基于光通信技术的物联网数据加密技术分析

赵 娜
内蒙古电力集团锡林郭勒供电分公司 内蒙古 锡林浩特 026000

摘 要：本文旨在系统性地分析基于光通信技术的物联网数据加密体系。首先，深入剖析了物联网数据安全的核心需求与传统加密范式的瓶颈；其次，详细阐述了光纤通信与自由空间光通信（FSO）两大主流光通信模式的技术原理及其为数据安全提供的独特物理基础；在此基础上，重点探讨了面向光通信物联网的多层次加密策略，包括物理层安全增强、传统密码算法的适应性优化以及前沿的量子密钥分发（QKD）技术的融合应用；最后，对当前技术面临的挑战与未来发展趋势进行了展望。研究表明，构建一个深度融合光通信物理特性的“物理-逻辑”协同加密体系，是实现物联网数据端到端、高可靠、抗量子攻击安全传输的根本路径。

关键词：光通信；物联网；数据加密；物理层安全；量子密钥分发

引言

物联网通过全面互联实现信息感知与智能处理，但其广泛连接也大幅扩展了攻击面，使数据安全成为发展瓶颈。物联网数据在全生命周期中面临窃听、篡改、伪造等多重威胁，尤其在资源受限的边缘设备与云端间传输时，保障机密性、完整性与可用性尤为关键。传统安全方案依赖TLS/SSL、AES等密码协议，计算与能耗开销大，难以适配低功耗终端；且基于计算复杂性的经典密码体系在量子计算威胁下面临根本性风险。在此背景下，光通信技术凭借高方向性、窄波束和抗非侵入式窃听等物理特性，为构建物理层安全防线提供了新路径。将加密技术与光通信深度融合，不仅能提升整体安全性，还可减轻上层协议负担，助力打造高效、绿色、安全的物联网通信体系。本文将围绕该融合策略展开系统探讨。

1 物联网数据安全需求与传统加密范式的挑战

1.1 物联网数据安全的独特需求

物联网数据安全的核心目标可概括为“CIA”三元组，即机密性（Confidentiality）、完整性（Integrity）和可用性（Availability），但在物联网场景下，这些目标被赋予了更具体的内涵。机密性要求防止未经授权的实体访问敏感数据，例如，智能家居中的用户行为数据、工业物联网中的生产参数等。完整性则确保数据在传输过程中未被恶意篡改或意外损坏，这对于远程控制指令的准确执行至关重要。可用性强调授权用户能够在需要时可靠地访问数据和服务，抵御拒绝服务（DoS）等攻击[1]。除此之外，物联网还特别强调轻量化和低功耗，因为大量终端设备（如传感器节点）通常由电池供电，且处理器性能有限，无法承担复杂的加密运算。同时，可扩展性也是一个关键考量，安全机制必须能够适应动态变化的、规模庞大的设备网络。

1.2 传统加密范式在物联网中的应用瓶颈

目前，物联网安全主要依赖于两种加密范式：对称加密和非对称加密。对称加密（如AES）因其加解密速度快、效率高，常用于保障数据传输的机密性。然而，其最大的挑战在于密钥管理。在一个拥有成千上万设备的物联网网络中，如何安全、高效地分发、更新和撤销对称密钥，是一个极其复杂的系统工程。非对称加密（如RSA、ECC）通过公私钥对巧妙地解决了密钥分发问题，并可用于数字签名以保证数据完整性。但其计算复杂度远高于对称加密，对于资源受限的物联网设备而言，执行一次非对称加密操作可能消耗大量的时间和能量，严重影响设备的续航能力和响应速度。更为严峻的挑战来自于量子计算的潜在威胁。Shor算法等量子算法理论上可以在多项式时间内破解当前广泛使用的RSA和ECC等公钥密码体制。虽然实用化的大规模量子计算机尚未问世，但“先窃取后解密”的攻击模式意味着，今天传输的、用经典公钥加密的敏感数据，未来一旦量子计算机成熟，就可能被解密。因此，寻求能够抵御量子攻击的新型安全机制，已成为物联网安全领域的战略制高点。

2 光通信技术：为物联网安全提供物理基石

2.1 光纤通信的安全特性

光纤通信是现代信息社会的骨干，其安全优势主要体现在以下几个方面。首先，信号封闭性强。光信号被约束在纤芯内部，通过全反射原理进行传输，外部环境几乎无法直接截获光信号。任何试图通过弯曲光纤来窃取光信号的行为（即“搭线窃听”）都会导致明显的光功率损耗，极易被通信双方通过光时域反射仪（OTDR）

等监测手段发现。其次，无电磁辐射。光纤本身是非金属介质，传输过程中不产生电磁辐射，这使得基于电磁信号侦测的传统窃听手段完全失效，极大地提升了系统的电磁兼容性和隐蔽性。最后，高带宽与低损耗。单根光纤即可承载Tbps级别的数据流量，且传输损耗极低，这为在物理层实施复杂的编码、调制和加密操作提供了充足的带宽资源，而不会显著影响有效数据的传输速率。

2.2 自由空间光通信（FSO）的安全特性

自由空间光通信利用激光在大气中进行点对点的数据传输，其安全特性同样突出。最核心的优势在于其极高的方向性和窄波束。激光束的发散角非常小，通常只有毫弧度级别，这意味着信号能量高度集中在一个非常狭窄的空间通道内。要成功窃听，攻击者必须精确地将接收器放置在这个狭窄的光束路径上，这在物理上极具挑战性，尤其是在动态变化的环境中。相比之下，射频信号以球面波形式向四周扩散，窃听者只需在信号覆盖范围内即可轻松截获[2]。此外，FSO链路具有天然的视距（LoS）限制，一旦光路被遮挡，通信即告中断，这使得非法接入变得异常困难。这些物理特性共同构成了FSO链路强大的物理层安全保障。

3 面向光通信物联网的多层次数据加密策略

为了充分利用光通信的物理安全优势，并克服传统加密范式的不足，有必要构建一个多层次、立体化的数据加密策略体系，该体系应涵盖物理层、链路层乃至应用层，形成纵深防御。

3.1 物理层安全增强技术的具体实现

物理层安全旨在利用信道的物理特性（如噪声、衰落、多径效应）来实现信息的保密传输，其安全性不依赖于计算复杂度假设。在光通信物联网中，可以采用多种技术来增强物理层安全。

3.1.1 基于信道状态信息（CSI）的保密编码

通过人工制造信道扰动，在合法收发端之间共享一个秘密的、快速变化的信道状态信息（CSI），并利用此信息对数据进行预编码或加扰。具体而言，发送端可以根据实时测量的信道冲激响应，设计一个预均衡滤波器，使得经过信道后的信号在接收端恰好恢复为原始信号，而对窃听者而言，由于其信道响应不同，接收到的将是严重失真的信号。这种方法在多输入多输出（MIMO）光通信系统中尤为有效，可以通过空间维度进一步增加安全裕度。其核心在于，合法信道与窃听信道的统计独立性，使得窃听者无法获得用于解码的有效CSI。

3.1.2 光学混沌加密系统

另一种方法是光学混沌加密，利用半导体激光器等器件产生的宽带、类噪声的混沌光信号作为载波或密钥流，对待传数据进行掩蔽。混沌系统对初始条件极度敏感，任何微小的扰动都会导致输出的巨大差异。在典型的外腔反馈半导体激光器混沌系统中，通过调节反馈强度、延迟时间和偏置电流等参数，可以产生带宽高达数十GHz的混沌信号。发送端将待传数据与混沌信号进行异或或相位调制，接收端则利用一个与发送端参数完全同步的混沌激光器作为本地振荡器，通过相关解调或同步解密的方式恢复出原始数据[3]。由于混沌系统的非线性和对参数的极端敏感性，非授权方即使知道系统模型，也几乎不可能重构出原始混沌信号，从而实现高安全性的物理层加密。近年来，基于光电振荡器（OEO）和集成光子芯片的混沌源因其稳定性好、体积小，成为研究热点。

3.2 传统密码算法的适应性优化路径

尽管物理层安全提供了强大的第一道防线，但为了满足端到端的安全需求，上层的逻辑加密仍然是必不可少的。针对物联网设备的资源受限特性，必须对传统密码算法进行适应性优化。

3.2.1 轻量级密码算法的选型与部署

一方面，可以采用轻量级密码算法，如PRESENT、Speck、ChaCha20等，这些算法在设计之初就充分考虑了硬件面积、功耗和计算速度等因素，非常适合在嵌入式设备上运行。例如，PRESENT算法是一种超轻量级分组密码，其S盒和P层设计极其简洁，可以在极小的硬件面积（约1570门电路）上实现，加解密一轮仅需几个时钟周期。ChaCha20则是一种流密码，其核心是ARX（Add-Rotate-XOR）操作，无需查表，对缓存攻击免疫，且在软件实现上速度极快。在部署时，应根据设备的具体资源（如RAM、ROM、CPU主频）和安全需求（如所需密钥长度、认证模式）进行精细化选型。

3.2.2 边缘计算辅助的安全卸载机制

另一方面，可以利用光通信的高带宽特性，将部分加密计算任务卸载到网络边缘或云端。例如，终端设备仅负责生成原始数据和简单的完整性校验（如CRC或HMAC-SHA256），而复杂的加密操作则在靠近终端的边缘计算节点上完成。这种“终端-边缘”协同的安全架构，既能保证数据在广域网传输过程中的机密性，又能最大限度地节省终端能耗。该机制的实现依赖于高效的边缘-终端安全协议，确保卸载过程本身的安全，例如，通过预共享的轻量级密钥建立安全通道，再在该通道内传输待加密的明文数据。

3.3 量子密钥分发（QKD）的融合应用与协议演进

量子密钥分发（QKD）是目前唯一被严格证明具有

信息论安全性的密钥分发技术。它利用量子力学的基本原理——海森堡不确定性原理和量子不可克隆定理，使得任何对量子信道的窃听行为都会不可避免地引入可被检测的扰动。

3.3.1 共纤传输与波分复用技术

将QKD与光通信技术深度融合，是构建未来抗量子攻击物联网安全体系的终极方案。在光纤网络中，QKD系统可以与经典数据信道共纤传输，通过波分复用（WMD）技术，将量子信号（通常在1310nm或1550nm波段）和经典信号（如1550nm C+L波段）复用在同一根光纤中，实现密钥分发与数据传输的协同。为了避免经典信号的拉曼散射噪声对单光子级别的量子信号造成干扰，通常需要在时间上或频率上进行严格的隔离[4]。例如，采用时间门控技术，只在经典信号静默的特定时间窗口内发送量子信号。

3.3.2 双场QKD（TF-QKD）及其长距离优势

近年来，双场QKD（TF-QKD）等新型协议的提出，更是将无中继QKD的传输距离突破至千公里量级。TF-QKD的核心思想是让两个远端用户（Alice和Bob）各自向一个位于中间的、不受信任的测量节点（Charlie）发送相位编码的弱相干脉冲。Charlie对这两个脉冲进行干涉测量，并将结果公开。Alice和Bob根据Charlie的结果和自己的发送信息，通过后处理就能生成共享密钥。由于密钥率主要取决于Charlie到Alice/Bob的单程损耗，而非传统QKD的双程损耗，因此TF-QKD的密钥率随距离的衰减大大减缓。这一突破为构建覆盖全国乃至全球的量子安全物联网奠定了坚实基础。通过QKD生成的、真正随机且无条件安全的密钥，可以用于一次一密（OTP）加密或定期更新上层对称加密算法的会话密钥，从而为物联网数据提供最高级别的安全保障。

4 挑战与未来展望

尽管基于光通信的物联网数据加密技术前景广阔，其大规模应用仍面临多重挑战。一是成本与集成度问题：高性能激光器、单光子探测器等核心器件价格高、体积大，难以嵌入小型终端，亟需发展低成本、低功耗的硅光子集成芯片。二是自由空间光通信（FSO）受大气湍流、雨雾等环境干扰严重，需借助自适应光学、MIMO等技术提升链路鲁棒性。三是缺乏统一标准，不同厂商在接口、协议和密钥管理上互不兼容，阻碍组网与互操作，亟需加快制定国际国内技术规范。展望未来，随着光子集成电路、人工智能与量子信息技术进步，该领域将迈向智能化、集成化与普适化：AI可动态优化加密策略，量子互联网则有望使QKD服务如宽带接入般普及，最终为万物互联构建坚实安全基石。

5 结语

物联网的蓬勃发展对数据安全提出了更高、更全面的要求。传统基于计算复杂性的加密范式在资源受限和量子威胁的双重压力下面临严峻挑战。光通信技术，凭借其固有的物理层安全特性，为构建下一代高安全物联网通信体系提供了革命性的解决方案。本文通过系统分析，论证了将物理层安全增强、轻量级密码算法优化与前沿的量子密钥分发技术相结合，形成多层次、协同化的加密策略，是应对当前及未来物联网安全挑战的有效路径。尽管在成本、环境适应性和标准化等方面仍存在障碍，但随着相关技术的不断成熟，基于光通信的物联网数据加密必将从理论走向实践，为数字经济时代的万物智联保驾护航。

参考文献

[1]陈伟东,张驰.基于光通信技术的物联网数据加密技术分析[J].光源与照明,2023,(11):78-80.

[2]陈宏君,蒋建军.基于光通信技术的物联网数据加密技术研究[J].激光杂志,2021,42(05):116-119.

[3]赵振江.试论光通信技术在物联网中的应用[J].中国信息化,2023,(01):73-74+70.

[4]徐梓元.光通信技术在物联网中的应用[J].数字通信世界,2021,(08):181-182.