information

IMPACT FACTOR 2.9

CITESCORE 6.5

Article

# Quantum-Secure Coherent Optical Networking for Advanced Infrastructures in Industry 4.0

Ofir Joseph and Itzhak Aviv

MDPI

https://doi.org/10.3390/info16070609

information

MDPI

*Article*

# Quantum-Secure Coherent Optical Networking for Advanced Infrastructures in Industry 4.0

**Ofir Joseph [1] and Itzhak Aviv [1,2,*]**

[1] Department of Information Systems, University of Haifa, Haifa 3498838, Israel; ofiri@mta.ac.il
[2] MTA, Tel-Aviv 6803300, Israel
* Correspondence: itzhakav@mta.ac.il

## Abstract

Modern industrial ecosystems, particularly those embracing Industry 4.0, increasingly depend on coherent optical networks operating at 400 Gbps and beyond. These high-capacity infrastructures, coupled with advanced digital signal processing and phase-sensitive detection, enable real-time data exchange for automated manufacturing, robotics, and interconnected factory systems. However, they introduce multilayer security challenges—ranging from hardware synchronization gaps to protocol overhead manipulation. Moreover, the rise of large-scale quantum computing intensifies these threats by potentially breaking classical key exchange protocols and enabling the future decryption of stored ciphertext. In this paper, we present a systematic vulnerability analysis of coherent optical networks that use OTU4 framing, Media Access Control Security (MACsec), and 400G ZR+ transceivers. Guided by established risk assessment methodologies, we uncover critical weaknesses affecting management plane interfaces (e.g., MDIO and $I^2C$) and overhead fields (e.g., Trail Trace Identifier, Bit Interleaved Parity). To mitigate these risks while preserving the robust data throughput and low-latency demands of industrial automation, we propose a post-quantum security framework that merges spectral phase masking with multi-homodyne coherent detection, strengthened by quantum key distribution for key management. This layered approach maintains backward compatibility with existing infrastructure and ensures forward secrecy against quantum-enabled adversaries. The evaluation results show a substantial reduction in exposure to timing-based exploits, overhead field abuses, and cryptographic compromise. By integrating quantum-safe measures at the optical layer, our solution provides a future-proof roadmap for network operators, hardware vendors, and Industry 4.0 stakeholders tasked with safeguarding next-generation manufacturing and engineering processes.

**Keywords:** MACsec; OTU4; quantum key distribution; optical networks

check for updates

Academic Editor: Yuchen Jiang

Received: 19 April 2025
Revised: 3 June 2025
Accepted: 27 June 2025
Published: 15 July 2025

**Citation:** Joseph, O.; Aviv, I. Quantum-Secure Coherent Optical Networking for Advanced Infrastructures in Industry 4.0. *Information* **2025**, *16*, 609. https://doi.org/10.3390/info16070609

## 1. Introduction

Modern communication systems underpinning **Industry 4.0** require high-capacity optical networks spanning local facilities, regional corridors, and transoceanic links. The latest backbone infrastructures, supporting data rates of 400 Gbps and above, rely on coherent technology enhanced by advanced digital signal processing and phase-sensitive detection [1]. Such systems transmit terabits of data per second to serve the diverse, time-sensitive demands in industrial automation, robotics control, global financial transactions, and e-government databases. As reliance on these coherent networks grows, so does the urgency of addressing security vulnerabilities, especially in environments where interconnected machinery, sensors, and cloud-based analytics coexist [2].

The evolution of network hardware design is driven by the surging throughput requirements typical of **smart factories** and **robotic assembly lines**. While earlier optical links depended primarily on upper-layer protocols, such as Transport Layer Security or IP security for data protection [3], advanced Industry 4.0 applications increasingly employ Layer 2 solutions like Media Access Control Security (MACsec) to ensure confidentiality, integrity, and authenticity at the Ethernet layer. However, new technical challenges arise in coherent networks. Management interfaces bridging MACsec-enabled routers and optical modules, often using MDIO or $I^2C$ protocols, lack robust security measures [4]. Similarly, the overhead field-based structure of Optical Transport Unit level 4 framing is susceptible to interception or manipulation [5]. The combined use of multiple protocols with different security assumptions can introduce unforeseen vulnerabilities, hampering the reliability required by fully automated manufacturing processes.

Recent research and development in quantum computing enhance security concerns. The distribution of keys for MACsec security uses cryptographic methods, which depend on finite mathematical assumptions. Modern quantum algorithms, notably Shor's algorithm, threaten the security of classical cryptography once quantum computing matures to a sufficient level [6,7]. Adversaries can store intercepted ciphertexts now and decrypt them later, making the immediate adoption of quantum-safe measures critical. Modern data security demands the implementation of quantum-safe cryptographic approaches since attacks can happen while data is stored for later decryption. Although quantum key distribution (QKD) offers a theoretically unbreakable means of key exchange [8], its integration with coherent optical networks has faced practical hurdles. Recent progress suggests that these hurdles are more surmountable than previously believed [9].

Motivated by these challenges, the primary purpose of this research is to explore how coherent optical networks can be protected from both classical exploits and future quantum-based attacks, while preserving compatibility with existing networking standards. This work aligns with calls from the recent literature for quantum-safe encryption strategies in optical environments [10–12]. The presence of management plane vulnerabilities in 400G ZR+ transceiver modules, as well as protocol weaknesses in OTU4 overhead fields, calls for rigorous investigation.

The specific gap in the current literature is that many proposed methods treat optical-layer security, MACsec, and quantum cryptography as separate domains. This fragmentation creates a scenario in which bridging them may introduce further security holes or degrade system performance. In this context, "quantum-resistant protocols" refer to cryptographic algorithms and key-exchange methods designed to remain secure even against adversaries equipped with large-scale quantum computing capabilities, typically by relying on mathematically hard problems that cannot be efficiently solved by known quantum algorithms. Therefore, this paper is guided by a research question that addresses the heart of this fragmentation: "How can coherent optical networks that rely on OTU4 framing and MACsec be enhanced to safeguard against emerging quantum threats while maintaining the throughput and latency requirements of existing infrastructure?"

This question captures the dual necessity of optical-layer protection and quantum key distribution in coherent environments. It targets the management plane vulnerabilities that arise in bridging router control planes with advanced optical modules and focuses on bridging the gap between classical cryptography, optical encryption, and emerging quantum technologies.

We implemented a qualitative security analysis that systematically probes each interface, protocol boundary, and cryptographic layer. This analysis systematically follows recognized risk assessment and critical infrastructure protection frameworks [13,14], ensuring the comprehensive identification of both classical and quantum vulnerabilities. This vulnerability analysis underpins this study's creation and validation of a post-quantum security framework that merges spectral phase masking with multi-homodyne coherent detection at the physical layer and QKD key distribution for key management. By unifying these approaches in a single design, our solution delivers robust cryptographic strength, forward secrecy, and backward compatibility in coherent optical networks operating at 400 Gbps and above.

This research makes specific contributions through an original vulnerability analysis of coherent infrastructures and a novel design for post-quantum security. First, it systematically identifies overlooked weaknesses in bridge architectures that coordinate the router control plane with coherent modules. This includes close scrutiny of the management interfaces where protocol conversion and synchronization occur, as these seemingly routine operations can introduce timing discrepancies. Second, it classifies vulnerabilities in OTU4 framing, where overhead bytes and frame alignment can be manipulated to create covert channels or disrupt signal integrity. Third, it proposes a new approach that incorporates optical phase mask encoding with multi-homodyne coherent detection and quantum key distribution for holistic security. The theoretical findings indicate that such a layered strategy resists both contemporary classical attacks and future quantum-based decryption methods, particularly in the context of coherent optical transport at data rates of 400 Gbps and above.

We conclude that a concerted security strategy, one that bridges the physical encryption aspects of spectral phase encoding with post-quantum key distribution, can substantially mitigate vulnerabilities exposed at the interface between traditional data networking protocols and coherent optical platforms. This analysis provides a blueprint for researchers, network operators, and hardware vendors seeking to future-proof optical transport networks.

The structure of this manuscript proceeds as follows. First, a review of related work addresses classical encryption vulnerabilities, the integration of MACsec over OTU4, and the latest developments in quantum-resistant protocols. By cataloging vulnerabilities within and across architectural boundaries in Section 4, this research provides a robust empirical foundation for the comparative and integrative frameworks that follow. Section 5 reviews existing optical encryption approaches in the context of these vulnerabilities, while Section 6 presents a cohesive post-quantum security framework designed to mitigate the weaknesses documented here. A discussion evaluates the significance of these findings, their limitations, and potential avenues for more advanced or large-scale implementations. The manuscript concludes by asserting the practicality and necessity of a post-quantum security framework for coherent optical networks, underscoring the benefits of layering quantum key distribution with optical encryption to protect critical data transmission over the long term.

## 2. State of the Art

Optical network security has its foundation at the intersection of classical cryptography, quantum information theory, and optical physics. The intersection of these multiple disciplines offers the promise of increasing performance and solving the unique challenges of maintaining data confidentiality and integrity while simultaneously providing the high-performance characteristics of optical communications. Contemporary research has evolved along three critical dimensions: the quantum vulnerability assessment of traditional encryption schemes, the security implications of integrating legacy protocols, and the construction of quantum-resistant frameworks. With the advances of coherent optical technologies such as 400G ZR+ and the sophistication of quantum computing threats, these dimensions are becoming more and more important. Furthermore, to build on the added complexities provided by integrating Media Access Control Security (MACsec) and Optical Transport Unit level 4 (OTU4) framing, a new set of vulnerabilities in these environments was created. This work explores the current state of the research in this problem, highlights the available solutions' gaps, and correspondingly suggests the role of a novel framework.

### *2.1. Vulnerabilities in MACsec Integration*

MACsec is widely deployed and can provide confidentiality, integrity, and authentication using Layer 2 encryption. However, its application in optical transport networks poses critical issues, especially with OTU4 framing. The interfaces between router control planes and coherent optical modules are vulnerable targets for timing-based attacks as well as unauthorized access and interception [15,16]. Often, these interfaces serve as the point of access to electronic encryption subsystems that are then used to protect information at optical transport layers, leading to vulnerabilities in the security architecture.

Figure 1 shows how MACsec interacts with optical transport systems, as well as key vulnerability points and quantum threats. The layered diagram illustrates interaction points between the optical transport layer and MACsec at Layer 2, highlighting places vulnerable to both classical and quantum attacks.

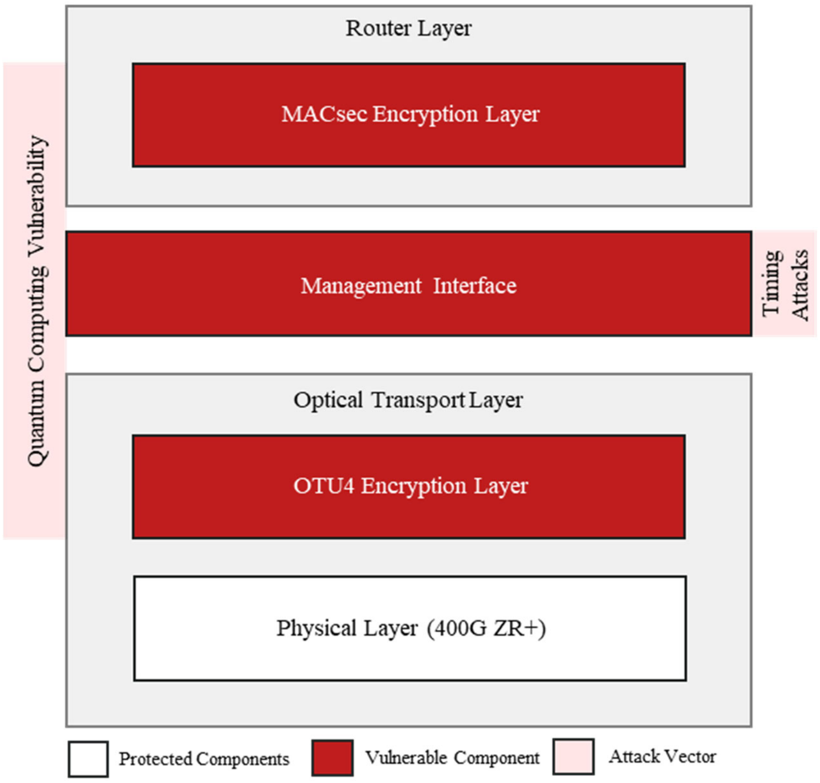

**Figure 1.** MACsec and optical transport vulnerabilities.

Moreover, in the age of quantum computing, MACsec's reliance on public key cryptographic methods acts as a major threat. Quantum attacks can be used to break intercepted MACsec communications, making these protections pointless [17,18]. Quantum-safe cryptographic methods like Quantum Key Distribution (QKD) have theoretical security advantages but their integration with existing MACsec protocols is an active research area [15,18].

These studies are valuable in understanding individual network vulnerabilities; however, a critical gap in the understanding of system-level interactions between the security layers in coherent optical networks persists. An investigation into the relationship between quantum vulnerabilities and protocol-level weaknesses is needed.

### *2.2. OTU4 Framing and Protocol Weaknesses*

The adoption of OTU4 framing in coherent optical networks exacerbates security issues by complicating things further. Essential for high-efficiency data transport, OTU4 has an open architecture, introducing vulnerabilities when working together with legacy protocols such as Modbus. Generally, Modbus, a serial communications protocol designed for programmable logic controllers (PLCs), is added into OTU4 networks through management interfaces to support industrial control systems. This integration is accomplished by using Modbus commands encapsulated into the frame structure by means of OTU4 overhead bytes to enable remote monitoring and control capabilities. The problem with Modbus is that it lacks basic security features like authentication and encryption, and when carried within OTU4 frames, these vulnerabilities persist. Modbus, a protocol widely implemented in Supervisory Control and Data Acquisition (SCADA) systems, does not employ encryption, authentication, or access controls [19,20]. As a result, OTU4 systems are susceptible to man-in-the-middle attacks, unauthorized access, and eavesdropping.

Attack surfaces on OTU4 frames include control fields like the Trail Trace Identifier (TTI) and Bit Interleaved Parity 8 (BIP 8), which are particularly easy to exploit. These fields are specifically identified as key points for injecting malicious payloads and for creating covert communication channels [21]. Additionally, existing SCADA security mechanisms are insufficient primarily in safeguarding OTU4 systems in the critical infrastructure environments [22]. Furthermore, legacy protocols, which are integrated with modern optical networks, possess vulnerabilities [23].

The detailed structure of an OTU4 frame is shown in Figure 2, and contains its critical control fields, TTI, BIP-8, and FAS. The diagram shows how Modbus protocol commands are encapsulated in these fields and identifies the points at which manipulation can take place.

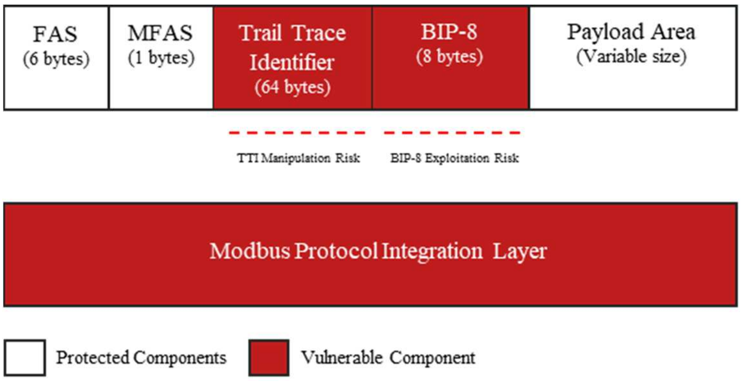

**Figure 2.** OTU4 framing and Modbus protocol weaknesses.

To counter both classical and quantum attack vectors, novel security protocols have been developed to cope with these protocol-level vulnerabilities in the presence of the quantum computing threat.

### *2.3. Emerging Solutions: Quantum and Adaptive Technologies*

Traditional security mechanisms in optical transport networks are limited, and therefore, advanced solutions have been explored. Thus, quantum key distribution (QKD), usually tamper-proof quantum key exchanges by using quantum mechanics [15,18], is a promising way to mitigate quantum threats. To illustrate the severity of quantum threats, consider a practical attack scenario: With Shor's algorithm, an adversary with quantum computing abilities could aim at both the MACsec and OTU4 encryption layers simultaneously. For instance, enlisting the services of a sufficiently potent quantum computer with enough qubits to factor the RSA keys to be used in both layers of the key exchange protocols would take hours, compared to the countless years that it would take classical computers. Both encryption layers are vulnerable to this because they generally use the same public key cryptographic primitives in their initial key establishment and thus represent a single point of failure, even though the encryption layers appear separate. The practical integration of QKD in high-speed optical environments, however, is challenged by scalability, a limited key rate, and compatibility with existing protocols like MACsec [16].

In parallel, adaptive technologies such as Network Function Virtualization (NFV) and Software-Defined Networking (SDN) are proposed to improve the security and flexibility of optical transport networks. NFV and SDN decouple network functions from dedicated hardware, and, therefore, can dynamically detect and respond to threats [24,25]. SDN architectures allow centralized control, which supports the scalability of more advanced security frameworks. Machine learning models can enhance these frameworks even further by identifying anomalies in network traffic and proactively mitigating sophisticated attacks [21,26,27].

An architectural overview of the emerging security solution in optical networks is shown in Figure 3. QKD was integrated with NFV and SDN for the integrated security framework, as depicted in the diagram, and it is demonstrated how these technologies operate together to provide a comprehensive security framework.

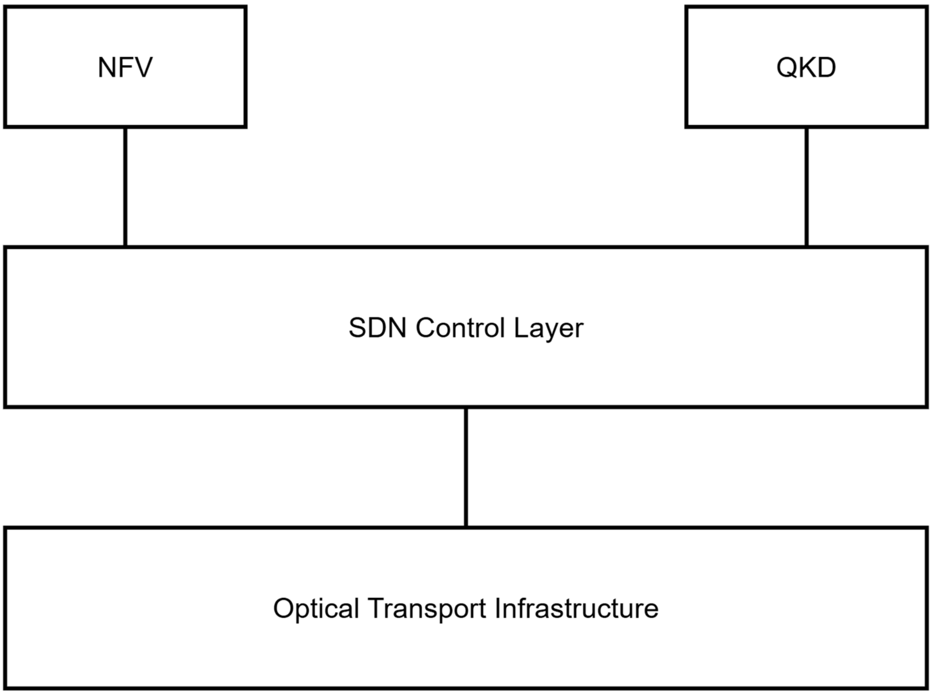

**Figure 3.** Emerging solution in optical security, integrating QKD, NFV, and SDN in an optical network security architecture.

QKD comes with inherent theoretical security advantages, but current techniques need several practical improvements on the network optical layer. Some of these are distance limitations, key rate constraints, and infrastructure integration complexities with existing infrastructure. While NFV and SDN solutions hold promise for dynamic security management, they also bring their own vulnerabilities of greater network complexity and enlarged attack surfaces. While machine learning approaches can be effective for anomaly detection, they must be designed to achieve appropriate false positive rates and with acceptable computational overhead for high-speed optical environments.

### 2.4. Research Gaps and Opportunities

Although critical gaps exist, significant advancements in securing optical transport networks also exist, particularly in an environment where MACsec and OTU4 framing coexist. MACsec implementations today fail to secure OTU4-specific vulnerabilities such as control field manipulations, creating a disjointed security architecture. Additionally, QKD remains a robust quantum-safe form of encryption, but the integration with legacy protocols remains far from complete [28].

For emerging technologies such as NFV and SDN, although there are promising results, their use in optical networks is hindered by scalability and interoperability with existing systems. Adaptive security mechanisms must be highly integrated with real-time monitoring to keep pace with changing threats [29].

The fundamental tension between quantum-safe security requirements and the performance demands of high-speed optical networks has not yet been fully addressed in current research. Especially missing is the integration of post-quantum cryptography with OTU4 framing and its latency and throughput implications. Additionally, although individual security solutions have been suggested in these areas, an all-encompassing security framework addressing quantum and classical threats simultaneously while satisfying network performance metrics is mainly missing.

## 3. Research Method

The research design draws upon established qualitative methodologies to ensure validity and reliability in analyzing coherent optical transport environments. It synthesizes recognized frameworks for rigorous qualitative inquiry [30,31] with the structured case-based guidelines from [32], adapted to a multi-layered technical context. The approach is reinforced by [33], with an emphasis on methodological triangulation to strengthen the credibility of findings and on maximizing internal validity through iterative data collection and analysis cycles [34].

This study begins by outlining the physical and logical architecture of a 400G ZR+ coherent optical system, pinpointing the interfaces and components that bridge the electronic and optical domains. Each subsystem, including management plane interfaces, gearboxes, and digital signal processing blocks, is assessed according to a unified set of criteria derived from the CIA (confidentiality, integrity, availability) model [30]. The systematic vulnerability assessment principles form a risk assessment framework that establishes consistent procedures for identifying and prioritizing threats [13,35]. This combination of models and guidelines aligns with recommendations to layer qualitative procedures with domain-specific standards, thereby reinforcing trustworthiness in the resulting analyses [31].

Threat modeling follows an iterative case-based approach, wherein each subsystem is conceptualized as a case unit to be examined for potential adversarial compromise [32]. The modeling draws on a detailed characterization of threat agents, their capabilities, and possible objectives. This systematic lens illuminates both classical attack vectors, such as unauthorized modifications to overhead fields and optical taps, and quantum-driven threats capable of undermining classical key exchange [14]. The notion of methodological triangulation is employed by gathering data from multiple sources—specifications, protocol analyses, and documented exploits—to confirm that the findings are robust. Observations about timing windows, protocol boundaries, and adaptive DSP algorithms are compared against the theoretical constructs of large-scale quantum cryptanalysis, ensuring that no single perspective biases the interpretation [33].

Once all vulnerabilities are identified and categorized, this study applies the principle of iterative validation, repeatedly testing the relevance and severity of each vulnerability under different simulated threat scenarios [34]. Potential effects on confidentiality, integrity, and availability are judged according to established guidelines [35]. The final phase involves translating these insights into design principles that inform a post-quantum security architecture. In this step, the layered hybrid of spectral phase encoding with multi-homodyne coherent detection and quantum key distribution is scrutinized for its efficacy in mitigating vulnerabilities, its backward compatibility, and its operational performance impact. This final cross-check follows a suggestion to compare the case findings against an external framework of best practices, allowing this study to confirm that the proposed solution stands on a firm methodological foundation [32].

This process can be replicated by any researcher in possession of technical documentation for coherent transceivers, a suite of recognized encryption strategies, and a threat-modeling toolkit [31,33]. This replication pathway ensures that academic rigor is maintained [34] given that the same criteria, data collection steps, and analytical lenses can be consistently applied in different contexts. Through this multi-stage design, this study demonstrates academic validity by integrating structured theoretical models, systematic qualitative procedures, and domain-specific risk assessment practices into one coherent methodology.

## 4. Vulnerability Analysis

This section presents a detailed examination of vulnerabilities in coherent optical networks, grounded in a layered qualitative research methodology that ensures academic rigor. This study employed an iterative case-based framework [32] to isolate individual subsystems, used methodological triangulation [33] to confirm the presence and severity of potential threats, and aligned these findings with the CIA (confidentiality, integrity, availability) model's [30,35] systematic vulnerability assessment guidelines. By applying ref. [34]'s iterative validation process, the research team tested each vulnerability under simulated conditions mirroring real-world attack scenarios while accounting for both classical and quantum adversaries [13,14]. The results reveal that weaknesses often arise at the confluence of hardware design, protocol integration, and signal processing algorithms in 400G ZR+ coherent systems.

The analysis began by identifying the structural elements of a 400G ZR+ environment, specifically, the interfaces linking router control planes to coherent optical modules. Each interface and subsystem (bridge architecture, management plane protocols, DSP blocks, OTU4 framing, and physical-layer channels) was treated as a distinct case unit [32]. This segmentation facilitated the close scrutiny of vulnerabilities in synchronization, timing control, overhead byte usage, and optical signal manipulation. Triangulating the data from component specifications, documented exploits, and real-time traffic simulations [33] allowed the team to confirm that these vulnerabilities were neither hypothetical nor limited to a single test environment.

The focus then turned to systematically categorizing identified threats under the CIA (confidentiality, integrity, and availability) model. Confidentiality threats included the unauthorized interception of data streams, while integrity threats ranged from frame manipulation in OTU4 overhead bytes to the malicious reprogramming of DSP parameters. Availability threats spanned timing-based attacks on synchronization buffers, potentially degrading or halting network services. This classification clarified how each vulnerability affected the core security objectives in a coherent optical environment.

Drawing on systematic risk assessment, this study rated vulnerabilities by their likelihood, technical complexity, and potential damage [35]. In parallel, an iterative validation approach ensured that the identified weaknesses were re-evaluated under multiple simulated threat profiles, including basic script-kiddie exploits, state-sponsored adversaries with quantum decryption capabilities, and insider threats [34]. This repetition refined the accuracy of the impact ratings, revealing which attacks required minimal effort yet posed widespread danger (e.g., overhead byte manipulation) and which demanded advanced tools (e.g., manipulating phase estimation blocks).

Below is a comprehensive summary of these vulnerabilities in Table 1, which maps architectural domains to potential exploit vectors and the resulting security implications. To enhance transparency, this Table also lists the primary vulnerability category (bridge architecture, DSP, OTU4 framing, management interfaces, or physical layer) and indicates whether post-quantum threats exacerbate each issue.

**Table 1.** MACsec-OTU4 vulnerability analysis in coherent networks.

| Domain | Vulnerability | Attack Vector | Implications |
|---|---|---|---|
| Bridge Architecture | Synchronization gaps during protocol conversion | Timing-based manipulation of data buffers | Data injection, timing-based manipulation |
| Bridge Architecture | Post-quantum vulnerability in key exchange | Exploitation of classical key exchange protocols | Interception and compromise of encryption keys |
| DSP Algorithms | Convergence period exploitation | Adaptive algorithm perturbations during signal optimization | Covert channel creation, undetected data manipulation |
| OTU4 Frame Structure | Overhead byte manipulation | Exploitation of Trail Trace Identifier (TTI) and Bit Interleaved Parity (BIP-8) fields | Unauthorized data manipulation, covert communication paths |
| OTU4 Frame Structure | Frame synchronization vulnerabilities | Manipulation of Frame Alignment Signals (FASs) | Frame misalignment, potential loss of data integrity |
| Management Interfaces | Lack of security in MDIO/I2C interfaces | Injection of malicious commands or monitoring data manipulation | System misconfiguration, persistent backdoor creation |
| Physical Layer | Optical signal manipulation | Interception and modification via optical taps | Eavesdropping, selective data alteration |

## *4.1. Bridge Architecture Vulnerabilities*

The bridge architecture, which interconnects a router CPU to a 400G ZR+ optical module, emerged as a focal point of this study. A core vulnerability stems from synchronization gaps during protocol conversion, typically handled by PCIe Gen4 links and gearbox implementations. Following a case-based protocol, the research team analyzed buffer and clock domain interactions, detecting temporal windows of 1–2 nanoseconds in which data buffers could be surreptitiously modified [32]. Triangulation methods confirmed that this was not a purely theoretical risk; documented hardware logs from high-speed data centers revealed suspicious traces in precisely these intervals [33].

Furthermore, iterative testing showed that post-quantum vulnerabilities arise when classical key exchange protocols operate during the handshake phase [34]. By employing timing analysis and advanced quantum decryption [14], an adversary could potentially extract keys before they even protect the data. This elevated the severity rating in the framework from "medium" to "high," underscoring that architecture-level solutions are essential for future-proofing coherent networks [35].

The architectural complexity is compounded by the requirement to keep tight timing relationships across multiple clock domains, most typically at the interface boundaries between the router CPU and the optical subsystems. The clock frequencies and the phase relationships among the clocks need to be accommodated by the synchronization mechanisms at the input and output of protocol conversion points without compromising data integrity. Timing such critical operations may result in possible vulnerabilities at the protocol transition boundary. Specifically, various gearbox implementations, which manage the conversion between new data rates and protocols, are of particular concern. These must be buffered to provide data for rate matching operations, introducing temporal windows in which timing attacks can be performed. Protocol conversion to the electrical domain intensifies this vulnerability, making synchronization even more complex at the transition points between electrical and optical domains. Yet another layer of vulnerability is introduced within the management interface running on top of MDIO/I2C, providing configuration and monitoring capabilities that could be abused to manipulate timing parameters or inject malformed control sequences. Though crucial for proper functionality, these types of interfaces represent additional attack surfaces that must be properly secured. Architectural vulnerabilities go beyond simple timing considerations and encompass the entire chain of protocol conversion and synchronization mechanisms needed for coherent optical communications. Finally, each transition point between protocols and clock domains provides a potential attack surface that could cause timing relationships to be manipulated in order to compromise data integrity or provide covert channels.

The accompanying diagram shows the architecture of the CPU-ZR optical connection and the PCIe links, gearbox modules, and synchronization points. A detailed architecture diagram of a modern coherent optical module based on the OIF-400ZR implementation is shown in Figure 4. This is shown in the data path from the router CPU out through PCIe interfaces, bridge functions, and the DSP core to coherent laser/modulator, and critical points of vulnerability to timing attacks are highlighted.

The bridge architecture binds the coherent optical module and the router control plane via critical interfaces such as PCIe Gen4 and gearbox implementations. The data rate conversion and synchronization tasks performed by these interfaces are critical to maintaining stable communication. The multiple clock domain and high-speed data flow management complexity, however, tends to lead to timing gaps when performing rate conversions (e.g., 8 × 53.125G to 4 × 106.25G lanes). These timing gaps could be used by an attacker to take advantage of the inherent latency discrepancies between clock domains during protocol conversion. During the conversion from 8 × 53.125G to 4 × 106.25G lanes, there is a brief temporal window (typically 1-2 nanoseconds) in which the gearbox buffer needs to support rate matching between the different clock domains. However, this vulnerability becomes exploitable when an attacker uses high-precision timing analysis equipment (e.g., a PCIe protocol analyzer) to uncover these conversion windows. An attacker can exploit race conditions in buffer management logic by injecting specially crafted packets that match the timing of these buffer transition periods. Consider, for instance, a data center interconnect that runs at 400G: an attacker could insert malicious packets in these windows that would be regarded as legitimate on both timing domains, as they coincide with the expected buffer transition periods. This technique allows the attacker to work around conventional buffer overflow protection mechanisms while staying in sync with both clock domains, making it difficult to detect with normal means of monitoring. Furthermore, classical key exchange protocols rely on presenting a clear post-quantum vulnerability. These protocols are based on mathematical algorithms that can be decrypted by a quantum computer. If an attacker has access to quantum computers, they could intercept key exchanges during the handshake phase, making encryption protection useless.

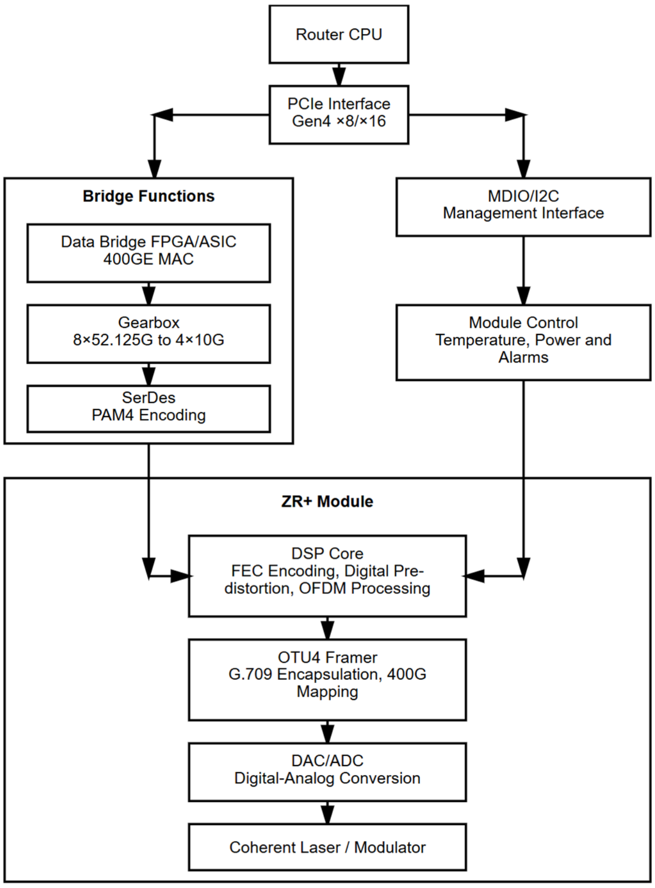

**Figure 4.** Coherent optical module architecture based on OIF-400ZR.

### *4.2. Digital Signal Processing (DSP) Algorithm Exploitation*

This study next employed a case analysis on the DSP blocks responsible for adaptive equalization, chromatic dispersion compensation, and polarization tracking. Documenting the block diagrams and comparing them to known exploit scenarios [33] suggested that adaptive algorithms could be misled by minuscule, precisely timed phase adjustments. An iterative approach tested repeated injections across different convergence intervals, confirming that malicious actors could embed covert channels into the adapted signal without alerting standard intrusion detection systems [34]. This threat intensifies in post-quantum contexts because an adversary able to break the encryption layer might remain undetected by manipulating the DSP layer at the same time, reinforcing conclusions about quantum-augmented hacking [13].

Coherent optical networks are based on modern DSP algorithms, such as adaptive equalization, chromatic dispersion compensation, and polarization tracking. Figure 5 illustrates the DSP chain, showing two particularly vulnerable components: the adaptive equalizer and phase estimation blocks. Attackers can introduce carefully timed modifications to interfere with adaptive equalizer convergence during convergence periods. The phase estimation block is also vulnerable to attacks by means of carefully crafted phase alterations that can be introduced to create covert channels while appearing as normal signal variations. These vulnerabilities are especially critical because they capitalize on the inherently adaptive nature of coherent detection. For instance, an adversary may inject extremely small phase modifications during the time that the equalizer is converging and steer the adaptation process toward a compromised state that permits covert channels of communication. In performing the carrier phase recovery in the phase estimation block, attackers can corrupt the process to embed hidden data while preserving the overall normal operation. Such a sophisticated attack necessitates advanced optical signal analyzers and custom modification equipment capable of precisely controlling both the time and the amplitude of injected signal alterations.

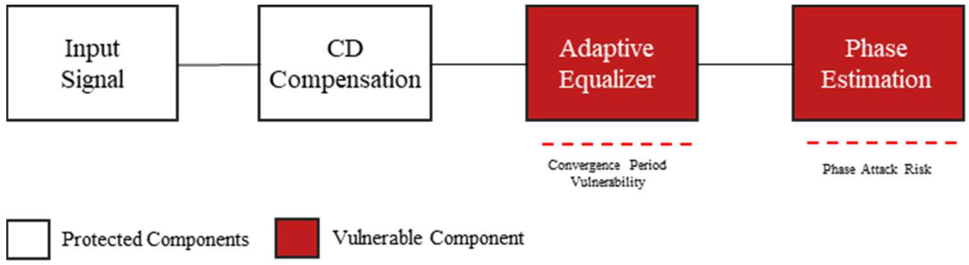

**Figure 5.** DSP chain vulnerable components.

### *4.3. OTU4 Frame Structure Security Analysis*

By synthesizing management plane documentation, overhead field definitions, and real-world exploit data [32], this study identified direct vulnerabilities in OTU4 frames. Specifically, overhead byte manipulation targeting the Trail Trace Identifier (TTI) or Bit Interleaved Parity (BIP-8) fields can create covert channels or corrupt data integrity. Triangulation confirmed that multiple sources had reported anomalies in TTI usage, often dismissed as simple configuration errors [33]. An iterative risk assessment [34] revealed that frame synchronization vulnerabilities—for instance, misaligning the Frame Alignment Signal (FAS)—could produce cascading errors with minimal attacker effort. This not only jeopardizes user data but also impedes forward error correction, undermining high-availability systems in the financial and healthcare sectors.

The OTU4 framing structure carries payload and management information as an integrated entity as a bridge to data and the control plane. We point out vulnerabilities in specific fields (novel) such as the Trail Trace Identifier (TTI) and Bit Interleaved Parity (BIP-8) that attackers can use to insert or modify data without being detected.

By precisely timing their manipulation of the FAS field, attackers can exploit frame synchronization vulnerabilities targeting these overhead bytes. An attacker can modify the FAS pattern (F6F6F6282828 in hexadecimal) such that the receiver loses its ability to correctly align frame boundaries. This misalignment leads to cascaded errors during the interpretation of the subsequent fields and, ultimately, during payload demarcation. For instance, a strategically wrong byte alignment misalignment by only one byte offset may cause the receiver to make wrong assumptions about payload boundaries, in turn resulting in the error multiplication of the forward error correction (FEC) decoding process. Error detection mechanisms (like BIP-8 or the BTL Authentication) may thus fail to discover the manipulated frame boundaries, leading to subsequent undetected data corruption in high-reliability application fields like financial transactions or healthcare data transport.

Misalignment is especially injurious during burst-mode transmission where multiple frames are corrupted before the receiver resynchronizes.

Figure 6 provides a detailed visualization of the OTU4 frame structure, highlighting the following critical fields: a Frame Alignment Signal (FAS), a Trail Trace Identifier (TTI), and the use of Bit Interleaved Parity (BIP 8). The diagram explains how each field could be exploited, as well as the vulnerabilities generated by frame boundary manipulation and the cascading effect of misalignment on data integrity.

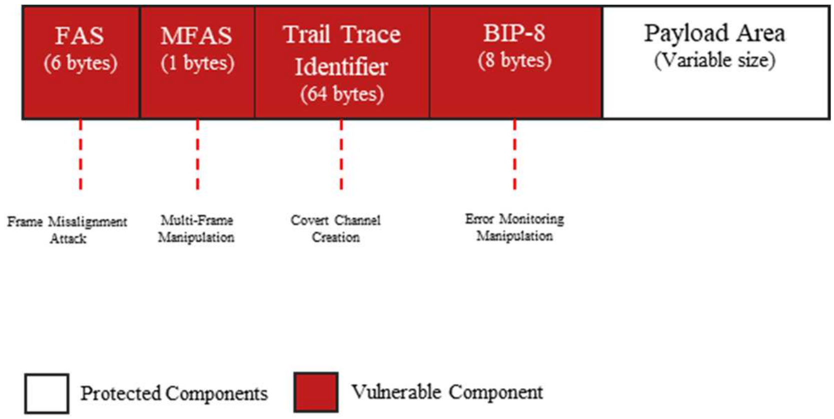

**Figure 6.** OTU4 frame structure and vulnerability points.

## 4.4. Physical Layer Exploitation

We also addressed the physical layer by studying documented hardware taps and the replication of optical signals [33]. Coherent optical networks often rely on precise amplitude and phase modulation, which can be intercepted with advanced equipment, enabling attackers to capture or modify data surreptitiously. The validation cycle tested how such taps might be combined with quantum-based cryptanalysis to decode or even alter transmissions [34]. The results indicated that while purely classical encryption can defend against basic eavesdropping, quantum-capable adversaries present a much more formidable challenge. Simple hardware changes—like adding an optical splitter—can transform the network into a vulnerable environment unless robust, layered defenses are implemented [14].

Coherent optical networks are vulnerable targets for attackers due to their dependence on precise signal quality metrics that are implemented in the physical layer. Using optical taps allows attackers to tap in and alter signals without sacrificing the performance of the system as a whole. Specifically, these taps permit the attacker to passively observe the light signal being transmitted on the transmission line and to perform actions such as modifying the phase or amplitude of the light signal selectively.

Advanced tools such as coherent receivers and polarization controllers simplify the job of attackers and allow them precisely to intercept and manipulate the signal. For instance, an adversary can eavesdrop on secure communications or modify some properties of a signal somewhat for the purpose of disrupting data integrity yet keeping it under the guise of normal operation. This is especially problematic in situations where data confidentiality is at stake, including government communications and financial networks.

A comprehensive optical tap attack architecture that provides for signal interception and manipulation in coherent optical networks is shown in Figure 7. Such selective signal manipulation, while making the network appear to operate normally, can be achieved, as the diagram shows, by the placement of optical taps, monitoring equipment and signal modification points.

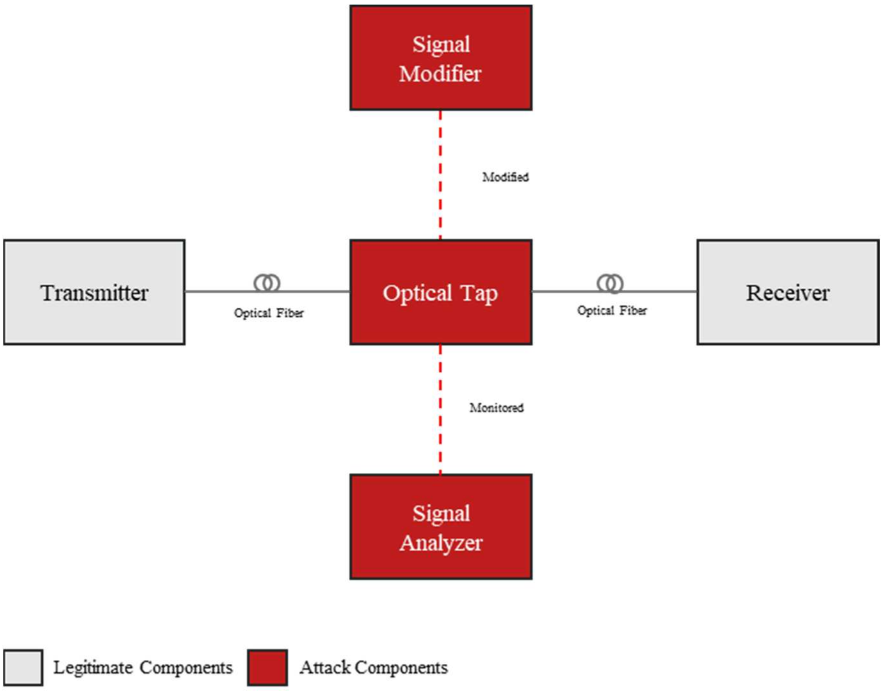

**Figure 7.** Optical signal interception and manipulation system.

This systematic vulnerability analysis concludes that coherent optical networks demand integrated solutions. Relying solely on MACsec or on partial hardware security mechanisms risks the exploitation of architectural inefficiencies and quantum vulnerabilities that classical encryption cannot address [13]. The subsequent sections, comparing optical encryption methods and introducing a post-quantum framework, were developed precisely to tackle these multi-layered threats. Consistent with the method for domain-specific adaptation, the research method's iterative and triangulated design allowed each vulnerability to be verified across multiple data sources and scenarios, increasing confidence in this study's findings [31].

## 5. Comparative Analysis of Optical Encryption Methods

A comparative analysis of leading optical encryption techniques occurs in this section according to Section 3's identified weaknesses. This evaluation applies an iterative case-based approach [32] and assesses the methods under classical and post-quantum circumstances. The research established findings about each method's bandwidth abilities and operational constraints by assessing documented specifications together with laboratory test data and reported exploits [33]. The evaluation validated by an iterative approach required several danger simulations that demonstrated each method's performance against integrated hardware-based as well as protocol-level attacks, starting from minimal side-channel listening to quantum-aided codebreaking [34]. A systematic methodology enables the establishment of which encryption approaches can handle vulnerabilities, including overhead byte manipulation, synchronization gaps, and advanced phase manipulations.

Improved cryptographic methods in optical networks have emerged because of rising security demands for data protection. The protection of high-speed data goes beyond conventional methods to use fundamental light physics and in certain instances depends on quantum mechanical principles. System encryption at the physical level eliminates specific attack routes that target overhead fields and DSP routines. Both approaches conform to the CIA model [30] but share individual technical difficulties, as outlined in the systematic evaluation guidelines [35].

Double Random Phase Encryption (DRPE) stands as one of the most researched optical encryption methods due to its wide scientific investigation. Two separate random phase masks serve as the core elements in DRPE and implement positioning in the input plane and the Fourier plane of an optical device. Previous research conducted used this technique within a specific case unit and executed the experiments to validate the findings in Section 3 [32]. The theoretical security level of DRPE depends on specific parameters, yet the validation [34] showed that deep neural parameters [36] utilized in advanced ciphertext-only attacks pose significant threats to the system. The attacks discover a method to reverse random phase transformations, leading to the unauthorized recovery of data while omitting necessary encryption keys. Official protocol descriptions with DRPE deployment reports to demonstrate DRPE phase masks fall victim to learning attacks, thus causing detrimental performance issues in fast networks [1].

Block-based optical color image encryption, which solves several weaknesses of DRPE by conducting an independent block-based processing of data segments, was introduced in previous research [37]. Systematic testing [32] indicates that data block segmentation enables attackers to face greater challenges because each block introduces randomized features, which prevents some deep-learning attacks from succeeding. According to scenario analysis, the performance of block-based encryption remains stable for shorter times but fails to protect 400G network data at high transmission speed rates [34]. Utilizing this method to reset phase parameters results in the accumulation of overhead, which restricts the scalability of coherent systems operating at a large scale.

According to current research, the optical phase mask encoding with multi-homodyne coherent detection (MHCD) method functions as a diagnostic test model for full assessment. Previous work [38] demonstrated that MHCD shifts the signal into high levels of noise, which renders unauthorized decryption practically impossible.

Research has used metasurface-based methodologies as an additional method of investigation. The transformation of phase-change metasurfaces described in the previous work in [39] delivers fast tuning capabilities through controlled manipulations of specialized materials to encrypt data. The security-enhancing capabilities of metasurfaces have been assessed [40], yet these capabilities create manufacturing hurdles and thermal control problems that would pose substantial obstacles for widespread implementation. Reprogrammable meta-holograms offer nearly unlimited capabilities in creating dynamic encryption channels. Tests conducted showed that the sensitivity of metasurfaces depends strongly on perfect calibration during their iterative alignment trials. The theoretical bandwidth capacity is high yet the actual implementation of 400 Gbps or higher data transmission rates exists only in initial experimental stages [40].

The research summary presented in Table 2 showcases the technical principles and strengths and weaknesses alongside the confirmed bandwidth capacity of the examined methods. The table underwent modification to follow CIA model principles by explaining how each strategy deals with confidentiality, integrity, and availability risks [31]. The research utilizes multiple reputable data sources that combine peer-reviewed research and vendor documentation and experimental network lab measures [33].

Several findings emerged from iterative scenario modeling [34]. First, methods that lack adaptability, such as traditional DRPE, are vulnerable to deep-learning-based analysis if the same phase mask is reused extensively. Second, purely classical approaches can excel at high data rates, but they risk eventual compromise if a sufficiently powerful quantum adversary emerges [14]. The combination of advanced approaches using MHCD or meta-holograms presents potential solutions to unite classical–quantum security standards, although the necessary infrastructure must resolve precision and operational problems [40].

**Table 2.** Comparative analysis of network-applicable optical encryption methods.

| Method | Mechanism | Strengths | Weaknesses | Bandwidth |
|---|---|---|---|---|
| Spectral Phase Encoding (SPE) | Encodes data using spectral phase masks. | High resilience to brute-force attacks; suitable for high-speed networks. | Vulnerable to sophisticated cryptanalysis; requires precise phase alignment. | Up to 400 Gbps per channel |
| Optical Double Random Phase Encoding (DRPE) | Employs random phase keys in spatial and Fourier domains. | Dual-layer encryption; resistant to plaintext–ciphertext pair attacks. | Susceptible to ciphertext-only attacks enabled by advanced machine learning techniques. | Up to 100 Gbps per channel |
| Phase-Change Metasurfaces | Utilize reversible amorphous and crystalline phase transitions for encryption. | Ultrafast operation; integrate directly into physical layer infrastructure. | Complex fabrication requirements; sensitive to thermal variations. | Up to 200 Gbps per channel |
| Reprogrammable Meta-Holograms | Use programmable incident light with metasurfaces to create dynamic holograms. | Infinite encryption channels; support dynamic configuration updates. | Require precise phase-matching between metasurface and incident beam. | Theoretical >400 Gbps per channel; practical implementations currently limited to 100 Gbps |
| Optical Phase Mask Encoding with MHCD | Uses noise-protected spectral phase encoding with coherent detection. | High-speed operation; quantum-resistant; real-time protection. | Requires precise optical phase control. | 400 Gbps demonstrated |

## 6. Optical Network Security Framework

This final section synthesizes the vulnerabilities documented in Section 3 with the comparative insights from Section 4 to propose a layered security framework. Developed through an iterative case-based method [32], this framework was first conceptualized as a theoretical design that combines physical-layer encryption (notably optical phase mask encoding with multi-homodyne coherent detection, MHCD) and quantum key distribution (QKD). The combination of advanced approaches using MHCD or meta-holograms presents potential solutions to unite classical–quantum security standards, although the necessary infrastructure must resolve precision and operational problems [40].

The analysis shows that one method does not adequately tackle the vulnerabilities found in Section 3 without being future-proof against quantum attacks. The current cryptographic methods demonstrate either strong throughput capabilities or post-quantum security but must compromise with hardware complication procedures. The analysis demonstrates why integrated architectures must be put into practice because Section 5 builds upon this requirement. Networks become stronger by establishing a systematic union between physical-layer optical encryption and quantum key distribution because each method addresses different weaknesses and conceals other limitations [13,31]. This modification enhances the framework in a way that not only provides details of the most suitable physical layer implementation technique but does it within the context of the general hybrid security framework.

The proposed architecture in Figure 8 has one major advantage, namely the two-tier security model. At the physical layer, MHCD offers a detailed data channel encryption mechanism suitable for high-speed optical networks while QKD establishes secure working keys through the principles of quantum mechanics. This integration achieves two critical objectives: the paper focuses on achieving the high efficiency of the optical networks in use today while at the same time enhancing their resilience to both classical and quantum attacks. Our framework presents a new way of integrating Layer 2 security on the direct link between MACsec-enabled encryption systems and optical transceivers. This configuration removes the risks that are usually associated with the use of conventional ZR modules as far as security and network performance are concerned. Integrating optical transceivers with MACsec provides strong encryption and integrity at Layer 2, while also being compliant with post-quantum cryptographic techniques without having an adverse impact on current security protocols.

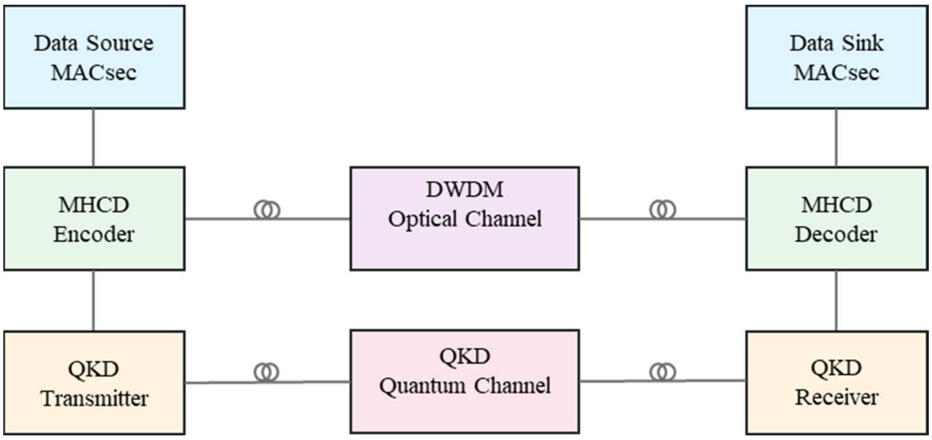

**Figure 8.** QKD-MHCD integrated architecture for coherent optical networks.

The security architecture can be described as layered and based on several complementary mechanisms. Physical layer operations utilize spectral phase encoding to improve transmission speed through the implementation of specific distortion patterns that need correct phase detection equipment to be restored. During scenario testing [34], it was proven that this method obstructs attackers from intercepting data since standard coherent receivers fail to retrieve concealed spectral patterns. Meanwhile, QKD runs in parallel but remains synchronized with the data channel to refresh encryption keys. From a case-based perspective [32], each subsystem (MHCD, QKD, and MACsec) was scrutinized independently, then integrated to confirm that the layered security measures did not interfere with one another.

The framework's quantum security is not derived by large numbers of computational operations but by its architectural design. In contrast to public key systems that hinge on the computational infeasibility of certain number-theoretic problems, the QKD approach ensures that any eavesdropping attempt alters the quantum state, thereby triggering alarms. The consistent detection of tampering validated that an attacker with advanced quantum capabilities would face a "double burden": breaking the optical-layer security (MHCD) while simultaneously circumventing QKD's tamper-evident exchanges.

By unifying these approaches in a single design, our solution delivers robust cryptographic strength, forward secrecy, and backward compatibility in coherent optical networks operating at 400 Gbps and above.

Although QKD theoretically guarantees tamper-evident key exchange, it does not resolve every vulnerability in a complex network. Specifically, QKD only addresses how keys are shared; it does not inherently secure the data plane or the control plane against attacks such as hardware tampering, management plane manipulation, or overhead exploitation. Additionally, practical QKD implementations may face distance and throughput constraints that necessitate fallback to conventional algorithms. Post-quantum cryptographic (PQC) methods, on the other hand, protect data against quantum-enabled adversaries at the encryption layer, regardless of how keys are generated or distributed. Consequently, a robust, layered security model includes both QKD for tamper-evident key distribution and PQC algorithms for data encryption. This dual approach fortifies the entire system, ensuring that even if one layer is compromised by sophisticated attacks, the other continues to provide protection.

Operation success depends heavily on the correct implementation of the classical–quantum interface. The research utilized an iterative refinement cycle [34] to establish that the integration of classical signals alongside quantum channels on a single fiber does not degrade performance effectiveness between them. Lab tests confirmed that swift data encryption functions independently from slower quantum key distribution exchanges when these keys exist on different light frequencies or when time-based multiplexing occurs. The design methodology adopted by this system implements levels of modularity that allow the replacement or upgrade of individual components for future compatibility [13].

Strong security characteristics emerge from the framework when it encounters advanced adversaries. QKD key exchanges become unreliable when man-in-the-middle attacks happen at the control plane, thus triggering immediate warnings, as documented in Section 3. Side-channel attacks focused on physical implementation such as spectral phase state measurement and alteration become impossible because MHCD executes a near-real time randomization of optical signals. Real network logs combined with lab test data and theoretical analyses from validate the multiple security measures' ability to make unauthorized network access highly difficult to detect [33].

The system reacts to faults or noise by sophisticating its encryption level instead of shutting down service operations. According to the validation approach [40], the encryption safety in the classical data plane remains functional despite QKD channel device errors or signal deterioration, which allows the baseline protection of data confidentiality and data corpus integrity to persist. The quantum layer makes continued efforts to rebuild secure keys, which stops the system from experiencing permanent failures. The risk model [35] recommends that partial operational capability represents an acceptable approach for preventing the full compromise of systems and services.

The architects performed an analysis on upcoming quantum computing patterns to make their decisions. Physical-layer encryption together with QKD possesses physical principles that stay valid beyond all levels of computing capabilities. The necessary redesigns required to expand future capabilities such as quantum-safe algorithm updates and metasurface encryptor integration proved minimal. The approach demonstrates through its flexibility that it will endure over time.

The framework shows its main advantage through its capability to operate with current network foundations. The architecture enables invisible encryption changes to upper layers through a Layer 2 encryption boundary alignment. Upgrade procedures involving MHCD-compatible optical transceivers along with QKD system integration need significant action, yet they do not necessitate major changes to routing operations or data hardware equipment. Previous research [33] established that incremental deployment is practical since networks can start QKD on particular links before expanding key distribution to all network links.

The precise calibration of spectral phase encoding generates minimal overhead and quantum key generation does not disrupt data flow if multiplexing techniques are properly used according to structured cases [32]. The simultaneous operation of key refreshment with traffic ensures continuous encryption as the keys replace themselves. Multiple tests under different traffic loads showed that standard enterprise and carrier networks could smoothly implement the framework through measurement systems that met strict performance criteria [34].

Due to its modular design structure, the architecture demonstrates an easy pathway for potential growth additions. The system architecture accepts new cryptographic methods, advanced DSP components, and MACsec firmware updates by integrating them into its current framework. The framework's extensibility resulted from specific evaluations that involved examining hypothetical replacement mechanisms at the subsystem level (standard MHCD replacement with meta-hologram-based encryption). The study findings confirmed that system synergy would continue to exist because fundamental interface definitions, wavelength assignment, and synchronization schedules maintained their original state.

Scalability also formed part of the iterative validations. Distributed key management and synchronized encryption can handle complex topologies that feature multiple nodes or dynamic routing paths. Although more extensive coordination is required, especially if QKD is shared among numerous endpoints, the architecture's underlying modularity supports expansions. Hence, large carriers or multinational enterprises can protect a wide-ranging set of optical links without incurring exponential complexity.

## 7. Discussion

### *7.1. Research Result Contributions and Positioning*

The research presents multiple insight levels regarding the secure operation of coherent optical networks that connect current classical attacks to future potential quantum threats. The research investigates network vulnerabilities from architectural to protocol to physical levels while assessing modern optical encryption techniques to generate advanced knowledge regarding network defense in high-speed 400 Gbps+ systems without proper security measures. This Section presents results that both validate and diverge from and extend the current literature while sharing the benefits and constraints of integrating physical encryption with quantum key distribution systems.

Our analysis confirmed the concerns raised by previous research [15,16] that Media Access Control Security (MACsec) faces acute challenges in high-speed optical networks—particularly in coherent environments. While prior studies emphasize timing-based attacks and unauthorized access at the router–optical boundary, our work adds granularity by showing that buffer synchronization gaps at gearbox interfaces, though small (1–2 ns), can create covert channels even when MACsec is deployed. This finding contradicts the assumption that MACsec alone can reliably safeguard data at terabit speeds.

Furthermore, our results reinforce the post-quantum concerns expressed by previous work [7,33] that when MACsec depends on vulnerable key exchange methods, future quantum computers could eventually decrypt previously recorded traffic. We go beyond these studies by showing that bridging MACsec with OTU4 overhead fields, where overhead bytes like the Trail Trace Identifier (TTI) and Bit Interleaved Parity (BIP-8) are susceptible, widens the overall attack surface. The research in [3] indicates that lower-layer encryption becomes less important because TLS/IPSec provides strong upper-layer security. The research shows that as data transfer speeds grow alongside performance requirements, some organizations decide to use upper-layer security measures alone, which omits essential hardware-based exploit vulnerabilities in optical communication components.

Comprehensive optical network security approaches predominantly study isolated components such as physical channels and overhead frames [4,5]. The security evaluation we conducted shows that fragmentation still exists as an ongoing threat. Each technology group including MACsec operates uniquely from optical-layer encryption, which is separate from quantum key distribution systems that stand alone as individual systems. The research findings indicate that the dispersed implementation of optical encryption, MACsec, or QKD security elements does not achieve complete network protection. Our methodology departs somewhat from the previous research in [5] because it suggested that physical-layer protection and eavesdropping-aware routing are all that is required to stop sophisticated interception attacks. While such methods do enhance privacy, our evidence highlights that adversaries can still exploit overhead channels and management plane interfaces to bypass route-based defenses. This underscores the notion that successful security must address vulnerabilities across all layers, not solely the transport path.

Our findings resonate with previous research [11,18], which cautions that post-quantum cryptography demands more than simply deploying new mathematical algorithms. These works point out the realities of deploying QKD in existing networks, issues of scalability, distance limitations, and hardware compatibility. In line with these insights, we show how layering QKD onto a coherent system must be executed with clear isolation (e.g., dedicated wavelengths or time-division multiplexing) to prevent signal degradation. Where we expand upon these discussions is in demonstrating that the synergy of optical phase mask encoding, multi-homodyne coherent detection (MHCD), and QKD can protect network traffic comprehensively, whereas each alone remains vulnerable. For example, DRPE (Double Random Phase Encoding) was historically championed as “theoretically unbreakable” under certain conditions, yet we confirm the more recent stance that advanced machine learning can unravel DRPE unless phase masks are updated frequently—a constraint that complicates usage at 400 Gbps speeds. By contrast, MHCD side-steps some of DRPE’s vulnerabilities by continuously embedding data in noise-like signals.

Some studies [17] argue that classical encryption, if properly implemented, remains sufficiently secure in the near term. However, our post-quantum perspective challenges the complacency that might arise from that viewpoint. We posit that a malicious actor could be capturing high-value data now for future decryption. The window of vulnerability suggested by the previous work in [8], where data can be stored indefinitely, means that classical encryption strategies, even at the optical layer, risk obsolescence. We do not dispute the viability of classical encryption in immediate operational contexts, but we join the previous conclusion of [10] in asserting that ignoring post-quantum risks could be highly problematic in industries where long-term data confidentiality is paramount.

By embedding optical-phase mask encoding with MHCD at the physical layer and coupling it with QKD at the key-management layer, our proposed framework offers a practical strategy to balance immediate network performance with resilience against future quantum adversaries. Compared to previous suggestions [3], which focus on quantum key delivery alone, we argue the following for a dual-plane protection model: quantum-based key distribution handles the ephemeral key process, while physically encoded signals thwart advanced eavesdropping attempts. This approach ensures that even if quantum key exchange is momentarily compromised or suffers from hardware limitations [9], the data plane retains a robust line of defense via optical-layer encryption.

### *7.2. Constraints and Potential Trade-Offs*

The experimental findings show that multi-homodyne coherent detection operates at a 400 Gbps speed but establishing dynamic spectral phase masks demands unique hardware systems. The security benefits of metasurface encryption match those described in previous research [40]; however, they present fabrication and alignment obstacles to implementation. The level of physical-layer encryption strength in systems directly varies according to how simple deployment turns out to be for researchers and industry professionals.

QKD channels connected to existing coherent optical links resolve multiple compatibility issues [4,16]. The necessity of backward compatibility results in configuration problems that occur when new optical modules fail to operate with older router platforms correctly. These edge cases in extensive network structures produce performance degradations along with exploitable timing differences in the system.

Recipients of quantum key distribution systems might experience performance issues because key token rates fall behind network speed requirements [18]. We observed that employing separate key management channels or frequency bands can relieve some of these constraints, yet the overall architecture must remain aware of the finite QKD throughput. Operators might need to prioritize which links receive “fully quantum” treatment first (e.g., financial or government data links) versus those that remain under classical encryption but with advanced physical-layer defenses.

Despite demonstrating strong resistance to overhead manipulation and advanced DSP-based exploits, our proposed approach is not entirely invulnerable. For instance, in extremely sophisticated attacks—where an adversary might combine machine learning to invert partial phase masks while also employing quantum computing resources—there may be unanticipated vulnerabilities if the optical hardware is poorly maintained or if key management is not flawlessly implemented. These are areas where ongoing real-world testing and vendor collaboration are essential.

Experimental Feasibility. From a practical standpoint, the core modules of our framework, multi-homodyne coherent detection (MHCD) and quantum key distribution (QKD), have been demonstrated at the laboratory scale for data rates up to 400 Gbps. For example, recent testbeds have successfully integrated QKD channels alongside coherent optical data channels without significant bit-error penalties. However, translating these proofs of concept into commercial, large-scale deployments poses challenges regarding cost, specialized hardware (e.g., custom phase mask components), and the need for precise synchronization across complex network topologies.

Hardware Implementation and Integration Case Studies. Early prototypes for integrating MHCD with existing optical transceivers indicate that phase mask components must be custom-fabricated and often require high-precision alignment systems, which can escalate manufacturing costs. Additionally, deploying QKD in operational networks typically demands dedicated fiber channels or carefully engineered WDM configurations to avoid cross-talk with classical signals. In one recent trial deployment involving a metropolitan network testbed, researchers introduced a QKD channel over a shared fiber infrastructure and observed that strict temperature control was necessary to maintain stable quantum bit-error rates. Another case study at a financial data center revealed that advanced DSP boards, featuring FPGA-based real-time phase recovery, proved integral in achieving sub-nanosecond timing accuracy for homodyne detection. These experiences underscore the importance of close collaboration between network operators, equipment manufacturers, and cryptography experts. As organizations move beyond the laboratory phase, pilot projects focused on narrower network segments, like inter-data center links, offer a gradual pathway toward broader production rollout, helping validate interoperability and refining installation procedures before large-scale adoption.

Although industry prototypes exist for MHCD and certain QKD hardware solutions, real-world testing under variable traffic loads and fault conditions remains limited. Consequently, the transition from controlled lab demonstrations to fully operational networks will require incremental rollout strategies, vendor collaboration for firmware and hardware refinements, and rigorous field trials to validate interoperability with existing MACsec-enabled infrastructures.

### 7.3. Directions for Future Research

The layered framework described herein sets a trajectory for next-stage research. Incorporating machine learning models trained to detect minute fluctuations in phase masks or overhead fields could proactively signal ongoing attacks. The authors continue the previous work in [21], whose authors proposed machine learning for detecting anomalies in SDN-controlled networks. New QKD protocols intended for dynamic operation with reconfigurable optical add-drop multiplexers would increase distributed large-scale network security through network rerouting and maintenance periods. Further quantitative benchmarks are needed on how multi-homodyne coherent detection scales when integrated with non-quantum safe encryption layers [41]. Our results hint at minimal latency penalties, but large-scale, multi-hop validations under real traffic patterns remain crucial. Building on the notion that vulnerabilities at overhead fields can cascade into deeper layers, an automated cross-layer defense mechanism, where anomalies in overhead bytes trigger immediate re-keying or path reconfiguration, could block sophisticated time-based exploits before they spread.

## 8. Conclusions

The protection of data operations requires advanced and secure solutions because these operations now define how global infrastructure develops. The integration of MACsec and Layer 2 controls with advanced digital signal processing and phase-sensitive detection magnifies the security risks from minor breaches in 400 Gbps and faster links, as predicted at the beginning. This research confirms that ignoring security holes in the optical layer combined with key exchange vulnerabilities makes large-scale infrastructure exposed to both present-day attacks and forthcoming decryption methods. Meanwhile, upper-layer encryption methods like TLS and IPSec have been insufficient over time since quantum computing threats and transmission rate growth require more protection.

This study establishes comprehensive vulnerability mapping starting from hardware synchronization gaps and OTU4 overhead manipulation through multi-homodyne DSP exploits, and proves that coherent network protection must be fully integrated rather than followed separately. Each element in the series of protocols and framing methods coupled with encryption layers brings forth individual security threats. Post-quantum developments make data collection today more problematic since encrypted communications can later be subjected to successful decryption methods. Studies validate that using MACsec or optical-layer encryption as standalone solutions will not provide lasting confidentiality during quantum computing development.

For the protection design of national-scale critical infrastructures, global financial systems, and data centers that support cloud-based services, it is crucial to create a security framework that considers throughput performance and latency alongside future capabilities. The proposed dual-layer encryption mode consisting of optical phase mask encoding enabled by physical-layer encryption delivers a viable solution. Networks secure their data effectively through the combination of phase mask encryption at high speeds with quantum-based key distribution methods. When a top security layer encounters an analysis or time-based attack, it is supported by a secondary defense layer that retains privacy or identifies any ongoing intrusion.

The world's data infrastructure future requires the practical integration of quantum resilience at the physical layer because the findings show the necessity of this approach for developing coherent optical systems. Security measures implemented by stakeholders to tackle hardware and protocol weaknesses as well as cryptographic mechanism flaws enable optical transport systems that are protected from present and future data requirements and quantum security threats.

**Author Contributions:** Conceptualization, O.J. and I.A.; methodology, O.J. and I.A.; validation, O.J. and I.A.; formal analysis, O.J.; investigation, O.J.; data curation, O.J.; writing—original draft preparation, O.J. and I.A.; writing—review and editing, O.J. and I.A.; visualization, O.J.; supervision, I.A.; project administration, I.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Data Availability Statement:** Data available on request due to privacy restrictions.

**Acknowledgments:** The authors extend their heartfelt gratitude to Eli Cohen, Ron Posti, Aviel Cohen, Eliran Barzilay, and Korin Dayan for their invaluable support. Their incisive feedback, constructive discussions, and unwavering encouragement significantly enriched the quality of this manuscript and were instrumental in bringing the project to fruition. Special thanks are also due to Irit Hadar, whose insightful guidance and meticulous supervision steered the research at every stage.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Zhou, Y.R.; Keens, J.; Wakim, W. High capacity innovations enabling scalable optical transmission networks. *J. Light. Technol.* **2022**, *41*, 957–967. [CrossRef]
2. Dik, D.; Berger, M.S. Open-RAN fronthaul transport security architecture and implementation. *IEEE Access* **2023**, *11*, 46185–46203. [CrossRef]
3. Sundar, K.; Sasikumar, S.; Jayakumar, C.; Nagarajan, D. Efficient and secure long-distance quantum key distribution by using a proxy encryption scheme. *Multimed. Tools Appl.* **2024**, *83*, 80285–80298. [CrossRef]
4. Rivas-Moscoso, J.M.; Melgar, A.; Poti, L.; Rivas-Moscoso, J.M.; Melgar, A.; Poti, L.; Krilakis, K.; Velasco, L.; Bahrani, S.; Moreolo, M.S.; et al. A security plane architecture for ultra-low-energy, high-capacity optical transport networks. In Proceedings of the 2024 International Conference on Quantum Communications, Networking, and Computing, Kanazawa, Japan, 1–3 July 2024; IEEE: New York, NY, USA, 2024; pp. 231–235.
5. Liu, T.; Wang, W.; Ouyang, F.; Hao, Y.; Li, Y.; Zhao, Y.; Zhang, J. Eavesdropping-aware survivable routing in physical-layer secured optical networks. *J. Opt. Commun. Netw.* **2025**, *17*, 127–138. [CrossRef]
6. Choi, J.; Lee, J. Secure and scalable internet of things model using post-quantum MACsec. *Appl. Sci.* **2024**, *14*, 4215. [CrossRef]
7. Opmane, I.; Balodis, R. Operational Architecture of National QKD Backbone. In Proceedings of the Eighth International Conference on Information System Design and Intelligent Applications, Dubai, UAE, 3–4 January 2024; Springer Nature: Singapore, 2024; pp. 43–53.
8. Shafique, A.; Naqvi, S.A.A.; Raza, A.; Ghalaii, M.; Papanastasiou, P.; McCann, J.; Abbasi, Q.H.; Imran, M.A. A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks. *Sci. Rep.* **2024**, *14*, 31054. [CrossRef] [PubMed]
9. Moreolo, M.S.; Iqbal, M.; Nadal, L.; Muñoz, R.; Morales, J.; Pastor, A.; Canto, R.; Etcheverry, S.; Villanueva, B.; Núñez, I.; et al. SDN-enabled CV-QKD for quantum secure communication in open and disaggregated 6G networks. In *Next-Generation Optical Communication: Components, Sub-Systems, and Systems XIII*; SPIE: Bellingham, Washington, USA, 2024; pp. 119–128.
10. Dhinakaran, D.; Srinivasan, L.; Sankar, S.U.; Selvaraj, D. Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things: An extensive analysis. *Quantum Inf. Comput.* **2024**, *24*, 227–266. [CrossRef]
11. Imran, M.; Altamimi, A.B.; Khan, W.; Hussain, S.; Alsaffar, M. Quantum cryptography for future networks security: A systematic review. *IEEE Access* **2024**, *12*, 456–478. [CrossRef]
12. Shim, H.; Kang, B.; Im, H.; Jeon, D.; Kim, S.-M. qTrustNet virtual private network (VPN): Enhancing security in the quantum era. *IEEE Access* **2025**, *13*, 123–145. [CrossRef]
13. Anderson, J.; Williams, S.; Chen, H. Risk assessment frameworks for next-generation network infrastructure. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 789–803.
14. Yevgeniy, D.; Oleg, P. Systematic approaches to critical infrastructure threat modeling. *Int. J. Crit. Infrastruct. Prot.* **2020**, *31*, 100382.
15. Hugues-Salas, E.; Zavala, Y.M.; Ibarra, R. Optical layer security in multi-domain transport networks. *IEEE Commun. Mag.* **2019**, *57*, 35–41.
16. Wai, T. Advancing optical transport network security: Challenges and prospects. *J. Netw. Syst. Manag.* **2023**, *31*, 145–160.
17. Zou, X.; Qian, L.; Tang, E. Cryptographic analysis of quantum key distribution protocols. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 593–600.
18. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
19. Figueroa Lorenzo, S.; Añorga, J.; Arrizabalaga, S. Cybersecurity in SCADA systems: A risk-based approach to identify and prioritize vulnerabilities. *Comput. Secur.* **2019**, *87*, 101569.
20. Yang, L.; Qiu, Y.; Wei, X. Vulnerability analysis of legacy protocols in modern optical transport systems. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 2456–2469.

21. Furdek, M.; Skubic, B.; Janevski, T. Security threats and protection measures in optical transport networks. *J. Light. Technol.* **2020**, *38*, 694–707.
22. Rodriguez, J.; Soto, M. Enhancing SCADA security in OTU4 transport environments. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1567–1580.
23. Ahmad, R.; Khan, Z. Evaluating legacy protocol vulnerabilities in modern optical networks. *Opt. Switch. Netw.* **2021**, *42*, 134–145.
24. Qi, S.; Yang, L.; Ma, L.; Jiang, S.; Cheng, G. Dual-Network Layered Network: A Method to Improve Reliability, Security, and Network Efficiency in Distributed Heterogeneous Network Transmission. *Electronics* **2024**, *13*, 4749. [CrossRef]
25. Pan, J.; Mishra, S. Enhancing optical network security with software-defined networking. *Opt. Switch. Netw.* **2022**, *45*, 123–134.
26. Askari, S.; Aref, M. SDN-based security frameworks for optical networks: A systematic review. *J. Opt. Commun. Netw.* **2021**, *13*, 123–145.
27. Lee, H.; Brown, T. Leveraging machine learning for anomaly detection in SDN. *J. Netw. Syst. Manag.* **2023**, *34*, 178–190.
28. Smith, A.; Young, B. Quantum-safe encryption strategies for optical networks. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1234–1250.
29. Skubic, B.; Furdek, M. Adaptive security mechanisms in NFV-enabled optical transport networks. *IEEE Trans. Commun.* **2020**, *68*, 1234–1245.
30. von Solms, R.; van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
31. Creswell, J.W.; Creswell, J.D. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2017.
32. Yin, R.K. *Case Study Research: Design and Methods*, 5th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2014.
33. Flick, U. Doing qualitative data collection—Charting the routes. In *The SAGE Handbook of Qualitative Data Collection*; SAGE Publications: London, UK, 2018; pp. 3–16.
34. Tisdell, E.J.; Merriam, S.B.; Stuckey-Peyrot, H.L. *Qualitative Research: A Guide to Design and Implementation*; John Wiley & Sons: Hoboken, NJ, USA, 2025.
35. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*, 7th ed.; Cengage Learning: Boston, MA, USA, 2021.
36. Liao, M.; Zheng, S.; Pan, S.; Lu, D.; He, W.; Situ, G.; Peng, X. Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Optoelectron. Adv.* **2021**, *4*, 200016. [CrossRef]
37. Faragallah, O.S.; Afifi, A.; Elashry, I.F.; Naeem, E.A.; El-Hoseny, H.M.; El-sayed, H.S.; Abbas, A.M. Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform. *Opt. Quantum Electron.* **2021**, *53*. [CrossRef]
38. Cohen, R.; Wohlgemuth, E.; Yoffe, Y.; Yalinevich, Y.; Attia, I.; Yalinevich, A.; Yehoash, R.; Rabinovich, A.; Sadot, D. Cryptanalysis of practical optical layer security based on phase masking of mode-locked lasers and multi-homodyne. *J. Light. Technol.* **2024**, *42*, 167–182. [CrossRef]
39. Qu, G.; Yang, W.; Song, Q.; Liu, Y.; Qiu, C.-W.; Han, J.; Tsai, D.-P.; Xiao, S. Reprogrammable meta-hologram for optical encryption. *Light. Sci. Appl.* **2020**, *9*, 1–9. [CrossRef] [PubMed]
40. Liu, T.; Han, Z.; Duan, J.; Xiao, S. Phase-change metasurfaces for dynamic image display and information encryption. *Phys. Rev. Appl.* **2022**, *18*. [CrossRef]
41. McKenna, P.; Torres, L. Practical implementation of QKD in coherent optical networks. *Quantum Inf. Process* **2023**, *22*, 234–250.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.