

The journey to quantum safe networking

Protecting vital information as it traverses global networks and the cloud

Executive Summary

With the proliferation and continuous enhancement of supercomputing and quantum processing capabilities, businesses, governments and defence organisations are racing to evolve their data security posture for stored operational data, as well as data-in-transit. The mathematical algorithm-based encryption techniques that have served global businesses and society over the past few decades are now more vulnerable than ever, especially when partial encryption information is known. This creates a significant commercial and compliance risk.

As a result, quantum safe networking has gained significance and momentum, along with demand for Quantum Key Distribution (QKD) and Quantum Key management. One of QKD's unique advantages is its ability to detect eavesdropping, thanks to the principles of quantum physics, where any interception attempt disturbs the quantum state, alerting the communicating parties to a potential breach. However, such QKD capabilities suffer from limitations in laws of physics, and are only deployable for a few hundred kilometres, with tailored solutions.

This paper outlines the weaknesses in traditional encryption techniques and identifies mechanisms to adopt a multi-layered 'defence in depth' approach for a holistic security of critical data, and describes recent advancements and collaborations needed to deliver the sophisticated, yet practical steps enterprises can take to defend their critical data that traverses over private and public networks, and cloud.

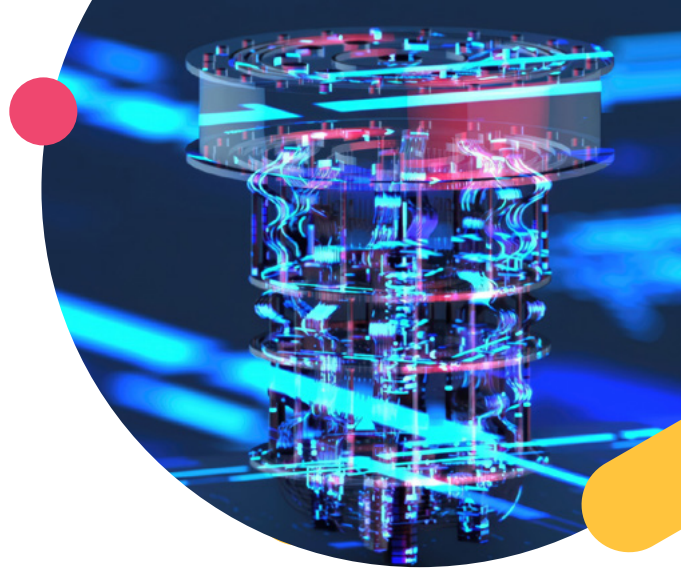
Such new mechanisms are vital not only to protect critical enterprise, finance, banking, defence and Government information, but also to achieve the regulatory compliance for NIS2, which now encompasses data-in-transit.

The threat vectors reshaping the cyber-security market

Significant attention has been paid to stored data and information and several security and privacy frameworks, laws and regulations exist to protect consumers' and enterprises' critical information. However, less attention has been paid to the security and privacy of data-in-transit, relying mainly on the application-level encryption, including PKI services at national and international levels. With human errors that can leave even RSA (a public-key cryptographic algorithm) ineffective to advancements in supercomputing, and now with quantum computing, there is a real risk that the data-in-transit can be harboured and decrypted, now or later, depending on the amount of information available on the encryption keys and the mathematics-based models used to create such keys.

This creates an unprecedented risk to business-critical information, to government operations and the effectiveness of defence organisations.

This risk has been recognised and amplified in the updated security regulations such as NIS2 and DORA. Compliance and penalties have been extended from their previous scope of the protection of stored data to data-in-transit. In addition, several regulators (ref 7) now demand data sovereignty, along with trusted suppliers of network equipment and services, to minimise the risk of foreign interference, enhancing trust in digital systems.





Cost of cyber-attacks is rising

As of February 2024, the global average cost of a data breach reached \$4.88 million, up from \$4.45 million in 2023

<https://www.statista.com/statistics/987474/global-average-cost-data-breach/>

This figure reflects the growing financial impact of large-scale cybersecurity incidents and proprietary data compromises across industries.

The implementation of quantum safe networks is not just about near-term ROI but about building readiness towards great potential. Financial services, as an example, have c.\$5-600B at stake by 2035 with banks being the top targets for cybercrime.

Quantum Safe Networking – the journey ahead

Several initiatives are underway to maintain trust in the digital fabric, to avoid access to and deciphering of critical communications and data-in-transit. These range from migrating asymmetric cryptography based PKI services to Quantum resistant PQC algorithms, to a departure from using mathematics-based algorithms to symmetric key generation and management i.e. PSK (Pre-shared Key) which cannot be compromised even by quantum computers. This is starting the Quantum Safe Networking revolution across data transport networks for enterprises, governments data centres and many more industries.

In the cases where Quantum Key Distribution and management is needed, terrestrial optical networks can be used to enable quantum key generation, key distribution and key management. This is currently restricted to 100km unamplified distance due to laws of physics, although it can be extended with trusted node deployments, in which every amplified spans requires a quantum trusted node as a quantum regeneration point.

This is not viable across subsea, long distance networks or Raman-amplified spans and intersecting borders. For enterprises that require quantum safe networking using QKD over longer distances, Nokia, Colt and Honeywell are planning to trial a satellite-based solution as a practical alternative to trusted node solutions. This journey is depicted in the following diagram:

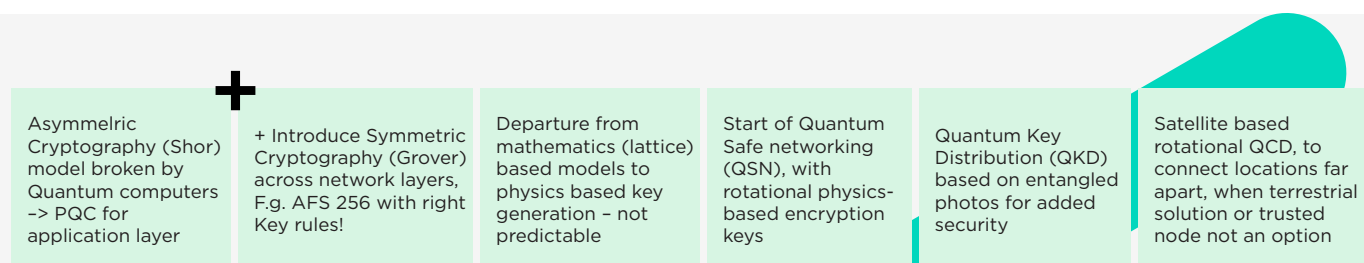


Figure 1

These capabilities come together to create defence in depth, where multiple layers in communication chains are made Quantum Safe, as depicted in figure below:

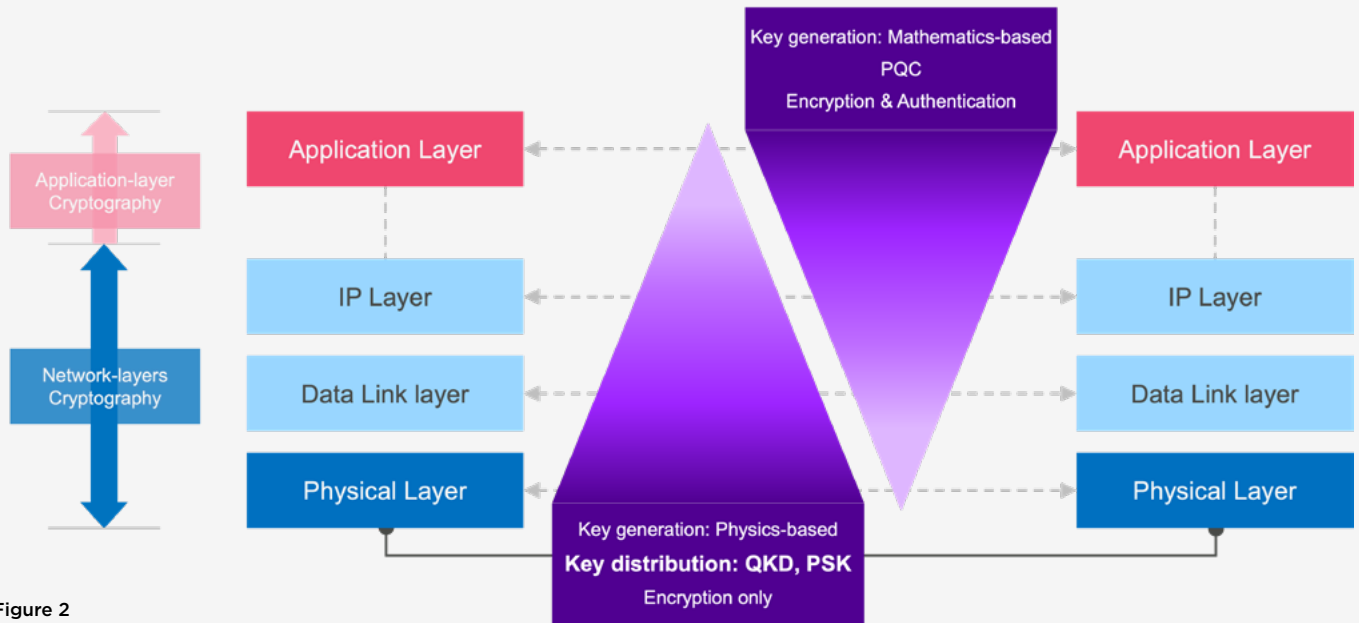


Figure 2

A partnership to deliver global success

To overcome the hurdle of providing long distance QKD enabled QSN, each of the three companies involved adds their specialist expertise to the new solution:

- Colt Technology Services is a global digital infrastructure provider to global enterprises, leveraging its vast terrestrial and subsea transport network. Colt places a high priority on safeguarding both its own data and that of its customers at every stage of data transmission, adhering to industry best practices, laws and policies. Colt has been offering classical encryption services to its customers on optical wave, private wave and packet products. In addition, Colt has recently made significant expansions to its subsea cable assets, including transatlantic and pan-European cables, as well as the Eurotunnel concession, delivering critical and growing capacity of up to 800 Gb/s, as illustrated in the map below.
- Nokia is a global telecommunications technology powerhouse, delivering networking solutions across mobile, fixed, transport and cloud networks. In this partnership, Nokia provides the Quantum Safe Networking systems across Optical and IP networks, physics based secure key creation, associated management system and operations, which are field proven, and deployed with 100+ networks globally
- Honeywell brings its pedigree in space communications, enabling quantum connectivity in space for North America, Europe and APAC customers. Since 2012 Honeywell has been a global leader in the space applications of quantum communications technologies beginning with the initial concept studies and technology development programs which ultimately led to the QEYSSat (Quantum Encryption and Science Satellite) mission. Through this mission, and subsequent private QKD demonstrators, Honeywell has developed a wealth of internal knowledge and capability in the field of free-space optical communications for quantum communications as well as quantum communication systems. Honeywell now leads a public-private partnership between themselves and ESA to deliver QKDSat, a first-to-market full stack satellite-based QKD system for the purpose of commercial QKD services offering globally.

This partnership brings a practical set of solutions to pilot QSN on land and in space to enterprise customers in a systematic & pragmatic manner, starting with the land-based solutions then adding the space-based QKD system management. The collaboration explores ways to effectively create a 'one-stop-shop' for regional and global enterprises to keep their data-in-transit safe from quantum and other threats and enable compliance with new regulations.

Colt's integration of terrestrial and satellite QKD with metro and subsea network layers, delivering defense in depth



Figure 3

Benefits of the solution include:

- Common components reused across terrestrial and Q-Sat services, providing the same look and feel for enterprise customers
- Colt's integration of terrestrial and satellite QKD with metro and subsea network layers
- Scaling up service for enterprise customers within a metro location or city across the country and globe
- A combination of terrestrial and subsea networks, enabling secure connectivity services for large enterprises, data centre and cloud providers
- Technology, professional services and service operations solutions to enable rapid adoption across multiple locations
- Comprehensive secure-key management system across full system

Trusted node vs QSat

Future quantum communication networks at scale will be constructed by combining terrestrial point-to-point infrastructure and quantum-enabled satellites. Both the QKD solution over satellite and terrestrial with or without trusted node will be complementary and will help to deliver quantum secured services end to end over long distance and metro networks.

Next steps

- There are a number of customers and segments already planning to deploy QSN services on Colt's infrastructure. Some early use cases include:
- Banking and finance: secure transaction channels, post-DORA compliance
- Data centres: secure east-west & inter-site data transfer
- Utilities and infrastructure: QKD-enabled SCADA communications
- Cable landing stations: QKD at key ingress/egress points

For businesses ready to explore Quantum Safe Networking with Colt, there are several options available:

- The QKD as a service for Metro locations will be available in Q3, 2025.
- The terrestrial QSN solution with symmetrical key distribution will be available in Q4, 2025 which can get enterprises started with a large number of use cases and deployment scenarios. Enterprises can start with network based QSN, all the way to Enterprise CPEs.
- The long distance QKD via satellite is planning to be tested in 2026, and should be globally available for commercial services at the end of 2027.

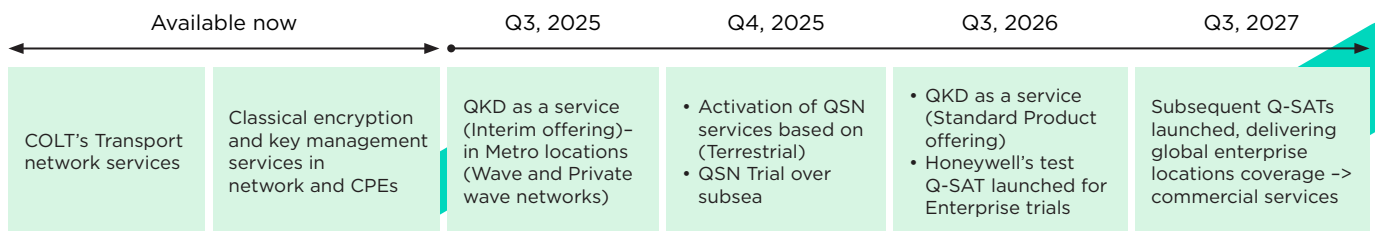


Figure 4

- Quantum key distribution deployment scenario over terrestrial and Satellite is highlighted in below figure 5.

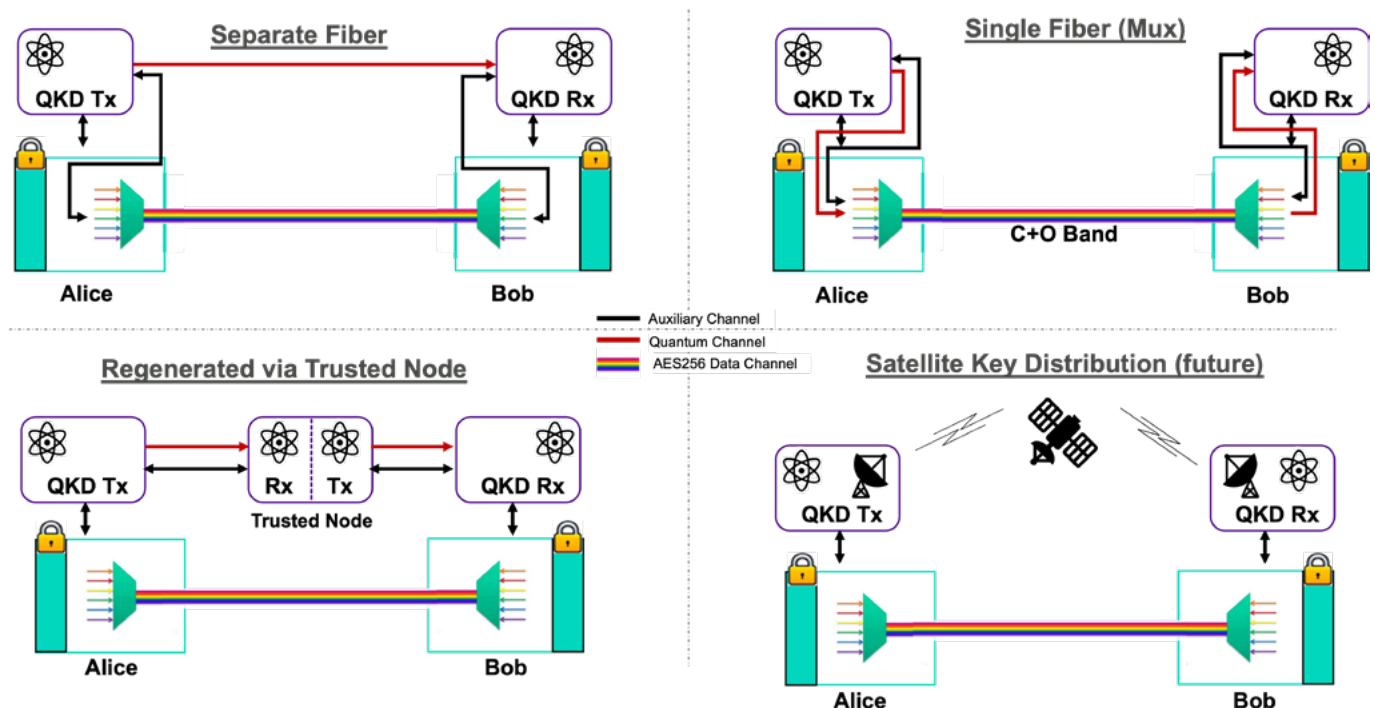


Figure 5



For more information, please contact Colt's dedicated team of QSN experts:

Zishan Ahmed Siddiquee

Senior specialist, Optical network engineering:

Zishan.siddiquee@colt.net

Anupam Lokdarshi

Associate Senior manager, Optical network engineering:

anupam.lokdarshi@colt.net

Vijay Mahajan

Lead consultant, optical network engineering:

Vijay.Mahajan@colt.net