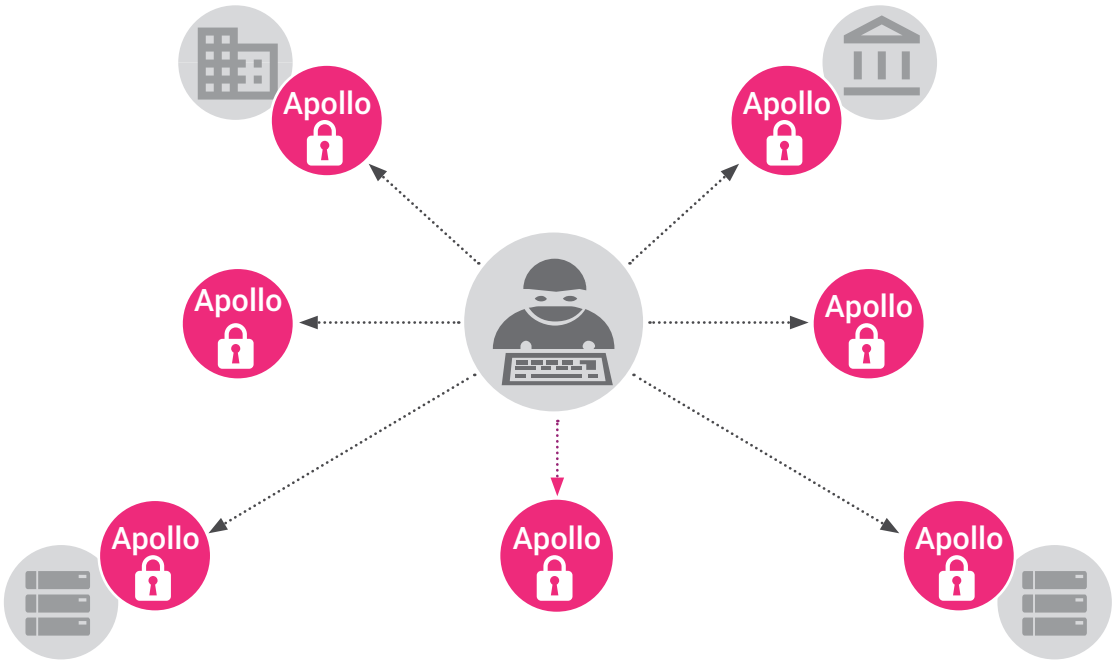
Apollo Layer 1 Optical Encryption

Complete protection against attacks on optical networks

Information must be secured today throughout the enterprise, data center, and interconnecting networks. Optical networks that support all communications traffic and cover the widest geographic areas are susceptible to attacks at multiple points. Layer 1 optical encryption has emerged as a powerful and cost-effective way to protect the integrity of information on optical networks. Ribbon's Apollo optical product line uniquely provides both per-service as well as per-link optical encryption. It covers all applications from point-to-point connections to mesh networks, and Apollo optically encrypted signals can even be transported as alien wavelengths on foreign networks.

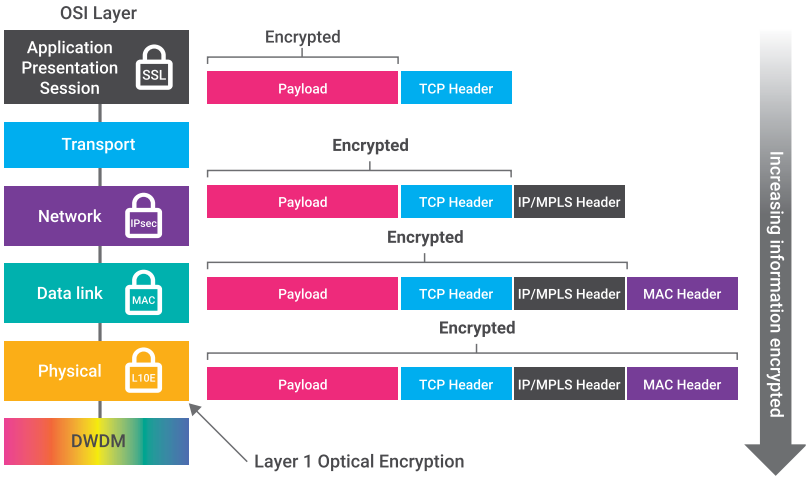
With an External Key Management capability, Apollo makes it easy to extend optical encryption as a value-added offering to enterprise customers that they can administer themselves. For ultimate security against hacking attacks in a rapidly changing world, Apollo supports parallel use of conventional and post-quantum cryptography key exchange mechanisms.

Ultra Low Latency operates at wire speed	**Value Added Service** for enterprise customers	**Standards Compliant** encryption, authentication, physical protection	**Conventional and Post Quantum Cryptography** key exchange



Value of Optical Encryption

Optical networks support all communications traffic and cover the widest geographic areas. They are susceptible to attacks at multiple points and can only be protected against snooping via fiber tapping using Layer 1 optical encryption (L1OE).



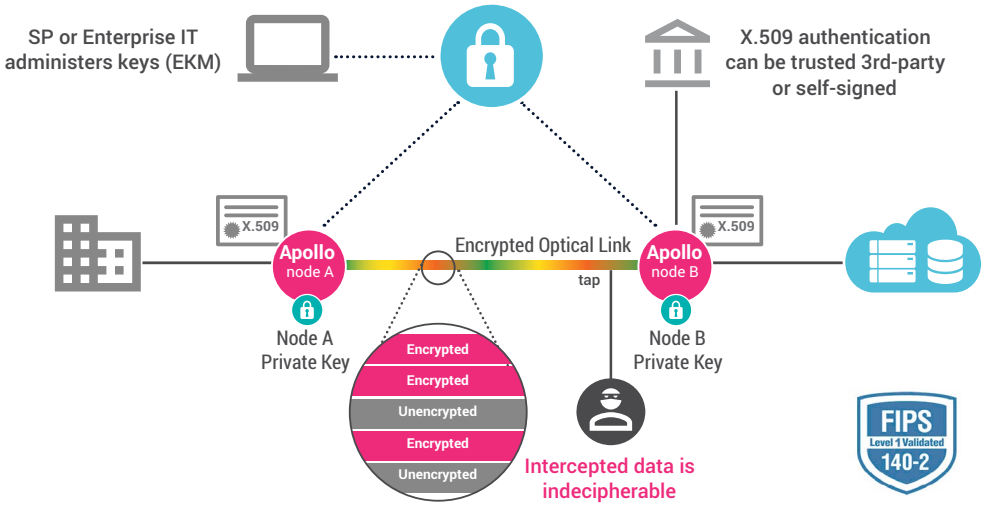
In contrast with Layer 2 or higher layer encryption, optical layer encryption adds no overhead and virtually no latency to the network and can be used to encrypt any service - not just Ethernet-based services. Even when customers use encryption above the optical layer, fiber tapping still exposes non-encrypted addressing information. This means that intercepted optical flows can reveal a customer's network architecture and communications patterns, as well as any data higher up in the OSI stack that is not protected by encryption.

Optical encryption is particularly attractive for businesses because it does not add any latency or overhead performance penalty. This is particularly important for latency-sensitive applications like synchronous data replication, when transactions are not committed until the data is mirrored in two locations.

Similar to the way that a home or a business uses multiple layers of security, optical encryption is increasingly the foundation layer for protecting communications networks. It reassures customers that their information safe, and assists in complying with government regulations and industry standards.

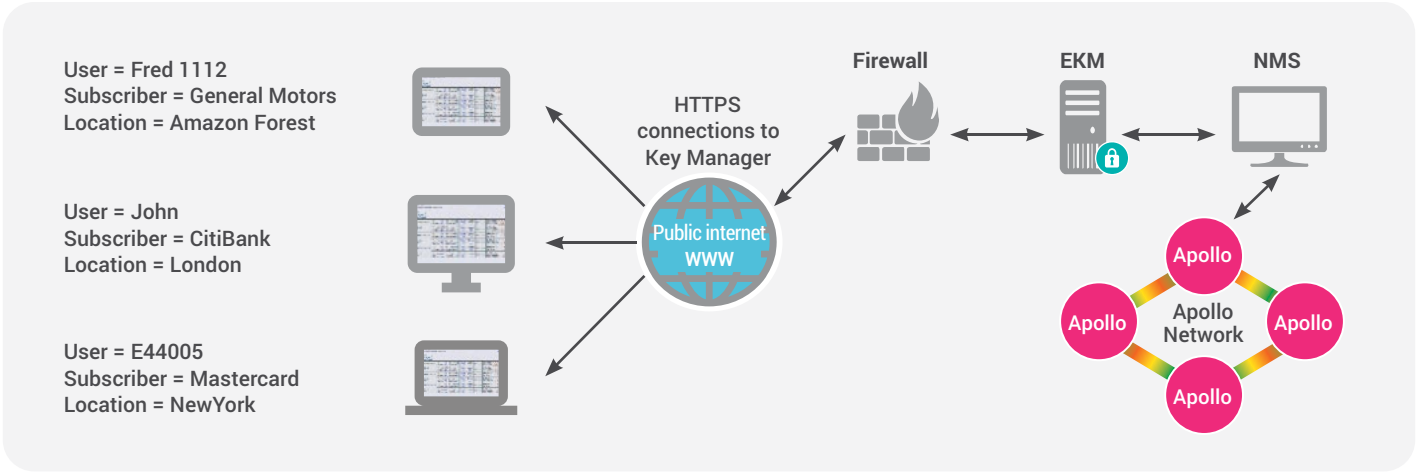
Apollo Optical Encryption Solution Overview

Apollo encrypts the service payload of an OTN-framed signal using standard, highly secure algorithms. The resulting signal can only be decoded by the intended recipient using a key obtained via similarly standard and universally deployed public-key exchange mechanisms. By encrypting only the OTN payload, the DWDM/OTN network can transport client services without interoperability issues. Since there is no information in the unencrypted OTN header about the content of the service, a hacker with access to the optical line cannot determine anything about the types of services carried, much less the content itself.



Key aspects of Apollo's Layer 1 optical encryption solution are:

- **Service transparency.** All services transported by Apollo can be encrypted. These include 1GbE to 100GbE, with hardware readiness to encrypt 400GbE clients, Fibre Channel 1 to 32, and SDH/SONET from STM-1/OC-3 to STM-64/OC-192.
- **Strongest encryption.** The service payload is encrypted using AES256-GCM coding, which is the strongest level of commercial encryption; it takes literally hundreds of years of compute time to decrypt an encoded signal. This is supplemented with an Initialization Vector that ensures no two messages are encrypted the same way, and a Message Integrity Check that safeguards against message tampering.
- **Ultra-secure key exchange.** Key exchange (which is the usual way encryption is attacked) is based on Diffie-Hellman public key exchange, which is the most broadly adopted mechanism in the industry. The private keys, which are part of this mechanism, never the leave the Apollo cards at the end-points of each link, and the process is asymmetric for each direction of the link. In response to emerging threats to this conventional method using quantum computing, Apollo additionally supports parallel operation of a post-quantum cryptography key exchange mechanism.
- **External key manager.** An external key manager (EKM) manages the key exchange process using a very secure transfer technique that does not actually transmit the keys themselves, but calculates them securely on-site. An advantage of EKM is that Enterprises who lease an encrypted optical connection from a service provider can manage all aspects of key administration themselves, from any location via a secure web-based application. It provides total separation between equipment management and key management. EKM allows each end-user to:
  - Enable/disable per-service encryption
  - Monitor the operational status of an encrypted optical service, and modify permissible attributes
  - Obtain security alarms
  - Update login password/profile
  - Rotate keys on FIPS-140-2 tamper proof cards
  - Configure per-service pre-shared secret configuration on FIPS 140-2 cards (future capability)



- **Trusted authentication.** X.509 end-point authentication, which is a part of the key exchange process, can be self-signed, as is often the case in a closed network, or can rely on a trusted 3rd-party.
- **Tampering security.** Apollo provides FIPS 140-2 compliant cards, which provides evidence if anyone tries physically tampering with the encryption and key management mechanisms. This certification is frequently required by government departments and regulated industries.

OTN Transport Encryption Options and Applications

Apollo provides highly flexible DWDM/OTN transport of service interfaces based on a family of small-medium-large platforms that use a common set of line cards for transponder, muxponder, amplification, and ROADM functions. Several cards support Layer 1 Optical Encryption with a focus on encrypting of individual services.

9600 Series
Flexible DWDM / OTN transport

Common cards for all platforms


OPT9603


OPT9608


OPT9624

Double slot cards

- **TM200EN** – Multiservice 200G coherent muxponder with per-service encryption for up to 20 clients
- **TM100_2EN** – Same as 200EN, but with two 100G gray line interfaces
- **TR10_12EN** – 6 x 10G multiservice encrypted transponders, with/without protection
- **'B' versions** – FIPS140-2, Level 2 certified

Single slot cards

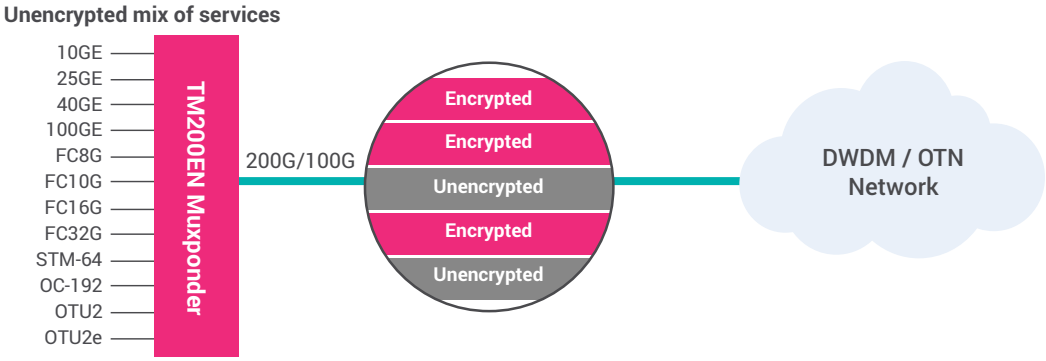
- **TR10_4EN** – 2 x 10G multiservice 10G encrypted transponders

Application – Multiservice Selective Encryption Multiplexed to 200G

The TM200EN provides per-service encryption for up to 100% of the 200G bandwidth, with each service having a unique secure session key for added security. It can support any mix of services up to the 200G limit. The OTN-framed output signal can be transported transparently as a native wavelength over an Apollo DWDM/OTN network, or carried as an alien wavelength over a third-party DWDM network.

Service providers can now install the hardware for a high-speed 200G network on day one and offer both encrypted and unencrypted services to their clients. Existing clients can be upsold at any time to an encrypted service without the need to replace any hardware, and the service can be enabled instantly via software commands. There is no need to install expensive hardware that will sit idly in anticipation of future encryption needs, and there is no need to give away encryption for free on a line, just because one client has requested that feature.

The TM100_2EN provides the same client interface and per-service encryption functionality but multiplexes the services into two cost effective 100G gray interfaces. This is useful to combine lower rate encrypted signals into higher rate 400G+ optical transport.

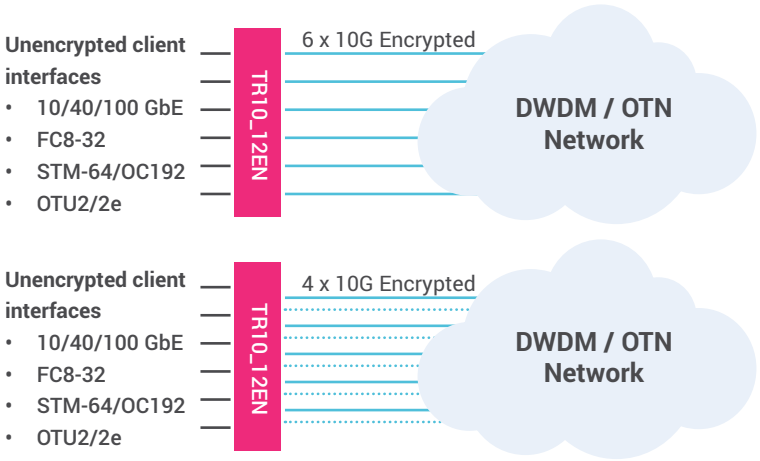


Application – Multiservice 10G Encrypted Transport

The TR10_12EN provides independent encryption of up to six 10G services. Alternatively, it can be configured to provide independent encryption of four line-protected 10G services, with redundant line outputs, eliminating the need for additional protection equipment.

The outputs are standard OTU2e formatted signals that can be transported transparently as native wavelengths over an Apollo DWDM/OTN network, or as alien wavelengths over a third-party DWDM network.

The TR10_4EN provides a compact alternative for two lines of 10G encrypted transport.

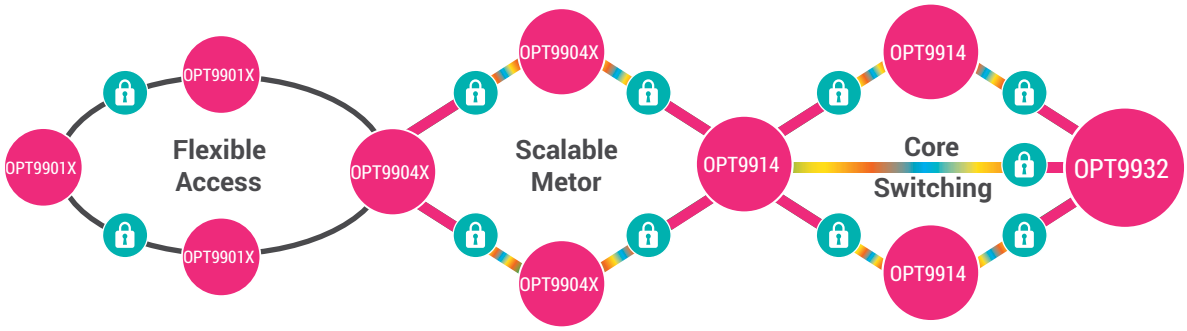


9900 Series - Scalable OTN switching				
Application	Access	Metro	Core L	Core XL
Model	OPT9901x	OPT9904x	OPT9914	OPT9932
Application	Access	Metro	Core L	Core XL
Switching Capacity	400G	2.8T	5.6T Scaled for 14T	16T Scaled for 32T

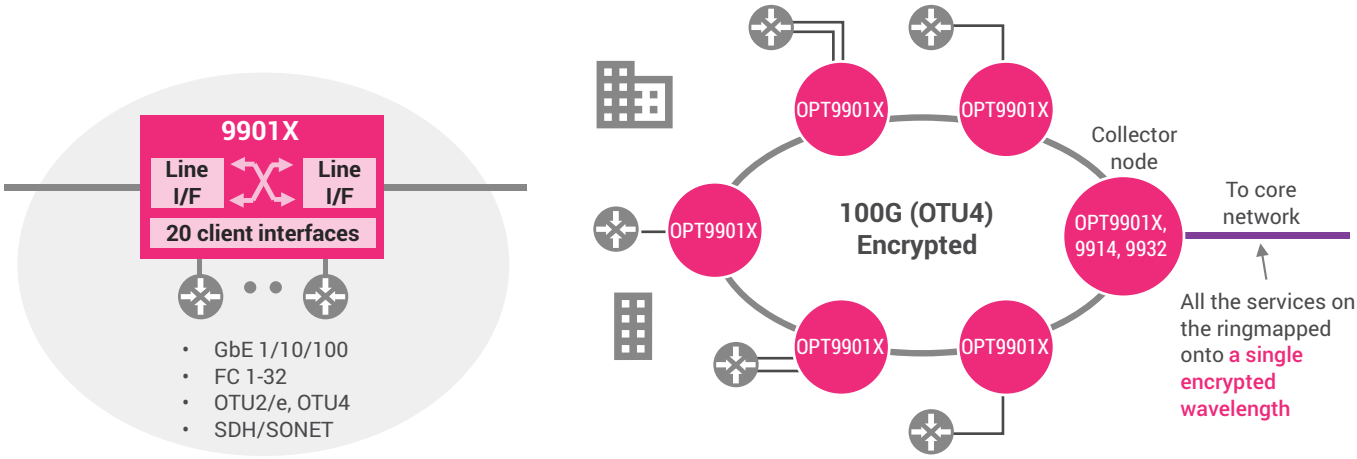
OTN Switching Encryption Options and Application

Apollo provides a scalable access-to-core OTN switching solution that enables automated grooming of services onto wavelengths, rapid service provisioning, and dynamic restoration. Since each link in an OTN switched network contains multiple services groomed densely together, the focus is on enabling the products to interwork with each other seamlessly to provide interoperable end-to-end OTN link encryption. This is enabled by:

- **HIO400EN** – Multiservice card for the OPT9914 and OPT9932 providing 200G encrypted links.
- **MIO200EN** – Multiservice card for the OPT9904X, providing 200G encrypted links. Its integrated switching matrix enables a modular encrypted switching capacity to 800G.
- **MIO700EN** – Multiservice card for the OPT9904X, providing 200G encrypted links. Its integrated switching matrix enables a modular encrypted switching capacity to 2.8T. (Note: This is a future capability of the MIO700 card, which initially is available without encryption.)



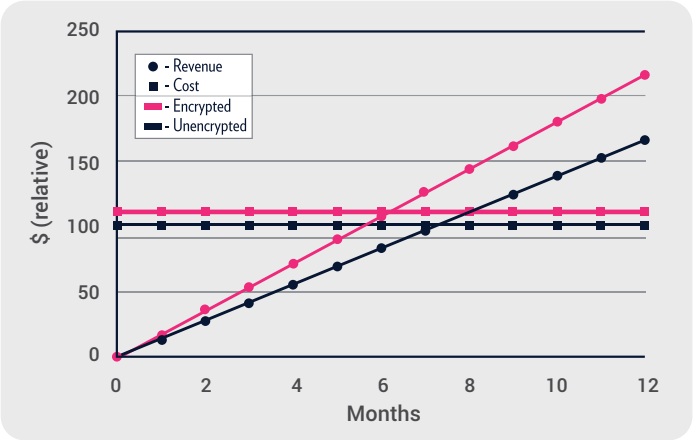
- **9901X** – Access OTN switch optimized to replace muxponders and F-OADMs to flexibly and rapidly provision multiple types of L1 services. The 9901X is a highly versatile platform that supports optical encryption in multiple configurations; both interworking with other OTN switches as well as in a standalone mode. A primary application, illustrated below, is a software-configurable Add-Drop Multiservice Multiplexer on an Access Ring. This gathers and grooms client traffic onto encrypted 100G wavelengths that can be processed end-to-end by Apollo OTN switches.



Optical Encryption as a Service

With an increased focus on security and the ease with which optical layer encryption can be added to any optical service or channel, optical encryption presents service providers with a value-added service offering to business customers. While this is often associated with financial networks, recent high-profile security breaches in Enterprise and Utility networks have made security a priority for other industries as well.

As an example of its value, using normalized pricing for Apollo 10G equipment and industry standard revenue from 10G services, the graph below shows the impact of charging a 30% premium for encrypted 10G services. Since the cost of the equipment is similar (within 10%) for encrypted versus unencrypted, the increase in revenue goes directly towards improving ROI, with payback reduced from 7 months to 6 months. These numbers demonstrate that adding encryption as a service does not increase the initial outlay significantly, and in the long-term, can lead to a higher revenue stream with little to no financial risk.



Optical encryption as a service also acts as a differentiator. By providing the same service at a similar price, but with the added security of optical layer encryption enabled by Apollo, service providers can differentiate their services from competitors who are unable or uninterested in providing optical layer encryption. The ROI will be essentially the same as an unencrypted service at the same price (a difference of less than a month in most cases), but the service would be significantly more attractive to end-users.

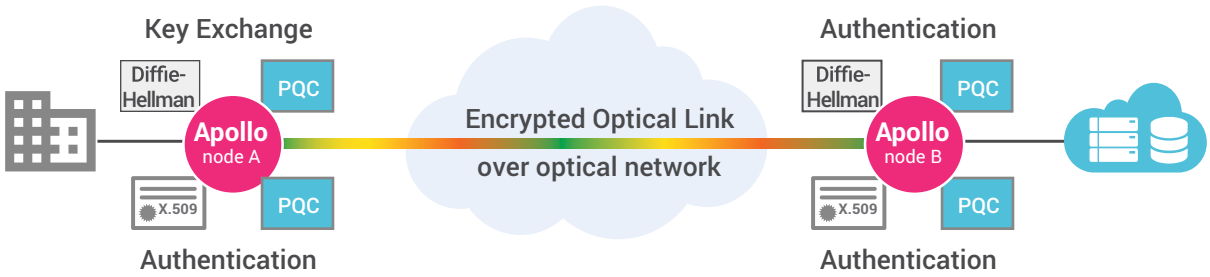
Post Quantum Cryptography Key Exchange

Quantum computing that is now starting to be commercialized has been demonstrated to break current public key-exchange algorithms. This is a concern for the entire encryption industry, which is pursing two main approaches to defeat quantum computing attacks.

Post Quantum Cryptography (PQC) achieves the same very high level of security against quantum computing attacks as does current key exchange mechanisms against conventional computing attacks. It is implementable using only software at a low incremental cost covering end-to-end encryption, and is commercially available for specific high-end applications.

Quantum Key Distribution (QKD) provides 100% detection of interception attempts, but is very expensive to implement requiring specialized hardware throughout a network.

Apollo is exploring both approaches, and can make available today PQC key exchange algorithms for both encryption (using KEM: Key Encapsulation Mechanism), and for authentication (using SIG: Digital Signature). These PQC algorithms can run in parallel with, or as a replacement for, existing Diffie-Hellman algorithms.



It's Time to Optically Encrypt

In a world where network and data security has become a daily concern, optical layer encryption is a powerful tool in the fight against unwanted intrusion. Ribbon's cost-effective and flexible Apollo optical networking system adds layer 1 optical encryption easily to any network, allowing network operators to use it for internal purposes or to extend it as a value-added service to end user customers. Apollo optical layer encryption adds no overhead and virtually zero latency. It blacks out all information about the payload and higher level addressing, and can be applied to any service type.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.

Contact Us Contact us to learn more about Ribbon solutions.