻量级分组密码算法仍然面临着如何提升安全性和性能、降低资源开销的需求和挑战。

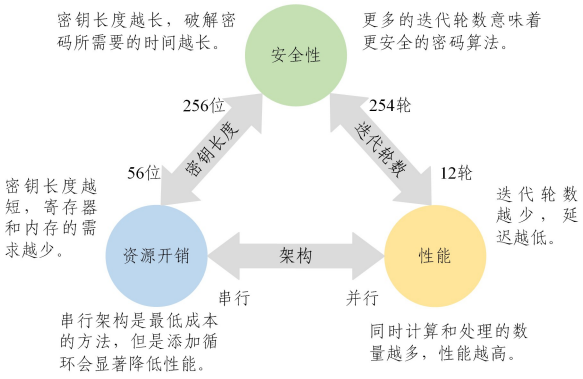

图 11 性能、安全性和资源开销间的相互关系

Fig. 11 Trade-off between performance, security and resources consumption

4.4 未来研究方向

理想的轻量级分组密码算法应当在提供足够安全性的同时，提升性能并降低资源开销，实现安全性、资源开销和性能三者间的平衡；此外，其算法的结构和模式需能抵御量子计算攻击等新型威胁，推进抗量子密码算法实用化研究。基于上述研究，我们确定了该领域的发展研究方向。

首先，密码算法的混淆性通常由其 S 盒提供，S 盒数量越多，混淆性越好、安全性越高，但同时也会增加内存和计算资源的消耗。通过选择高效且适当数量的 S 盒，可以使算法在安全性和性能之间达到平衡[43]。PRESENT 借鉴 AES 的设计思路，将 S 盒的数量从 8 个减少到 1 个，在降低内存和计算资源开销的同时，提供了足够的安全保护。因此，1）如何设计简单、快速且具有强大混淆性和安全性的算法结构，对于平衡性能、安全性和资源开销具有现实意义；2）如何使用其他更先进的混淆技术取代 S 盒，在保证安全性的同时实现更低的资源开销和更优的性能仍是未解决的问题之一。

其次，密钥调度算法需要保证生成的轮密钥具有足够的随机性和复杂性，以防止攻击者破解算法。因此，1）如何在保证安全性的同时减小密钥长度以降低资源开销仍有待研究；2）如何在不降低安全性的情况下减少迭代轮数仍然值得进一步研究。

此外，量子分析技术展现出强大的运算能力，在大整数分解、离散对数计算等多个计算问题上体现出显著优势。Grover[89]，Simon[90]，Kuperberg[91] 和 HHL[92] 等算法已被证实能够降低分组密码算法的穷举复杂度，对轻量级分组密码的安全性构成了威胁[93]。其中，在 Q1 模型下，Bonnetain 等[94] 提出了针对 AES 的量子平方攻击，实现了多项式量级攻击加速；在 Q2 模型下，Dong 等[95] 提出了量子版的高级滑动攻击[96]，实现了指数级攻击加速，可以在多项式时间内破解 2/4K-Feistel 和 2/4K-DES。

虽然分组密码算法的多种结构和模式被证明满足量子可证明安全性[97-98]，同时研究人员也针对一些分组密码算法提出了优化方案[99-100]，但实例层面的抗量子轻量级分组密码设计仍然有待探索。因此，（1）多少轮迭代可达到量子强伪随机性仍然有待研究；（2）如何在不增加或少增加密钥长度的情况下满足量子安全强度要求，亟待研究解决。

结束语 在万物互联的时代，随着 5G、云计算等技术的广泛应用，物联网产业正在蓬勃发展，数以亿计的设备将接入网络，但是随之而来的安全问题日益严峻，成为制约其进一步发展的瓶颈。本文详细介绍了三十余种先进的轻量级分组密码算法，并依据多维度评价指标进行了总结和分析，最后对该领域面临的技术挑战和未来可能的研究热点进行阐述。

研究者们提出了多种不同结构的轻量级分组密码算法，对于保障物联网设备的信息安全作出了重要贡献。在物联网领域，轻量级分组密码算法与传统的密码算法相比优势明显，然而，随着量子计算等技术的快速发展，现有密码技术仍然有待进一步提升，不仅要在安全性、资源开销和性能间达到更好的平衡，还要加强量子安全性分析、抗量子密码算法研究等。

参 考 文 献

[1] MOHD B J, HAYAJNEH T, VASILAKOS A V. A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues[J]. Journal of Network & Computer Applications, 2015, 58(C): 73-93.

[2] SINGH S, SHARMA P K, MOON S Y, et al. Advanced Lightweight Encryption Algorithms for IoT Devices: Survey, Challenges and Solutions[J]. Journal of Ambient Intelligence and Humanized Computing, 2017, 4: 1-18.

[3] MOHD B J, HAYAJNEH T. Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques[J]. IEEE Access, 2018, 6: 35966-35978.

[4] BANAFA A. Three Major Challenges Facing IoT: IEEE Internet of Things[EB/OL]. (2017-03-14)[2023-04-14]. https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html.

[5] BHARDWAJ I, KUMAR A, BANSAL M. A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoTs[C]// International Conference on Signal Processing, Computing and Control(ISPCC). IEEE, 2017: 504-509.

[6] DIEHL W, FARAHMAND F, YALLA P, et al. Comparison of Hardware and Software Implementations of Selected Lightweight Block Ciphers[C]// International Conference on Field Programmable Logic and Applications(FPL). IEEE, 2017: 1-4.

[7] HANLEY N, ONEILL M. Hardware Comparison of the ISO/IEC 29192-2 Block Ciphers[C]// IEEE Computer Society Annual Symposium on VLSI. IEEE, 2012: 57-62.

[8] BANSOD G, RAVAL N, PISHAROTY N. Implementation of a New Lightweight Encryption Design for Embedded Security[J]. IEEE Transactions on Information Forensics and Security, 2014, 10(1): 142-151.

[9] KERCKHOF S, DURVAUX F, HOCQUET C, et al. Towards Green Cryptography: A Comparison of Lightweight Ciphers from the Energy Viewpoint[C]// Cryptographic Hardware and Embedded Systems. Springer, 2012: 390-407.

[10] SHAH A, ENGINEER M. A Survey of Lightweight Crypto-

graphic Algorithms for IoT-Based Applications[C]// Smart Innovations in Communication and Computational Sciences. Springer,2019:283-293.

[11] SALLAM S,BEHESHTI B D. A Survey on Lightweight Cryptographic Algorithms[C]// IEEE Region 10 Conference. IEEE, 2018:1784-1789.

[12] THORAT C G,INAMDAR V S. Implementation of New Hybrid Lightweight Cryptosystem[J]. Applied Computing and Informatics,2018,16(1):195-206.

[13] HOSSEINZADEH J,HOSSEINZADEH M. A Comprehensive Survey on Evaluation of Lightweight Symmetric Ciphers:Hardware and Software Implementation[J]. Advances in Computer Science:an International Journal,2016,5(4):31-41.

[14] DAR A B,LONE M J,HUSSAIN N. Revisiting Lightweight Block Ciphers: Review, Taxonomy and Future Directions[J/OL]. https://ia. cr/2021/476.

[15] MOHAJERANI K,HAEUSSLER R,NAGPAL R,et al. FPGA Benchmarking of round 2 candidates in the NIST lightweight cryptography standardization process: methodology, metrics, tools,and results[J/OL]. https://ia. cr/2020/1207.

[16] DIFFIE W,HELLMAN M E. Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard[J]. Computer,1977,10(6):74-84.

[17] FYSARAKIS K,HATZIVASILIS G,RANTOS K,et al. Embedded Systems Security Challenges[C]// International Conference on Pervasive and Embedded Computing and Communication Systems. 2014:255-266.

[18] MANIFAVAS C,HATZIVASILIS G,FYSARAKIS K,et al. A Survey of Lightweight Stream Ciphers for Embedded Systems [J]. Security and Communication Networks,2016,9(10):1226-1246.

[19] INDESTEEGE S,KELLER N,DUNKELMAN O,et al. A Practical Attack on KeeLoq[C]// Advances in Cryptology—EUROCRYPT. Springer,2008:1-18.

[20] LAI X,MASSEY J L. A Proposal for a New Block Encryption Standard[C]// Advances in Cryptology—EUROCRYPT. Springer,1991:389-404.

[21] WHEELER D J,NEEDHAM R M. TEA, A Tiny Encryption Algorithm[C]// International Workshop on Fast Software Encryption. Springer,1995:363-366.

[22] AOKI K,ICHIKAWA T,KANDA M,et al. Camellia:A 128-Bit Block Cipher Suitable for Multiple Platforms—Design and Analysis[C]// International Workshop on Selected Areas in Cryptography. Springer,2001:39-56.

[23] BERTONI G,BREVEGLIERI L,FRAGNETO P,et al. Efficient Software Implementation of AES on 32-Bit Platforms[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer,2003:159-171.

[24] EISENBARTH T,GONG Z,GÜNEYSU T,et al. Compact Implementation and Performance Evaluation of Block Ciphers in ATtiny Devices[C]// International Conference on Cryptology in Africa. Springer,2012:172-187.

[25] BOGDANOV A,KNUDSEN L R,LEANDER G,et al. PRESENT:An Ultra-Lightweight Block Cipher[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer,2007:450-466.

[26] LIM C H,KORKISHKO T. mCrypton—A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors[C]// International Conference on Information Security Applications. Springer,2006:243-258.

[27] LIM C H. A Revised Version of CRYPTON:CRYPTON V1. 0 [C]// International Workshop on Fast Software Encryption. Springer,2001:31-45.

[28] WANG C,HEYS H M. An Ultra Compact Block Cipher for Serialized Architecture Implementations[C]// Canadian Conference on Electrical and Computer Engineering. IEEE, 2009: 1085-1090.

[29] CHENG H,HEYS H M,WANG C. PUFFIN:A Novel Compact Block Cipher Targeted to Embedded Digital Systems[C]// EUROMICRO Conference on Digital System Design Architectures, Methods and Tools. IEEE,2008:383-390.

[30] LEANDER G,PAAR C,POSCHMANN A,et al. New Lightweight DES Variants[C]// International Workshop on Fast Software Encryption. 2007:196-210.

[31] KILIAN J,ROGAWAY P. How to Protect DES Against Exhaustive Key Search(an Analysis of DESX)[J]. Journal of Cryptology,2001,14:17-35.

[32] SATOH A,MORIOKA S. Small and High-Speed Hardware Architectures for the 3GPP Standard Cipher KASUMI[C]// International Conference on Information Security. Springer, 2002: 48-62.

[33] KNUDSEN L,LEANDER G,POSCHMANN A,et al. PRINTCIPHER:A Block Cipher for IC-Printing[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer,2010:16-32.

[34] YAP H,KHOO K,POSCHMANN A,et al. EPCBC—A Block Cipher Suitable for Electronic Product Code Encryption[C]// International Conference on Cryptology and Network Security, 2011:76-97.

[35] STANDAERT F X,PIRET G,GERSHENFELD N,et al. SEA: A Scalable Encryption Algorithm for Small Embedded Applications[C]// International Conference on Smart Card Research and Advanced Applications. Springer,2006:222-236.

[36] LI X C,ZHONG W D,ZHANG S W,et al. A New Threshold Implementation of the S-box inSM4[J]. Journal of Cryptologic Research,2018,5(6):641-650.

[37] PEI C. A Method of Masking SM4 and Analysis against DPA Attacks[J]. Journal of Cryptologic Research,2016,3(1):79-90.

[38] ZHANG W,BAO Z,LIN D,et al. RECTANGLE:A Bit-Slice Lightweight Block Cipher Suitable for Multiple Platforms[J]. Science China Information Sciences,2015,58:1-15.

[39] KARAKOÇ F,DEMIRCI H,HARMANCı A E. ITUbee:A Software Oriented Lightweight Block Cipher[C]// International Workshop on Lightweight Cryptography for Security and Privacy. Springer,2013:16-27.

[40] BEAULIEU R,SHORS D,SMITH J,et al. The SIMON and SPECK Families of Lightweight Block Ciphers[C]// ACM/EDAC/IEEE Design Automation Conference(DAC). IEEE, 2015:1-6.

[41] MORADI A,POSCHMANN A,LING S,et al. Pushing the Li-

mits: A Very Compact and a Threshold Implementation of AES [C]// Advances in Cryptology—EUROCRYPT. Springer, 2011: 69-88.

[42] NIKOVA S, RIJMEN V, SCHLÄFFER M. Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches[J]. Journal of Cryptology, 2011, 24: 292-321.

[43] PIRET G, ROCHE T, CARLET C. PICARO—A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance[C]// International Conference on Applied Cryptography and Network Security. Springer, 2012: 311-328.

[44] GÉRARD B, GROSSO V, NAYA-PLASENCIA M, et al. Block Ciphers That Are Easier to Mask: How Far Can We Go? [C]// International Conference on Cryptographic Hardware and Embedded Systems. Springer, 2013: 383-399.

[45] GROSSO V, LEURENT G, STANDAERT F X, et al. LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations[C]// International Workshop on Fast Software Encryption. Springer, 2015: 18-37.

[46] BORGHOFF J, CANTEAUT A, GÜNEYSU T, et al. PRINCE—A Low-Latency Block Cipher for Pervasive Computing Applications[C]// Advances in Cryptology—ASIACRYPT. Springer, 2012: 208-225.

[47] ALBRECHT M R, DRIESSEN B, KAVUN E B, et al. Block Ciphers—Focus on the Linear Layer(feat. PRIDE)[C]// Advances in Cryptology—CRYPTO. Springer, 2014: 57-76.

[48] ALDABBAGH S S M, AL SHAIKHLI I F T, ALAHMAD M A. HISEC: A New Lightweight Block Cipher Algorithm[C]// International Conference on Security of Information and Networks. 2014: 151-156.

[49] ZHENG Y, MATSUMOTO T, IMAI H. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses[C]// Advances in Cryptology—CRYPTO. Springer, 1990: 461-480.

[50] SUZAKI T, MINEMATSU K. Improving the Generalized Feistel[C]// International Workshop on Fast Software Encryption. Springer, 2010: 19-39.

[51] BOGDANOV A. Cryptanalysis of the KeeLoq Block Cipher[J/OL]. https://ia.cr/2007/055.

[52] GONG Z, NIKOVA S, LAW Y W. KLEIN: A New Family of Lightweight Block Ciphers[C]// International Workshop on Radio Frequency Identification: Security and Privacy Issues. 2012: 1-18.

[53] BEIERLE C, JEAN J, KÖLBL S, et al. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS[C]// Advances in Cryptology—CRYPTO. Springer, 2016: 123-153.

[54] HUANG X, LI L, YANG J. IVLBC: An Involutive Lightweight Block Cipher for Internet of Things [J/OL]. https://doi.org/10.1109/JSYST.2022.3227951.

[55] IZADI M, SADEGHIYAN B, SADEGHIAN S S, et al. MIBS: A New Lightweight Block Cipher[C]// International Conference on Cryptology and Network Security. Springer, 2009: 334-348.

[56] WU W, ZHANG L. LBlock: A Lightweight Block Cipher[C]// International Conference on Applied Cryptography and Network Security. Springer, 2011: 327-344.

[57] 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.

[58] RAMADAN R A, ABOSHOSHA B W, YADAV K, et al. LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices[J]. Computers, Materials & Continua, 2021, 67(3): 3563-3579.

[59] FENG J Y, LI L. SCENERY: A Lightweight Block Cipher Based on Feistel Structure[J]. Frontiers of Computer Science, 2022, 16(3): 163813.

[60] ZHU D, TONG X J, WANG Z, et al. A Novel Lightweight Block Encryption Algorithm Based on Combined Chaotic System[J]. Journal of Information Security and Applications, 2022, 69: 103289.

[61] SHIRAI T, SHIBUTANI K, AKISHITA T, et al. The 128-Bit Blockcipher CLEFIA (Extended Abstract)[C]// International Workshop on Fast Software Encryption. Springer, 2007: 181-195.

[62] AKISHITA T, HIWATARI H. Very Compact Hardware Implementations of the Blockcipher CLEFIA[C]// International Workshop on Selected Areas in Cryptography. Springer, 2012: 278-292.

[63] OJHA S K, KUMAR N, JAIN K. TWIS—A Lightweight Block Cipher[C]// International Conference on Information Systems Security. 2009: 280-291.

[64] SHIBUTANI K, ISOBE T, HIWATARI H, et al. Piccolo: An Ultra-Lightweight Blockcipher[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2011: 342-357.

[65] SUZAKI T, MINEMATSU K, MORIOKA S, et al. Twine: A Lightweight, Versatile Block Cipher[C]// ECRYPT workshop on lightweight cryptography. 2011: 146169-146192.

[66] BANIK S, BAO Z, ISOBE T, et al. WARP: Revisiting GFN for Lightweight 128-Bit Block Cipher[C]// International Conference on Selected Areas in Cryptography. Springer, 2021: 535-564.

[67] YAN L Y, LI L, GUO Y. DBST: A Lightweight Block Cipher Based on DynamicS-box[J]. Frontiers of Computer Science, 2023, 17(3): 173805.

[68] HONG D, SUNG J, HONG S, et al. HIGHT: A New Block Cipher Suitable for Low-Resource Device[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2006: 46-59.

[69] HONG D, LEE J K, KIM D C, et al. LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors[C]// International Workshop on Information Security Applications. Springer, 2014: 3-27.

[70] KOO B, ROH D, KIM H, et al. CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices[C]// International Conference on Information Security and Cryptology. Springer, 2018: 3-25.

[71] CHEN S Y, FAN Y H, SUN L, et al. SAND: An AND-RX Feistel Lightweight Block Cipher Supporting S-box-based Security Evaluations[J]. Designs, Codes and Cryptography, 2022, 90: 155-198.

[72] ZHANG X, TANG S, LI T, et al. GFRX: A New Lightweight Block Cipher for Resource-Constrained IoT Nodes[J]. Electronics, 2023, 12(2): 405.

[73] DE CANNIERE C，DUNKELMAN O，KNEŽEVIĆ M. KATAN and KTANTAN—A Family of Small and Efficient Hardware-Oriented Block Ciphers[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer，2009：272-288.

[74] DAS S. Halka：A Lightweight，Software Friendly Block Cipher Using Ultra-Lightweight 8-Bit S-box[J/OL]. https://ia. cr/2014/110.

[75] ENGELS D，FAN X，GONG G，et al. Hummingbird：Ultra-Lightweight Cryptography for Resource-Constrained Devices[C]// International Conference on Financial Cryptography and Data Security. Springer，2010：3-18.

[76] ENGELS D，SAARINEN M J O，SCHWEITZER P，et al. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm[C]// International Workshop on Radio Frequency Identification：Security and Privacy Issues. Springer，2012：19-31.

[77] PEI C，XIAO Y，LIANG W，et al. Trade-off of Security and Performance of Lightweight Block Ciphers in Industrial Wireless Sensor Networks[J]. EURASIP Journal on Wireless Communications and Networking，2018，2018(1)：117-134.

[78] ROLFES C，POSCHMANN A，LEANDER G，et al. Ultra-Lightweight Implementations for Smart Devices—Security for 1000 Gate Equivalents[C]// International Conference on Smart Card Research and Advanced Applications. Springer，2008：89-103.

[79] HATZIVASILIS G，FYSARAKIS K，PAPAEFSTATHIOU I，et al. A Review of Lightweight Block Ciphers[J]. Journal of cryptographic Engineering，2018，8：141-184.

[80] BATINA L，DAS A，EGE B，et al. Dietary Recommendations for Lightweight Block Ciphers：Power，Energy and Area Analysis of Recently Developed Architectures[C]// International Workshop on Radio Frequency Identification：Security and Privacy Issues. Springer，2013：103-112.

[81] PLOS T，GROß H，FELDHOFER M. Implementation of Symmetric Algorithms on a Synthesizable 8-Bit Microcontroller Targeting Passive RFID Tags[C]// International Workshop on Selected Areas in Cryptography. Springer，2011：114-129.

[82] CAZORLA M，MARQUET K，MINIER M. Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks[C]// International Conference on Security and Cryptography(SECRYPT). IEEE，2013：1-6.

[83] DINU D，CORRE Y L，KHOVRATOVICH D，et al. Triathlon of Lightweight Block Ciphers for the Internet of Things[J]. Journal of Cryptographic Engineering，2019，9：283-302.

[84] RINNE S，EISENBARTH T，PAAR C. Performance Analysis of Contemporary Light-Weight Block Ciphers on 8-Bit Microcontrollers[C]// Software Performance Enhancement for Encryption and Decryption. 2007：1-12.

[85] ENGELS S，KAVUN E B，PAAR C，et al. A Non-Linear/Linear Instruction Set Extension for Lightweight Ciphers[C]// IEEE Symposium on Computer Arithmetic. IEEE，2013：67-75.

[86] KONG J H，ANG L M，SENG K P. A Comprehensive Survey of Modern Symmetric Cryptographic Solutions for Resource Constrained Environments[J]. Journal of Network and Computer Applications，2015，49：15-50.

[87] KOUSALYA R，KUMAR G A S. A Survey of Light-Weight Cryptographic Algorithm for Information Security and Hardware Efficiency In Resource Constrained Devices[C]// International Conference on Vision Towards Emerging Trends in Communication and Networking(ViTECoN). IEEE，2019：1-5.

[88] AHMED S F，ISLAM M R，NATH T D，et al. G-TBSA：A Generalized Lightweight Security Algorithm for IoT[C]// International Conference on Electrical Information and Communication Technology(EICT). IEEE，2019：1-6.

[89] GROVER L K. A Fast Quantum Mechanical Algorithm for Database Search[C]// ACM Symposium on Theory of Computing(STOC). ACM，1996：212-219.

[90] SIMON D R. On the Power of Quantum Computation[J]. SIAM Journal on Computing，1997，26(5)：1474-1483.

[91] KUPERBERG G. A Subexponential-Time Quantum Algorith for the Dihedral Hidden Subgroup Problem[J]. SIAM Journal on Computing，2005，35(1)：170-188.

[92] HARROW A W，HASSIDIM A，LLOYD S. Quantum Algorithm for Linear Systems of Equations[J]. Physical Review Letters，2009，103(15)：150502.

[93] BIJWE S，CHAUHAN A K，SANADHYA S K. Quantum Search for Lightweight Block Ciphers：GIFT，SKINNY，SATURNIN[J/OL]. Cryptology ePrint Archive，2020，1485. https://ia. cr/2020/1485.

[94] BONNETAIN X，NAYA-PLASENCIA M，SCHROTTENLOHER A. Quantum Security Analysis of AES[J]. IACR Transactions on Symmetric Cryptology，2019，2019(2)：55-93.

[95] DONG X，DONG B，WANG X. Quantum Attacks on Some Feistel Block Ciphers[J]. Designs，Codes and Cryptography，2020，88(6)：1179-1203.

[96] BIRYUKOV A，WAGNER D. Advanced Slide Attacks [C]// Advances in Cryptology—EUROCRYPT. Springer，2000：589-606.

[97] ANAND M V，TARGHI E E，TABIA G N，et al. Post-Quantum Security of the CBC，CFB，OFB，CTR，and XTS Modes of Operation[C]// International Conference on Post-Quantum Cryptography. Springer，2016：44-63.

[98] HOSOYAMADA A，IWATA T. 4-Round Luby-Rackoff Construction is a qPRP[C]// Advances in Cryptology—ASIACRYPT. Springer，2019：145-174.

[99] ALAGIC G，RUSSELL A. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts[C]// Advances in Cryptology-EUROCRYPT. Springer，2017：65-93.

[100] HOSOYAMADA A，IWATA T. Provably Quantum-Secure Tweakable Block Ciphers[J]. IACR Transactions on Symmetric Cryptology，2021，2021(1)：337-377.

ZHONG Yue，born in 1993，Ph. D，lecturer. Her main research interests include artificial intelligence，data analytics and data security.

（责任编辑：何杨）