新型智算中心以太网物理层安全(PHYSec)架构白皮书

（2024 年）

发布单位：中移智库

编制单位：中国移动通信研究院

前　言

随着 AI 大模型对算力的需求呈现指数级增长，具有大规模算力的智算中心正在全球范围内进行大规模建设与部署。智算中心通过以太网传输涉及到企业安全生产的 AI 模型参数以及敏感数据，其在传输的过程中面临着泄露的风险，具有极高的安全诉求。本白皮书面向未来智算中心规模建设和 AI 大模型发展及部署需求，提出以太网物理层安全（PHYSec）体系架构及技术方案，解决 RDMASec、MACSec 等现有安全方案在智算中心场景下面临的安全漏洞与性能瓶颈问题，为智算中心的网络保驾护航。

本白皮书旨在提出中国移动及产业合作伙伴对以太网物理层安全 PHYSec 技术的愿景、架构设计和能力要求。希望能够为产业在规划设计以太网物理层安全相关技术、产品和解决方案时提供参考和指引。

本白皮书由**中国移动通信有限公司研究院**主编，**腾讯云、清华大学、东南大学、华为技术有限公司、中兴通讯有限公司、博通公司、默升科技（上海）有限公司、上海橙科微电子科技有限公司、烽火通信科技股份有限公司、新华三技术有限公司、锐捷网络股份有限公司、英特尔（中国）有限公司、苏州盛科通信股份有限公司、杭州云合智网技术有限公司、深圳市楠菲微电子有限公司、篆芯半导体（南京）有限公司、苏州旭创科技有限公司、索尔思光电、苏州卓昱光子科技有限公司、武汉光迅科技股份有限公司、迈普通信技术股份有限公司(中国电子-迈普通信)、思博伦通信科技（北京有限公司）、是德科技**

（中国）有限公司、唯亚威通信技术（北京）有限公司、珠海星云智联科技有限公司、中科驭数（北京）科技有限公司、上海云脉芯联科技公司、深圳云豹智能有限公司联合编撰。

目 录

1. 技术背景与需求

随着AI大模型的迭代速度呈指数级增长，AIGC（AI-Generated Content）等应用预计将在全球范围内产生数万亿美元的经济价值。作为 AI 技术发展的基础设施底座，智算中心也逐渐在全球范围内大规模建设和部署。传统数据中心网络存在时延及吞吐受限、负载分担不均、拥塞控制精度低、安全保护机制难部署等问题。针对这些问题，全调度以太网（GSE）在兼容现有以太生态前提下，提出基于虚拟容器的调度转发，逐包的动态负载均衡机制，以及精细流控反压等创新技术,获得业内广泛认可，并在中国通信标准化协会（CCSA）TC3 工作组推动《全调度以太网总体技术要求》和《智能计算中心网络协议能力总体技术要求》立项，为智算中心提供开放标准的网络解决方案。

当前，智算中心以大量数据为资源，利用强大算力驱动AI大模型对数据进行深度加工，产生各种智慧计算能力，以云服务形式提供给组织及个人。在此过程中，涉及大量数据资源在入算、算内和算间网络场景的处理和传递。这些数据已成为企业十分重要的商业资产，一旦被窃听攻击或泄露，将产生难以估计的经济损失，因此如何保障数据安全将是智算中心发展的核心问题。对于入算场景，互联网或者用户设备实时上传的敏感或隐私数据须经过广域网或城域网等入算网络到达智算中心用于AI大模型训练，这些数据在传输过程中存在泄露的风险。对于算内场景，AI 训练与推理过程中使用到的模型、参数以及用户数据需要在计算节点间频繁传递，同样存在泄露或被窃

听的风险。对于算间场景，用于传输智算中心间算力资源的高速互联光纤链路以及相关设施暴露在物理环境中，存在被攻击窃听的风险。综上所述，用户数据在入算上传、算内传递以及算间传输这三个场景都存在安全加密的需求。

上述智算中心三个网络场景的底层承载网络主流技术是以太网，为此须对以太网提供安全认证、密钥管理以及数据加解密能力，以应对日益严峻的安全挑战。考虑到智算中心场景所承载的 AI 与 HPC 业务对时延、带宽等网络性能的极致追求，智算中心以太网安全技术需要具备如下核心能力：

一是存量设备和芯片的兼容能力。为了使加密流量可以达到线速，加密模块会在芯片中硬化实现。以太网已部署的存量设备可能存在硬件芯片无法更换的情况，因此以太网数据加密技术需要利旧现有网络设备，具备向下兼容能力。

二是低时延、低开销的数据加解密能力。随着 AIGC 等应用的发展，对海量算力芯片间高吞吐、低时延数据传输的需求更为迫切。因此在对以太网链路提供安全加密的同时，也需要关注数据加解密带来的时延与开销。

三是以太帧和管控协议的全加密能力。以太网链路会发送一些特殊的协议帧，如基于优先级的流量控制帧等。这些特殊的协议帧无法被传统的网络安全机制所保护。针对隐私保护要求高的场景，也需要对以太帧进行全加密保护，包括加密帧头部以及掩盖帧发送频率、帧长等流量特征，以防止流量分析攻击。

四是简单高效的认证和密钥管理机制。认证和密钥管理涉及大量的安全会话，需要消耗计算节点的 CPU 以及网卡内存资源，影响计算节点的算效。因此需要简单高效的认证和密钥管理机制降低安全会话数量。

现有安全加密机制可以提供不同网络层级的数据安全防护，但是无法同时满足上述的关键能力需求。在传统数据中心网络中，RDMA 技术得到了广泛应用。部分标准组织提出在 RDMA 的网络层实现端到端的数据加密机制（RDMASec）[1]。业界已有厂家发布基于 IPSec 的改进方案，来尝试满足智算中心的安全需求[2]。此外，基于 IEEE 802.1AE 标准的 MACSec 可以为以太网设备之间提供数据链路层逐帧的安全加密通信，在园区办公场景得到较广泛应用[3]。然而 RDMAsec 及 MACSec 应用于智算中心场景时仍存在如下问题：1）难以兼容全部存量设备。业界现有芯片硬化的 RDMASec 及 MACSec 方案，需要在 PHY 芯片中进行比特流到包或帧的背靠背转换，将引入额外的实现复杂度与转换时延，也需要对设备硬件进行替换。2）引入封装开销。尤其是对短帧场景，会明显挤占业务带宽，影响 AI 业务算效。3）暴露以太帧头部信息，且无法完全掩盖报文长度、发包频率等流量特征，易被利用进行流量分析攻击[3,4]。无法保护基于优先级的流量控制帧（PFC）或 pause 帧等以太帧。4）认证机制仅限于服务器、交换机等网络设备，无法对光模块进行认证；密钥管理机制安全复杂度高，需要消耗大量的 CPU 资源及网卡内存资源来维护节点间建立的安全会话，影响算效。

针对上述智算中心安全需求以及 RDMASec、MACSec 存在的问题，中国移动联合业界合作伙伴提出以太网物理层安全（PHYSec）技术架构，通过在以太网物理层对比特流进行加解密来保护所有上层协议，通过掩盖流量特征，解决流量分析攻击带来的安全威胁，同时实现低时延、低开销、协议透明的数据加解密。本白皮书的发布有望推动 PHYSec 技术的标准共识、技术成熟与商用落地，支撑智算中心的安全建设与快速发展。

2. 以太网物理层安全技术架构

2.1 技术愿景

物理层加密的概念早在 1989 年就在标准 ISO 7498-2 中有所提及，但基于物理层加密的以太网技术还未曾出现[5]。现有网络安全技术的加密层次及密文保护范围如图 2-1 所示。从各层次网络安全技术的演进过程可以看到，越往上层的安全机制越灵活，而越往下层的加密机制可以提供更大的保护范围，且更易于与硬件结合。RDMASec 是介于 IPSec 与 TLS 之间的改良技术，但是引入的时延与开销难以满足智算中心的安全需求。以太网物理层处于网络协议栈的更低层次，将安全加密与以太网物理层特性相融合来构建全新的以太网安全机制，有望解决上述 RDMASec 及 MACSec 所不能解决的问题。同时，物理层的加密更便于实现低时延、低开销、高吞吐、高安全的数据加密，满足智算中心场景对安全技术的要求。

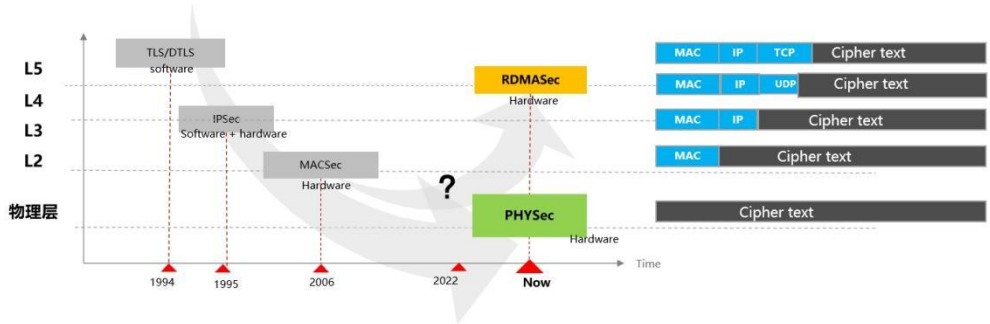


图 2-1 安全机制演进趋势

本白皮书提出将物理层加密的理念与以太网物理层技术相融合构建以太网物理层安全技术—PHYSec，以实现低时延、高吞吐、高安全、低开销和协议透明等特性的安全加密机制，满足数据链路层及所

有上层协议的信息防护。如前所述，PHYSec 是一种工作在以太网物理层的安全加密技术，对物理层的比特流进行加解密。所有以太帧、所有的管控协议以及帧间空隙均被物理层统一编码，可以被 PHYSec 有效保护，从而掩盖流量特征，具有极高的安全性。如图 2-2 所示，为明文数据、MACSec 加密以及 PHYSec 加密三种传输方式的示例。PHYSec 可以加密包括以太帧头部在内的全部用户信息，掩盖帧频率以及帧长度等流量特征，解决了 RDMASec 和 MACSec 难以防护流量分析攻击的问题。与此同时，PHYSec 的加密对象是物理层的比特流，对上层业务和协议透明，构建加密对象时可以不受限于报文，与业务转发逻辑和协议处理无关。在构造合适的加密对象之后，PHYSec 利用物理层原生 OAM 码块承载加解密所必需的安全参数，具有低开销的优势。

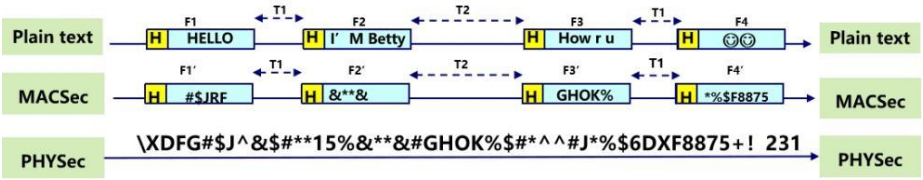


图 2-2 明文传输、MACSec 加密以及 PHYSec 加密示例

2.2 设计原则

2.2.1 兼容性原则

PHYSec 技术可以在以太网物理层 PHY 的不同位置实现。在 PHY 单元实现，要求兼容 IEEE802.3 标准，不影响标准规范的功能与协议；在 PMD 模块实施，要求兼容 PMD 模块已有标准及架构，不影响标准规范的功能与协议。

2.2.2 互通性原则

PHYSec 原则上可支持链路级和通道级的技术方案，类似 MACSec（802.1AEbw-2013 for port，802.1AEcg-2017 for channel），实施部署载体可以是 PHY 接口，也可是光模块或其他载体。同一层次方案，要求技术与协议一致，满足互联互通要求。协议承载方案，要求少占用或不占用业务带宽。

2.2.3 一致性原则

对于 IEEE802.3 规范的以太网 100G/200G/400G/800G/1.6T 接口，虽然 PHY 各逻辑子层技术方案有区别，但 PHYSec 原则上要求采用一套解决方案和协议。协议的承载方式可以根据 PHY 逻辑子层的要求变化，但要求遵循前述兼容性原则与互通性原则等设计原则。

PHYSec 作为网络安全技术，技术逻辑同 MACSec（解决如何将密码学算法应用于数据链路层的问题）、IPSec（解决如何将密码学算法应用于网络层的问题），解决如何将密码学算法应用于网络物理层的问题。

2.3 技术体系与关键机制

本白皮书提出的 PHYSec 技术体系架构主要包括三个层次：认证通道层、密钥管理层和数据加解密层，如图 2-3 所示。

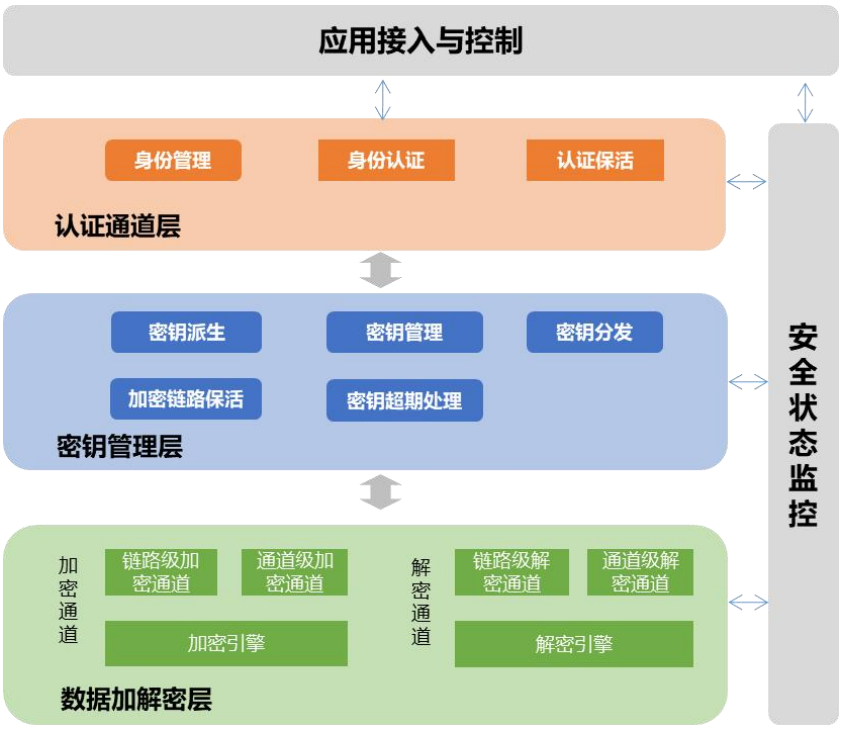


图 2-3 PHYSec 技术体系架构

- 认证通道层：负责对设备及光模块的身份认证与身份管理，确保相互通信的两端是合法的以太网设备。认证通过后，需要对认证通道进行保活。认证通道层的功能主要由平台业务软件实现。
- 密钥管理层：负责运行过程中密钥的派生与管理、密钥定期更新分发以及密钥超期等异常状态处理。密钥分发完成后，还需要对使用该密钥的加密链路进行保活。密钥管理层的功能主要由平台业务软件实现。
- 数据加解密层：分为链路级加解密与通道级加解密。基于系统下发的密钥，分别通过加密引擎和解密引擎对信号进行加密和解密操作。数据加解密层可以在光模块或 PHY 芯片实现。

PHYSec 的认证通道层、密钥管理层以及数据加解密层都可以与更上层的管控系统进行交互，从而对安全状态进行监控，如查询安全身份是否过期、密钥超期上报、以及加解密失败告警等安全管控操作。

应用接入与控制平台也可以实时对认证通道层的安全身份进行管理与控制。

PHYSec 的整体流程包含加密能力查询及初始化、身份认证、密钥协商与管理以及数据加解密，如图 2-4 所示。

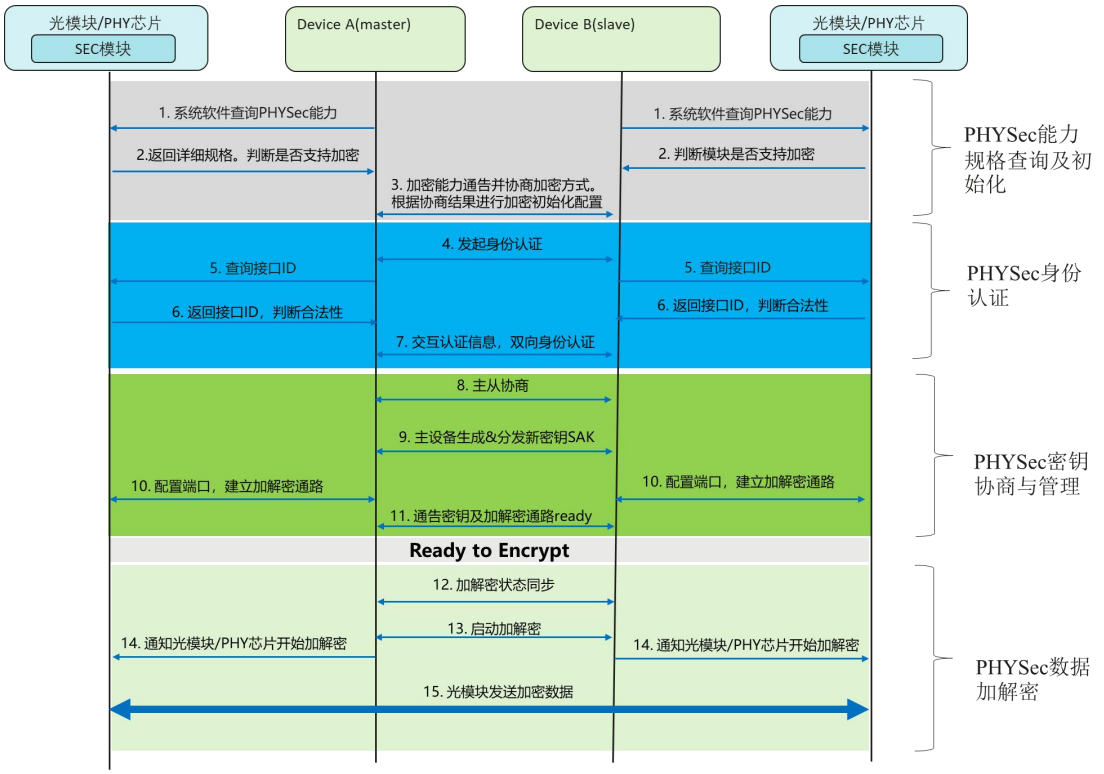


图 2-4 PHYSec 整体技术流程

- 加密能力查询及初始化：在加密协商开始前，软件通过调用驱动接口获取光模块/PHY 芯片的规格。若返回规格失败，则终止流程；若返回规格成功，则软件判断光模块/PHY 芯片是否具备加密能力。如果不支持加密则中止流程；如果支持加密，则向对端通告加密能力，并协商加密方式，平台业务软件根据协商结果进行加密初始化配置。
- 身份认证：PHYSec 的身份认证机制主要是确保相互通信的设备及光模块具有合法身份。

- 密钥协商及管理：PHYSec 的密钥协商机制主要是确保相互通信的设备协商出相同的对称密钥，并负责加解密运行过程中密钥的更新与切换。当密钥协商完成后，相互通信的设备建立起安全通道。
- 数据面加解密：在完成认证与密钥协商后，PHYSec 基于系统下发的密钥对物理层比特流采用“流加密”方式进行加密发送与接收解密。需要停止加解密时，系统下发停止加解密的指令，模块内对应的密钥信息清除，同时清除各种统计信息。

PHYSec 链路级方案的数据加解密和通道级方案的数据加解密在以太网物理层的不同层次实现，以 200G/400G/800G 为例，PHYSec 的部署层级架构如图 2-5 所示。

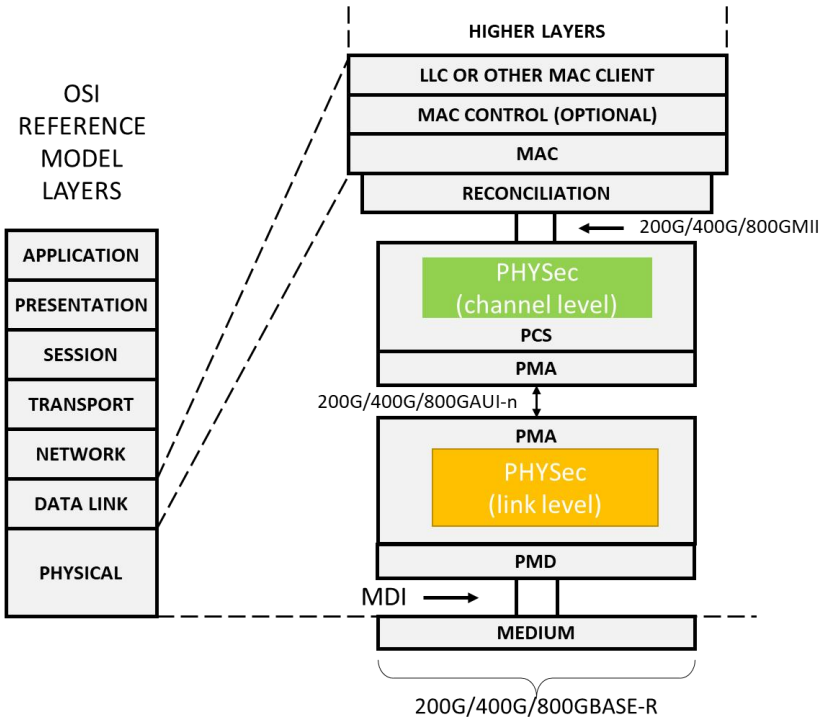


图 2-5 PHYSec 部署层级位置

2.3.1 物理层身份认证机制

PHYSec 的身份认证机制主要是确保相互通信的两端是合法的以

太网设备。传统以太网认证方式是基于链路层设备（如交换机）端口认证的机制，如 802.1X、MAC 地址认证等。这种认证方式在认证过程中只利用了通信设备的信息，并没有利用接口上光模块的信息，所以无法确认光模块的合法性，存在一定的安全风险。如图 2-6 所示为 PHYSec 的身份认证框架。PHYSec 的认证机制将光模块的唯一身份标识（ID）融入到认证过程当中，确保了设备与光模块均具有合法性。

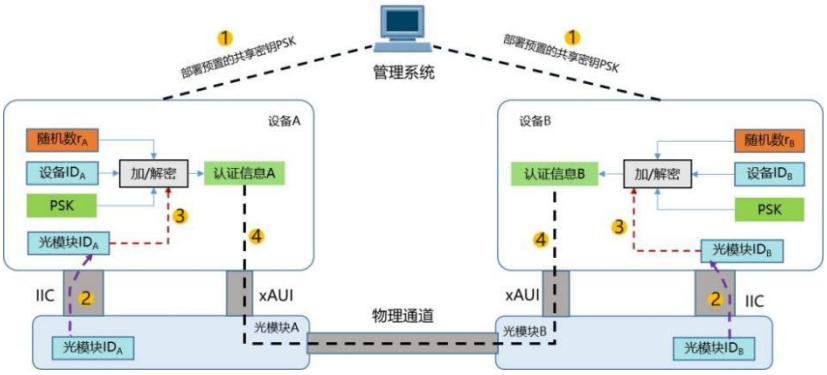


图 2-6 PHYSec 身份认证框架

通信设备通过提前配置预共享密钥 PSK，设备通过 IIC 接口将存放在光模块中的标识 ID 读取到设备内，双方设备通过交互认证信息进行双向身份认证。认证信息可以是设备 PSK 对设备 ID、光模块 ID 以及安全随机数进行加密运算得到的密文。此处对加密算法不做限制，满足安全性要求即可，如标准化的 AES 或 SM4 算法。当执行插拔以及更换光模块等操作时，需要重新进行认证流程。

2.3.2 物理层密钥管理机制

PHYSec 的密钥管理机制主要是解决数据加密密钥派生、分发和管理的问题。如图 2-7 所示，在加密通信前，通信节点间首先会建立安全通道并持续维护安全通道的状态；在建立了安全通道后，通信双

方会运行密钥协商协议，从而安全、及时地分配用于数据面加密的对称密钥。

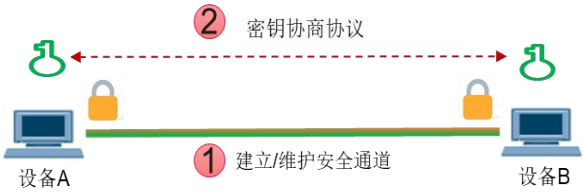


图 2-7 安全通道建立示意图

现有的安全技术如 TLS、IPSec 以及 RDMASec 等在 N 个通信节点的组网场景下，理论上都需要建立 N^2 级的安全会话数。如图 2-8 与图 2-9 所示，对于每个通信节点，在 worst case 下每个节点需要和其他 N-1 个节点建立安全会话，共有 N 个这样的节点，所以建立的安全会话数是 N×(N-1)。若考虑节点 A 和节点 B 之间通常只需要建立一条双向的安全会话，则总的安全会话数是 N×(N-1)/2。对于大规模通信网络，比如具有上万个计算节点的智算中心，每个节点峰值期间需要维护大量的安全会话与密钥，安全管控面复杂度太高，这对节点 CPU 资源以及网卡中内存资源提出极大挑战。

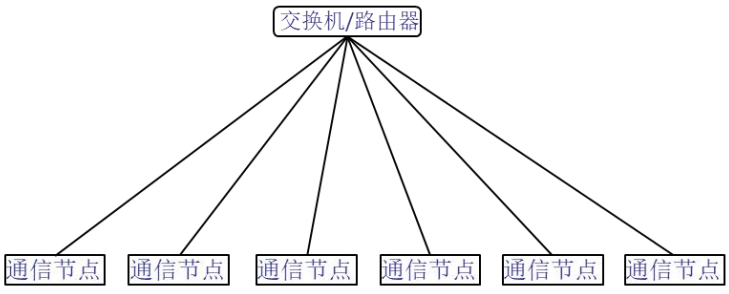


图 2-8 示例拓扑：6 个通信节点

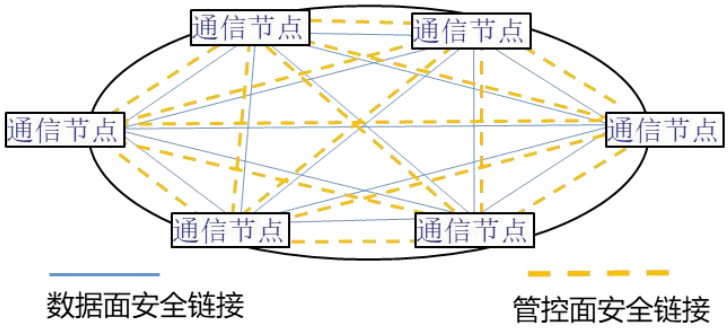


图 2-9 传统安全机制通信节点间数据面与管控面安全链接

针对类似图 2-8 所示的组网连接，PHYSec 的密钥管理机制选定交换机/路由器作为密钥服务器 key server。仅需要 key server 与其他通信节点间建立管控面安全会话，由 key server 进行密钥生成与分发，其他节点只接收密钥，简化密钥管理。如图 2-10 与图 2-11 所示，安全管控面仅需要建立 N 条安全会话数，实现安全管控复杂度从 $O(N^2)$ 降为 $O(N)$。

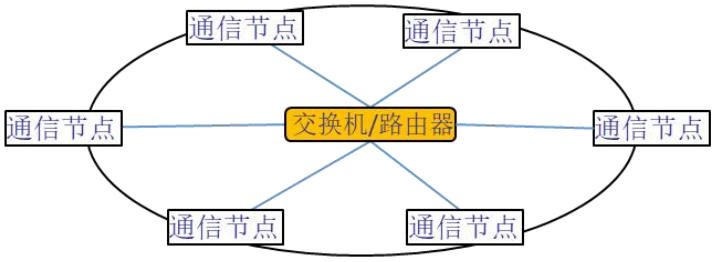


图 2-10 PHYSec 数据面安全连接示意图

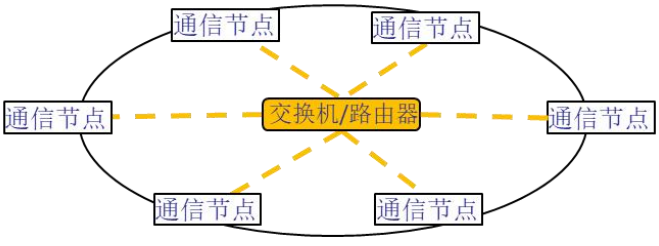


图 2-11 PHYSec 管控面安全连接示意图

针对多个节点服务于一个业务的场景，比如智算中心内部多个节点共同执行同一 AI 训练任务，PHYSec 密钥管理机制对属于同一个业务的所有通信节点配置相同的 PSK，进一步简化密钥管理。Key server 通过预配置的 PSK 生成会话密钥 SAK，将 SAK 加密后分发给同一业务

的其他通信节点，节点间使用 SAK 对通信数据进行加解密。同样，多个节点服务于一个租户的场景也可以采用此简化方案。

2.3.3 物理层数据加解密机制

PHYSec 的数据加密解密主要提供数据的机密性保护与完整性保护，防止数据泄露及被篡改。PHYSec 提供链路级方案与穿越 OTN/SPN 等设备的通道级方案，满足未来网络安全诉求，如图 2-12 所示。

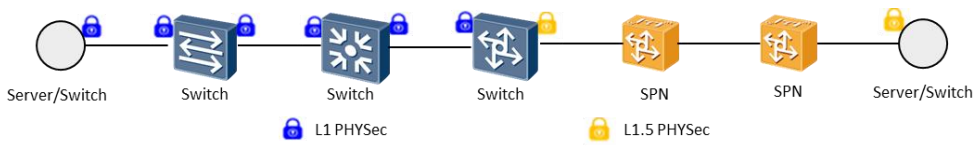


图 2-12 PHYSec 链路级与通道级解决方案示意

PHYSec 基于对称加密算法对数据进行加解密，可选算法有 NIST 标准化算法 AES 与中国国家商用密码标准 SM4，可以根据使用场景灵活选择。以 AES 为例，PHYSec 采用密钥长度为 256 bit 的对称加密，安全性极高。PHYSec 在物理层将加解密算法卸载到底层芯片或模块中，实现线速加解密，加密和解密流程如图 2-13 所示。

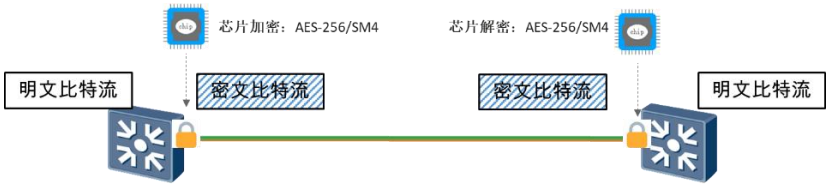


图 2-13 PHYSec 数据加密流程

2.3.3.1 链路级加解密技术方案

考虑 PHYSec 优先在模块内部署，其加密架构如图 2-14 所示。数据帧从发端 MAC 层经过 RS 进入发端 PHY 芯片后变成数据比特流，经

过编码、扰码、对齐标记（Alignment Marker，AM）插入、FEC 等物理层处理流程后进入光模块。发端光模块的 oDSP 先对收到的比特流进行 AM 锁定，然后将 AM 锁定后的比特流组合为复帧进入 oDSP 内的加密模块进行加密变成密文比特流后发送到对端。收端光模块收到密文后先进行 AM 锁定恢复复帧比特流，然后 oDSP 内的解密模块对密文比特流解密恢复成明文比特流后送入收端 PHY 芯片内进行后续处理。

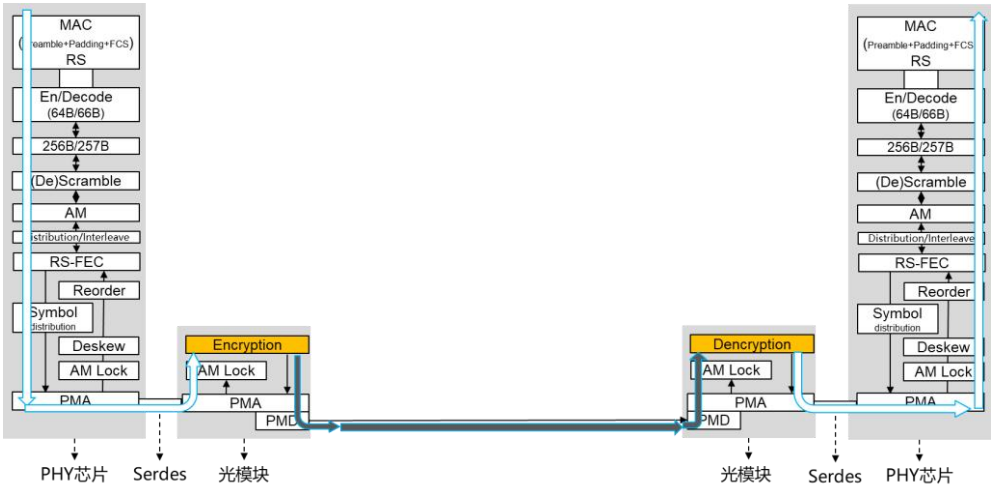
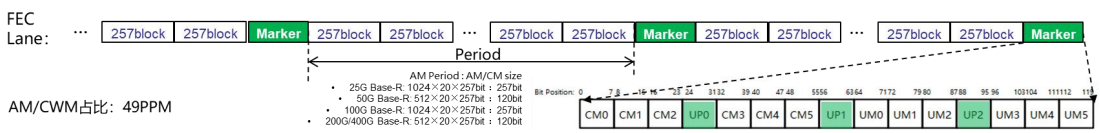


图 2-14 PHYSec 链路级加密解密架构

PHYSec 在以太网物理层 PCS 底层实现加解密。将 N（N 由接口速率确定）个 AM 数据段复合形成复帧比特流，作为 PHYSec 的最小加解密单元。以 200G/400GE 接口为例，如图 2-15 所示,使用 AM block 部分字段（例如 UP0、UP1、UP2）承载初始化向量（IV）、密钥标识（Key Index）等安全相关信息与同步标识(复帧头部、MF Status)，用于控制加解密。为了保证所述字段承载信息后仍然维持直流均衡，建议所述字段实施字节 0/1 均衡（例如：UP0、UP1、UP2 的低 4 bit 承载信息，高 4 bit 为低 4 bit 取反）。



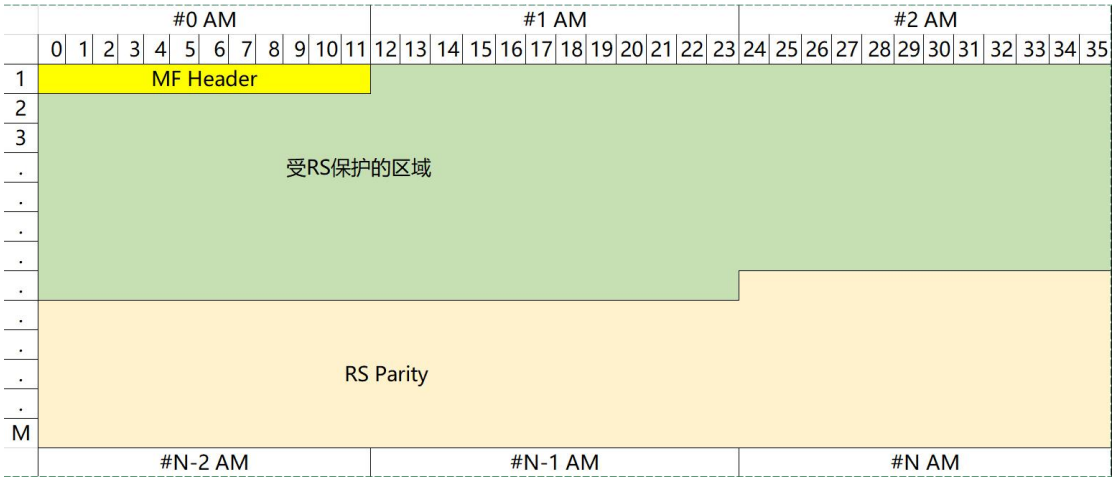


图 2-15 复帧结构

当光模块 DSP 容量预算不足或未加载 DSP 单元，该加密解密方案也可以部署于 PHY 芯片。该技术方案与部署方式解耦，具体部署方式参见 3.2 小节。

2.3.3.2 通道级加解密技术方案

PHYSec 通道级加解密技术方案需要在 PHY 芯片内部署，其加密架构如图 2-16 所示。数据帧从发端 MAC 层经过 RS 进入发端 PHY 芯片 PCS 高层编码为 64B/66B 码块流，针对此码块流进行 65B 压缩（同时可以压缩部分 IDLE 码块），然后全部加密，密文封装到 64B/66B 类似为数据码块的 64bit 区域，然后增加 1 个 D 码块承载解密所需的参数，最后首位添加 S、T 码块，构造一个完整的加密段（Segment），然后再实施 PHY 层其他处理。接收端收到加密段，从第一个 D 码块提取解密所需的参数，对其余 D 码块内的用户信息实施解密，然后还原为 65B 码块流，再解压缩为 64B/66B 码块流。整个加密和解密流程都以 IEEE 802.3 标准规范的 64B/66B 码块流实施加密解密，前向兼容 IEEE 802.3 MAC/PHY 标准功能。

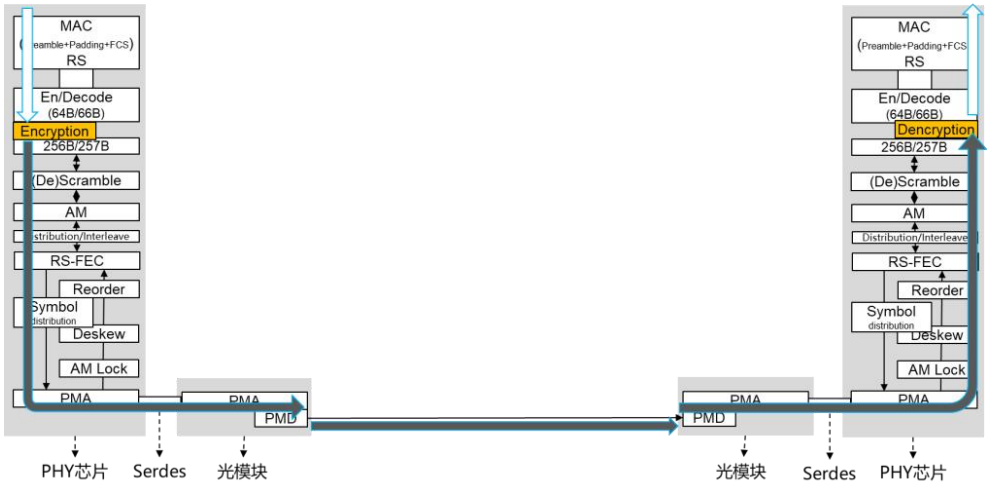


图 2-16 PHYSec 通道级加密解密架构

PHYSec 在以太网物理层 PCS 高层加解密，加密侧流程如图 2-17，解密侧是加密侧的逆操作。考虑压缩部分 IDLE，PHYSec 通道级加解密技术方案可以做到不占用用户开销；考虑 Worst case 情况下，不压缩 IDLE，并在 Segment 之间保留 400PPM 的 IDLE 资源，Segment 采用 N 个 D 码块装载 M 个用户码块，再设置 1 个 D 码块承载加密和解密参数，首尾添加 S 和 T 码块，T 后再追加 1 个 IDLE 码块，则利用率为$U = \frac{N}{M+2+1+1}$, 且要求满足$M \times 64 = N \times 65$, 选择合适的 M 与 N，可以做到>97%的高利用率和低开销。

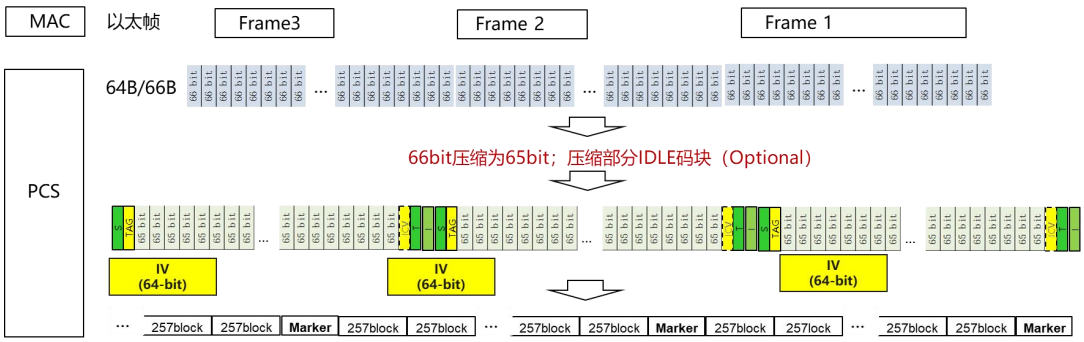


图 2-17 PHYSec 通道级技术方案加密侧流程

2.4 技术优势

相比于 RDMASec、MACSec 等加密机制，PHYSec 在安全性、带宽

利用率、时延等方面都有优势，具体比较如表 2-1 所示：

表 2-1 不同加密机制对比

比较项	RDMASec	MACSec	PHYSec
加密层次	传输层	链路层	物理层（全 bit 流）
用户流量特征	暴露	暴露	完全掩盖
加密开销	大(逐包开销 40B)	中(逐包开销 24-32B)	低(接近 0)
加密时延*	微秒级	微秒级	几十纳秒
加密配置	相对复杂	简单	简单
加密性能(线速)	达到线速（实现代价大）	达到线速	达到线速

*加密时延与加密对象带宽速率有关。以 400G 为例，基于硬件实施 MACSec 的安全 PHY，时延 100~200ns，而在 PHY 层实施的 PHYSec，时延约 40ns。

（1）高安全

PHYSec 在物理层实现了全加密，相比于 RDMASec、MACSec，PHYSec 可以加密所有的链路层及以上的协议与用户信息，掩盖了流量特征，如表 2-2 所示。

表 2-2 RDMASec、MACSec 及 PHYSec 保护能力对比

比较项	RDMASec	MACSec	PHYSec
能否保护载荷	是	是	是
能否保护应用层协议	是	是	是
能否保护 TCP/UDP 头部	是	是	是
能否保护 IP 头部	否	是	是
能否保护以太帧头部	否	部分	是
能否隐藏数据包发送频率	否	否	是
能否隐藏数据包长度	否	否	是
能否保护 VLAN-Tag	否	是	是
能否保护 ARP/NDP	否	是	是
能否保护 802.3ah	否	否	是
能否保护生成树协议	否	否	是
能否保护 ICMP	是	是	是

能否保护链路自动发现协议 LLDP	否	否	是
能否保护链路聚合协议 LACP	否	否	是
能否保护 IGMP	否	是	是
能否保护(g)PTP	否	是	是
能否保护 PFC/Pause	否	否	是
能否保护 IEEE 1722(AVB)	否	是	是

（2）低开销

现有的链路层及以上的安全机制如 RDMASec、MACSec 都会带来较大的加密开销，如表 2-1 所示。RDMASec 逐包加密，通常每帧需要引入 40 字节的开销，包括 8 字节的 UDP header 与 32 字节的加解密参数与完整性校验值，对于短帧场景（比如每帧 64 字节），RDMASec 的有效带宽利用率不足 70%。MACSec 逐帧加密，通常每帧需要引入额外开销 32 字节来承载加解密参数与完整性校验值等。对于短帧场景（比如每帧 64 字节），MACSec 的有效带宽利用率不足 70%。如图 2-18 所示。PHYSec 使用以太网物理层的 OAM 码块来承载加解密参数，不引入额外的带宽开销，对于智算中心互联及企业园区等带宽敏感的使用场景具有带宽利用率高的优势。

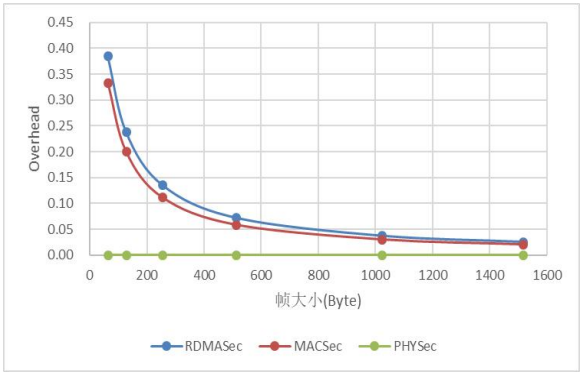


图 2-18 RDMASec、MACSec 及 PHYSec 加密开销对比

（3）低时延

相较于 RDMASec 和 MACSec，PHYSec 工作在物理层，易于在硬件或芯片上实现，时延可以达到几十纳秒级别，如表 2-1 所示，对于重视低时延的智算中心场景有明显优势。

（4） 低复杂度

RDMASec/MACSec PHY 架构将加密功能下沉到 PHY 芯片内实现，只需要对交换机/路由器等设备端口进行升级便可支持加密功能，对设备的改动相对较小。这种架构将加解密运行时所需的功耗、算力都卸载到 PHY，分担了上层芯片的负担。但这种架构需要在 PHY 芯片中执行背靠背操作，即将 PHY 中的比特流恢复到包或帧，然后对恢复后的包或帧进行加解密。加解密后再处理成比特流送入后续的 PHY 处理模块，处理过程如图 2-19 所示。这种背靠背的架构实现需要在 PHY 中引入更多的芯片实现代价、处理时延和功耗。PHYSec 是针对物理层比特流的加解密机制，避免了上述背靠背操作引入的额外芯片实现代价、时延和功耗。

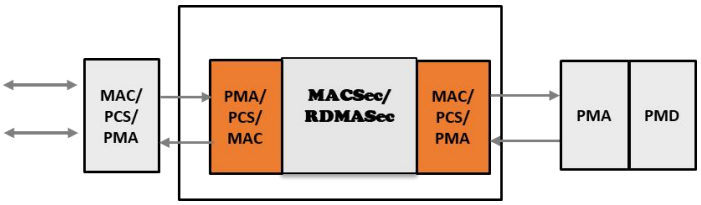


图 2-19 MACSec/RDMASec 芯片架构

（5）协议透明

PHYSec 的加密对象是物理层的比特流，可以做到对上层业务和协议进行透明加解密，即不感知上层业务和协议，如图 2-20 所示。透明加解密会带来如下优势：

- 不影响上层业务，如上层转发机制、Cut-through 机制等。

- 上层增删业务时，无需修改安全配置与安全实例。
- 加解密操作由 MAC 层下沉到 PHY，分担了上层芯片（如 ECU、CPU、NP 芯片）的负担。

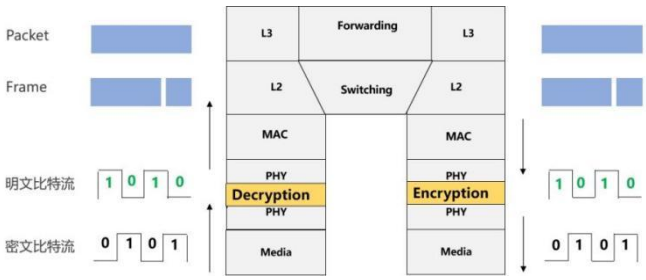


图 2-20 PHYSec 加密层级

3. 应用与部署

3.1 应用场景

PHYSec 技术可以被应用于各种以太网链路级安全场景，本白皮书重点介绍 PHYSec 在智算中心相关应用场景，包括智算中心入算流量安全、算内节点间互联安全以及算间节点间互联安全。

（1） 智算中心

a. 智算中心入算流量安全

入算对安全的主要诉求是高安全、低开销。

AI 大模型及其应用需要大量的数据作为训练集，企业等高价值用户通过灵活的接入专线技术随时、随地、随需接入智算中心，上传用户敏感数据到智算中心或从智算中心下载训练好的模型及参数等敏感资产，如图 3-1 所示，在此过程中用户的数据存在被窃听泄露的风险。

低开销对接入智算中心专线至关重要，相比于使用 RDMASec/MACSec 带来的 20%以上的开销，PHYSec 占用极少的用户带宽，节省专线成本。此外，PHYSec 可以对用户所有信息和所有的网络管控协议全加密，更安全。

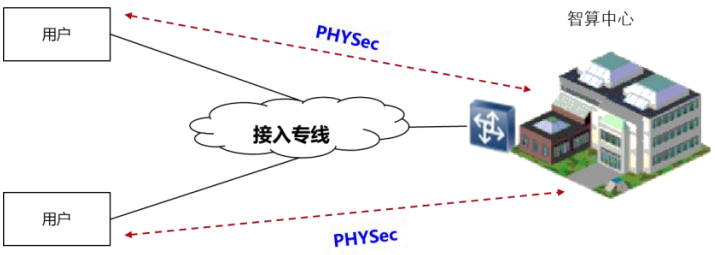


图 3-1 智算中心流量入算场景

b. 智算中心内安全

算内对安全的主要需求是低时延、高吞吐。

传统的数据中心内无网络安全机制，对东西向流量无安全防护，演进到智算中心时代，存在模型、参数及数据等敏感资产泄露的风险。通信链路、设备端口暴露，网络扩容升级、频繁运维、多租户等典型场景都需要加强安全防护。例如，智算中心服务商提供设备及服务器等基础设施出租的业务，不同租户共用相同的机房或机架或通信设备，服务器与网络难以精确物理隔离，不同租户根据需求频繁租用或退租，需要计算节点之间对所有通信流量加密，确保租户的模型架构、参数与数据安全。

智算中心内典型的组网拓扑包含 Clos 架构与直连（dragonfly）架构，如图 3-2 所示。使用 RDMASec、MACSec 等安全机制，面临安全加密实例多，加解密额外引入的时延大，以及加解密带宽开销大的挑战。PHYSec 适用于这两种常见的智算中心组网拓扑，可以将加解密时延降低至百纳秒级，且安全加密实例数低，不占用用户带宽。如果通过光模块实现 PHYSec,则无需更换服务器、交换机等硬件设备，易于部署。

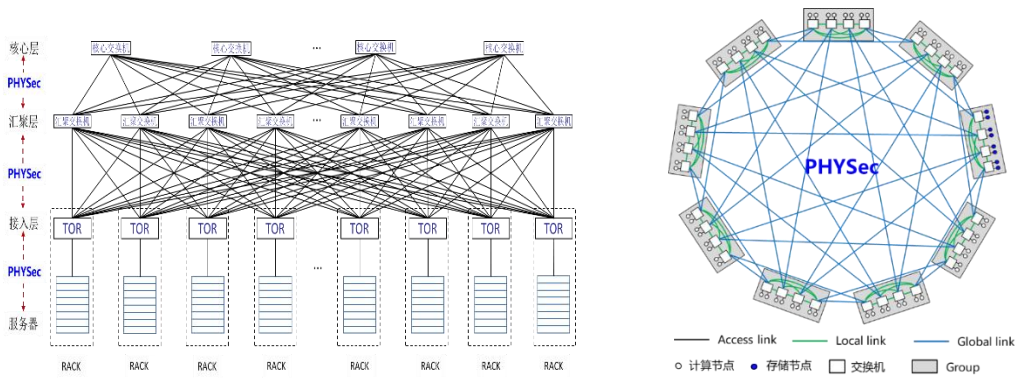


图 3-2 智算中心典型拓扑示例。①CLOS 架构②直连架构

c. 智算中心间安全

算间对安全的主要诉求是高安全、高吞吐。

智算中心间的高速互联光纤以及铺设光纤的管井等暴露的物理设施，存在被攻击窃听的风险。使用 PHYSec 光模块可以杜绝光纤信号被窃听的风险，而且不需要更换现有的智算中心网络互联设备，如图 3-3 所示。高安全对智算中心高速互联场景至关重要，相比于使用 MACSec 对互联链路进行保护，PHYSec 可以对用户所有信息和所有的网络管控协议全加密。

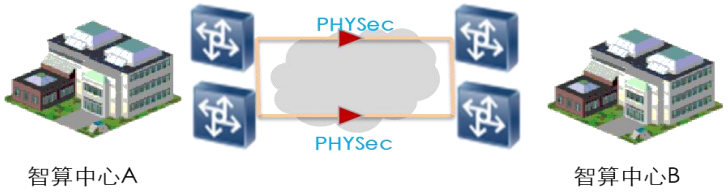


图 3-3 智算中心互联场景

3.2 部署架构

PHYSec 可以根据不同场景来灵活选择合适的部署模式。不同的 PHYSec 部署方式，其实现架构与具体的加密位置略有不同。

1) 面向以太网中已有存量设备无法进行硬件芯片更换的场景，可以在存量设备中插入已部署 PHYSec 的光模块实现数据加解密，直接兼容现有网络设备，迅速升级链路安全通信能力，保护现有设备与通信资产。加解密功能主要运行在以太网物理层的 PCS 底层，由光模块中电芯片（如数字信号处理芯片）实现，其架构如图 3-4 所示。即使网络原来不具备安全能力，这种 PHYSec 部署模式也可以提供补救升级的机会。

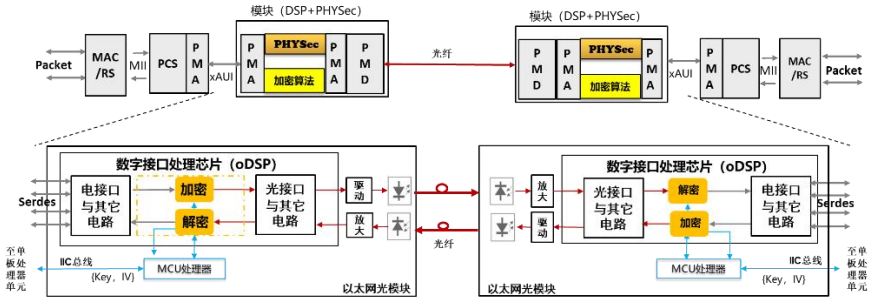


图 3-4 PHYSec 实现方式—光模块部署

2）面向以太网新增设备的安全加密需求，可以考虑在新增设备的 PHY 芯片中部署 PHYSec，保护整个设备端口加链路，兼容现有光模块。加解密功能主要运行在以太网物理层的 PCS 层，其架构如图 3-5 所示。

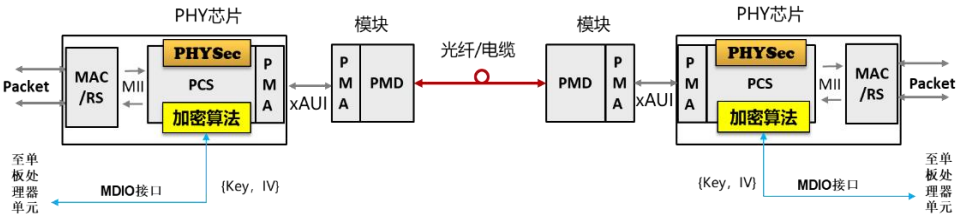


图 3-5 PHYSec 实现方式—PHY 芯片部署

3）面向以太网链路两端分别为存量设备和新增设备的安全场景，可以在新增设备的 PHY 芯片中部署 PHYSec，在存量设备中插入已部署 PHYSec 的光模块，即可升级链路安全通信能力，其架构如图 3-6 所示。其中，PHY 芯片主要在 PCS 层实现 PHYSec，光模块中由电芯片（如数字信号处理芯片）实现 PHYSec。

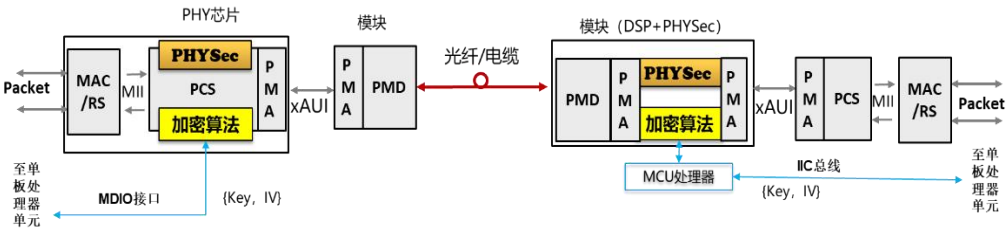


图 3-6 PHYSec 实现方式—混合部署

4. 总结与展望

随着 AI 技术的快速发展，大量敏感数据与 AI 模型参数在以太网上进行传输。PHYSec 作为以太网物理层安全技术，可以保护智算中心以太网安全，防止数据泄露，具有低时延、低开销、高安全、灵活易部署等优点，符合技术与产业的发展趋势。同时，PHYSec 在卫星互联网、数据中心、物联网、园区以及电信网络等领域也具有巨大的应用潜力，将为 IT 和电信领域的安全市场创造巨大的价值增长点。例如，卫星通信网络具有信道开放、动态拓扑的特征，在星地互联、星间互联都面临着链路传输的数据、信令等被截获或破解的风险。不仅如此，卫星通信的链路带宽资源极为珍贵，对带宽利用率有极高的要求。PHYSec 在保护卫星通信链路安全的前提下，实现极低开销，满足卫星通信高带宽利用率的需求。在可以预见的未来，PHYSec 作为下一代以太网安全技术将带来巨大的市场空间，并将得到广泛应用与长足发展。

值得注意的是，随着高性能量子计算机的出现，基于伪随机数的传统密钥加密算法面临着被破译的风险。量子密钥利用光子偏振特性，依靠对光子进行编码、传输、测量等操作完成量子态的密钥传输，其安全性由量子力学的基本原理保证，是唯一理论证明的绝对安全、不会被监听或截取的密钥分发技术。如果利用量子密钥分发技术为 PHYSec 提供密钥，将为以太网带来史无前例的安全性，可以应对高性能量子计算机带来的安全挑战。

缩略语列表

缩略语	英文全名	中文解释
AI	Artificial Intelligence	人工智能
AIGC	AI Generated Content	人工智能生成内容
HPC	High Performance Computing	高性能计算
CPU	Central Processing Unit	中央处理单元
EEPROM	Electrically Erasable Programmable Read Only Memory	电可擦除可编程只读存储器
IEEE	Institute of Electrical and Electronics Engineers	电气与电子工程师协会
UDP	User Datagram Protocol	用户数据报协议
IP	Internet Protocol	网际协议
RDMA	Remote Direct Memory Access	远程直接内存访问
NP	Network Processor	网络处理器
ECU	Electronic Control Unit	电子控制单元
PFC	Priority-based Flow Control	基于优先级的流量控制
TLS	Transport Layer Security	传输层安全协议
IPSec	Internet Protocol Security	因特网协议安全协议
RDMASec	Remote Direct Memory Access Security	远程直接内存访问安全协议
MACSec	Media Access Control Security	媒体接入控制安全协议
PHYSec	Physical Layer Security	物理层安全协议
AES	Advanced Encryption Standard	高级加密标准
NIST	National Institute of Standards and Technology	美国国家标准与技术局
PSK	Pre-Shared Key	预共享密钥
SAK	Secure Association Key	安全联盟密钥
oDSP	optical Digital Signal Processor	光数字信号处理芯片
MF	Multi-frame	复帧
PCS	Physical Coding Sublayer	物理编码子层
IV	Initialization Vector	初始化向量
VLAN	Virtual Local Area Network	虚拟局域网
ARP	Address Resolution Protocol	地址解析协议
NDP	Neighbor Discovery Protocol	邻居发现协议

LLDP	Link Layer Discovery Protocol	链路层发现协议
LACP	Link Aggregation Control Protocol	链路聚合控制协议
IGMP	Internet Group Management Protocol	互联网组管理协议
gPTP	generalized Precision Time Protocol	广义精确时间协议
AVB	Audio Video Bridging	音频视频桥接
TOR	Top of Rack	机柜交换机

参考文献

[1] RFC 5042：Direct Data Placement Protocol (DDP)/Remote Direct Memory Access Protocol (RDMAP) Security

[2] Google white paper: PSP Architecture Specification, 2022

[3] IEEE 802.1AE-2018：Media Access Control (MAC) Security

[4] RFC 9347：Aggregation and Fragmentation Mode for Encapsulating Security Payload (ESP) and Its Use for IP Traffic Flow Security (IP-TFS)

[5] ISO 7498-2：Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture