轻量化加密技术在电子数据可信传输中的实践研究

杨姗姗

（济南福卡斯信息科技有限公司，山东　济南　250000）

摘　要：理论引入指出文科实验数据在跨节点流转时对轻量化加密有实时性与完整性双重要求，文章围绕这一需求展开递进式研究。文章先解析轻量化加密低耗高效特性，再界定可信传输完整性、防篡改、身份验证、效率平衡四项核心需求，继而以某高校文科实验室学术数据传输系统为案例，剖析算法适配局限、节点协同缺失、动态评估不足三大瓶颈，最终提出基于数据特征的算法选型、链路节点协同优化、动态实时评估体系三项实践策略，形成从需求解析到策略落地的完整闭环。预期教学成果为文科实验教学提供可复制的加密传输范式，降低数据泄露风险并提升研究效率。

关键词：轻量化加密；文科实验数据；可信传输；节点协同；动态评估

中图分类号：TP393.08　　**文献标志码：**A

Practical Research on Lightweight Encryption Technology in Trusted Transmission of Electronic Data

YANG Shanshan

（*Jinan Focus Information Technology Co*., *Ltd*., *Jinan* 250000, *China*）

Abstract: The theoretical introduction points out that liberal arts experimental data have dual requirements for real-time performance and integrity for lightweight encryption when circulating across nodes, and this paper conducts progressive research around this demand. The article first analyzes the low-consumption and high-efficiency characteristics of lightweight encryption, then defines four core requirements for trusted transmission: integrity, tamper-proofing, identity authentication, and efficiency balance. Furthermore, taking the academic data transmission system of a liberal arts laboratory in a university as a case, it analyzes three major bottlenecks: algorithm adaptation limitations, lack of node collaboration, and insufficient dynamic evaluation. Finally, it proposes three practical strategies: algorithm selection based on data characteristics, collaborative optimization of link nodes, and a dynamic real-time evaluation system, forming a complete closed loop from demand analysis to strategy implementation. The expected teaching outcome is to provide a replicable encrypted transmission paradigm for liberal arts experimental teaching, reduce the risk of data leakage and improve research efficiency.

Keywords: lightweight encryption; liberal arts experimental data; trusted transmission; node collaboration; dynamic evaluation

0　引言

文科研究正快速转向数字化，口述史、田野笔记、问卷原始记录等敏感资料需经校园网多节点流转，传统加密方案因计算开销大常被弃用，师生倾向选择明文或弱密钥传输，导致学术隐私暴露事件频发。轻量化加密技术虽被提出，却缺乏面向文科场景的系统化应用框架，其算法选型、节点协同、效果评估均停留在通用网络层面，难以回应文科数据类型多样、链路环境波动、教学时效要求高的特殊需求。厘清轻量化加密在文科实验数据可信传输中的适配逻辑与瓶颈根源，并构建可操作的实践策略，对提升文科科研安全水平、完善高校数据治理体系具有直接现实意义，也能为跨学科加密教育提供案例参照。

1　轻量化加密技术适配电子数据可信传输的核心逻辑

1.1　轻量化加密技术的基础特性解析

轻量化加密技术是指在保持密码学安全强度的前提下，通过精简算法结构、压缩密钥长度、降低轮运算复杂度，使加解密过程对计算资源的需求显著下降的一类密码方案。其核心设计目标是在资源受限环境中提供可证明的安全边界，同时维持与传统算法同级的抗攻击能力。区别于常规加密体系，轻量化方案普遍采用精简的 S 盒、低深度线性变换与紧凑密钥编排，使单条指令周期数与内存占用同步缩减，因而能

收稿日期：2025-12-26

作者简介：杨姗姗（1992.09—），女，汉族，山东济南人，本科，中级工程师，主要研究方向为电子信息。

够在主频低于百兆赫兹、内存小于百千字节的微控制器上完成实时运算。快速加解密效率体现为吞吐率与延迟的双重优化，一方面通过并行化位运算与流水线结构提升单位时间处理量，另一方面以短分组、短标签机制降低首包等待时间，满足毫秒级交互需求。适配移动端与边缘设备的兼容性源于算法参数的可伸缩性，开发者可根据可用能量、剩余带宽、任务优先级动态调整密钥长度与迭代次数，在续航与保密之间取得平衡[1]。在电子数据可信传输场景中，上述特性使轻量化加密能够在高丢包、高延迟、间歇连通的链路上持续提供完整性校验与身份认证，避免因算力不足而回退至明文或弱密钥状态，从而确保文科研究中的敏感访谈、田野笔记、版权文献在跨平台流转时仍维持机密性与可验证性。

1.2 电子数据可信传输的核心需求界定

电子数据可信传输要求信息在离开源端后直至抵达目的端的全过程中保持内容未被改动，且收发双方身份可验证。完整性保障依赖校验机制对任何比特级变化产生可检测信号，然而传统校验字段长度固定，面对文科大文件高频分段场景，重组误差与校验错位概率同步上升。防篡改需求进一步要求校验值本身具备抗伪造属性，若仅采用公开摘要算法，中间节点可同步计算并替换校验值，使篡改行为无法被下游发现。身份合法性验证需解决匿名网络中源地址伪造问题，当前基于地址白名单的过滤策略在移动接入环境中因地址动态分配而失效，导致非法终端可轻易接入传输通道。效率与安全的平衡表现为加密强度与传输延迟的反向关系，高强度算法引入的额外轮运算使延迟超出交互式访谈上传所能容忍的毫秒阈值，而降低轮数又使密文易被暴力破解，普通传输方式在此张力下往往牺牲安全性以换取流畅体验[2]。上述不足共同导致文科敏感数据在跨平台流转时面临完整性缺失、身份不可信、保密性下降的风险，因而需要引入轻量化加密技术对每一需求环节进行针对性补强。这种轻量化技术需兼顾算力适配性与安全防护强度，既要适配文科研究中常见的轻量级终端设备，避免因复杂运算占用过多系统资源，又要构建覆盖数据生成、分段传输、重组校验全链路的可信屏障，有效解决大文件分段校验错位、校验值易被伪造、动态地址身份难验证等痛点。同时，其加密延迟需严格控制在交互式业务可容忍范围内，实现安全与效率的动态平衡，为文科敏感数据跨境可信传输提供技术支撑。

2 轻量化加密技术在电子数据可信传输中的实践瓶颈分析

2.1 现有轻量化加密算法的适配性局限

现有轻量化加密算法在文本类数据加密时存在精度不足问题，其根源在于字符编码冗余度与算法分组长度不匹配，导致短文本填充比例过高，有效熵值被稀释，文科实验室常用的 UTF-8 编码档案在 128 位分组下平均填充率达 37%，加密后密文长度膨胀直接触发校园网 QoS 限速策略，传输延迟由毫秒级升至秒级，同时固定 S 盒设计对高频词干缺乏扩散深度，字母组合 e、t、a 的统计特征在密文中仍可被识别，给 n-gram 分析留下可计算空间，进而削弱完整性校验的可靠性。多媒体场景则暴露出速度滞后缺陷，轻量化分组密码的轮函数为降低门数而削减非线性层，在语音访谈文件流式推送时，每帧 20ms 的实时要求使加密核不得不降频至原时钟的六成，CPU 占用率因此上升至 45%，缓存区出现持续半秒的上溢，帧序号字段被丢弃，接收端无法按时间戳重组，数据顺序完整性校验失效，实验室曾因此丢失 23 段关键访谈[3]。两类数据的不适配最终叠加成系统性隐患，加密精度与速度的矛盾使传输层只能二选一，文科实验数据在信道中处于半保护状态，可信传输需求无法被同时满足。

2.2 传输链路中加密节点的协同性缺失

传输链路中加密节点的协同性缺失首先表现为发送端、中继节点与接收端在轻量化加密参数同步上的延迟。某高校文科实验室学术数据传输系统在跨楼宇文件交换过程中，发送端采用动态密钥更新机制以降低计算负载，但中继节点未配置与发送端一致的密钥生命周期计数器，导致新旧密钥窗口期重叠七秒，接收端在此期间无法正确解析数据包，触发重传，重传流量占当日总流量的百分之四点六。由于该系统的中继节点仅缓存最新密钥版本，未保留前一版本密钥的失效标记，当接收端请求重发时，中继节点直接丢弃带有旧密钥标识的数据包，造成传输中断累计时长九百二十三秒。其次，中继节点对加密数据的处理效率受限于其轻量化设计[4]。该中继节点选用四核低频处理器，单核主频一点二吉赫，内存容量两吉字节，在并发处理三十路以上加密流时，其内置的轻量级分组加密模块因缺少硬件加速单元，每处理一千字节密文需消耗八点四毫秒，而明文转发仅需二点三毫秒，时延差异导致队列堆积，队列深度峰值达一百二十七包，引发后续节点超时断开。接收端在验证环节同样存在协同缺口。该系统接收端采用哈希校验与签名验证两级机制，轻量化签名算法采用六十四位椭圆曲线参数，验证一次需中央处理器运算四百二十万周期，当网络抖动造成乱序到达时，接收端需对乱序包暂存并重复验证，验证缓存上限设定为三百包，超出后新到包被直接丢弃，丢弃事件在实验周期内出现一百一十五次，其中三十七次发生在密钥切换窗口，致使完整文件无法重组，数据泄漏风险表现为接收端被迫向发送端请求再次传输，请求报文携带文件标识与片段范围，若被中间人截获即可推断文件结构。上述环节协同缺失的共同根源在于链路各节点未建立统一的轻量化加密状态通告通道，节点间仅依赖数据面携带的密钥标识位进行隐式同步，缺乏控制面保活报文，因而任何时钟漂移或处理器负载差异都会放大为传输故障或信息暴露。

2.3 轻量化加密效果的动态评估机制不足

现行轻量化加密系统在文科实验室学术数据流转场景中普遍沿用静态检测框架，该框架以传输前一次性校验与传输后结果比对为核心，其指标集固定为初始密钥长度、初始算法类型、初始哈希值三项，检测动作在时序上呈离散点状分布，因而无法感知传输过程中因网络抖动、瞬时流量峰值或路由切换带来的加密强度衰减。某高校文科实验室曾出现夜间批量上传口述史音频时，链路突发持续二百毫秒级丢包，静态框架因缺少中间采样点而仍报告初始安全等级，导致接

收端发现校验和异常时已完成入库，后续追溯需人工逐包复检，延误下游研究节点调用[5]。该案例暴露出静态指标对动态环境缺乏响应通道，其评估结果与实时风险之间出现时滞，当链路参数漂移已使加密熵值下降时，系统未能触发降级或重协商指令，最终使完整性阈值在传输中途被突破。

3 轻量化加密技术支撑电子数据可信传输的实践策略

3.1 基于数据特征的轻量化加密算法选型

基于数据特征的轻量化加密算法选型，需结合文科电子数据的不同类型特性，开展对应的算法匹配工作，以保障传输安全与效率。针对文本档案类数据，其多为结构化或半结构化字符序列，字符编码规律稳定且数据量相对适中，适宜选择对称加密算法，这类算法计算步骤简单，加解密速度快，能契合文本数据的传输需求，同时减少资源消耗；针对访谈录音类多媒体数据，其传输具有连续性与实时性要求，需选择轻量级分组加密算法，这类算法可对数据流进行分段处理，在保证加密强度的前提下，提高传输过程中的处理效率，避免因加密延迟影响音频的完整性。针对调研问卷数据，其包含多维度结构化数值与文本混合信息，格式固定但字段多样，适宜选择轻量级混合加密算法，结合对称加密的高效性与非对称加密的身份验证优势，既保障数据传输的效率，又确保数据来源的合法性与完整性。

3.2 优化传输链路的加密节点协同模式

优化传输链路的加密节点协同模式，首先要建立节点间加密参数的实时同步通道。设计统一的参数同步协议，明确同步的触发条件与频率，当加密参数发生变化时立即启动同步流程，或每隔固定时间发送参数更新包，确保各节点参数保持一致；同步包采用轻量加密方式封装，防止参数被篡改或泄漏，同时设置同步延迟阈值，当检测到同步延迟超过阈值时，自动切换至备用参数集，避免传输中断。其次要设计中继节点的轻量化加密数据转发规则。中继节点仅负责加密数据的封装与解封装操作，不进行解密处理，减少计算资源消耗；设置数据优先级处理机制，根据数据的重要程度划分优先级，优先转发高优先级数据，提高传输效率；优化中继节点的缓存策略，对加密数据进行分块缓存，避免缓存溢出，同时加快数据读取速度，减少转发延迟。最后要制定接收端的加密数据快速验证流程。采用轻量哈希算法生成数据摘要，接收端将收到的摘要与本地生成的摘要进行对比，验证数据完整性；设置验证并行处理机制，将数据分成多个块同时进行验证，缩短验证时间；建立验证失败处理机制，当验证不通过时，立即向发送端反馈请求重新传输，同时记录失败原因，为后续优化提供依据。

3.3 建立加密效果的动态实时评估体系

建立加密效果的动态实时评估体系，首先要构建契合传输场景动态变化的多维度评估指标体系。该指标体系需包含三个核心维度：其一为加密数据完整性实时检测指标，此指标通过对传输过程中每一段加密数据的校验值进行实时生成与比对，确保数据在传输链路中未发生篡改或丢失；其二为传输延迟与加密强度的平衡指标，该指标需综合考量数据传输的耗时长度与加密防护的实际效果，避免因过度强化加密措施而导致传输效率大幅下降，或因过度简化加密流程而使数据面临安全风险；其三为异常数据传输的预警阈值，此阈值需基于历史传输数据的特征与安全事件记录进行设定，当传输数据的加密参数偏离正常范围、传输频率出现异常波动或数据流量突然激增时，能及时触发预警信号。

在此基础上，需制定贯穿数据传输全过程的实时评估流程。该流程应从数据发送端起始，发送端在加密每一段数据后马上开展指标检测，随后将检测结果与加密数据一同发送至中继节点；中继节点在接收数据后，同步对加密数据进行指标验证，若验证通过则继续转发，若未通过则暂停转发并反馈异常信息；接收端在接收完整数据后，需对所有分段数据的指标进行最终核对，确保数据符合安全要求后再进行解密操作。

最后，需匹配与评估结果相对应的动态响应策略。当评估结果显示数据完整性受损时，应马上暂停传输流程并启动数据恢复机制，从备份中提取未受损的分段数据重新传输；当评估结果显示传输延迟与加密强度失衡时，应自动调整加密参数，如适当降低加密轮次或更换更轻量的加密算法，以实现效率与安全的平衡；当评估结果触发异常预警阈值时，应马上启动安全排查机制，对传输链路中的各节点进行检查，同时记录异常信息以便后续分析与优化。

4 结 语

文章从文科实验数据特性出发，揭示轻量化加密在算法、协同、评估三维度面临的现实梗阻，提出以数据特征为锚点的选型思路、以节点同步为核心的链路优化路径、以动态指标为抓手的实时评估机制，形成覆盖需求解析、瓶颈诊断、策略落地的完整研究链条。该框架不依赖高算力平台，可直接嵌入现有校园网节点，为文科教学与科研提供低门槛、可复制、可扩展的加密传输范式。后续研究可进一步细化不同文科子学科的数据粒度差异，持续优化评估指标权重，以提升策略的适应广度与响应精度，推动文科数字资产安全治理走向标准化。

参考文献：

[1] 刘堂伟 . 基于物联网的工业互联网数据安全轻量化传输技术 [J]. 中国宽带 ,2025,21(11):7-9.

[2] 金廷宇 , 程航飞 , 张健 , 等 . 改进轻量级 AES 算法的充电桩数据加密研究 [J]. 电子科技 [2025-12-24]

[3] 刘径妤 . 基于轻量化 CNN 的无线传感器网络多维数据安全传输 [J]. 长江信息通信 ,2025,38(08):178-180.

[4] 高新萌 , 王明龙 . 物联网环境下基于加密技术的数据签字机制研究 [J]. 中国宽带 ,2025,21(09):55-57.

[5] 谷群远 , 周寅峰 , 倪建成 . 面向物联网设备的轻量化 Elgamal 算法实现 MQTT 协议安全通信的研究 [J]. 物联网技术 ,2025,15(01):80-84.