加密传输机制在网络安全中的应用

邓正伟 冯沛林 吴伟毅 文瑞阳

联通数字科技有限公司，北京市，100000；

摘要：加密传输机制作为网络安全防线的核心技术之一，直接影响信息在开放网络中的保密性与完整性。本文聚焦对称加密与非对称加密的协同机制，系统分析传输层安全协议（如 TLS 1.3、QUIC）在 Web 应用、物联网、数据合规与边缘计算中的部署方式与性能影响。通过构建从原理到应用的逻辑路径，指出密钥生命周期管理、协议兼容与加密域划分是当前实践中的关键难题。文章归纳出加密传输在不同行业场景下的性能、安全与合规三重制约，并提出适用于工程落地的多维对策，强调加密机制应嵌入系统架构设计之中，成为网络安全的内生能力。

关键词：加密传输；TLS 1.3；密钥管理；物联网安全

DOI：10.69979/3041-0673.26.02.097

引言

近些年来，随着计算机时代的迅速发展，网络通讯的应用也越来越广泛，随之而来是大量信息安全问题。在没有安全加密的环境下，信息泄露的可能性非常大，恶意程序会不断侵入用户隐私领域，威胁用户的信息安全，这会成为一个不可忽视的安全隐患，所以网络安全问题就显得尤为重要。数据加密技术也成为大众研究及关注的热点，是网络信息安全的核心技术[1]。在此背景下，构建安全、高效的加密传输机制已成为网络通信体系的关键命题。相较于传统静态防护，加密机制能够在传输链路中实现动态防御与信任确认，为数据构筑实时的保护屏障。

1 加密传输机制的基本原理与分类

1.1 对称加密与非对称加密原理

加密传输的要义在于把可读信息稳定地转化为受控密文，使中途窃听只见“噪声”而难以复原。对称加密以同一把密钥完成加密与解密，典型代表为高级加密标准（AES，Advanced Encryption Standard）与国家商用密码算法（SM4）。非对称加密以成对密钥运作，常见的有椭圆曲线密码（ECC，Elliptic Curve Cryptography）与基于大整数难题的 RSA。现实网络更倚重“混合加密”：握手阶段借助非对称机制完成实体认证与会话密钥协商（如基于椭圆曲线的临时密钥交换 ECDHE），数据阶段交给对称算法执行高吞吐加密与完整性校验（如 AES-GCM、SM4-GCM）[2]。关键瓶颈并不在公式，而在密钥生命周期——生成的熵源是否可靠、分发链路是否可审计、存储介质是否抗侧信道、轮换与撤销是否自动化。为降低传输开销与延迟，宜把“对称负责跑量、非对称负责立信”作为工程准则，并配合短周期会话密钥与前向保密策略收敛风险。面向量子计算的压力不容忽视，过渡期可采用传统密钥交换叠加抗量子机制的“双轨”方案，既维持兼容性，也为未来的算法切换留出窗口[3]。

1.2 加密传输协议综述

协议把密码学原理织入可互操作的报文与状态机，决定握手往返、算法协商与异常处置的具体细节。传输层安全协议（TLS，Transport Layer Security）在网络服务中占据主导，最新版 TLS 1.3 压缩了握手流程，默认启用前向保密与精简套件，显著缩短建联时延；零往返数据虽有性能优势，却引入重放风险，适合只读或幂等场景。互联网协议安全（IPSec，Internet Protocol Security）位于网络层，以封装安全载荷 ESP 和鉴别头 AH 构造隧道或传输模式，依托互联网密钥交换第二版（IKEv2）建立安全关联，常用于分支互联与跨域专线。快速 UDP 互联网连接协议（QUIC，Quick UDP Internet Connections）把加密与传输合而为一，具备连接迁移与精细拥塞控制的能力，作为 HTTP/3 的基座在弱网环境表现稳健，同时对中间设备的可观测提出新要求[4]。数据报传输层安全协议（DTLS，Datagram TLS）以无连接语义服务实时与物联网业务，处理乱序与丢包的能力更强。选择标准可围绕三项指标展开：端到端保护边界是否清晰、算法与参数是否具备敏捷切换、部署对现有网络是否友好；不同行业据此在 TLS、IPSec、QUIC、DTLS 之间形成错位应用。

1.3 加密机制与网络架构的耦合关系

加密是与架构共振的系统能力。沿 OSI 各层布置加

密形成多种取舍：应用层的超文本安全（HTTPS，基于 TLS）靠近业务语义，便于细粒度访问控制与审计；传输层的双向传输层安全（mTLS）在服务网格中承载“东西向”流量的身份与加密；网络层的 IPSec 适合跨域隧道与多站点拓扑；数据中心内还可在链路层引入介质访问控制安全（MACsec）抑制物理侧风险。工程上常见“TLS 终止”放置在负载均衡或反向代理，若其后段为明文，等于在边界创造一个明文回落区，宜配套最小明文域、细粒度分段与零信任访问策略化解隐患[5]。密钥与证书管理决定安全上限：企业级公钥基础设施（PKI）需要自动证书管理环境（ACME，Automatic Certificate Management Environment）驱动签发与轮换，私钥落地硬件安全模块（HSM）提升抗篡改能力，撤销应结合证书吊销列表（CRL）与在线状态协议（OCSP）避免“失效悬空”。密文广布会削弱传统流量可视性，可在端侧引入可验证日志与最小化元数据探针保持运维韧性。面对国密与国际算法的“双栈”现实，建议以“加密域”为架构边界，预设算法协商优先级与兼容矩阵，并把硬件加速与可编程网卡纳入容量规划，使性能与安全在同一设计面内达成平衡。

2 加密传输机制在典型网络安全场景中的应用分析

2.1 Web 应用安全中的加密部署实践

在高并发与强合规并行的互联网场景中，传输加密的核心不在于“启用证书”这一表面动作，而在于建立稳定、高效、可审计的安全传输体系。当前主流网站与 API 接口已普遍升级至传输层安全协议 1.3 版（TLS 1.3），其缩短握手轮次并强化前向保密机制，在性能与安全之间实现较优平衡。但零往返数据模式虽能提升访问速度，却更适用于读取类业务，对写入或交易类操作则应谨慎关闭，以防遭遇重放攻击。2024 年 Cloudflare 报告显示，全球 HTTP/3 流量占比超过三成，而中国大陆仍有过半流量停留在 HTTP/1.x，反映出存量系统升级滞后与加密策略落地的不均衡现象。

在部署实践中，证书根升级与兼容性验证常引发“链式影响”。以 2024 年支付行业的根证书更新为例，平台要求合作方全面检查 TLS/SSL 库与信任根的匹配，以避免握手异常或降级风险。这一过程实质上是一种供应链层面的安全治理，需要将证书轮换、撤销检查与在线状态验证（OCSP）纳入统一变更计划。综合来看，稳健的加密部署应坚持三个导向：压缩明文区段、强化自动化轮换与保持透明可观测性。企业可在边界层启用双向认证（mTLS）并配合自动证书管理环境（ACME）实现短周期签发，同时设置兼容池平稳淘汰旧版本终端。在 IPv6 高速普及背景下，握手延迟与路径不对称问题亦需纳入容量规划，以保障全链路加密传输的连续性与可靠性。

2.2 物联网（IoT）中的轻量级加密传输机制

物联网的核心挑战源于“安全负载与硬件资源”的失衡。终端设备运算能力与电源受限，却需承担身份认证、密钥协商和报文加密等任务。在此背景下，数据报传输层安全协议（DTLS）凭借无连接和抗乱序特性成为主流方案，而在国密体系下，采用双证书的传输层密码协议（TLCP）及 SM 算法家族的嵌入式适配也在加速落地。近年来，开源与商用框架推出多种轻量化实现，可在数十至数百 KB 的内存预算中完成握手与加密通信，使低功耗设备得以在有限资源下维持安全态。

从产业数据看，截至 2024 年底，中国蜂窝物联网连接用户数已达 26.56 亿，安全接入与密钥管理呈爆发式增长，传统的人工登记与长期凭据方式已无法满足可追溯与自动化要求。硬件信任根的引入成为主流趋势，独立安全芯片与可信存储模块正在成为模组的标准配置，为设备级身份提供了稳定载体。针对实际部署，可采用“网关前移”的思路：由网关统一完成证书验证与密钥下发，终端以预共享密钥或椭圆曲线协商快速建立会话。此结构既减少端侧计算负担，又能集中管控安全策略。对于高能耗敏感型设备，可在采集周期边界执行握手，并结合会话恢复机制延长续航。由此构建的“安全域—接入域—应用域”三层体系，使物联网加密传输在能耗、可管控性与长期可维护性之间达成平衡。

2.3 数据隐私保护与法律合规背景下的传输加密策略

数据传输加密在隐私与合规治理中承担核心角色。根据《中华人民共和国个人信息保护法》及相关配套标准，个人信息处理者需采取必要技术措施确保数据传输安全，其中“安全通道”与“加密机制”被明确列为必备要求。国家标准《数据安全技术 政务数据处理安全要求》进一步指出，所有政务及政企系统在传输环节必须采用加密通道以维护数据机密性，这已成为系统验收的重要指标。在数据跨境传输环节，监管部门提出“安全评估—认证—标准合同”三路径机制，要求企业在出境链路中配置具备前向保密的加密通道并实现可持续合规运营。

在技术策略上，应以“数据分级”为核心。敏感信

息需绑定强认证、强加密和高频密钥轮换策略；一般数据则可采用标准加密强度并延长会话周期。对跨境传输接口，应建立基于硬件安全模块的端到端通道，并利用在线证书状态协议（OCSP）与短期证书机制保持动态信任。双栈架构系统可配置国密与国际算法的灰度切换清单，确保兼容与安全兼得。若系统处于网络安全等级保护 2.0 三级及以上级别，则应在通信层部署密码保障完整性、机密性与可审计性机制，使传输加密真正成为支撑合规治理的技术基石。

2.4 边缘计算与分布式系统中的加密通信挑战

边缘计算强调低延迟与实时响应，而加密传输机制的引入既是保障安全的必需，也带来了额外性能代价。在公有云与边缘平台架构中，传输加密已成为默认配置。例如，云专线与边缘节点服务普遍内置加密通道，以防公网暴露，并在指标体系中将端到端时延控制在 20 毫秒以内，从而在性能预算中留出加密开销的空间。随着协议栈的“内化趋势”增强，传统网络监测依赖的明文数据已逐步消失，运维手段正在向端侧可验证日志与链路指标转型。

现实中，融合内容分发、物联接入与安全加速的边缘体系，普遍将加密、连接迁移与就近计算集成为一体。然而，证书的规模化管理与多租户环境下的密钥隔离问题依旧突出。优化的方向主要包括三方面：其一，构建以“工作负载身份”为核心的动态信任体系，实现短期证书自动签发与撤销，避免人工分发风险；其二，对 HTTP/3 非幂等请求关闭零往返数据，防止边缘重放导致的数据紊乱；其三，针对 IPv6 与移动网络比例攀升的现实，在边缘节点侧完成握手并复用密钥，以减少跨域延迟。整体而言，边缘加密通信的目标不在“更快”，而在“更稳”——以可验证信任链和最小明文域为前提，实现安全与性能的动态平衡。

表 1 典型网络安全场景中的加密传输关键指标

序号	应用场景	关键指标/事件	数据值/描述	年份	来源与说明
1	Web 加密传输协议升级	全球 HTTP/3（基于 QUIC）流量占比	>30%	2024 年	Cloudflare 全球流量报告
2	Web 协议版本使用结构	中国大陆 HTTP/1.x 流量占比	>50%	2024 年	同上
3	网络基础条件	活跃 IPv6 用户总数	7.94 亿（移动流量占比 64.56%）	2024 年 5 月	国家市场监管总局 IPv6 专项通报
4	网络带宽需求	移动互联网累计流量	3066 亿 GB	2024 年 11 月	工业和信息化部官方统计报告
5	物联网终端侧传输能力	蜂窝物联网（IoT）用户数量	26.56 亿户	2024 年底	工信部及各省通信管理局数据汇总
6	边缘计算节点通信时延控制	边缘节点端到端通信平均时延指标	<20 毫秒	2024 年	阿里云边缘计算产品白皮书
7	数据合规与隐私加密要求	政务数据传输强制加密策略	“应部署安全通道并采用数据加密”	2024 年	国家密码管理局 TC260 官网标准解读
8	加密基础设施运维风险	支付平台根证书升级兼容性校验要求	明确检查 TLS/SSL 库与信任链	2024 年	支付宝开放平台根证书公告

注：表中数据采集时间范围为 2022 年至 2024 年，均来源于公开渠道或国家主管部门发布材料，确保客观真实。

3 结语

加密传输机制在保障网络通信安全中发挥基础性作用，其架构嵌入深度与协同机制的合理性直接影响系统稳健性。本文梳理了主流加密协议的适配模式，分析了 Web、物联网、数据合规与边缘场景下的部署难点，指出密钥管理、性能开销与协议兼容是当前需优先解决的问题。面向未来，建议构建“最小明文域+自动密钥生命周期+多算法兼容”三位一体的设计框架，同时关注量子抗性与软硬件协同优化，推动加密机制成为网络安全架构中的稳定支点。

参考文献

[1]马艳娥,李瑞金.基于 DFT-S-OFDM 的网络信息安全加密传输仿真[J].计算机仿真,2022,39(1):358-361+393.
[2]方芳,李广华,汪冬辉,等.变电站内传输 IEC 62351 通信密钥的加密传输方法[J].中国电力,2019,52(10):26-30+122.
[3]汤陈燕.基于属性加密的通信网络信息安全加密传输系统[J].常州工学院学报,2025,38(3):40-45.
[4]王尚.基于改进 AES 算法的网络隐私信息安全加密传输方法研究[J].软件,2025,46(8):167-169.
[5]陈赫.同步脉冲数字通信加密传输系统在网络安全中的应用[J].长治学院学报,2023,40(5):4-7.