Fiber Quantum Communications Across 600 km

RESEARCHERS

Mirko Pittaluga (mirko.pittaluga@crl.toshiba.co.uk), Toshiba Europe Ltd., Cambridge, UK, and University of Leeds, Leeds, UK

Mariella Minder, Toshiba Europe Ltd. And University of Cambridge, Cambridge, UK

Marco Lucamarini, **Mirko Sanzaro**, **Robert I. Woodward**, **Zhiliang Yuan** and **Andrew J. Shields**, Toshiba Europe Ltd., Cambridge, UK

Ming-Jun Li, Corning Inc., Corning, New York, USA

REFERENCES

1. M. Lucamarini et al. Nature **557**, 400 (2018).
2. J.-P. Chen et al. Phys. Rev. Lett. **124**, 070501 (2020).
3. M. Pittaluga et al. Nat. Photon. **15**, 530 (2021).

Communication technologies based on quantum light offer new opportunities for securing long-distance data transmission. One such approach, quantum key distribution (QKD), establishes a shared string of bits between two distant users which can be used for encryption. Importantly, unlike conventional cryptography, QKD is resistant to attacks by a quantum computer.

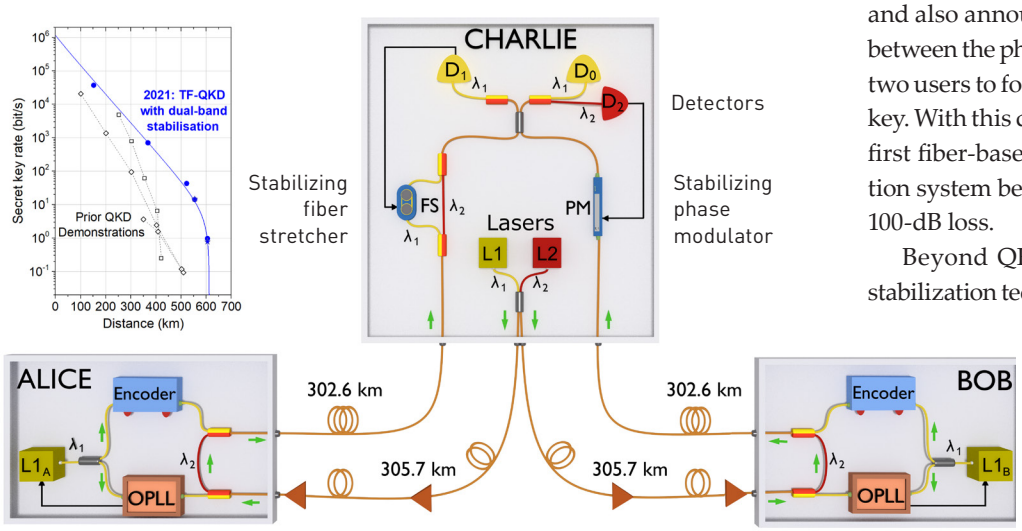
When single photons are sent through a communication channel such as optical fiber, they are scattered by the medium and have only a small probability of reaching the end of the line. A rigorous theorem limits to 1.44η the number of secure bits delivered by point-to-point QKD, where η is the channel transmission. This "repeaterless secret key capacity" was until recently considered the ultimate limit for QKD with today's technology.

This changed with the recent introduction of the twin-field QKD (TF-QKD) protocol,[1] which offers a key rate that scales proportionally to the square root of channel loss. However, as TF-QKD is based on first-order interference, a major practical challenge is the requirement for a phase-stable channel. This demands active compensation over long distances of phase changes arising from factors such as vibrations and temperature fluctuations. While compensation techniques have been demonstrated using time-multiplexed reference signals alongside encoded bits, these have been fundamentally limited in distance due to their length-dependent noise.[2]

This year, we developed a new technique to solve this problem: the dual-band stabilization.[3] We first established that the main limitation of time-multiplexed stabilization techniques was the need for brighter reference signals as fiber lengths increased; this leads to double Rayleigh backscattering, which pollutes the weak quantum signals. Dual-band stabilization overcomes this issue using an additional multiplexed wavelength as a reference to cancel rapidly varying fluctuations, leaving to the original phase reference (necessarily at the same wavelength as the quantum light) the simpler task of fine adjustment.

Our full QKD system implementing this technique comprises two distant users who prepare and transmit phase-encoded, attenuated laser light, and a central interference station. The latter supplies the two reference wavelengths and also announces the measured correlations between the photons it receives. This enables the two users to form a perfectly secure encryption key. With this design, we have implemented the first fiber-based secure quantum communication system beyond the barriers of 600 km and 100-dB loss.

Beyond QKD, we believe our dual-band stabilization technique is relevant to other quantum technology applications, such as enabling DLCZ-type quantum repeaters, longer-baseline telescopes, quantum fingerprinting over longer distances or a phase-based architecture for the quantum internet. OPN



In the experimental setup, two users ("Alice" and "Bob") establish a secure quantum key by transmitting phase-encoded pulses at wavelength λ_1 to a central station ("Charlie"). Charlie provides two phase reference wavelengths (λ_1 and λ_2) that are used for dual-band stabilisation. Inset, top right: Secure key rate performance vs. distance.