

TQSN

**TERRA QUANTUM'S
SECURE NETWORK**

FOR GLOBAL
COMMUNICATIONS



**LEVERAGING END-TO-END
PHYSICAL LINE CONTROL**

WWW.TERRAQUANTUM.SWISS

MAY 2023



THE RISE OF QUANTUM KEY DISTRIBUTION

AND THE FALSE PROMISE OF PUBLIC KEY CRYPTOGRAPHY

Imagine your most precious secrets and sensitive data, encrypted and secured with the latest technology. You trust that no one can break through the walls of protection that you've built. But what if you learned that those walls were not as strong as you thought?

One of the main protocols used today for secure communications is public key cryptography. However, it crucially relies on certain assumptions that were originally considered very sound but are now known to be false. The idea was that the protocol could not be broken by even the best computers running the best algorithms unless they were left to run for far longer than a human lifetime.

This idea was torn down by quantum researchers from all over the world. The first tear was when a new algorithm was devised that was exponentially faster than its predecessors. The saving grace for internet users was that this algorithm could only be run on a type of computer yet to be developed — a quantum computer.

However, the tear is growing larger as the race to build quantum computers intensifies.

HOW TERRA QUANTUM IS CHANGING THE GAME

Companies are concerned about having their encrypted data intercepted, copied and saved for a later date when quantum computers will be ready to reveal their secrets. So what's the solution?

Quantum Key Distribution (QKD) is the game-changer for secure communications. QKD is a revolutionary technology that leverages the quantum mechanical properties of light and allows for the distribution of cryptographic keys with absolute security, making decryption impossible.

However, many approaches to QKD do not work well over long distances and do not offer high bit rates. Until now. The exception is Terra Quantum's patented Secure Network solution (TQSN) that overcomes both of these drawbacks. **It is the world's first scalable, zero-trust Secure Network for global communications.**

TQSN: THE TERRA QUANTUM SECURE NETWORK

The essence of the Terra Quantum solution is the ability to infer whether transmission losses have occurred naturally or due to the attempts of an eavesdropper. The natural losses arise from phenomena known as Rayleigh scattering and Raman scattering. Terra Quantum has developed ways to make sure these are well-characterized so they can be distinguished from deliberate, malicious attempts to covertly gain access to the transmitted optical signals. The ability to make this distinction is what allows high key generation rates at distances of 40,000 km.

FEATURES



LEVERAGING QUANTUM-GENERATED ENTROPY

Securing the information with quantum keys, generated by Terra Quantum's single-photon QRNG.



END-TO-END PHYSICAL LINE LOSS CONTROL

Identifying the source of transmission losses with an astounding Leakage Detection Precision of 0.001%.



USING EXISTING OPTICAL FIBER

Compatible with existing telecommunications infrastructure, using dark fiber.



ULTRAFAST KEY TRANSMISSION RATE

Thanks to signal repetition through optical amplification, our protocol reaches up to 1 Gbit/s data transmission rates.



REACHING GLOBAL DISTANCES

Propelled by optical amplifiers, the Terra Quantum Secure Network can transfer keys securely across distances of up to 40,000 km.

Terra Quantum's Single Photon Quantum Random Number Generator (QRNG)

used to generate the keys for the TQSN solution has been designed and implemented according to the latest NIST Standard (SP 800-90B) and is certified by METAS.





HOW IT WORKS

DISTRIBUTED SIGNAL LOSSES ARE TURNED INTO HEAT

For a properly installed optical fiber, the natural losses are distributed fairly evenly across its full length. When the fiber is first set up, Terra Quantum's users — let's call them Alice and Bob — can measure these distributed losses. This is done using optical reflectometers that detect backscattered light.

An eavesdropper, Eve, would not be able to collect a significant proportion of this lost light because it would involve setting up an antenna that spans many kilometers and it would be completely infeasible to do this without anyone noticing. Even state-of-the-art measuring devices could not cover more than a few centimeters of the line.

Terra Quantum's optical fibers can include dissipative cladding that causes the light escaping the fiber to undergo inelastic secondary scattering that transforms it into heat. This transformation makes the information that was encoded in the light absolutely irretrievable to the eavesdropper.

Suppose that an undeterred Eve gained local physical access to the optical fiber, perhaps 0.1% or 1% of its total length. She could deliberately create additional local losses (by either removing the cladding and bending the fiber or by performing more sophisticated manipulations) and then attempt to exploit the information she has gained.

However, Alice and Bob can continuously monitor the losses with optical reflectometers, which means they would notice any newly appearing local signal leaks. By employing careful records of time delays, the locations of these loss "events" can be determined. Upon detection, Alice and Bob can adapt their protocol to ensure they are resistant to eavesdropping.

OPTICAL AMPLIFIERS DRIVE SIGNAL REPETITION

Terra Quantum's scheme uses amplifiers that are spaced out along the optical fiber. These optical amplifiers are technologically mature – examples include in-line Erbium doped fiber amplifiers and Raman amplifiers. These amplifiers do not have to be trusted because the integrity of the scheme solely depends on the actions of the legitimate users, namely Alice and Bob.

The amplifiers maintain the security of the communication protocol and, by compensating for the decay of the signal, enable global transmission distances and high key distribution rates.

If Eve steals a small proportion of the signal, it will be useless to her because it will be obscured by noise. (In the case of the coherent photon states that are used in this protocol, the noise is technically known as Poissonian shot noise. It arises due to the quantum mechanical uncertainty relationship between the number of photons in the signal and their phase.)

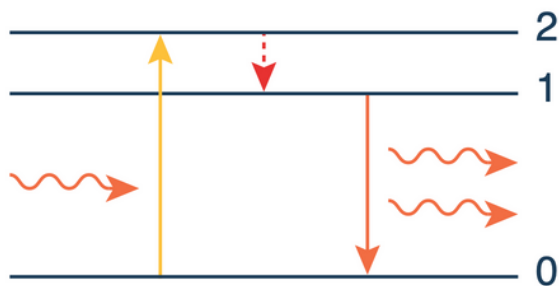


Figure 1. Energy diagram showing light amplification in an erbium-doped fiber.

'Due to the optical reflectometers, it is always possible to accurately estimate the proportion of the signal that is stolen.'

If Alice and Bob decide that the proportion that has been stolen is uselessly small, they can adapt some of the protocol parameters to maximize the key generation rate. If they decide that the proportion is too high, they can simply abort before any information is given away.

FLUCTUATIONS MAKE UNDETECTABLY LOW SIGNAL LOSSES IRRETRIEVABLY NOISY

Alice and Bob can agree on an encoding scheme where a low number of photons in a pulse corresponds to a 0 and a high number corresponds to a 1. Counting the photons in each pulse is straightforward but quantum mechanics necessitates that the photon number fluctuates to some extent. (In particular, the fluctuations are proportional to the square root of the photon number.)

Consider the effect this has on Eve if she steals a small fraction of the photons. Because she gets so few photons, the fluctuations are far more severe for her. She simply cannot distinguish between a 0 and a 1 because she receives a similar number of photons in either case. Bob receives a lot more photons than Eve. This means he can easily decode the message since the number of photons he expects to get for a 0 is very different from the number he expects for a 1.

As explained in the previous page, it is always possible for Alice and Bob to accurately estimate the proportion of stolen photons. They can then adapt the protocol to ensure that Eve can never distinguish between 0 and 1 - either they adjust the parameters of the protocol or, in a fail-safe manner, they decide to abort their communication.

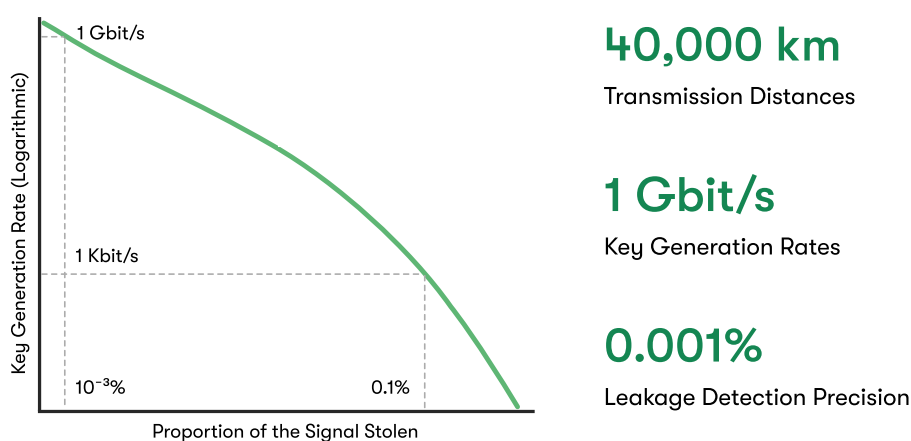


Figure 2. Adaptation of the Terra Quantum Secure Network solution based on signal leakage detection

HOW CAN YOU ADOPT IT?

YOUR ROADMAP TO QUANTUM SECURITY

- **Conduct a thorough inventory to determine what systems and processes use public-key cryptography.**

Clarity should be obtained on how the cryptography is used to protect the confidentiality and integrity of data at rest, data in use and data in motion.

- **Assess what quantum-secure technology upgrades are appropriate.**

Seek to discover any technical constraints that your systems may have with regards to implementing security upgrades.

- **Coordinate adoption within your organization's ecosystem in order to preserve the interoperability of the existing infrastructure.**

- **Get in touch with Terra Quantum so that together we can scope out your implementation of the TQSN solution, based on your needs.**

- **Adopt a long-term, quantum-agile strategy when it comes to security updates.**




GET IN TOUCH

Protect your sensitive information and stay ahead of the evolving security curve by adopting the world's first scalable, zero-trust Secure Network solution for global communications.

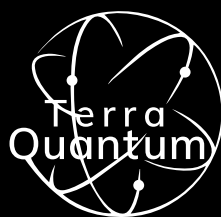
**Quantum in Now.
Quantum-secure your network!**

 info@terraquantum.swiss

 www.terraquantum.swiss

 +41 71444 0000

QUANTUM
is NOW.



www.terraquantum.swiss