面向边缘侧的电力物联网轻量级加密算法设计与实现

郑吉祥　戴　睿　杨　懿　李崇茳　伍梓涵
国网四川省电力公司信息通信公司　四川成都　610041

摘　要：电力物联网的迅猛进步促使电力系统由集中管控模式逐步转向分布式架构，在此过程中，边缘计算技术对数据获取、信息传递及即时分析的重要性日益突出。但边缘终端设备通常面临计算能力不足、能源供应受限以及存储容量短缺等挑战，常规加密方法在具体应用场景中经常出现执行效能低下、响应迟缓及资源占用过多等缺陷，无法充分适应电力物联网对即时响应与安全防护的严苛标准。针对边缘计算环境的安全需求，轻量化加密技术因其计算资源占用少、架构可定制及兼容性优异等特点，成为解决终端安全问题的理想方案。本研究立足于电力物联网边缘节点的防护要求，系统剖析了系统架构与数据传输环节的潜在威胁，融合当前轻量密码学领域的技术演进方向，创新性地设计了基于优化分组模式的轻量加密方案，并在主流边缘终端上完成了方案验证与效能测试。

关键词：电力物联网；边缘计算；轻量级加密；算法实现

引言

随着电力系统的发展，电力物联网终端数量急剧增加，网络传输数据量爆发式增长，传统云计算难以满足全部需求，因此边缘计算获得越来越多的关注。边缘计算旨在解决云计算遇到的数据处理、存储及传输问题，可采用边缘网关进行分布式部署，就近进行数据采集、处理、协议转换及数据分析等，极大缓解网络传输与数据中心的压力。但受限于边缘设备的硬件资源约束，当处理高强度加密计算和海量安全通信任务时，往往会出现性能下降与能耗激增的问题，这给系统安全带来了不容忽视的潜在风险。传统加密技术虽然能够提供较高的安全防护水平，但其复杂的运算机制难以满足资源受限环境的需求。针对电力物联网边缘计算场景的特殊要求，开发适合该领域的精简加密方案显得尤为重要。本研究重点探讨了轻量级加密技术的核心设计理念、具体实施方法及其在电力物联网中的实际效用，旨在为构建更加完善的电力物联网安全防护系统提供技术参考和实施方案。

作者简介：
1.郑吉祥，1994年1月，男，汉族，四川宜宾，工程师，硕士研究生，安全传输技术研究；
2.戴睿，1980年9月，男，汉族，四川成都，高级工程师，信息技术；
3.杨懿，1983年11月，女，汉族，安徽淮北，高级工程师，硕士研究生，信息技术；
4.李崇茳，1997年2月，男，汉族，四川宜宾，助理工程师，本科，计算机科学与技术；
5.伍梓涵，1999年12月，女，汉族，四川资阳，助理工程师，硕士研究生，网络运维管理。

一、面向边缘侧的电力物联网安全需求与轻量化设计理论基础

（一）电力物联网边缘侧的体系结构与安全风险

电力物联网的架构设计普遍采用三层模型，由数据采集层、边缘计算层和业务服务层构成。作为承上启下的关键环节，边缘计算层主要负责信息整合、即时分析和区域决策等核心任务。该层级部署的智能终端涵盖计量装置、监测设备、调控节点以及配网自动化系统等，这些设施对维持供电稳定性和优化系统性能具有决定性影响。然而，这类终端设备通常存在运算性能不足、功耗约束严格以及存储资源匮乏等固有缺陷，致使安全防御机制存在明显短板，极易被不法分子利用。从具体威胁层面来看，风险在于通信数据可能遭到监听和非法修改，这将直接威胁电力调度指令的保密性；是身份认证环节的漏洞，攻击者通过伪造合法设备身份可能引发电网运行异常；此外，边缘计算节点的物理安全防护不足，若被恶意操控将造成严重的电力系统故障。

（二）轻量级加密算法的设计原则与理论依据

资源受限场景催生了轻量级加密技术的诞生，这类算法旨在以最低的计算开销和存储占用确保敏感信息的保密性与防篡改性。相较于常规加密方案，轻量级版本更注重运算精简度和能耗经济性。其设计准则包含以下

关键要素：追求运算简约与执行高效，算法架构应当规避繁复的迭代函数和庞大的查找表操作，从而优化处理效率；保持足够的安全强度，即便采用简化运算，仍需具备对抗典型攻击手段（包括差分分析与线性破译）的防护能力；具备可调节特性，能依据不同终端设备的硬件配置动态变更参数与实施方案；实现防护效能与运行表现的合理权衡，在保障基础安全需求的前提下，尽可能减少电力消耗与时间延迟。从理论基础分析，当前密码学体系中的对称加密技术、分组密码机制以及流密码模式，为轻量级加密算法的研发奠定了可靠框架。

（三）边缘计算与加密算法的融合逻辑

边缘计算作为新型数据处理架构，为轻量级加密技术的实施创造了有利条件。其融合特性具体表现在四个维度：基于本地化数据处理能力，边缘计算显著降低了对中心化服务器的需求，有效缩短了加密传输的时延，增强了系统响应速度；轻量级加密方案与边缘设备的低功耗特性高度匹配，能够在资源受限的终端实现可靠的安全保障；边缘架构的分布式本质赋予加密技术更灵活的配置选择，使得安全防护能够贴近数据产生节点，大幅优化防御体系；在协同计算场景下，加密机制必须与边缘系统的任务分配策略相协调，实现安全性能与运行效率的平衡。从整体来看，边缘计算技术与轻量化加密方案的协同应用，既能显著改善常规安全体系的缺陷，也为电力物联网建立立体化安全防护架构奠定了可靠的理论基础。

二、电力物联网边缘侧轻量级加密算法设计的关键问题与优化方向

（一）加密算法在资源受限边缘设备上的性能瓶颈

边缘设备在硬件配置方面的不足成为阻碍常规加密技术部署的关键因素。当前主流的高强度加密方案通常涉及多次循环运算、复合型非线性变换以及大容量存储操作，这些要求普遍超出了边缘终端的处理极限。具体而言，其负面影响主要体现在三个方面：运算响应时间明显延长，干扰了数据流转与即时处理的时效性；电力消耗急剧上升，持续进行加密操作会快速耗尽设备电源，削弱其长效运行性能；存储资源分配失衡，部分算法需要维护庞大的查找索引或临时变量区域，引发系统运行异常。这些运行限制不仅削弱了终端设备的处理效能，更可能由于安防措施延迟执行而导致潜在威胁。

（二）数据传输与隐私保护中的安全漏洞

电力物联网的终端数据传输网络结构多元，既包含终端设备间的直接交互通道，也涉及多层级的中继传输路径，这种架构特性使信息传递环节存在显著安全隐患。典型威胁类型涉及传输层劫持、数据包复制窃取以及非授权监听等恶意行为。若核心数据被不法分子获取，既会造成个人敏感信息外泄，更可能干扰电网运行调控与电能供应稳定性。同时，边缘计算节点的身份核验体系普遍存在缺陷，使得伪装终端能够轻易渗透系统，从而大幅提升数据流转过程中的安全威胁等级。在用户隐私安全领域，电力消费数据往往蕴含着极具价值的个人行为特征，这些信息一旦遭到泄露将引发重大风险。当前主流的安全防护方案在边缘计算环境中实施难度较大，难以同时满足系统安全性和资源效率的双重要求。

（三）现有轻量级加密方案在电力物联网中的适配性不足

当前阶段，PRESENT、SPECK、LEA等轻量级加密技术在物联网领域获得了部分实际部署，然而针对电力物联网边缘计算场景的适用性仍面临挑战。具体来看，PRESENT算法虽然具备精简的架构设计，但其对抗差分密码分析的能力存在明显缺陷；SPECK方案在运算效率方面表现突出，但关于其安全强度的学术争论始终未平息；LEA算法虽然适配高性能嵌入式系统，但在超低功耗应用环境中能耗控制效果不尽理想。电力物联网的特殊应用场景对数据防护和响应速度提出了双重标准，但当前轻量级加密方案在功耗控制、防护能力与适用性维度存在明显短板。这种技术匹配缺陷不仅降低了现场实施成效，更制约了相关算法在专业领域的普及应用。

（四）边缘侧算法优化的技术瓶颈与发展趋势

边缘计算场景下，轻量级加密技术的实际部署遭遇多重制约因素。从硬件层面来看，专用加速模块的缺失使得算法性能提升受限，多数终端设备不得不通过软件方案进行性能调优。在标准化建设方面，各能源企业采用的密码规范存在显著差异，这种碎片化现状严重阻碍了跨系统协同运作。此外，当这类算法需要与人工智能、海量数据处理等创新技术结合时，在确保安全强度的同时实现智能功能的有效整合，构成了新的技术挑战。未来发展方向主要涵盖：强化硬件与算法的协同配合，促进芯片级精简安全单元的研发；健全行业规范，构建统一的安全协议与算法体系；研究融合机器学习技术的自适应轻量加密方案，达成灵活的安全保障。

三、面向边缘侧的电力物联网轻量级加密算法实现与应用路径

（一）基于改进分组结构的轻量级加密算法设计

在电力物联网边缘计算场景下，优化分组密码架构

是增强轻量级加密效能的关键手段。主要技术路线涵盖精简轮运算模块、改良S盒与P盒配置、压缩迭代轮数等策略，旨在维持安全强度的同时提高运算效率。具体而言，运用精简型替换–置换组合结构能够有效缩减存储资源占用；而改进的密钥编排方案则可在简化运算流程的同时强化密钥派生过程的安全性。该设计在边缘计算资源受限的条件下仍能保持高效的加解密处理速度，有效兼顾了电力物联网对响应时效与运行可靠性的双重需求。同时，优化后的模块化架构显著提升了算法适应性，使其能够灵活部署于各类性能差异化的边缘终端设备。

（二）算法在边缘设备上的实现与性能评估

算法的实用价值必须借助真实场景的测试与效能分析进行确认。在资源受限设备上部署精简加密方案时，应当重点考察程序指令集的精简程度与运算速度。测试环节可选取具有代表性的物联网终端设备（例如基于ARM Cortex–M架构的芯片），通过比对处理时长、存储消耗及电力损耗等参数，系统性地检验算法表现。实验数据证实，经过优化的分组加密方案在运行效能方面明显超越常规加密方法，电力消耗指标下降幅度达到显著水平，特别适配持续工作的电力设备场景。安全性验证环节显示，该方案对差分分析及线性破译均展现出良好的防御能力，实际安全等级符合应用要求。这些测试结论既佐证了技术路线的科学性，也为电力物联网领域的规模化实施奠定了实证基础。

（三）边缘计算环境下的安全协同机制构建

在边缘计算的多节点协作场景下，仅依靠轻量级加密算法的独立部署难以全面保障数据安全传输。首要措施是实施去中心化的密钥分发体系，确保各计算节点间的通信既保持独立性又具备足够防护能力；应结合边缘计算特有的任务调度模式，设计可动态调整的安全策略框架，使加密强度能随任务安全等级自动适配；此外，充分利用边缘节点的网络拓扑特性，建立联防联控机制，实现对异常行为的实时监测与快速处置。这种综合防护方案能在控制计算资源消耗的前提下，显著增强网络系统的整体抗攻击能力，为构建电力物联网的立体化安全防护网络奠定技术基础。

（四）算法应用推广与未来发展方向

轻量级加密技术在多个领域展现出广阔的应用潜力，特别适用于智能计量装置、配电控制终端、远程监控系统以及用户端能耗管理等场景。这类技术在实际推广时，必须严格遵循相关行业规范，促进加密方案在电力物联网各层级的标准化应用，确保不同平台和设备间的无缝衔接。与此同时，必须重视量子计算可能引发的安全隐患，积极研发具有量子抗性的精简加密方案，确保电力系统在未来能够保持稳定运行。需要促进不同学科间的交叉协作，整合人工智能技术、海量数据分析以及分布式边缘计算等前沿科技手段，加速精简加密算法的智能化升级进程。

结语

本研究聚焦于电力物联网边缘计算领域的安全防护需求，系统性地探讨了轻量级加密技术的设计准则、核心挑战及性能提升策略，同时构建了基于新型分组架构的轻量级算法开发框架。实验数据证实，经过优化的轻量级加密方案在确保信息安全的前提下，显著减少了运算资源消耗与电力损耗，完全适配边缘计算终端的应用场景要求。在具体实施与效能验证阶段，该算法表现出优异的兼容性和安全防御性能，有效确保了电力物联网的平稳运转。特别值得注意的是，融合边缘计算的分散式架构特点，建立安全协作体系将成为后续发展的关键路径。

参考文献

[1]邓喆，吴亚洁.边缘计算场景下无线传感器网络信息轻量级加密算法[J].信息技术与信息化，2024（1）：157–160.

[2]张海超，赖金山，刘东，等.边缘计算下的轻量级联邦学习隐私保护方案[J].计算机技术与发展，2023，33（9）：161–167.

[3]朱宏颖，张新有，邢焕来，等.边缘计算环境下轻量级终端跨域认证协议[J].网络与信息安全学报，2023，9（4）：74–89.

[4]刘雪娇，宋庆武，夏莹杰.基于区块链的车联网矩阵计算安全卸载方案[J].浙江大学学报：工学版，2023，57（1）：144–154.

[5]郑嘉诚，何亨，陈月佳，等.边缘计算中基于区块链的轻量级密文访问控制方案[J].计算机系统应用，2024，33（4）：69–81.