

Telstra InfraCo Advanced Fibre Technology Enhances QKD Encryption Performance

Issued: October 2023

Introduction

The initial [‘Telstra InfraCo Express Intercity Fibre Network’ white paper](#) [1] referenced that the use of Corning® SMF-28® ULL fibre with advanced bend will better support the introduction of nascent quantum technologies, such as Quantum Key Distribution (QKD). QKD is expected to provide an additional layer of security against cyber-attacks in optical fibre networks compared to traditional encryption methods. As such, QKD adoption is projected to grow worldwide, evident from recent conference debates, product demonstrations, and announcements by carriers. To meet its growing customer needs for stronger data transmission security, Telstra InfraCo has commenced the preparation of its network infrastructure by rolling out Corning’s SMF-28 ULL fibre with advanced bend.

“An advantage of an ultra-low-loss fibre is in its ability to achieve QKD-encrypted data transmission over a longer distance or to provide QKD-encrypted security to more businesses.”

An advantage of an ultra-low-loss fibre is in its ability to achieve QKD-encrypted data transmission over a longer distance or to provide QKD-encrypted security to more businesses. There are two major challenges when dealing with quantum technologies: the quantum signals are much weaker and fragile compared to traditional telecom signals, and the so-called “no cloning” principle of quantum mechanics also means they cannot be amplified. As a result, trusted nodes are required to extend the QKD transmission to the desired distance. Utilizing an ultra-low attenuation fibre, like Corning’s SMF-28 ULL fibre with advanced bend provides significant value to this type of network – by extending the quantum information reach and reducing the number of trusted nodes. Trusted nodes are generally expensive as they are housed in a guarded facility to prevent tampering. Hence, reducing the number of trusted nodes may help realise cost savings in the network.

To simulate the performance improvements that could be expected from Telstra InfraCo’s Express Intercity Fibre Network, an experiment was carried out at Ciena’s laboratory in Ottawa, Canada to test the secure encryption capabilities of Ciena’s Waveserver platform and ID Quantique quantum equipment over SMF-28 ULL fibre with advanced bend in a lab environment. This white paper discusses the findings of the lab demonstration and provides further insights on new market application opportunities.

Why Encryption?

In today’s digital age, the Internet has become an integral part of our lives, facilitating seamless communication, online transactions, and the exchange of sensitive information. However, this increased connectivity has also exposed individuals, organizations, and governments to significant security risks. In 2022 the industry observed: [2]:

1. One potential intrusion is identified every 7 minutes.
2. The top-3 most targeted industries are technology, telecommunications, and manufacturing.
3. Telecommunications is the top targeted industry by nation state threats.

It becomes apparent that continuous innovation in stronger encryption is essential to help withstand evolving data transmission security threats, since the attackers have adapted and found creative ways to circumvent the existing defense mechanisms. Further threats are expected to occur with the emergence of quantum computers, which have computational capabilities that significantly exceed even the most powerful supercomputers used today. It is widely believed that such quantum computers may appear within the next decade, some have speculated as early as 2030, hence, new quantum resistant or quantum secure encryption methods need to be explored today to help withstand those future security threats.

Quantum Key Distribution (QKD) Based Encryption

Quantum Key Distribution (QKD) is a technique that leverages the principles of quantum mechanics to establish secure cryptographic keys between the two entities. This makes QKD fundamentally more secure than traditional encryption methods, making it significantly more difficult for unauthorized parties to intercept or eavesdrop on the key exchange process. QKD enables two parties to create a shared secret key that only they know, even if an eavesdropper has complete control over the communication channel. As such, QKD is more secure against attackers with unlimited computational resources, including a quantum computer. One of the key metrics associated with QKD is the Secret Key Rate (SKR), which is the rate at which the secret key is generated between the two parties [3]. A higher SKR means that more secret key material can be generated in any given amount of time, making the communication more efficient. Conversely, an insufficiently low SKR may make the QKD system infeasible due to the slow generation of the secret key. In the process of deploying quantum-secured optical channels, network operators must first establish the Required Secure Key Rate (RSKR).

The link RSKR ($RSKR_L$) can be calculated according to Equation 1, assuming all dense wavelength-division multiplexed (DWDM) channels utilize the same key length and key refresh rate [3]:

$$RSKR_L = L_K \times R_K \times N_{DC}$$

L_K : Required key length associated with data channel k (bits)

R_K : Required key refresh rate associated with data channel k (per second)

Eq-1

N_{DC} : Total number of channels per link

As stated previously, one of the challenges associated with QKD is that QKD signals cannot be amplified, and the means to regenerate those signals via a quantum repeater are still at the early stages of development. This poses a very real challenge of transmitting QKD signals over longer distances, which is where SMF-28 ULL fibre with advanced bend provides a significant advantage on how far QKD signals can be transmitted. Another challenge stems from very low powers required for QKD transmission, often making conventional telecom-grade components unsuitable for QKD signal generation and detection, requiring a more specialized set of components.

In addition to the use of advanced fibre, the QKD reach can be further extended by using trusted nodes, which convert the signal from optical domain to electrical, regenerated, and converted back to optical for onwards retransmission. In simple terms, trusted nodes can resemble traditional optical amplification sites but with a much higher site security to help protect any unauthorized interference from rogue actors.

Possible QKD Scenarios

In this paper we consider two distinct QKD scenarios: intra-city and inter-city. The first one is confined to the Metro area, where the distances are relatively short and are often confined to 100 kilometres (km). This corresponds to the single-hop transmission of quantum keys without the need for intermediate trusted nodes. The second scenario connects different cities, and the distance can vary greatly. In particular, we study the Sydney-Melbourne, Australia route that is approximately 900 km long.

Scenario 1: Intra-City

To simulate this scenario, an experimental setup was assembled at Ciena’s lab in Ottawa, Canada. In this setup ID Quantique Cerberis XG QKD system was used to establish a secure quantum channel, and Ciena’s Waveserver® 5 (WS5) was used for transmission of optical channels over typical G.652.D-compliant fibre (NDSF: non-dispersion shifted fibre) and SMF-28 ULL fibre with advanced bend (Fig. 1). The NDSF was chosen to represent a fibre type still prevalent in many existing networks around the world. The Waveserver® 5 receives keys from ID Quantique Cerberis system via ETSI compliant API to establish 800 Gbps quantum secured channel.

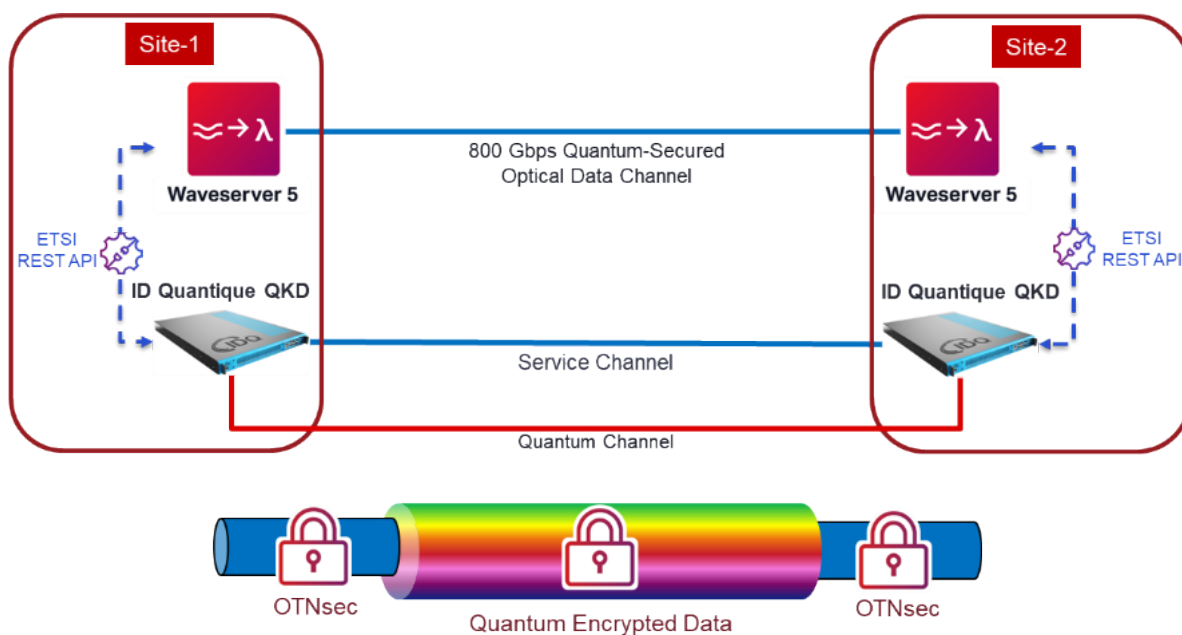


Fig. 1 Schematic diagram for a QKD transmission

First, we studied the extension in reach enabled by using SMF-28 ULL fibre with advanced bend, compared to NDSF fibre for the same target SKR of ~1.2 kbit/s. The use of SMF-28 ULL fibre allowed to extend the reach from 80 km to 100 km, compared to NDSF (Table 1).

Fiber Type	Max. Attenuation at 1550 nm (dB/km)	Distance (km)	SKR (bit/s)
NDSF	0.20	80	1231
SMF-28 ULL fibre	0.16	100	1153

Table 1. An increase in reach enabled by SMF-28 ULL fibre compared to NDSF

“... an increase in distance by 25% corresponds to the additional area coverage of ~56% for the second data centre placement .”

An increase of 25% in reach is a substantial improvement and could enable Telstra InfraCo to provide QKD-encrypted connectivity to data centres that are spread further apart, perhaps closer to renewable energy plants located on the outskirts of the city or simply to the area where the land is less expensive. We also note that an increase in distance by 25% corresponds to the additional area coverage of ~56% for the second data centre placement (given that the coverage area scales quadratically with distance).

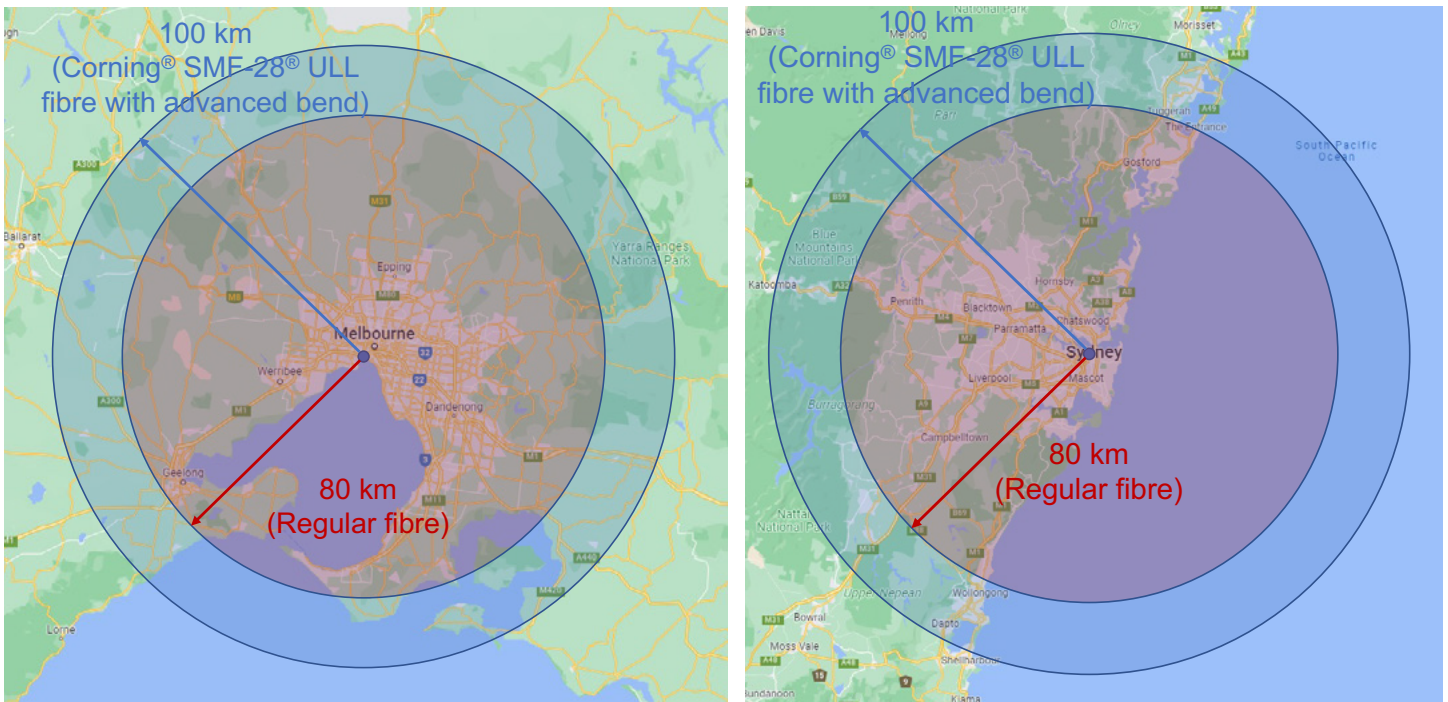


Fig. 2. SMF-28 ULL fibre with advanced bend can extend QKD-based connectivity between the data centers compared to NDSF (25% longer reach → 56% extra area coverage)

Second, we studied the increase in SKR enabled by SMF-28 ULL fibre with advanced bend, compared to NDSF fibre for the same distance of 80 km. This can be relevant when the location of the data centres is pre-determined due to geographical or historical constraints and moving them further away from each other may not be feasible. An increase in SKR can ultimately be translated into how many more businesses can be served with QKD-level security.

We concluded that the use of SMF-28 ULL fibre can significantly increase the SKR compared to NDSF for the same reach of 80 km (Table 2). Referring to Eq-1, $RSKR_L = L_K \times R_K \times N_{DC}$, we can calculate the number of supported 800 Gbit/s channels, N_{DC} , described below. Here we assume that the $L_K = 256$ bits, corresponding to AES encryption commonly used for optical data channels, and $R_K = 0.33$ (1/3), which is the quantum key refresh rate between the ID devices, one key every three

seconds. These results show that the use of SMF-28 ULL fibre can increase the number of 800G channels by 71% (from 14 to 24) that can be secured using QKD compared to NDSF, increasing the total amount of QKD-secured capacity from 11.2 to 19.2 Tbit/s. This could allow for the delivery of QKD-grade security to 71% more users or businesses at the highest traffic channel rate commercially available today.

Fiber Type	Distance (km)	Loss (dB)	SKR (bit/s)	# of 800 Gbit/s channels	QKD-secured capacity (Tbit/s)
NDSF	80	16	1231	14	11.2
SMF-28 ULL fibre	80	12.8	2100	24	19.2

Table 2. An increase in SKR and number of supported 800G channels using SMF-28 ULL fibre compared to NDSF (for the same key refresh rate of 1 key every 3 seconds)

Scenario 2: Inter-City

As noted before, to achieve a long-distance QKD transmission, the industry currently relies on the use of trusted nodes until high-performance quantum repeaters are invented and become commercially available at scale. Such trusted nodes are generally expensive to build, and their maintenance is often significantly more costly compared to traditional amplifier sites, because of the need to achieve a much higher site security. Our prior intra-city analysis showed that the use of SMF-28 ULL fibre can increase the reach from 80 to 100 km compared to NDSF fibre for the same SKR of ~ 1.2 kb/s. Extending this to a ~ 900 km Sydney – Melbourne route, we can conclude that the use of SMF-28 ULL fibre with advanced bend can eliminate the need for three trusted nodes (from 11 to 8) compared to NDSF (Fig. 3). This could provide substantial savings on cost, maintenance, security, and energy consumption.

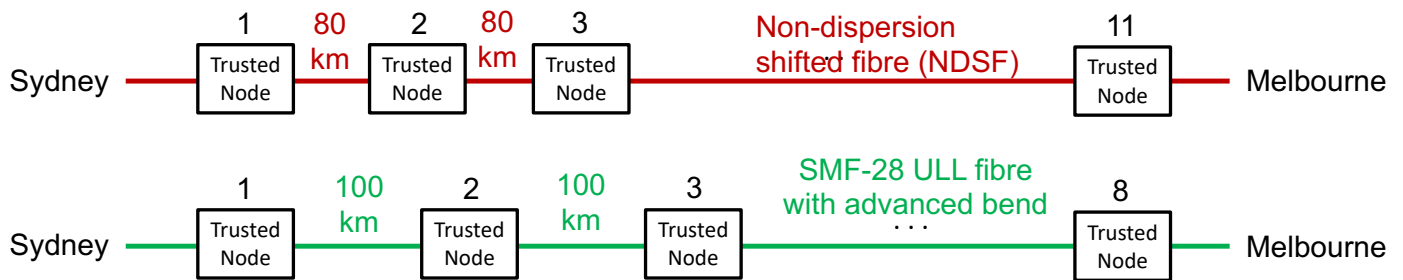


Fig. 3. A hypothetical example of how SMF-28 ULL fibre with advanced bend can help reduce the total number of trusted nodes for a long-haul Sydney – Melbourne route.

Future Technology Enablement

Continuing with the established principles tested, we can conclude that combination of three key elements, including fiber technology, quantum SKR and encrypted channel data rate determines the maximum quantum secured data throughput.

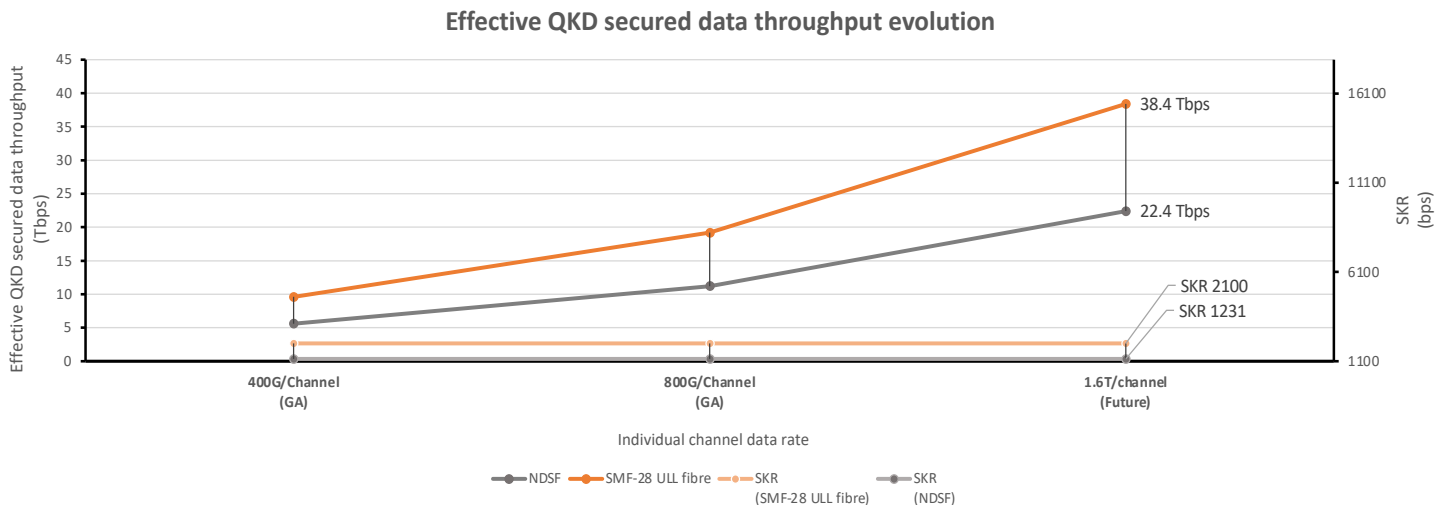


Fig. 4. Effective QKD secured data throughput evolution

As the channel rate of the encryption solution increases, it increases the benefit of using the SMF-28 ULL fibre solution by supporting an increased effective encrypted throughput using the same achieved SKR. Future 1.6T per channel encryption solutions will double this benefit again.

Conclusion

Evolving security threats prompt network operators to continuously upgrade their defense mechanisms, and quantum key distribution (QKD) is seen as a promising technology that can enhance network protection. This white paper discussed options and the practical considerations related to the potential deployment of QKD technology in Telstra InfraCo's Metro and Core networks. Compared to a non-dispersion shifted fibre, the use of SMF-28 ULL fibre with advanced bend achieved a 25% longer transmission distance for quantum signals, or significantly increased the number of 800G channels that have QKD-grade security, preparing today's network for the next-generation.

References

- [1] <https://www.corning.com/media/worldwide/coc/documents/Fiber/white-paper/WP8787.pdf>
- [2] CrowdStrike 2022 Threat Hunting Report
- [3] "On the Required Secure Key Rate for Quantum-Secured Optical Channels",
Farzam Toudeh-Fallah , Robert Keys , Dave Atkinson, arXiv:2306.15031, 2023

Authors

Sergejs Makovejs, Senior Commercial Technology Associate, Corning Incorporated
Miled Abdunour, Fibre Principal, Asset Management, Telstra InfraCo
Harry Sinodinos, Fibre Senior Technology Engineer, Asset Management, Telstra InfraCo
Aman Bhalla, Senior Solutions Consultant-Telstra Group, Ciena
David Fasken, CTO-Telstra Group, Ciena