Phase Noise in Real-World Twin-Field Quantum Key Distribution

ADVANCED QUANTUM TECHNOLOGIES
www.advquantumtech.com

Phase Noise in Real-World Twin-Field Quantum Key Distribution

Gianluca Bertaina, Cecilia Clivati, Simone Donadello, Carlo Liorni, Alice Meda, Salvatore Virzì, Marco Gramegna, Marco Genovese, Filippo Levi, Davide Calonico, Massimiliano Dispenza, and Ivo Pietro Degiovanni*

The impact of noise sources in real-world implementations of twin-field quantum key distribution (TF-QKD) protocols is investigated, focusing on phase noise from photon sources and connecting fibers. This work emphasizes the role of laser quality, network topology, fiber length, arm balance, and detector performance in determining key rates. Remarkably, it reveals that the leading TF-QKD protocols are similarly affected by phase noise despite different mechanisms. This study demonstrates duty cycle improvements of over a factor of two through narrow-linewidth lasers and phase-control techniques, highlighting the potential synergy with high-precision time and frequency distribution services. Ultrastable lasers, evolving toward integration and miniaturization, offer promising solutions for agile TF-QKD implementations on existing networks. Properly addressing phase noise and practical constraints allows for consistent key rate predictions, protocol selection, and layout design, crucial for establishing secure long-haul links for the quantum communication infrastructures under development in several countries.

1. Introduction

Quantum key distribution (QKD) protocols have the potential to revolutionize the cryptographic environment, with solutions that enable to share keys between distant parties, with security claims guaranteed by the laws of quantum mechanics,[1,2] without assumptions on the computational power of the attacker. After almost 40 years of theoretical work, numerous proof of principle experiments, and deployment of testbeds,[3–7], nowadays the real objective is the integration of this technology in long-distance fiber networks already utilized for classical telecommunication.[8–13] It is well understood that the range of QKD links is limited by channel losses, with the link maximum key rate upper limited by the repeaterless secret-key capacity or Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound,[14] which is stricter than a previous upper bound result.[15] Trusted nodes are used to extend the achievable range, a temporary solution waiting for true quantum repeaters[16] to become deployable in the field.

Twin-field quantum key distribution (TF-QKD) is a solution that was proposed a few years ago[17] to mitigate the negative impact of channel loss, reaching key rates beyond the PLOB bound without the use of a trusted node. TF-QKD is a type of measurement-device-independent QKD (MDI-QKD)[18] in which the parties Alice and Bob encode information in the properties of dim laser pulses that are sent through optical fibers to a central untrusted relay node, Charlie, where they undergo single-photon interference that overcomes security challenges related to real device imperfections.[19,20] An important assumption, that makes these protocols more complex to deploy than, e.g., time-bin encoded Bennett-Brassard 1984 (BB84), is that optical pulses need to be phase-coherent when they are generated in distant locations, and they must preserve coherence throughout the propagation to Charlie in spite of vibrations, seismic noise and temperature fluctuations encountered along the path. The first requirement was initially achieved by mutually phase-locking the photon sources in Alice and Bob, distributing reference-phase information through a service fiber link, while the second is addressed by interleaving the QKD signals with bright reference pulses that probe the fiber to detect and compensate its noise, recovering stable interference visibility as required for low-error operation.[21,22] These approaches become less effective with long-distance links, reducing the actual duty cycle of the QKD transmission. In recent years, other solutions have been proposed,[23,24] based on dual-wavelength transmission and

G. Bertaina, C. Clivati, S. Donadello, A. Meda, S. Virzì, M. Gramegna, M. Genovese, F. Levi, D. Calonico, I. P. Degiovanni
Istituto Nazionale di Ricerca Metrologica
Strada delle Cacce 91, Turin I-10135, Italy
E-mail: s.donadello@inrim.it

C. Liorni, M. Dispenza
Leonardo Labs
Quantum Technologies Lab
Via Tiburtina, km 12.400, Rome I-00131, Italy

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202400032

DOI: 10.1002/qute.202400032

active stabilization of the QKD lasers and the connecting fibers. Since the first proposals, many noise cancellation variants have been implemented, trading off performance with equipment and infrastructural complexity, which is a concern in the quest for realizing deployed and operational QKD networks at reasonable cost. Emerging laser integration technologies[25–27] and interferometric techniques for fiber length stabilization can play a role in this challenge. In addition, strong synergy exists with the concurrent realization of network-integrated services for the distribution of accurate time and ultrastable optical frequencies at a continental scale,[28–31] also in the frame of European initiatives such as the European Quantum Communication Infrastructure (EuroQCI).[32] Recently, TF-QKD has been demonstrated up to very long distances of 800–1000 km.[33,34] These impressive results have been obtained by using controlled low-loss fiber spools, high repetition rates, and ultra low-noise cryogenic superconducting single-photon detectors. Here, we focus on setups that could be realistically deployed in the near future, partially employing existing infrastructures.

The present work aims at providing a general formalism to model relevant impairments occurring in real-world point-to-point TF-QKD implementations, as well as the impact of practical constraints, such as the length imbalance between the arms of the interferometer, the quality of the employed stabilization laser, the adopted network topology and the characteristics of the channel. The results of this analysis are then used to evaluate the performance of different TF-QKD protocols in terms of key rate versus channel loss/length. Relevant information is condensed in a minimal set of parameters that enables tailoring the analysis to other practical cases and is useful in the design and performance optimization of TF-QKD in real-world scenarios, in view of the establishment of long-haul operational connections. While, for the sake of conciseness, we present simulation results varying a few of the relevant parameters, we provide a comprehensive and open source model[35] to ease fast comparison among different scenarios.

This article is organized as follows. In Section 2, we introduce the standard scheme of a TF-QKD setup. In Section 3, we introduce two prominent TF-QKD protocols and discuss the role of phase noise. In Section 4 we describe the main sources of phase noise in a TF-QKD scheme and model their contribution in view of estimating the achievable key-exchange performances. In Section 5, we discuss the relevant figures of merit in the detection part of the TF-QKD apparatus and their impact on the key rate. Having outlined the complete model, in Section 6, we report the results of the simulation of TF-QKD key rates during standard operation (namely absence of attack) under different scenarios stemming from the choice of phase stabilization, the length imbalance, and the detector parameters. Finally, in Section 7, we draw our conclusions and consider future perspectives. For completeness, the Appendices contain more details on our model of the phase fluctuations spectrum for different scenarios and a detailed recap of the simulated protocols and their parameters.

2. Elements of TF-QKD

A minimal model of a TF-QKD setup between two parties, Alice and Bob (abbreviated by A and B, respectively, and collectively indicated by *they*) must take into account sources, channels, phase-coherence, detectors, and protocol. **Figure** 1a illustrates the typical elements of a TF-QKD setup.

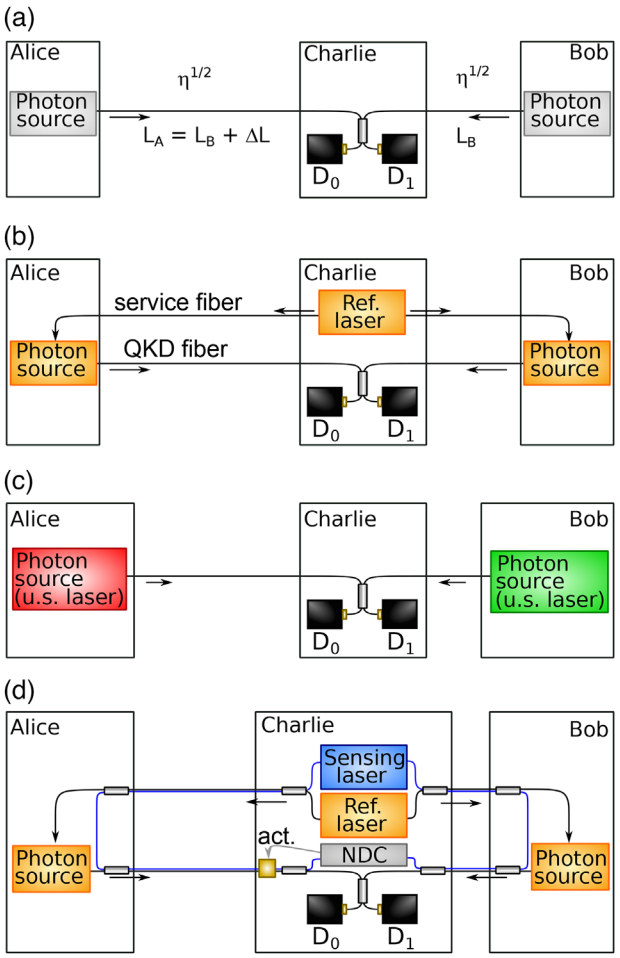

Figure 1. a) Principle scheme of a generic TF-QKD setup, characterized by total effective transmittance η, length of the interferometer arms L_A and L_B, length imbalance ΔL, and with D_0 and D_1 the single-photon detectors. b) Scheme of the common-laser approach to TF-QKD, based on a reference laser source (ref. laser). c) Scheme of the independent-lasers approach to TF-QKD, based on ultrastable laser sources (u.s. lasers). d) Scheme of common-laser TF-QKD with fiber stabilization, based on a noise detection and cancellation system (NDC), and on an actuator for fiber stabilization (act.).

- *Sources*: We consider attenuated laser sources, producing weak coherent states, characterized by intensities μ_i and phases φ_i, which can be both independently modulated in time by *them* at a certain nominal clock rate ν_s. Phase noise of the sources is described in Section 4.
- *Channels*: We consider optical fibers characterized by total attenuation (loss) A_T or, equivalently, total transmittance $\eta = 10^{-A_T/10}$, with A_T measured in dB. The total loss $A_T = \alpha L + A_+$ is customarily given by a term proportional to the distance L, with (average) attenuation coefficient α, plus additional losses A_+ due to instrumentation. Since in TF-QKD both of *them* send signals to the auxiliary node Charlie (C), the relevant distances are L_A, on the segment AC between Alice and Charlie,

and L_B, on the segment BC between Bob and Charlie. Without loss of generality, we assume $L_A \geq L_B$ and define the residual channel length imbalance as $\Delta L = L_A - L_B$. In order to maximize interference contrast in C, we balance the transmittances of the two segments in C, i.e. $\eta_A = \eta_B$, by assuming that a variable optical attenuator is introduced by Charlie on the CB segment. Therefore, the total effective transmittance between A and B is $\eta = (\eta_A)^2$, corresponding to an effective total fiber length $2L_A$, which is in general larger than $L_A + L_B$.

- *Coherence*: Phase coherence between photon pairs generated at distant locations and interfered in Charlie is a peculiar prerequisite of TF-QKD and affects the overall quantum bit error rate (QBER) and transmission duty cycle. As a figure of merit for phase coherence, we introduce the variance of the phase fluctuations φ observed at the detector in Charlie σ_φ^2, and quantify its contribution to the QBER as[24]

$$e_\varphi = \int \sin\left(\frac{\varphi}{2}\right)^2 P(\varphi)\mathrm{d}\varphi \approx \frac{\sigma_\varphi^2}{4} \tag{1}$$

where it is assumed that the phase fluctuations are Gaussian distributed. All protocols include dedicated hardware and routines to keep σ_φ^2 below a certain threshold during the key transmission, possibly introducing some dead time and reducing the key rate. We model this effect by multiplying estimated key rates by a duty cycle $d = \tau_Q/(\tau_Q + \tau_{PS})$, namely the ratio between the maximum uninterrupted time τ_Q that is used in the quantum part of the key distribution protocol, and the total time including the subsequent overhead spent for phase stabilization τ_{PS}. σ_φ^2 and τ_Q are not independent: lower system phase noise allows for increasing τ_Q. Conversely, τ_Q is upper-bounded by the time it takes for the system to reach a significant threshold for σ_φ^2. These aspects are treated in Section 4.
- *Detectors*: Charlie performs single-photon interference and detection on the two output branches of the interferometer, besides any phase stabilization. The security proofs of the TF-QKD protocols guarantee that Charlie can be untrusted,[17,36,37] namely his actions can at worst deny QKD operation, but not leak information to an attacker (Eve). Detectors are characterized by efficiency $\eta_D \leq 1$, that reduces the channels' transmission to $\hat{\eta} = \eta\eta_D$. Each detector is crucially characterized by dark counts per transmitted pulse p_{DC}, given by the ratio of the dark count rate P_{DC} and the clock rate $p_{DC} = P_{DC}/\nu_s$. The interferometer is affected by polarization misalignment θ, which introduces an error $e_\theta = (\sin\theta/2)^2$, whose impact depends on the used protocol. Considerations about the characterization and improvement of detectors are made in detail in Section 5.
- *Protocols*: After the announcement of measurements by Charlie, Alice and Bob perform classical post-processing, exchanging information via a classical authenticated channel and estimating error rates from a small sample of the bits that are declared. To guarantee unconditional security, they perform error correction, to reconcile the raw bits, and privacy amplification, to remove the information possessed by Eve.[38,39] Error correction reduces the key size by an amount $f_{EC} Q H_2(E)$, where Q is the total gain of the signals and E is their total bit-flip QBER. $H_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy and f_{EC} is the inefficiency of error correction, that we customarily set to $f_{EC} = 1.15$.[1,17] The actual amount of privacy amplification is specific to each QKD implementation, as it depends on the detailed security analysis, protocol, and parameters values. When the tagging argument[39] and the decoy-state approach[40–42] are applied, typically the key length is reduced by an amount $\underline{n}_1 H_2(\bar{e}_1^{ph})$, where $\underline{n}_1$ is the estimated lower bound on the rate of single photon signal states at the detector and $\bar{e}_1^{ph}$ is the estimated upper bound on the single photon phase error rate. The total gain and single photon gains possibly include sifting factors depending on the specific protocol. Finally, the lower bound for the secure key per transmitted qubit $\underline{R}$ is to be multiplied by the source repetition rate ν_s and the duty cycle d to obtain the total key rate. In the absence of quantum repeaters, the upper bound to secure key rate per transmitted qubit in a channel of total transmission η is the PLOB bound, namely the secret-key capacity of the channel $SKC_0 = -\log_2(1-\eta)$, that scales as $1.44\,\eta$ at large losses.[14] In TF-QKD, what matters is the branch with the largest loss, corresponding to η_A. One has thus a much weaker dependence on the total distance, since $\eta_A = \eta^{1/2}$ when the AC and BC losses have been balanced. This enables overcoming the PLOB bound and represents the most relevant achievement introduced by TF-QKD.

3. TF-QKD Protocols and Role of Laser Phase Noise

In this Section, we discuss two established TF-QKD protocols, sending-or-not-sending (SNS) and Curty-Azuma-Lo (CAL). In the original proposal of TF-QKD by Lucamarini et al.,[17] it was assumed that Eve cannot perform a collective beamsplitter attack, which relies on the knowledge of the global phase. This information is in fact leaked by the original protocol in order to match the phases chosen by Alice and Bob. Provably secure protocols in the assumption of coherent attacks were later introduced, like SNS and CAL, that rely on separating the communication in signal windows and decoy windows, used for precise parameter estimation. Both the SNS (see refs. [36, 43, 44] for details) and the CAL (see refs. [37, 45, 46]) protocols employ weak coherent states in two complementary groups: phase mixtures and phase-definite states. Before reporting the key rates of the two protocols (and detailing their main steps in Appendices A and B), we generically comment on their reciprocity. Phase mixtures are phase-randomized coherent states of intensity μ, which are seen by Charlie and Eve as statistical mixtures of number states $|n\rangle$ with Poissonian statistics $p_n^\mu = e^{-\mu}\mu^n/n!$. Since the intensity is weak, these mixtures mostly correspond to zero or one photon, and the security proofs relate those states to the eigenstates of the Z operator. These states are then said to belong to the Z basis and the corresponding measurement is related to photon counting. In contrast, by phase-definite states, we mean coherent states that are to be employed in an interferometric measurement, which requires that a reference global phase is declared (either before or after Charlie's communication). These states are said to refer to the X basis, because they are related to the coherent superposition of zero and one photons in the security proofs.

The SNS protocol uses the Z basis for encoding,[36] depending on the decision by Alice and Bob to send a number state or

not. The decoy-state approach to phase error estimation is performed via interferometric measurement in the X basis. For applying standard decoy expressions, notice that the global phase is still randomized by Alice and Bob, but can be reconciled after Charlie's communication of measurement outcome. In contrast, in the CAL protocol, the X basis is used for encoding,[37] and coherent states with two possible phases with π difference are interfered in Charlie. Complementary, the counting Z basis is used in the decoy-state analysis, without need for reconciling the global phase. Both protocols remove the possible security issue in the original TF-QKD protocol, related to the need of revealing the global phase at each time window.

The secret key per transmitted qubit for the original SNS protocol is formulated in Equation (A1) of Appendix A, and we report here its formulation when sending-or-not-sending with actively odd-parity pairing (SNS-AOPP) is used:

$$\underline{R} = p_Z^2 \left[\underline{n}_1' \left(1 - H_2 \left(\bar{e}_1'^{\mathrm{ph}} \right) \right) - f_{\mathrm{EC}} n_t H_2(E_Z') \right] \tag{2}$$

While the description of the symbols in the equation is postponed to the appendix, here we discuss the effect of phase fluctuations in the lasers and in the fiber on the error terms, which dominate the behavior of the key rate formula. E_Z', the bit-flip error rate, is inherently independent of the phase fluctuations, since the encoding in the Z basis is phase-independent, given the previous considerations. The QKD phase error rate $\bar{e}_1'^{\mathrm{ph}}$, on the other hand, contains terms related to the phase fluctuations, since there the parties perform an interferometric measurement. In the CAL protocol, the secret key per transmitted qubit is estimated as Equation (B2) of Appendix B, that we report here:

$$\underline{R}_{X,k_c k_d} = \frac{1}{\nu_s} p_{XX}(k_c, k_d) \times \left[1 - f_{\mathrm{EC}} H_2(e_{X,k_c k_d}) - H_2(\min\{1/2, \bar{e}_{Z,k_c k_d}\}) \right] \tag{3}$$

In this case, contrary to the SNS protocol, the bit-flip error $e_{X,k_c k_d}$ is increased in the presence of phase fluctuations while $\bar{e}_{Z,k_c k_d}$ does not depend on them, since in the Z basis the states used for the decoy analysis are phase-randomized.

4. Model for the Laser Phase Noise

As discussed in Section 3, poor phase coherence between photon pairs interfering in Charlie increases the QBER and reduces the final key rate, although its actual impact significantly depends on the used protocol. In this Section, we explicitly derive decoherence effects for most common TF-QKD topologies and quantify the corresponding QBER.

As a relevant metric to quantify decoherence, in Equation (1) we introduced the phase variance σ_φ^2 and its relation to e_φ, suggesting its relation to τ_Q. Indeed, the integration time that is relevant for calculating σ_φ^2 during the key transmission corresponds to the maximum uninterrupted transmission time τ_Q. To operationally quantify the relation between σ_φ and τ_Q, we will employ spectral analysis, as it gives more insight into relevant noise processes, simplifies calculations, and is directly related to measurable quantities. We then introduce the noise power spectral density of a variable $\gamma(t)$, $S_\gamma(f) = \mathcal{F}[\mathcal{R}(\gamma)]$, i.e., the Fourier transform of its autocorrelation function $\mathcal{R}(\gamma)$, and will exploit its properties throughout the text.[47] According to the Wiener-Kintchine theorem, σ_φ can be conveniently expressed in terms of the phase noise power spectral density $S_\varphi(f)$:

$$\sigma_\varphi^2(\tau_Q) = \langle \Delta^2 \varphi \rangle_{\tau_Q} = \int_{1/\tau_Q}^{\infty} S_\varphi(f)\, df \tag{4}$$

$S_\varphi(f)$ is dominated by two contributions. First, photons travel along telecommunication fibers, whose index of refraction n and physical length L change due to temperature, seismic, and acoustic noise in the surrounding environment. As a consequence, the phase accumulated by photons traveling through them changes over time. A second contribution comes from the fact that the initial phases of twin photons generated in Alice and Bob cannot be perfectly matched, and the way this mismatch maps onto their interference in Charlie strictly depends on the experimental layout. We will now compare the most used topologies, providing relevant models for the various terms.

4.1. Common-Laser

The typical way to ensure mutual phase coherence between Alice and Bob is to send them common laser radiation, that can be used as a phase reference to stabilize the local photon sources, so that they copy the phase of incoming light. This topology is depicted in Figure 1b. The reference laser can be conveniently, though not necessarily, hosted by Charlie. Incoming light in Alice and Bob is then a replica of the reference laser phase with additional noise due to propagation in the fiber (we assume that the stabilization of local laser sources to incoming light does not introduce noise). The residual phase noise recorded upon interference in Charlie is (see Appendix E for derivation):

$$S_\varphi(f) = 4 \sin^2 \left(\frac{2\pi f n \Delta L}{c} \right) S_{l,C}(f) + 4 \left[S_{F,A}(f) + S_{F,B}(f) \right] \tag{5}$$

where $S_{l,C}(f)$ is the noise of the reference laser, assumed to be at Charlie, and $S_{F,A}(f)$ ($S_{F,B}(f)$) is the noise of the fiber connecting Charlie to Alice (Bob). The first term accounts for self-delayed interference of the reference laser: it vanishes if the propagation delays to Alice and Bob are equal, and progressively grows for larger length mismatches, with characteristic periodical minima at $f = kc/(2n\Delta L)$, with k integer, being c the vacuum speed of light and $n = 1.45$ the typical fiber refraction index.

Evidently, the quality of the reference laser impacts the residual noise of the interference. In this work, we consider representative cases of commercial, integrated, diode lasers as well as state-of-the-art ultrastable lasers. Expressions and coefficients for the laser noise in these configurations are reported in Appendices F, G and Table F1. Intermediate values are also possible, depending on the available technology and specific layout constraints.

The second term in Equation (5) accounts for the fiber noise and depends on the environment where they are placed: metropolitan fibers affected by vehicle traffic and buildings' vibrations show larger levels of noise than cables of similar length in

country areas or seafloors. Similarly, suspended cables are found to be noisier than buried cables.[48] Finally, the fiber noise may exhibit peaks around mechanical resonances of hosting infrastructures. Reasonable scaling rules hold for buried cables, which are the majority of those used for telecommunications on regional areas, under the assumption that the noise is uncorrelated with position and homogeneously distributed along the fiber. In this case, the noise can be assumed to scale linearly with the fiber length L via an empirical coefficient l,[49] and its expression includes a faster roll-off above a characteristic cut-off Fourier frequency f_c':

$$S_F(f, L) = \frac{lL}{f^2}\left(\frac{f_c'}{f + f_c'}\right)^2 \tag{6}$$

from which $S_{F,A}(f) = S_F(f, L = L_A)$ and $S_{F,B}(f) = S_F(f, L = L_B)$ follow. The multiplication factor four for these terms in Equation (5) considers that noise is highly correlated for the forward and backward paths and adds up coherently. This is the actual scenario for parallel fibers laid in the same cable at Fourier frequencies $f \ll c/(nL_A)$ and $f \ll c/(nL_B)$. In other cases, this factor is reduced to two[49] and Equation (5) provides thus a conservative estimation. Values for l and f_c' are derived in Appendix G and reported in Table F1.

Remarkably, the common-laser approach can be conveniently implemented also in a Sagnac interferometer scheme,[45,50,51] where two counter-propagating signals are launched from the central in opposite directions along the same fiber loop, reaching A and B, then looping-back to C. This configuration is inherently immune to length mismatches, hence the first term of Equation (5) can always be neglected, making the Sagnac-loop approach particularly convenient in the case of multi-user ring networks. Nonetheless, our analysis is mainly focused on a different kind of architecture and context, specifically on point-to-point schemes, which can offer longer absolute reaches between two distant users when implemented with the active phase noise cancellation techniques described subsequently.

4.2. Independent-Lasers

Another approach is based on independent lasers at the two terminals,[36] that are phase-aligned once at the start of the key transmission window and then let evolve freely for a finite amount of time, after which a new realignment is needed. This topology is sketched in Figure 1c. Following the same approach used to derive Equation (5), the phase noise of the interference signal in Charlie can then be modeled as:

$$S_\varphi(f) = S_{l,A}(f) + S_{l,B}(f) + S_{F,A}(f) + S_{F,B}(f) \tag{7}$$

where the first and second terms describe the noise of the lasers at the two nodes, and the third and fourth terms indicate the noise of the fibers. In this topology, fiber noise appears with coefficient 1, because the photon sources in A and B are independent and there is no round-trip of the radiation into connecting fibers (the auxiliary fiber has no role in this topology, besides classical communication services). All relevant parameters are reported in Table F1. We note that again the quality of the used laser sources impacts the ultimate performances of the system, and overall higher instability and longer duty cycles could be achieved by employing lasers with superior phase coherence.

When compared to the case of a common laser, discussed in the previous Section, the independent-lasers approach is convenient from the point of view of the fiber network topology, since only a single fiber is required, and a round-trip is not necessary to distribute the reference laser. However, this introduces the drawback of the requirement of two ultrastable lasers, one in A and one in B. Indeed, here the laser quality plays an important role: in Equation (7) the laser noise terms sum up in Charlie, and they never cancel out as happens in the case of a common laser with balanced arm lengths as derived in Equation (5).

4.3. Fiber Noise Cancellation Strategies

The most impacting term in Equation (5) and (7) is fiber noise, which imposes the need for periodical phase realignment, thus reducing the duty cycle d. This aspect can be addressed with a passive approach in the Sagnac-loop configuration, where to the first order the fiber noise at low frequencies is common-mode, self-compensating with a bandwidth limit that depends on the loop length.[45,52] For long-range point-to-point connections, recent proposals[23,24] suggested an alternative, usually referenced to as dual-band stabilization, that considerably relaxes the phase-realignment need, allowing to achieve $d > 0.9$ exploiting high-bandwidth active phase noise cancellation techniques. This approach exploits an auxiliary sensing laser, traveling the same fiber as the single-photon packets, although at a detuned wavelength. Spectral separation techniques as those used in classical wavelength-division-multiplexing enable to detect interference signals produced by the sensing laser or the quantum signal on separate detectors with minimal cross-talks. The former is used to detect the fiber noise, while the latter performs the usual key extraction. First demonstrations of this approach were applied to the common-laser setup (the corresponding scheme is depicted in Figure 1d), and subsequently adapted to the independent-lasers approach.[53] Because there is no need to attenuate the sensing laser to the photon counting regime, its interference signal can be revealed by a classical photodiode with high signal-to-noise ratio (SNR). The measurement and compensation of the differential phase noise between the two arms in C allows to overcome the limit given by the light travel delay, observed in alternative noise cancellation schemes.[49,52] As a result, the fiber can be phase-stabilized in real time and with high bandwidth, e.g., by applying a suitable correction on an in-line phase or frequency modulator. Experimental demonstrations showed efficient rejection of the fiber noise, down to the limit:

$$S_F(f, L) = \frac{(\lambda_s - \lambda_q)^2}{\lambda_s^2}\frac{lL}{f^2} \tag{8}$$

where λ_s and λ_q are the wavelengths of the sensing laser and quantum key transmission signal respectively, and the suppression factor $(\lambda_s - \lambda_q)^2/\lambda_s^2$ is set by the fact that the fibers are stabilized based on the information from the former, while the quantum interference occurs at the latter.[24] Other reasons for deviation from the expected behavior may be short fiber paths

that are not common between the two lasers (e.g., wavelength-selective couplers), whose fluctuations cannot be perfectly canceled. Advanced correction strategies can further suppress these contributions and ensure virtually endless phase stability.[23] Finally, the detection noise of the sensing laser interference may represent the ultimate practical limit on very lossy links. This aspect is discussed in Appendix G.

Interestingly, it can be seen that if the sensing laser is phase-coherent to the reference laser, the residual reference laser noise is canceled out together with the fiber noise. Phase-coherence between lasers separated by 50GHz or 100GHz (the minimum spectral separation that allows optical routing with telecom devices) can be achieved by locking multiple lasers to the same cavity or by phase-modulation-sideband locking. This concept has been further developed in ref. [53], that successfully conjugates the independent-lasers approach with fiber stabilization.

5. Improving Detection SNR

The maximum communication distance is limited by the dark count rate P_{DC} of the single-photon detectors (SPDs), i.e., the intrinsic level of noise of the detector in the absence of any signal. P_{DC} depends on the kind of SPD used and on the operating conditions. At telecom wavelengths, the most common solutions are InGaAs/InP single-photon avalanche diodes (SPADs), with either thermoelectric or Stirling cooling, and superconductive nanowire single-photon detectors (SNSPDs). More details and less common technologies can be found in ref. [54]. SNSPDs can reach dark count rates as low as $P_{DC} < 0.01$Hz,[55] photon detection efficiency above 90%,[56] sub-3ps timing jitter[57] and dead time below 1ns.[58] These interesting properties come at the significant cost of requiring cryostats capable to operate in the range 1–4K, which is expensive and adds technical limitations. Commercial solutions are now available that allow high-efficiency detection and quite low dark count level (typically 10Hz), but SPADs are still generally preferred for in-field applications, accepting lower general performance. Modern SPADs, working in gated mode, present photon detection efficiency around 30%,[59] timing jitter below 70ps[54] and short dead times, allowing to reach maximum count rates of more than 500 MHz with experimental devices (see, e.g., ref. [60]). Dark count rates vary considerably depending on the temperature of the sensor. Units that use thermoelectric cooling (around -40°C) report values of hundreds or thousands of counts per second.[61] More effective Stirling coolers (reaching -100°C) instead have P_{DC} <100Hz.[62] Depending on the applications, other properties like maximum gating frequency, after-pulsing probability, back-flash probability, and detection area need to be taken into account.

In a real-world QKD implementation, residual background photons due to the environment could be present in the dark fiber. It is important to reduce the background photons at the same level or below the rate of the dark counts of the detectors. There are several sources of background photons. Photons may leak into the dark fiber from nearby fibers laid in the same cable, possibly hosting data traffic at wavelengths close to those used for the TF-QKD encoding. Moreover, in Sagnac-loop and time-multiplexed protocols, where strong classical signals at the quantum wavelength travel along the same fibers, single and double Rayleigh scattering can represent an important source of background photons.[45,63] The implementation of dual-band strategies for phase stabilization allows to strongly suppress these effects,[23] since phase stabilization relies on a different wavelength that can be suppressed by spectral filters. Nonetheless, advanced approaches to TF-QKD as those described before pose additional challenges. For instance, photons from the reference laser sent from Charlie to Alice and Bob through a separate fiber in the common-laser scheme (Section 4) can be Rayleigh-scattered and evanescently couple to the fiber dedicated to the quantum transmission. Despite the probability of this process, combined with evanescent coupling, is small, the reference laser power must be carefully attenuated to ensure reliable referencing of slave lasers while keeping the background count rate suitably low. For example, the Rayleigh scattering effect becomes negligible when the power of the reference laser sent from Charlie to Alice and Bob through the respective service fibers is of the order of 20μW.[24] This guarantees sufficient reference signal for locking and regenerating the independent lasers in Alice and Bob separated by hundreds of km, before being attenuated to the single photon level and encoded, giving a negligible contribution to dark counts.

When dual-band noise detection and cancellation are considered, relevant sources of background photons in the quantum channel are the amplified spontaneous emission (ASE) of employed laser sources and the spontaneous Raman effect. ASE noise from diode or fiber lasers considerably exceeds the spectral separation of the sensing and quantum lasers in a dual-band transmission. As the two co-propagate in the quantum fiber, efficient filtering is required at the SPDs in Charlie. Standard Bragg-grating filters employed in classical telecommunications have relevant drops in efficiency outside the range 1300–1600 nm, which may result in background ASE photons to fall on the SPDs, and must therefore be complemented by dedicated equipment in TF-QKD setups. Raman scattering of the sensing laser propagating in the quantum fiber generates background photons on a broad spectrum, that extends to the QKD wavelength channel. As such it cannot be efficiently filtered out, and the only mitigation strategy is again a careful adjustment of the launched sensing laser power to meet a condition where the Raman photon background remains negligible with respect to the quantum signal.

Instead of focusing on ultra-low-noise detectors, in our analysis we considered two realistic scenarios with different commercial detectors: one using best-in-class InGaAs/InP SPADs, with Stirling cooler and dark count rate from 3 to 60Hz, corresponding to a quantum efficiency respectively of 10% and 25%; the other adopting lower-noise and more efficient, but still commercially available, SNSPDs, with dark count rate of 10Hz and quantum efficiency of 90%.

6. Results for the Simulation of Realistic Key Rates

Having discussed in the previous Sections the main experimental parameters that characterize the standard operation of the TF-QKD setup, in this Section, we evaluate their impact on the expected key rates, focusing on the role of phase noise and detector performance. We consider various configurations that are possible for a TF-QKD layout, characterized by either common or independent sources, which are stabilized or not, with or without fiber stabilization, and with varying detector

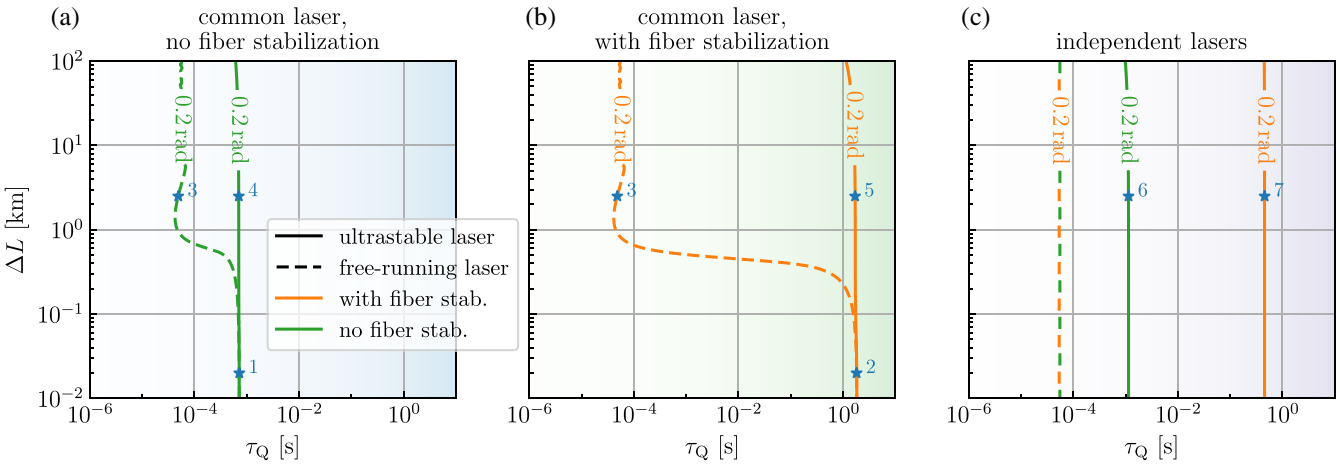

Figure 2. Level curves at constant phase standard deviation σ_φ, calculated in the space of fiber length mismatch ΔL and integration time τ_Q, for each possible combination of laser source configuration and fiber stabilization, at fixed short arm length $L_B = 100$ km. The corresponding σ_φ maps are reported in Figure H2. The numbered points represent the specific scenarios of Table 1, which are considered in the simulations.

performance. For each combination, we calculate the phase noise and corresponding variance σ_φ^2 from Equation (4). We fix an upper limit to tolerated phase fluctuations of $\sigma_\varphi = 0.2$rad, that leads to $e_\varphi = 0.01$ from Equation (1), which is a standard conservative value for the phase-misalignment contribution to QBER. The integration time τ_Q at which this threshold is achieved determines the duty cycle d, which is then used to evaluate the key rate. Notice that the duty cycle saturates to unity for integration times $\tau_Q \gg \tau_{PS}$, and that, anyway, $\tau_Q \gtrsim 1$s is probably unrealistic due to general realignment processes that are nevertheless to be performed. In particular, polarization drift given by fiber birefringence and thermal effects introduce polarization mismatch errors that must be corrected periodically. Experimental experience and literature show that these effects occur on slow timescales, and polarization re-alignment procedures are usually implemented at low rates of a few Hz.[53,64] Moreover, due to frequency drifts of the free-running local oscillators used to clock encoders and decoders, typically time re-synchronization routines must be performed periodically every few seconds to maintain the required synchronization between the nodes. Our approach of fixing the phase error threshold could be relaxed, in a more refined approach, by optimizing τ_Q and σ_φ to maximize the key rate for each protocol and distance separately.

In **Figure 2**, we report the isolines matching $\sigma_\varphi = 0.2$rad as a function of τ_Q and fiber length mismatch $\Delta L = L_A - L_B$ at which such threshold is reached. As a reference, the length of the shorter interferometer arm BC is considered constant and equal to $L_B = 100$ km. We observe that the most favorable configuration, with τ_Q exceeding 1s, is reached with a common cavity-stabilized laser, with fiber stabilization (panel b, solid line). This configuration is mostly insensitive to fiber length mismatch, over any reasonable range. On the contrary, if an unstabilized free-running laser is considered (dashed line), the mismatch causes τ_Q to drop rapidly below 100 μs for ΔL greater than a few hundred meters. This distance represents the crossover to a regime where the integrated laser noise exceeds the given phase noise threshold, and scales as the coherence length of the laser. The analogous configurations without fiber stabilization (panel a) show similar behaviors, although the highest τ_Q values are lower by more than three orders of magnitude due to fiber noise. Finally, as expected, the configurations with independent laser sources (panel c) do not show any dependence on the fiber length mismatch. In particular, the configurations with free-running independent laser sources (dashed lines) correspond to very low τ_Q values. Conversely, when ultrastable lasers are considered, we observe a significant increase in τ_Q, similar to the common-laser case. Details of this analysis are described in Appendix H.

To study the impact of these parameters on key rate, we now restrict our attention to the seven realistic scenarios listed in **Table 1**, representing specific configurations and values of ΔL, and we mark them as stars in Figure 2. Since with just a few hundred meters mismatch the impact of unstabilized laser source noise is significant,[53] in Scenarios 3, 4, and 7 we set a representative significant length mismatch $\Delta L = 2.5$km, while for Scenario 1 and 2 we model a negligible mismatch of $\Delta L = 20$m. Even in the most favorable configurations, τ_Q was limited to 100 ms to conservatively account for general realignment processes (polarization, time re-synchronization) required beyond this limit. Based on these scenarios, we simulate the key rates of the CAL

Table 1. Considered scenarios, marked as stars in Figure 2, whose key rates are evaluated in Figure 3 and 4. They are characterized by the source and fiber configurations, and by the length mismatch ΔL.

Source configuration	Fiber stabilization	ΔL	Scenario
Free-running common laser	NO	20m	1
	YES	20m	2
	ANY	2.5km	3
Ultrastable common laser	NO	2.5km	4
	YES	2.5km	5
Ultrastable independent lasers	NO	ANY	6
	YES	ANY	7

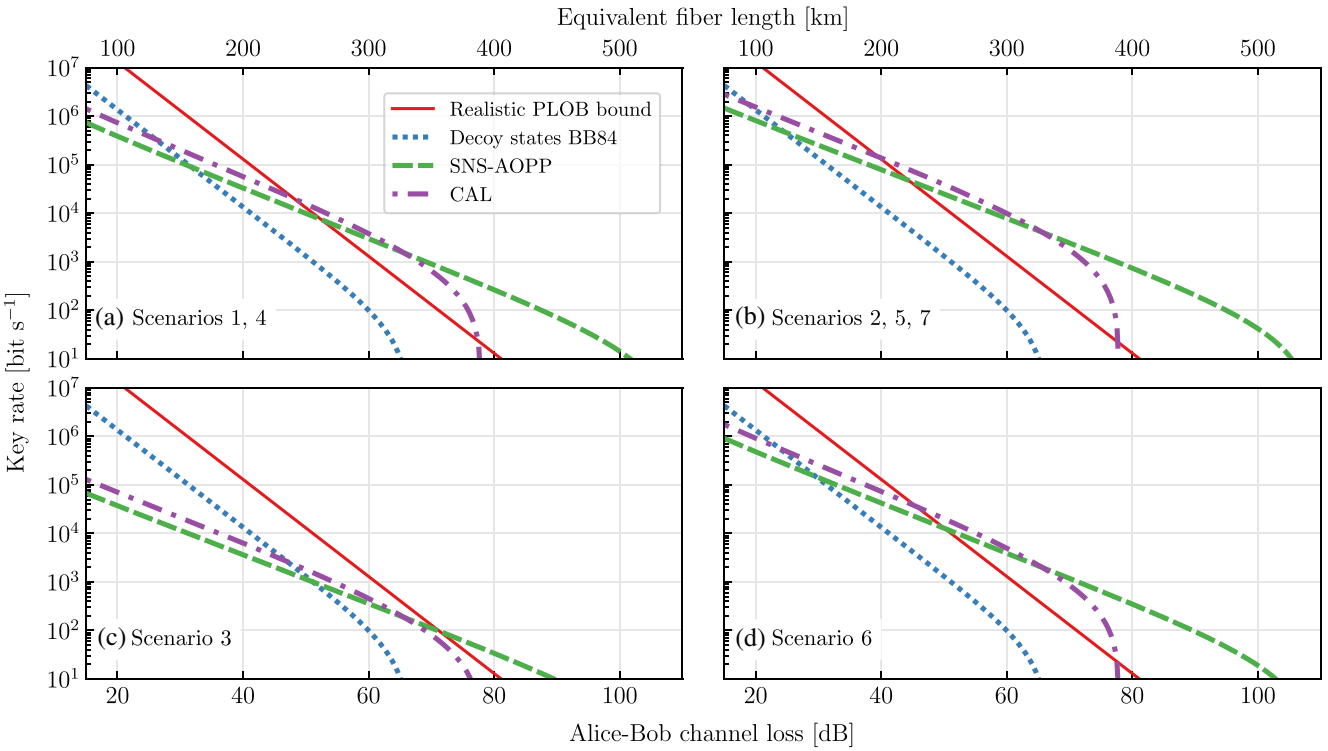

Figure 3. Simulated key rates of the BB84, SNS-AOPP, and CAL protocols in the scenarios described in Table 1, with varying total loss and considering SNSPDs. A reference PLOB bound with effective attenuation is plotted. Panel a (b) reports simulations of Scenario 1 (2), which are graphically indistinguishable from those of Scenario 4 (5, 7).

and SNS-AOPP protocols, assuming a phase-synchronization overhead of $\tau_{PS} = 1$ms.[24] As a reference, we consider a "realistic" PLOB bound, where the transmission is effectively multiplied by the same detection efficiency η_D employed in the simulations of the other protocols, and we also evaluate the key rate for the phase-based efficient BB84 protocol endowed with decoy states.[40–42,65,66] The latter employs the same decoy parameter estimation and channel and detector models as described in Appendix A and summarized in Appendix C, however assuming no role for phase noise. The parameters used in the simulations are described in Appendix D. To analyze the impact of detector performance, we reproduce the scenarios considering either SNSPDs or SPADs, as described in Section 5.

Because of similar values of τ_Q, some of the seven scenarios of Table 1 result in the same or very similar key rates, therefore we group them in four representative panels of **Figure 3**, where representative SNSPDs are considered. These results show that unstabilized fibers are usually the largest contribution to decoherence and limit τ_Q to less than 1ms (Scenarios 1, 4, and 6), except for the case when unstable lasers are used and no care is taken to match the optical paths' length. In this case, the residual self-delayed laser noise limits τ_Q to about 50 μs (Scenario 3). Using fiber and laser stabilization, either with a single common laser (Scenario 5) or a pair of independent lasers (Scenario 7), ensures $\tau_Q > 100$ ms even in the presence of a large imbalance in the interferometer arms, with corresponding duty cycles approaching 100% and no impact on the QBER. Scenario 2 is the only unstabilized laser case matching Scenarios 5 and 7, only because there is negligible length mismatch and the dominant noise is taken care of by fiber stabilization. In all scenarios, a prepare-and-measure approach features worse key rates than TF-QKD, for losses significantly larger than those typical of metropolitan networks. In **Figure 4**, the same scenarios are considered, but the detectors are best-in-class SPADs, as representative of more standard in-field setups. Quite generically, the increased dark count rate reduces the maximum reachable distance, while the lower efficiency reduces the key rates for any distance. Besides these very noticeable differences with respect to Figure 3, the considerations that we made pertaining to the role of phase noise are unaffected.

In the simulations shown here and in Appendices A and B, we recall that we make the assumption that asymmetric channels are treated by adding losses A_+ in the channel with higher transmittance. Optimized protocols have been proposed for both SNS[67] and CAL[21,68,69] for such asymmetric case. The intensities of the signals and decoy intensities at the two transmitters, among the other parameters, are independently optimized, achieving a higher key rate than with adding losses. We point out that these approaches only solve the problem of mismatched intensities at Charlie. Fiber length mismatches will still introduce problems related to distributed laser coherence, as discussed in detail in Section 4. The length imbalances are intrinsically compensated in the case of Sagnac fiber-loop networks.[50,51,69] Conversely, the mismatch effects are evident when using free-running lasers in point-to-point schemes, where the fiber lengths should be matched at the order of 100m to obtain an optimal transmission window. Although being feasible in the laboratory, this can represent an important limit to implement TF-QKD in realistic networks, where the fibers and the communication nodes are

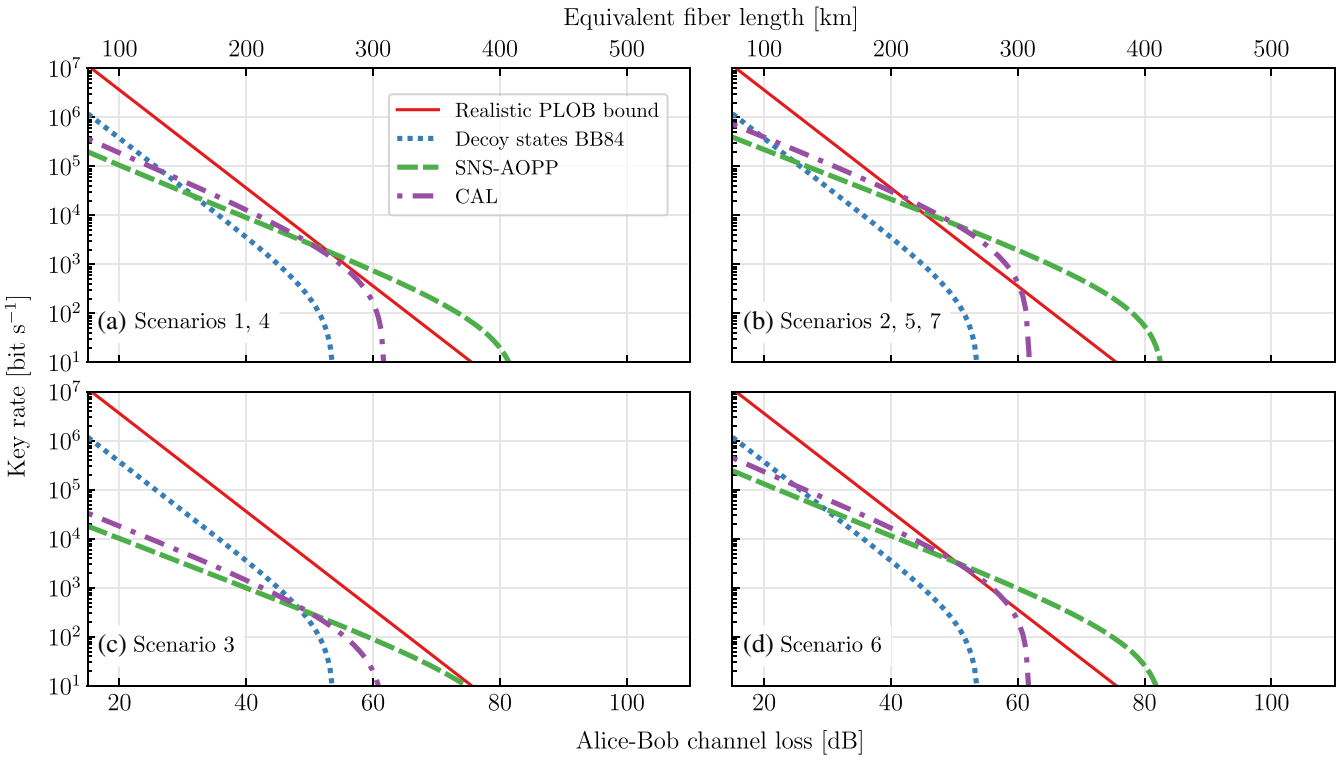

Figure 4. Key rates as in Figure 3, but considering representative SPADs.

deployed according to different criteria, typically interconnecting inhabited towns along existing infrastructures and depending on the territory topology. This way, the imbalance between nodes is typically of several km, which in principle can be compensated with the addition of dedicated fiber spools, possibly in the service channels. However, balancing the interferometer arm lengths by using fiber spools needs preliminary calibrations, requires additional hardware to be installed at the telecom shelters, and limits the flexibility in terms of possible dynamic network reconfiguration. All these factors pose constraints to the fiber providers, which are not negligible in production environments. Our results show that such requirements can be strongly relaxed by taking advantage of the reduced phase noise resulting from ultrastable lasers and fiber noise cancellation techniques, improving the applicability of TF-QKD to realistic network scenarios.

7. Conclusion

TF-QKD is one of the most promising candidate solutions for extending the range of real implementation of QKD in fiber. Here, we have discussed the impact of the dominant noise sources in TF-QKD protocols when implemented in real-world conditions, providing a significant contribution toward their in-field use. We provided an open and unified framework for the modeling of major noise sources and the estimation of key rates, and we specifically addressed the phase noise of photon sources and connecting fibers, showing how implementation aspects such as the quality of the used lasers, the adopted topology, the fiber length and imbalance in the two arms play a role in the final key rate and duty cycle. Interestingly, we observed that both the CAL and SNS protocols are impacted by phase noise in a similar way, although the relevant parameters enter the process via different mechanisms. We also highlighted the role of detector performance in significantly affecting the maximum achievable distance. We showed as well how the overall key rate can be improved by a factor $\gtrsim 2$ using narrow-linewidth lasers and phase-control techniques as those developed to compare remote optical clocks on continental scales. With best-in-class but realistically deployable setups, we show that distances up to 500 km can be considered. Synergy with the concurrent development of high-precision time/frequency distribution services[28] is thus advisable, to lower the cost of deployment and achieve optimal usage of TF-QKD equipment. Ultrastable lasers are nowadays found on the market in plug-and-play, compact, and portable setups, and the technology is rapidly evolving toward further integration and miniaturization. We envisage these to be fruitfully combined with advanced phase-stabilization procedures,[53] towards an efficient and flexible TF-QKD implementation strategy on existing networks. These approaches would also allow to relax the constraints on the fiber network operators, hence facilitating the adoption of TF-QKD on a larger and operative scale. A critical application will be the establishment of long-haul links in the upcoming European Quantum Communication Infrastructure,[32] aiming at securely connecting distant quantum metropolitan area networks. Very recently, new MDI-QKD protocols such as mode-pairing QKD were proposed, that although first-order insensitive on laser and fiber noise, may still benefit from their active stabilization.[53] Also, we prospect that our considerations can be useful in the implementation of continuous-variable QKD,[70,71] where similar challenges are encountered.

Proper handling of the phase noise and practical constraints of a given real-world network enables to consistently predict the expected key rate of a TF-QKD link and choose the optimal protocol, layout design, and operating parameters depending on the network topology, available infrastructure and target performance. The code for the reproduction of the results of this study, and for the estimation of key rates with varying setup and protocol parameters, is openly available at ref. [35].

Appendix A: Sending-or-Not-Sending Protocol

In this Appendix the SNS protocol is discussed, starting with a description of the protocol, the estimation of the secret-key rate and then a highlight on how to include errors coming from phase instability in the channel. After its first proposal,[36] this protocol attracted significant interest, with several works improving its security in practical cases (see, e.g., ref. [43]), increasing the achievable range[44] and comparing it with other TF-QKD solutions.[22,23]

It can be partitioned in the following steps:

- at each time slot, the parties commit to a Signal window with probability p_Z or to a Decoy window with probability $p_X = 1 - p_Z$.
- if Alice (Bob) chooses Signal, with probability ϵ, she (he) decides *sending* and fixes a bit value 1 (0). With probability $(1-\epsilon)$ she (he) decides not-sending and fixes a bit value 0 (1);
- if sending was chosen, *they* send a phase-randomized weak coherent state $|\sqrt{\mu_Z}\rangle \exp(i\phi')$, with intensity μ_Z and phase ϕ' (never disclosed);
- following the decision of not-sending, *they* send out the vacuum state (or, more generally, a phase-randomized coherent state with very small intensity μ_0). Notice that *sending* or *not sending* determines the bit value, not the intensity, phase or photon number;
- if *they* chose Decoy, *they* send out a phase-randomized coherent state with intensity randomly chosen from a predetermined set $|\sqrt{\mu_k}\rangle \exp(i\phi')$, $k = 1, 2, 3 \ldots$. Note that the phase values in the decoy windows will be disclosed after the end of the whole transmission session, in order to reconcile the phase slices and estimate the phase error rate;
- afterward, *they* classify the time windows in the following way:
- Z window: *they* both chose Signal;
- $\tilde{Z}$ window: Z window in which only one sends;
- $\tilde{Z}_1$ window: $\tilde{Z}$ window in which a single-photon state is sent. This may contribute to the key rate;
- X_k window: *they* both chose Decoy, and the same decoy intensity μ_k;
- effective window: Charlie announces only one detector click. Only these cases may contribute to building the final key. Double-click and zero-click events are discarded and they therefore contribute to the bit-flip QBER;
- key distillation starts by the declaration by Charlie of the n_t effective Z windows;
- *they* publicly choose a small sample of effective Z windows, which will have to be discarded (asymptotically this is negligible), for estimating the bit-flip error rate $E_Z = (n_{NN} + n_{SS})/n_t$. For this sample, *they* indeed disclose whether *they* both chose sending (rate n_{SS}/n_t) or both not-sending (rate n_{NN}/n_t);
- estimate number of untagged bits: only effective $\tilde{Z}$ windows. Indeed multiphoton signals must be considered tagged (attacked by Eve). Their number cannot be measured. Their lower bound $\underline{n}_1$, and the upper bound $\bar{e}_1^{ph}$ of their phase error, can be estimated using decoy states, in particular using effective X_k windows (see Appendix C).

The secret key per transmitted qubit with unity duty cycle can be estimated with the following expression[44]

$$\underline{R} = p_Z^2 \left[\underline{n}_1 \left(1 - H_2 \left(\bar{e}_1^{ph} \right) \right) - f_{EC} n_t H_2(E_Z) \right] \tag{A1}$$

Asymptotically, we let the sifting factor $p_Z^2 = 1$, however notice that the decoy measurements might be inefficient with large enough phase errors or losses, or short keys, so that it could be unrealistic to fix $p_X \approx 0$.

In order to keep under control the bit-flip error rate, small values of the sending probability ϵ must be chosen (a few percent). Error rejection techniques[44] can be applied before the parameter estimation stage to reduce the bit-flip errors, allowing the use of larger values of ϵ. The steps can be organized as follows:

- First of all, one can take into account in the key rate expression that the bit-flip error rates for bits 0 and 1 are intrinsically different in this protocol.
- Afterwards, the parties perform synchronized random pairing of their raw key bits. Then, they compare the parity of the pairs, discarding pairs with different parity and keeping the first bit of pairs with the same parity. The effect is a rejection of a fraction of bit-flip errors, at the cost of a cut in the length of the raw key.
- By scrutinizing the residual bit-flip error rate of the survived bits, it turns out that it is still high for even-parity pairs. One can keep just the odd-parity pairs, the number of which will be on average $N_{odd} = N_0 N_1/(N_0 + N_1)$, where N_0 (N_1) represent the number of 0s (1s) in the raw key string of Bob.
- SNS-AOPP: the last evolution consists in substituting the random pairing with actively pairing the bits in odd-parity pairs. In this case, the number of odd-parity pairs will increase to $N_{odd}^{AOPP} = \min(N_1, N_0)$. Also in this case, only the first bit in each pair is kept. The final key rate can be estimated as Equation (2), where n_t is the length of the string after AOPP, of which $\underline{n}'_1$ are untagged, while $\bar{e}_1^{'ph}$ and E'_Z are the phase and bit-flip error rate after AOPP. Complete expressions can be found in ref. [44].

Appendix B: Curty-Azuma-Lo Protocol

The CAL protocol was proposed in 2019 by M. Curty, K. Azuma, and H.-K. Lo in ref. [37] and a proof-of-principle experimental demonstration can be found in ref. [45]. The protocol relies on the pre-selection of a global phase and is conceptually very simple, consisting in the following steps:

- First of all, Alice (Bob) chooses with probability p_X the X basis (key generation) and with probability $p_Z = 1 - p_X$ the Z basis (control). In the time slots in which her (his) choice was the X basis, she (he) draws a random bit b_A (b_B). Then, she (he) prepares an optical pulse a (b) in the coherent state $|\zeta\rangle_{a(b)}$ for $b_A = 0$ ($b_B = 0$) or $|-\zeta\rangle_{a(b)}$ for $b_A = 1$ ($b_B = 1$). In the time slots in which her (his) choice is the Z basis, she (he) prepares an optical pulse a (b) in a phase-randomized coherent state $\hat{\rho}_{a,\beta_A}$ ($\hat{\rho}_{B,\beta_B}$) where the amplitude β_A (β_B) is chosen from a set $S = \{\beta_i\}_i$ of real non-negative numbers $\beta_i \geq 0$, according to a probability distribution p_{β_A} (p_{β_B}).
- Alice and Bob transmit the optical pulses a and b over channels with transmittance $\sqrt{\eta}$ toward the middle node C and synchronize their arrival.
- Node C interferes the incoming optical pulses a and b on a 50:50 beamsplitter. The output ports are coupled to two threshold detectors, D_c and D_d, associated respectively to constructive and destructive interference.
- C announces publicly the measurement outcomes k_c and k_d corresponding to detectors D_c and D_d. A click event is indicated by $k_i = 0$ and a no-click event by $k_i = 1$, with $i = c, d$.
- The raw key is generated by Alice and Bob concatenating the bits b_A and b_B (b_A and $b_B \oplus 1$) when node C announces $k_c = 1$ and $k_d = 0$ ($k_c = 0$ and $k_d = 1$) and Alice and Bob chose the X basis.

The protocol requires a common phase reference between Alice and Bob for the key generation basis. Local phase randomization is applied in the Z basis, allowing the application of the decoy-state technique to infer the contribution of vacuum, single-photon, and multi-photon events. For the security proof, the authors invoke a "complementarity" relation

between the phase and the photon number of a bosonic mode. The details can be found in ref. [37].

The final secret key per time slot can be lower bounded by the following expression, summing the contribution from the single-click events ($k_c = 1, k_d = 0$) and ($k_c = 0, k_d = 1$)

$$\underline{R}_X = \underline{R}_{X,10} + \underline{R}_{X,01} \tag{B1}$$

where

$$\underline{R}_{X,k_c k_d} = p_{XX}(k_c, k_d)[1 - f_{EC} H_2(e_{X,k_c k_d}) - H_2(\min\{1/2, \bar{e}_{Z,k_c k_d}\})] \tag{B2}$$

In the expression above, $p_{XX}(k_c, k_d)$ represents the total gain when Alice and Bob choose the X basis, $e_{X,k_c k_d}$ is the bit error rate in the X basis, while $\bar{e}_{Z,k_c k_d}$ is the upper bound on the phase error rate. The estimation of these quantities is detailed in the following paragraphs.

The total gain for the generation events can be expressed as

$$\begin{aligned} p_{XX}(k_c, k_d) &= \frac{1}{4} \sum_{b_A, b_B = 0,1} p_{XX}(k_c, k_d | b_A, b_B) = \\ &= \frac{1}{2}(1 - p_d)\left(e^{-\gamma\Omega(\sigma_\varphi,\theta)} + e^{\gamma\Omega(\sigma_\varphi,\theta)}\right)e^{-\gamma} - (1 - p_d)^2 e^{-2\gamma} \end{aligned} \tag{B3}$$

The second expression is obtained by modeling the channel for simulations, see supplementary information of ref. [37] for details. The model consists in a loss $\sqrt{\eta}$, a phase mismatch σ_φ and a polarization mismatch θ, giving rise to the parameters $\gamma = \sqrt{\eta}\mu_\zeta$ (with $\mu_\zeta = |\zeta|^2$ the intensity of the signal states) and $\Omega = \cos\sigma_\varphi \cos\theta$.

The bit error rate can also be estimated by the channel model as

$$e_{X,k_c k_d} = \frac{e^{-\gamma\Omega(\sigma_\varphi,\theta)} - (1 - p_d)e^{-\gamma}}{e^{-\gamma\Omega(\sigma_\varphi,\theta)} + e^{\gamma\Omega(\sigma_\varphi,\theta)} - 2(1 - p_d)e^{-\gamma}} \tag{B4}$$

The phase error rate requires a more involved analysis. Following Equations 10 to 15 of ref. [37] and its supplementary material, one can obtain the following expression for the upper bound on the error in the Z basis

$$\bar{e}_{Z,k_c k_d} \leq \frac{1}{p_{XX}(k_c, k_d)} \sum_{j=0,1} \times \left[\sum_{(m_A, m_B) \in S_j} c^{(j)}_{2m_A + j} c^{(j)}_{2m_B + j} \sqrt{\bar{p}_{ZZ}(k_c, k_d | 2m_A + j, 2m_B + j)} + \Delta_j\right]^2 \tag{B5}$$

We only keep the $\bar{p}_{ZZ}$ gains for low number of photons (defined in the set $\mathcal{S}_j$), while the other probabilities are trivially upper-bounded by 1 and are included in the term Δ_j. In ref. [37] a numerical method to estimate the $\bar{p}_{ZZ}$ gains for a finite number of decoy intensities is reported. In ref. [46], instead, these quantities are estimated analytically for two, three and four decoy intensities. Since one can show that realistic implementations with three or four decoy intensities are almost optimal, in this work the gains are analytically estimated assuming an infinite number of decoy intensities, following the Supporting Information of ref. [37]. Similarly to the simulations in ref. [37], the sets are chosen as $\mathcal{S}_0 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ and $\mathcal{S}_1 = (0, 0)$ and the bounds may be improved by adding more terms in the estimation. It turns out that the phase error rate is independent of the phase mismatch, while it has an important effect on the bit error rate. To keep the phase error rate low enough, small values of the signal intensity must be chosen, around 0.02. In the SNS protocol, on the other hand, small values of the sending probability are chosen to lower the error rate, leading to comparable effects on the key rate.

Appendix C: Decoy State Expressions

For completeness, we report here the expressions for the error estimates in the three-decoy-state approach,[40–42] that we used both in the phase-encoded BB84 calculations and for the phase error in the SNS protocol.

The gain for each laser intensity $\mu = u, v, w$ and effective transmission $\hat{\eta}$ is:

$$Q_\mu = 1 - (1 - p_{DC})e^{-\mu\hat{\eta}} \tag{C1}$$

The corresponding total QBER is modeled as

$$E_\mu = \left[\frac{p_{DC}}{2} + \left(e_\theta + e_\varphi - \frac{p_{DC}}{2}\right)e^{-\mu\hat{\eta}}\right]/Q_\mu \tag{C2}$$

where e_θ and e_φ are the optical and the phase noise errors, respectively, as defined in the main text. For the phase-encoded BB84 protocol, which has only a single channel of length $L_A + L_B$ along which interfering photons are separated only by a few ns, we assume $e_\varphi = 0$.

Assuming that intensity $\mu = u$ is matched to the relevant signal intensity and that $u > v > w$, then the lower bounds for the zero and single-photon yield are given by

$$\underline{Y}_0 = \frac{vQ_w e^w - wQ_v e^v}{v - w} \tag{C3}$$

$$\underline{Y}_1 = \frac{u^2(Q_v e^v - Q_w e^w) - (v^2 - w^2)(Q_u e^u - \underline{Y}_0)}{u(u - v - w)(v - w)} \tag{C4}$$

so that the single-photon lower bound for the gain and upper bound for the phase error are estimated by

$$\underline{Q}_1 = \underline{Y}_1 u e^{-u} \tag{C5}$$

$$\bar{e}_1^{ph} = \frac{E_v Q_v e^v - E_w Q_w e^w}{(v - w)\underline{Y}_1} \tag{C6}$$

In the case of the phase-encoded BB84 model, the key rate expression that we use is

$$R = d\left[\underline{Q}_1\left(1 - H_2(\bar{e}_1^{ph})\right) - f_{EC} Q_u H_2(E_u)\right] \tag{C7}$$

with duty cycle asymptotically set to $d = 1$ in the efficient imbalanced basis selection setting.

Appendix D: Parameters of Key Rate Simulations

Common parameters employed in the simulations are reported in **Table D1** and discussed here. A representative attenuation coefficient $\alpha = 0.2\text{dB km}^{-1}$ is chosen, considering that the typical attenuation in real-field can exceed 0.25dB km^{-1}, while new-generation laboratory fibers reach 0.16dB km^{-1}.[22,34] As a best-in-class commercial SNSPD, we consider dark count rate $P_{DC}^{SNSPD} = 10\text{Hz}$, corresponding to dark counts per pulse

Table D1. Parameters of key rate simulation.

α	ν_s	τ_{PS}	e_θ	P_{DC}^{SNSPD}	η_D^{SNSPD}	P_{DC}^{SPAD}	η_D^{SPAD}
0.2dB km^{-1}	1GHz	1ms	0.02	10Hz	0.9	50Hz	0.25

u	v	w	μ_Z	μ_0	μ_ζ	ϵ	f_{EC}
0.4	0.16	10^{-5}	0.2	5×10^{-6}	0.018	0.25	1.15

Table F1. Recap of analytical models for the various terms needed to evaluate the phase jitter and coefficients extrapolated from experimental data.

Laser (free)	$S_{\mathrm{l,free}}(f) = \frac{r_3}{f^3} + \frac{r_2}{f^2}\left(\frac{f_c}{f+f_c}\right)^2$	r_3 $3\times10^6\,\mathrm{rad^2\,Hz^2}$	r_2 $3\times10^2\,\mathrm{rad^2\,Hz}$	f_c 2 MHz	
Laser (stable)	$S_{\mathrm{l,stab}}(f) = S_{\mathrm{cavity}}(f) + \left\lvert\frac{1}{1+G(f)}\right\rvert^2 S_{\mathrm{l,free}}(f)$				
Cavity	$S_{\mathrm{cavity}}(f) = \frac{C_4}{f^4} + \frac{C_3}{f^3} + \frac{C_2}{f^2}$	C_4 $0.5\,\mathrm{rad^2\,Hz^3}$	C_3 $0\,\mathrm{rad^2\,Hz^2}$	C_2 $2\times10^{-3}\,\mathrm{rad^2\,Hz}$	
Loop	$G(f) = G_0\frac{1}{(2\pi i f)^2}\frac{if+B\gamma}{if+B\delta}$	B 300kHz	γ 0.1	δ 10	G_0 $3.55\times10^{13}\,\mathrm{Hz^2}$
Fiber (free)	$S_{\mathrm{F}}(f,L) = \frac{lL}{f^2}\left(\frac{f_c'}{f+f_c'}\right)^2$	l $44\,\mathrm{rad^2\,Hz\,km^{-1}}$	f_c' 100Hz		
Fiber (stable)	$S_{\mathrm{F,s}}(f,L) = \frac{(\lambda_s-\lambda_q)^2}{\lambda_s^2}\frac{lL}{f^2} + s_0\left(\frac{f_c''}{f+f_c''}\right)^2$	s_0 $1\times10^{-8}\,\mathrm{rad^2\,Hz^{-1}}$	f_c'' 200kHz	λ_s 1543.33nm	λ_q 1542.14nm

$p_{\mathrm{DC}}^{\mathrm{SNSPD}} = P_{\mathrm{DC}}^{\mathrm{SNSPD}}/\nu_s = 10^{-8}$, with efficiency $\eta_{\mathrm{D}}^{\mathrm{SNSPD}} = 90\%$ and nominal source clock rate $\nu_s = 1$GHz. As a more common best-in-class commercial SPAD, we consider dark count rate $P_{\mathrm{DC}}^{\mathrm{SPAD}} = 50$Hz, corresponding to dark counts per pulse $p_{\mathrm{DC}}^{\mathrm{SPAD}} = 5\times10^{-8}$, with efficiency $\eta_{\mathrm{D}}^{\mathrm{SPAD}} = 25\%$. The total intensities for the three decoy states u, v, w used in the SNS-AOPP and phase-encoded BB84 protocols are taken from ref. [22]. Intensities for the *sending* and *not sending* choices in the SNS-AOPP protocol are set to $\mu_Z = u/2$ and $\mu_0 = w/2$, respectively, while intensity for the Alice signal in BB84 corresponds to u, and signal intensity in the CAL protocol is set to the value optimized in ref. [45].

Appendix E: Derivation of the Common-Laser Phase Noise Spectrum

Following the scheme shown in Figure 1b, let us assume that the instantaneous phase of the reference laser in Charlie is $\varphi_{\mathrm{l,C}}$. While traveling to Alice and Bob, the signal acquires additional phase $\varphi_{\mathrm{F,X}}$, with X = A,B. Here and in the following we adopt a compact notation in which $\varphi_{\mathrm{F,X}}(t_{\mathrm{out}})$ identifies the integrated phase of a fiber with length L_{X} accumulated during the whole journey, from the moment radiation enters in it ($t_{\mathrm{out}} - nL_{\mathrm{X}}/c$) till the moment it exits (t_{out}). Photon sources in Alice and Bob are phase-locked to incoming light and have therefore instantaneous phase $\varphi_{\mathrm{l,X}}(t) = \varphi_{\mathrm{l,C}}(t - nL_{\mathrm{X}}/c) + \varphi_{\mathrm{F,X}}(t)$. This is a replica of the original reference laser phase, with additive noise due to propagation in the fiber. In turn, these photons are sent to Charlie, acquiring further phase due to backward trip in the quantum fiber. Assuming the noise of the auxiliary and quantum fibers to be highly correlated (this is justified as they are housed in the same optical cable), the relative phase of interfering photons in Charlie at time t is thus rewritten as:

$$\begin{aligned}\Delta\varphi(t) = {} & \varphi_{\mathrm{l,C}}(t - 2nL_{\mathrm{A}}/c) + \varphi_{\mathrm{F,A}}(t - nL_{\mathrm{A}}/c) + \varphi_{\mathrm{F,A}}(t) \\ & - \varphi_{\mathrm{l,C}}(t - 2nL_{\mathrm{B}}/c) - \varphi_{\mathrm{F,B}}(t - nL_{\mathrm{B}}/c) - \varphi_{\mathrm{F,B}}(t)\end{aligned} \tag{E1}$$

Under the assumption that the fiber deformations change on timescales much longer than the light round-trip time, $\varphi_{\mathrm{F,X}}(t) \approx \varphi_{\mathrm{F,X}}(t - nL_{\mathrm{X}}/c)$ and these two terms add up coherently. Computing the autocorrelation function of the various terms of Equation (E1) and the corresponding Fourier transforms, and using the property that the Fourier transform $\mathcal{F}[y(t+\Delta)] = e^{2\pi f i\Delta}\mathcal{F}[y(t)]$, Equation (5) follows.

In the case a sensing laser is used to determine the instantaneous fiber phase variations, the corresponding interferometric error signal upon interference in Charlie can be computed adopting the same reasoning and takes the same form as Equation (E1), with the subscript s instead of l. It follows that, if $\varphi_{\mathrm{l}}(t) \approx \varphi_{\mathrm{s}}(t)$, i.e., the two lasers are phase coherent, the error signal derived by interfering the sensing laser can be exploited to cancel residual noise of the common reference laser in addition to the fiber noise, and further improve phase stability.

Appendix F: Models for the Laser Noise

In general, the noise of standard diode lasers used in frequency dissemination follows a law of the type:

$$S_{\mathrm{l,\,free}}(f) = \frac{r_3}{f^3} + \frac{r_2}{f^2}\left(\frac{f_c}{f+f_c}\right)^2 \tag{F1}$$

where r_3 and r_2 depend on the laser technology, and the cutoff frequency f_c is related to the modulation (control) bandwidth of the laser. The linewidth of these lasers is typically of the order of 1 to 100kHz and the coherence time is <100 µs, even though performances of commercially-available solutions are continuously improving.[72,73] Narrow-linewidth lasers can grant superior phase coherence between successive realignments. They can be realized in several ways, e.g., nanofabrication,[26,27] delay-line

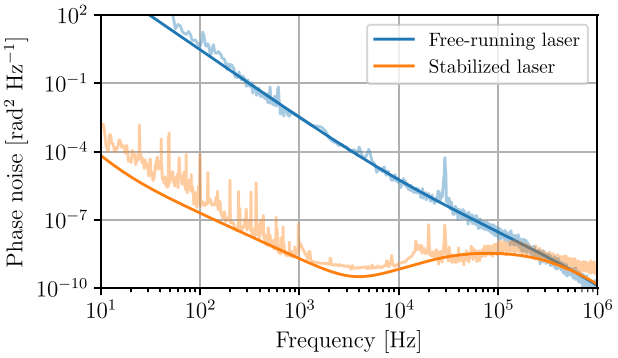

Figure G1. Measured (lighter) and modeled (darker) values for a free-running (blue) and cavity-stabilized (orange) diode laser noise.

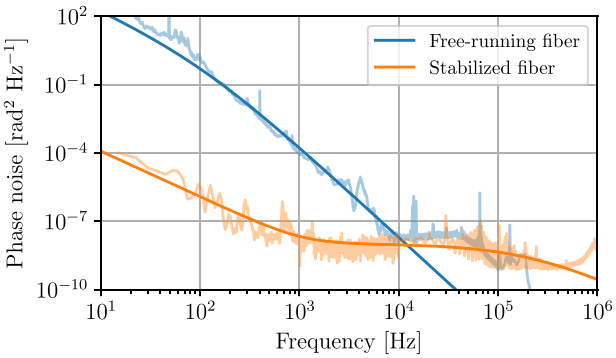

Figure G2. Measured and modeled noise of a 114km long free-running (blue) and stabilized (orange) fiber, traveled in a double-pass.[24] To account for the double-pass, the instance of the fiber noise model is multiplied by a factor of four.

stabilization,[74] or external high-finesse cavity stabilization.[25,75,76] We provide coefficients for the latter approach as it is the one with the best performances today. The interested reader can refer to the literature for the optimal compromise in terms of size, weight, and power versus performance.

The noise of a cavity-stabilized laser $S_{\text{l,stab}}(f)$ depends on the local cavity noise $S_{\text{cavity}}(f)$ at low Fourier frequencies, and on the intrinsic noise of the used laser source $S_{\text{l,free}}(f)$ (Equation (F1)) at high Fourier frequencies, via the gain function $G(f)$ that regulates the control loop response:

$$S_{\text{l,stab}}(f) = S_{\text{cavity}}(f) + \left|\frac{1}{1+G(f)}\right|^2 S_{\text{l,free}}(f) \tag{F2}$$

The cavity noise is usually parametrized by:

$$S_{\text{cavity}}(f) = \frac{C_4}{f^4} + \frac{C_3}{f^3} + \frac{C_2}{f^2} \tag{F3}$$

with coefficients that depend on the cavity material, geometry, and passive isolation, and on technical noise.[25,75,76] Typical coefficients for a compact, portable cavity system that is suited to the considered application, are reported in **Table F1**.

The loop function model follows general concepts of control theory, and includes considerations on the bandwidth allowed by all sub-systems. The overall loop function can be described by a complex function in Laplace space:

$$G(f) = G_0 \frac{1}{(2\pi i f)^2} \frac{if + B\gamma}{if + B\delta} \tag{F4}$$

which includes a second-order integrator to provide high gain at low frequencies, a single integrator stage emerging at a corner frequency $B\gamma$, with B the loop bandwidth and $\gamma < 1$, and is ultimately limited by the finite response of the system, featuring at least one pole at frequency $B\delta$, with $\delta > 1$. The parameters γ, δ determine the exact positions of the knees in the loop response (zero and pole respectively) relative to the loop bandwidth, $G_0 = (2\pi B)^2(1+\delta)/(1+\gamma)$. All of these terms are fine-tuned empirically to maximize the noise rejection and adapt to possible poles present in the subsystems transfer function, but good design values are $\gamma \approx 0.1$ and $\delta \approx 10$.

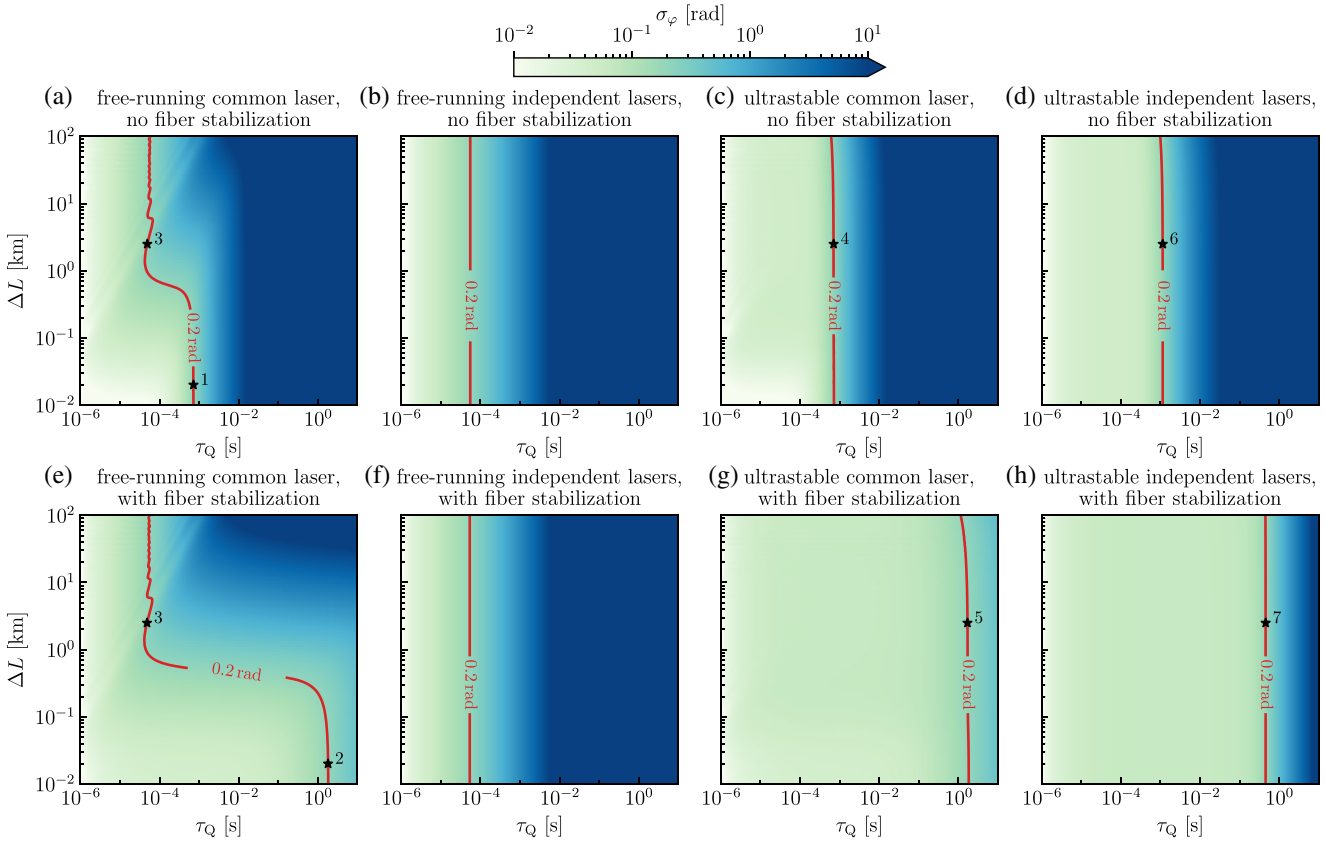

Figure H1. Maps of the phase standard deviation σ_φ, calculated in the space of fiber length mismatch ΔL and integration time τ_Q, for each possible combination of laser source configuration and fiber stabilization at fixed shorter arm $L_B = 100$km. The isolines corresponding to characteristic σ_φ values are also reported. The numbered stars represent the specific scenarios considered in Section 6, where representative values of ΔL are chosen.

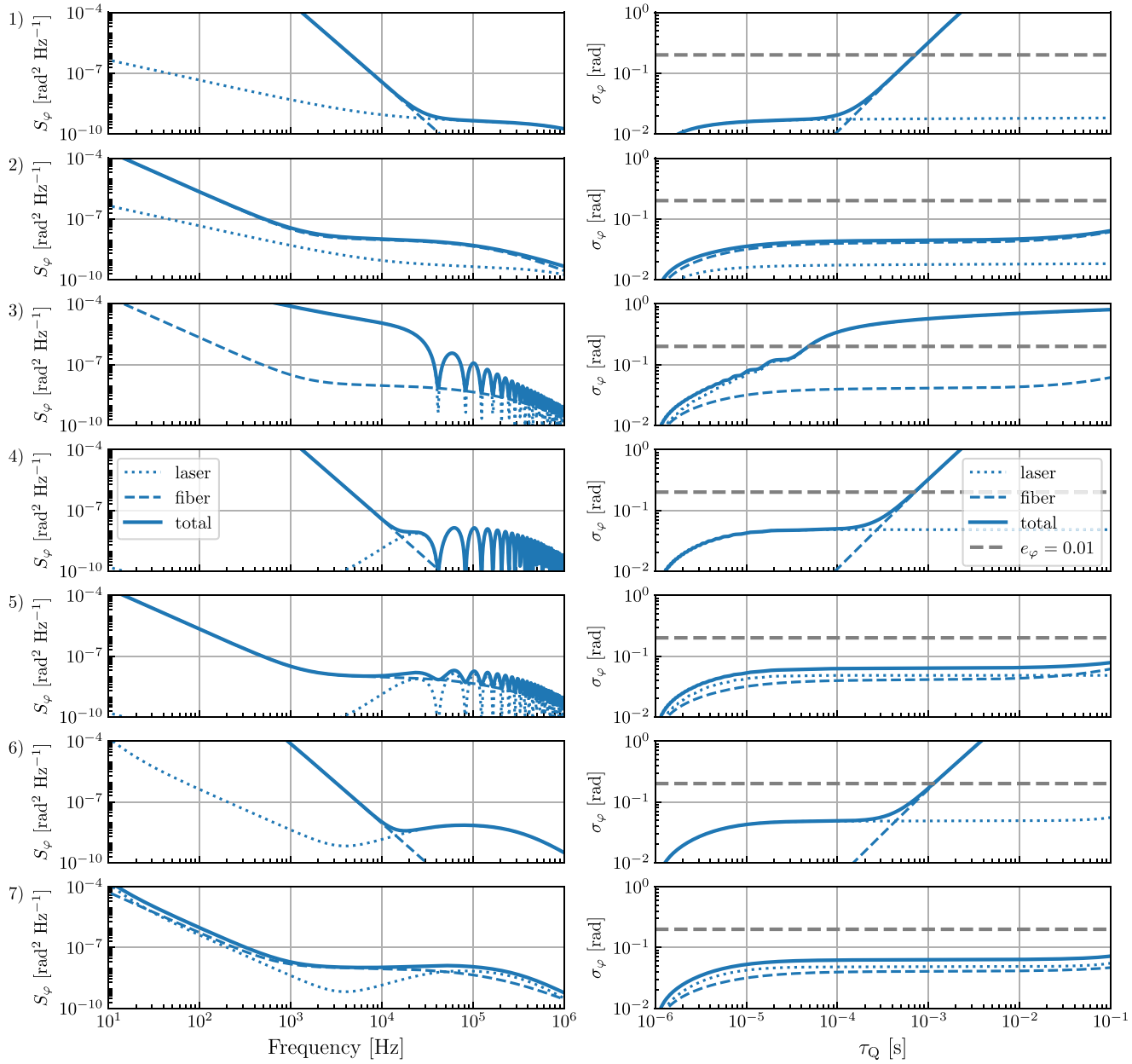

Figure H2. Phase noise as a function of frequency (left) and phase variance as a function of the interrogation time (right) for the seven scenarios reported in Section 6, at fixed shorter arm L_B = 100km. Noise expressions were derived from Equations (5) and (7), together with the detailed laser and fiber noise contributions of Equations (F1), (F2), (6),(8).

Appendix G: Derivation of Model Coefficients

Figure G1 (blue) shows the experimentally measured power spectral density of a <10kHz-linewidth planar waveguide extended-cavity diode laser in a butterfly package (PLANEX by RIO Inc., see also[72,73,77,78] for other laser types), and the noise of the same laser when stabilized to an external 5cm-long Fabry-Perot cavity with Finesse exceeding 10^5 (orange). Darker shades represent instances of the respective models according to Equation (F1) and (F2) for the coefficients shown in Table F1. The spur observed at about 30kHz both on the free-running and stabilized laser (in the latter case, reduced by a factor corresponding to the stabilization loop efficiency at this frequency) is not considered by the model and is attributed to an electrical disturbance on our diode laser current driver. Especially on the stabilized laser below 1kHz, noise peaks are found at specific frequencies: they are due to residual acoustic and seismic solicitations of the resonator and do not significantly affect the results.

Deriving a unique estimate for the fiber noise on a generic layout is more complicated, as the l coefficient primarily depends on the environment where the fiber is housed.[48] In general, field noise levels exceed those of spooled fibers with equal length, and up to a factor ten variation is observed between the various installations (e.g., compare values in refs. [24, 49, 79–84]). As a reference, **Figure G2** (blue) shows the measured noise of a 114km fiber traveled in a round-trip.[24] The fiber was deployed on an intercity haul running parallel to a highway for the majority of its part. The corresponding model is obtained from Equation (6) with a coefficient $l = 44\text{rad}^2\text{Hz km}^{-1}$. In the figure, the modeled noise is multiplied

by a factor of four to account for the fact that the fiber noise is measured in a round-trip.

Fiber noise in a stabilized condition is well explained by Equation (8) below 1kHz of Fourier frequency, according to the fact that we stabilized the fiber at $\lambda_s = 1543.33$nm and observed the effect at $\lambda_q = 1542.14$nm. To explain the experimental observations at higher frequencies, we also include a white phase noise detection floor of the form $S_{\text{detection}}(f) = s_0\left[f_c''/(f + f_c'')\right]^2$, with coefficient $s_0 = 1 \times 10^{-8}\text{rad}^2\,\text{Hz}^{-1}$ corresponding to a typical SNR of $80\text{dBrad}^2\text{Hz}^{-1}$ for the sensing laser interference, upper-limited at a cutoff frequency of $f_c'' = 200$kHz.

Appendix H: Derivation of the Integration Time for Scenarios Shown in Section 6

Figure H1 reports the full maps of $S_\varphi(f)$ and σ_φ, calculated for each combination of laser source configuration and fiber stabilization discussed in Section 6. The contour lines plotted in Figure 2 were extracted from these maps, and the characteristic scenarios are represented as numbered points. In panels a and e, the strong apparent dependence of τ_Q on ΔL is related to the laser coherence length, as discussed for Figure 2. Notice that, in Scenario 3, the laser noise always dominates the total noise, both with and without fiber stabilization (see **Figure H2**, panel 3 on the right).

Figure H2 (left panels) shows the phase noise contributions of laser(s) and fibers, as well as their combined effect, for the seven scenarios of Section 6. Panels on the right indicate the corresponding phase standard error as a function of τ_Q derived from Equation (4) and the threshold corresponding to a phase-misalignment QBER $e_\varphi = 1\%$ as derived from Equation (1). For evaluating the fiber noise, we considered the shortest interferometer arm to be of length $L_B = 100$km, and included length mismatches as indicated in Table 1. We assume the fiber noise contributed by arms A and B to be equal in magnitude, with coefficients derived from Table F1, but uncorrelated. Similarly, for Scenario 6 and 7, we assumed local lasers noise to be equal in magnitude but uncorrelated.

Acknowledgements

The results presented in this article had been achieved in the context of the following projects: QUID (QUantum Italy Deployment) and EQUO (European QUantum ecOsystems) which are funded by the European Commission in the Digital Europe Programme under the grant agreements number 101091408 and 101091561; Qu-Test, which had received funding from the European Union's Horizon Europe under the Grant Agreement number 101113901; project ARS01_00734-QUANCOM (European structural and investment funds MUR-PON Ricerca & Innovazione 2014-2020); EMPIR 19NRM06 METISQ, that received funding from the EMPIR program cofinanced by the Participating States and from the European Union Horizon 2020 research and innovation program; NATO Grant SPS G6026.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are openly available in Zenodo at https://zenodo.org/doi/10.5281/zenodo.10529402, reference number 10529402.

Keywords

phase noise, phase stabilization, quantum key distribution, secret-key rate, simulation

Received: January 23, 2024
Revised: April 24, 2024
Published online:

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301.
[2] C. H. Bennett, G. Brassard, *Theoretical Computer Science* **2014**, *560*, 7.
[3] H.-K. Lo, M. Curty, K. Tamaki, *Nat. Photon.* **2014**, *8*, 595.
[4] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden, *Adv. Opt. Photon.* **2020**, *12*, 1012.
[5] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, et al., *New J. Phys.* **2009**, *11*, 075001.
[6] V. Martin, A. Aguado, P. Salas, A. Sanz, J. Brito, D. R. Lopez, V. Lopez, A. Pastor, J. Folgueira, H. H. Brunner, S. Bettelli, F. Fung, L. C. Comandar, D. Wang, A. Poppe, M. Peev, in *OSA Advanced Photonics Congress (AP) 2019 (IPR, Networks, NOMA, SPPCom, PVLED)*, Optica Publishing Group, Washington, DC **2019**, p. QtW3E.5.
[7] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, et al., *Nature* **2021**, *589*, 214.
[8] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, et al., *Opt. Express* **2011**, *19*, 10387.
[9] H. Takesue, T. Sasaki, K. Tamaki, M. Koashi, *Nat. Photon.* **2015**, *9*, 827.
[10] M. Avesani, L. Calderaro, G. Foletto, C. Agnesi, F. Picciariello, F. B. L. Santagiustina, A. Scriminich, A. Stanco, F. Vedovato, M. Zahidy, G. Vallone, P. Villoresi, *Opt. Lett.* **2021**, *46*, 2848.
[11] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, H. Weinfurter, *Nature* **2022**, *607*, 687.
[12] A. A. E. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, T. Gehring, *arXiv:2305.19642*, **2023**.
[13] D. Ribezzo, M. Zahidy, G. Lemmi, A. Petitjean, C. De Lazzari, I. Vagniluca, E. Conca, A. Tosi, T. Occhipinti, L. K. Oxenløwe, A. Xuereb, D. Bacco, A. Zavatta, *Phys. Rev. Appl.* **2023**, *20*, 044052.
[14] S. Pirandola, R. Laurenza, C. Ottaviani, L. Banchi, *Nat. Commun.* **2017**, *8*, 15043.
[15] M. Takeoka, S. Guha, M. M. Wilde, *IEEE Trans. Inf. Theory* **2014**, *60*, 4987.
[16] H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **1998**, *81*, 5932.
[17] M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, *Nature* **2018**, *557*, 400.
[18] H.-K. Lo, M. Curty, B. Qi, *Phys. Rev. Lett.* **2012**, *108*, 130503.
[19] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, M. Genovese, *Light Sci Appl* **2017**, *6*, e16261.
[20] A. Huang, S. Barz, E. Andersson, V. Makarov, *New J. Phys.* **2018**, *20*, 103016.

[21] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, Z.-F. Han, *Phys. Rev. X* **2019**, *9*, 021046.
[22] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, A. J. Shields, *Nat. Photon.* **2019**, *13*, 334.
[23] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, A. J. Shields, *Nat. Photon.* **2021**, *15*, 530.
[24] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, M. Lucamarini, I. P. Degiovanni, D. Calonico, *Nat. Commun.* **2022**, *13*, 157.
[25] M. L. Kelleher, C. A. McLemore, D. Lee, J. Davila-Rodriguez, S. A. Diddams, F. Quinlan, *Opt. Express* **2023**, *31*, 11954.
[26] W. Loh, J. Stuart, D. Reens, C. D. Bruzewicz, D. Braje, J. Chiaverini, P. W. Juodawlkis, J. M. Sage, R. McConnell, *Nature* **2020**, *588*, 244.
[27] H. Lee, M.-G. Suh, T. Chen, J. Li, S. A. Diddams, K. J. Vahala, *Nat. Commun.* **2013**, *4*, 2468.
[28] CLONETS, https://www.clonets.eu/clonets.html, (accessed: September **2023**).
[29] C. Clivati, M. Pizzocaro, E. Bertacco, S. Condio, G. Costanzo, S. Donadello, I. Goti, M. Gozzelino, F. Levi, A. Mura, M. Risaro, D. Calonico, M. Tønnes, B. Pointard, M. Mazouth-Laurol, R. Le Targat, M. Abgrall, M. Lours, H. Le Goff, L. Lorini, P.-E. Pottie, E. Cantin, O. Lopez, C. Chardonnet, A. Amy-Klein, *Phys. Rev. Appl.* **2022**, *18*, 054009.
[30] M. Schioppo, J. Kronjäger, A. Silva, R. Ilieva, J. W. Paterson, C. F. A. Baynham, W. Bowden, I. R. Hill, R. Hobson, A. Vianello, M. Dovale-Álvarez, R. A. Williams, G. Marra, H. S. Margolis, A. Amy-Klein, O. Lopez, E. Cantin, H. Álvarez Martínez, R. Le Targat, P. E. Pottie, N. Quintin, T. Legero, S. Häfner, U. Sterr, R. Schwarz, S. Dörscher, C. Lisdat, S. Koke, A. Kuhl, T. Waterholter, et al., *Nat. Commun.* **2022**, *13*, 212.
[31] E. F. Dierikx, A. E. Wallin, T. Fordell, J. Myyry, P. Koponen, M. Merimaa, T. J. Pinkert, J. C. J. Koelemeij, H. Z. Peek, R. Smets, *IEEE Trans. Ultrason. Ferroelectr. Freq. Control* **2016**, *63*, 945.
[32] Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci, (accessed: September **2023**).
[33] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, Z.-F. Han, *Nat. Photon.* **2022**, *16*, 154.
[34] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2023**, *130*, 210801.
[35] G. Bertaina, C. Clivati, S. Donadello, C. Liorni, A. Meda, S. Virzì, M. Gramegna, M. Genovese, F. Levi, D. Calonico, M. Dispenza, I. P. Degiovanni, Software for: Phase Noise in Real-World Twin-Field Quantum Key Distribution, **2024**, https://doi.org/10.5281/zenodo.10529402.
[36] X.-B. Wang, Z.-W. Yu, X.-L. Hu, *Phys. Rev. A* **2018**, *98*, 062323.
[37] M. Curty, K. Azuma, H.-K. Lo, *npj Quantum Inf.* **2019**, *5*, 64.
[38] P. W. Shor, J. Preskill, *Phys. Rev. Lett.* **2000**, *85*, 441.
[39] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, *Quantum Info. Comput.* **2004**, *4*, 325.
[40] H.-K. Lo, X. Ma, K. Chen, *Phys. Rev. Lett.* **2005**, *94*, 230504.
[41] X. Ma, B. Qi, Y. Zhao, H.-K. Lo, *Phys. Rev. A* **2005**, *72*, 012326.
[42] K. Tamaki, M. Curty, M. Lucamarini, *New J. Phys.* **2016**, *18*, 065008.
[43] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, X.-B. Wang, *Sci. Rep.* **2019**, *9*, 3080.
[44] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, X.-B. Wang, *Phys. Rev. A* **2020**, *101*, 042330.
[45] X. Zhong, J. Hu, M. Curty, L. Qian, H.-K. Lo, *Phys. Rev. Lett.* **2019**, *123*, 100506.
[46] F. Grasselli, M. Curty, *New J. Phys.* **2019**, *21*, 073001.
[47] S. U. P. Athanasios Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, New York **2002**.
[48] C. Clivati, A. Tampellini, A. Mura, F. Levi, G. Marra, P. Galea, A. Xuereb, D. Calonico, *Optica* **2018**, *5*, 893.
[49] P. A. Williams, W. C. Swann, N. R. Newbury, *Journ. Opt. Am. Soc. B* **2008**, *25*, 1284.
[50] X. Zhong, W. Wang, L. Qian, H.-K. Lo, *npj Quantum Inf.* **2021**, *7*, 1.
[51] X. Zhong, W. Wang, R. Mandil, H.-K. Lo, L. Qian, *Phys. Rev. Appl.* **2022**, *17*, 014025.
[52] C. Clivati, D. Calonico, G. A. Costanzo, A. Mura, M. Pizzocaro, F. Levi, *Optics Letters* **2013**, *38*, 1092.
[53] L. Zhou, J. Lin, Y. Jing, Z. Yuan, *Nat. Commun.* **2023**, *14*, 928.
[54] F. Ceccarelli, G. Acconcia, A. Gulinatti, M. Ghioni, I. Rech, R. Osellame, *Adv. Quantum Technol.* **2021**, *4*, 2000102.
[55] W. Pernice, C. Schuck, O. Minaeva, M. Li, G. Goltsman, A. Sergienko, H. Tang, *Nat. Commun.* **2012**, *3*, 1325.
[56] I. Esmaeil Zadeh, J. W. N. Los, R. B. M. Gourgues, V. Steinmetz, G. Bulgarini, S. M. Dobrovolskiy, V. Zwiller, S. N. Dorenbos, *APL Photonics* **2017**, *2*, 111301.
[57] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble, M. Colangelo, G. M. Crouch, A. E. Dane, T. Gerrits, A. E. Lita, F. Marsili, G. Moody, C. Peña, E. Ramirez, J. D. Rezac, N. Sinclair, M. J. Stevens, A. E. Velasco, V. B. Verma, E. E. Wollman, S. Xie, D. Zhu, P. D. Hale, M. Spiropulu, K. L. Silverman, R. P. Mirin, et al., *Nat. Photon.* **2020**, *14*, 250.
[58] A. Vetter, S. Ferrari, P. Rath, R. Alaee, O. Kahl, V. Kovalyuk, S. Diewald, G. N. Goltsman, A. Korneev, C. Rockstuhl, W. H. P. Pernice, *Nano Lett.* **2016**, *16*, 7085.
[59] C. Scarcella, G. Boso, A. Ruggeri, A. Tosi, *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 17.
[60] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, A. J. Shields, *J. Appl. Phys.* **2015**, *117*, 083109.
[61] PDM-IR, http://www.micro-photon-devices.com/Products/Photon-Counters/PDM-IR, (accessed: September **2023**).
[62] ID230 infrared single-photon detector, https://www.idquantique.com/quantum-sensing/products/id230/, (accessed: September **2023**).
[63] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2020**, *124*, 070501.
[64] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, Q. Zhang, L. You, F. Xu, J.-W. Pan, *Phys. Rev. Lett.* **2023**, *130*, 250802.
[65] W.-Y. Hwang, *Phys. Rev. Lett.* **2003**, *91*, 057901.
[66] X.-B. Wang, *Phys. Rev. Lett.* **2005**, *94*, 230503.
[67] X.-L. Hu, C. Jiang, Z.-W. Yu, X.-B. Wang, *Phys. Rev. A* **2019**, *100*, 062337.
[68] F. Grasselli, Á. Navarrete, M. Curty, *New J. Phys.* **2019**, *21*, 113032.
[69] W. Wang, H.-K. Lo, *New J. Phys.* **2020**, *22*, 013020.
[70] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, U. L. Andersen, *Nat. Photon.* **2015**, *9*, 397.
[71] J. Dias, M. S. Winnel, N. Hosseinidehaj, T. C. Ralph, *Phys. Rev. A* **2020**, *102*, 052425.
[72] R. Bouchand, X. Xie, M. Giunta, W. Hänsel, M. Lezius, R. Holzwarth, C. Alexandre, P.-A. Tremblin, G. Santarelli, Y. Le Coq, *IEEE Photon. Technol. Lett.* **2017**, *29*, 1403.
[73] W. Liang, Y. Liu, *Opt. Lett.* **2023**, *48*, 1323.
[74] F. Kéfélian, H. Jiang, P. Lemonde, G. Santarelli, *Opt. Lett.* **2009**, *34*, 914.
[75] S. Herbers, S. Häfner, S. Dörscher, T. Lücke, U. Sterr, C. Lisdat, *Opt. Lett.* **2022**, *47*, 5441.

[76] D. G. Matei, T. Legero, S. Häfner, C. Grebing, R. Weyrich, W. Zhang, L. Sonderhouse, J. M. Robinson, J. Ye, F. Riehle, U. Sterr, *Phys. Rev. Lett.* **2017**, *118*, 263202.
[77] C. Clivati, D. Calonico, C. Calosso, G. Costanzo, F. Levi, A. Mura, A. Godone, *IEEE Trans. Ultrason. Ferroelectr. Freq. Control.* **2011**, *58*, 2582.
[78] K. Numata, J. Camp, M. A. Krainak, L. Stolpner, *Opt. Expr.* **2010**, *18*, 22781.
[79] S. Droste, F. Ozimek, T. Udem, K. Predehl, T. W. Hänsch, H. Schnatz, G. Grosche, R. Holzwarth, *Phys. Rev. Lett.* **2013**, *111*, 110801.
[80] O. Lopez, A. Haboucha, F. Kéfélian, H. Jiang, B. Chanteau, V. Roncin, C. Chardonnet, A. Amy-Klein, G. Santarelli, *Opt. Express* **2010**, *18*, 16849.
[81] T. Akatsuka, T. Goh, H. Imai, K. Oguri, A. Ishizawa, I. Ushijima, N. Ohmae, M. Takamoto, H. Katori, T. Hashimoto, H. Gotoh, T. Sogawa, *Opt. Express* **2020**, *28*, 9186.
[82] T. Akatsuka, H. Ono, K. Hayashida, K. Araki, M. Takamoto, T. Takano, H. Katori, *JPN J. Appl. Phys.* **2014**, *53*, 032801.
[83] C. Clivati, R. Aiello, G. Bianco, C. Bortolotti, P. D. Natale, V. D. Sarno, P. Maddaloni, G. Maccaferri, A. Mura, M. Negusini, F. Levi, F. Perini, R. Ricci, M. Roma, L. S. Amato, M. S. de Cumis, M. Stagni, A. Tuozzi, D. Calonico, *Optica* **2020**, *7*, 1031.
[84] D. Husmann, L.-G. Bernier, M. Bertrand, D. Calonico, K. Chaloulos, G. Clausen, C. Clivati, J. Faist, E. Heiri, U. Hollenstein, A. Johnson, F. Mauchle, Z. Meir, F. Merkt, A. Mura, G. Scalari, S. Scheidegger, H. Schmutz, M. Sinhal, S. Willitsch, J. Morel, *Opt. Express* **2021**, *29*, 24592.