Comparison of Discrete Variable and Continuous Variable Quantum Key Distribution Protocols with Phase Noise in the Thermal-Loss Channel

S. P. Kish[1,2], P. J. Gleeson[2], A. Walsh[2], P. K. Lam[3,2], and S. M. Assad[3,2]

[1]Data61, CSIRO, Marsfield, NSW, Australia.

[2]Centre of Excellence for Quantum Computation and Communication Technology, Department of Quantum Science and Technology, Research School of Physics, The Australian National University, Canberra, ACT, Australia.

[3]Institute of Materials Research and Engineering, Agency for Science, Technology and Research (A*STAR), Singapore, 138634, Singapore.

Discrete-variable (DV) quantum key distribution (QKD) based on single-photon detectors and sources have been successfully deployed for long-range secure key distribution. On the other hand, continuous-variable (CV) quantum key distribution (QKD) based on coherent detectors and sources is currently lagging behind in terms of loss and noise tolerance. An important discerning factor between DV-QKD and CV-QKD is the effect of phase noise, which is known to be more relevant in CV-QKD. In this article, we investigate the effect of phase noise on DV-QKD and CV-QKD protocols, including the six-state protocol and squeezed-state protocol, in a thermal-loss channel but with the assumed availability of perfect sources and detectors. We find that in the low phase noise regime but high thermal noise regime, CV-QKD can tolerate more loss compared to DV-QKD. We also compare the secret key rate as an additional metric for the performance of QKD. Requirements for this quantity to be high vastly extend the regions at which CV-QKD performs better than DV-QKD. Our analysis addresses the questions of how phase noise affects DV-QKD and CV-QKD and why the former has historically performed better in a thermal-loss channel.

S. P. Kish: sebastian.kish@data61.csiro.au
P. K. Lam: ping.lam@anu.edu.au
S. M. Assad: cqtsma@gmail.com

Introduction

Quantum key distribution (QKD) enables the sharing of keys between two parties, Alice and Bob. Once a quantum secret key is established, it can later be used by both parties to unlock encrypted communication with total confidentiality. In fact, this form of communication is guaranteed to be secure against an eavesdropper, Eve, by the laws of quantum physics. QKD has become a viable cyber-security technology with increasing interest across government agencies and commercial corporations [1].

The first proposed QKD protocol was based on discrete variables (DV) using two polarization bases, now known as BB84 after its authors Bennett & Brassard [2]. BB84 and its three-polarization-basis variant, the six-state (6S) protocol, rely on the use of single-photon states and remain robust QKD protocols to this day [2, 3]. Fifteen years afterward, QKD was extended to continuous variables (CV), initially using entangled multi-photon two-mode squeezed states (TMSV) with low-noise coherent detection [4, 5, 6]. An equivalent scheme known as the squeezed-state protocol was proposed shortly afterwards [7], requiring preparation only of modulated squeezed states. Subsequently, the GG02 protocol [8, 9, 10] with reverse reconciliation and the SRLL02 protocol [11] based on Gaussian modulation of coherent states eliminated the need for preparing experimentally-challenging squeezed states [12]. However, the squeezed-state protocol remains relevant due to its ideally better performance and compatibility with certain quantum repeater architectures [13].

A comparison between measurement-device-independent (MDI) DV-QKD and CV-QKD protocols, taking into account experimental imperfections was done by Pirandola et. al [14]. This comparison in terms of source and detector technologies was discussed in Ref. [15, 16]. Subsequently, a technology-independent comparison of DV-QKD and CV-QKD protocols in a noisy channel with ideal sources and detectors have been investigated in Ref. [17]. It was shown that CV-QKD protocols are generally robust against noise when loss is low to moderate whereas DV-QKD protocols are superior in very low and strong loss regimes. However, in Ref. [17], the analysis for DV-QKD assumed distinguishability between signal photons and noise photons, leading to favourable results for DV-QKD noise tolerance in the very low loss regime. In practical channels, stray photons from background noise are indistinguishable from the signal photon [18]. In addition, the magnitudes of secret key rates of the QKD protocols were ignored as a metric for the comparison. High key rates are an important requirement for a full QKD network to service many users [19, 20].

We hypothesize that one of the factors for the consistent historical performance of DV-QKD protocols is mainly due to their robustness to phase noise, which plagues CV-QKD protocols that rely on encoding information in phase as well as amplitude [5]. We test this hypothesis by introducing a phase noise model consistent with both DV-QKD and CV-QKD.

In this article, we compare idealized DV-QKD and CV-QKD protocols, the BB84 protocol, the six-state (6S) protocol, and the squeezed-state protocol, by assuming perfect sources, detectors, and reconciliation efficiency in a thermal-loss channel. In doing so, we avoid the dependence on practical implementation and current technological limitations. In the first half of the article, we delve into key-rate comparisons in the thermal-loss channel of QKD protocols. For completeness, we consider the strategy of "fighting noise with noise" for improved performances in both the DV-QKD and the CV-QKD protocols. We also identify gaps, if any, between the ideal performances of these QKD protocols and known bounds on the key capacity in the thermal-loss channel.

In the second half of the article, unlike previous works [14, 15, 17], we address phase noise in both DV-QKD and CV-QKD, which is a discerning factor for the performance of QKD. We make use of the fact that in the DV-QKD protocol, the thermal-loss and phase noise channels are equivalent to the depolarizing and dephasing channels, respectively. Furthermore, we present results in the combined thermal-loss and phase noise channels. Our work addresses an important question about which QKD protocol performs better by various metrics for a given thermal-loss and phase noise channel. Finally, we discuss and conclude our results in the context of real-world implementations, and possible future directions.

1 Thermal-loss in QKD

In this section, we present the security models and secret key rate expressions for the DV-QKD and CV-QKD protocols in the thermal-loss channel. We then present the results of the secret key rate of these calculations.

1.1 Thermal-loss in the BB84 (and six-state) dual-rail protocol

We make use of the dual-rail BB84 protocol which is one possible implementation of the original BB84 protocol. In the original BB84 protocol, Alice sends a polarization qubit to Bob with a channel that can support both polarizations. This is equivalent to Alice utilising two quantum channels, each supporting only a single polarization. We present this dual-rail BB84 protocol in Fig. 1 a) and 1 b). In the BB84 protocol, Alice prepares a single qubit in either the rectilinear Z-basis $\{|0\rangle, |1\rangle\}$ or the diagonal X-basis $\{|+\rangle, |-\rangle\}$. In the rectilinear basis shown in Fig. 1 a), a logical **0** is prepared by Alice sending a single photon state $|1\rangle$ in the top a_1 mode and a vacuum state $|0\rangle$ in the bottom a_2 mode. Similarly, a logical **1** is prepared by sending the vacuum state $|0\rangle$ in the top a_1 mode and a single-photon state $|1\rangle$ in the bottom a_2 mode. The qubits pass through a thermal-loss channel represented by a beamsplitter parameter with transmissivity $0 \leq \eta_{1,2} \leq 1$ and thermal state $\hat{\rho}_{\text{Th}}$ with N_{Th} thermal photons in the auxiliary port.

Bob, after deciding randomly (discussed in detail later) to measure the Z-basis, measures each mode output with single-photon detectors, only

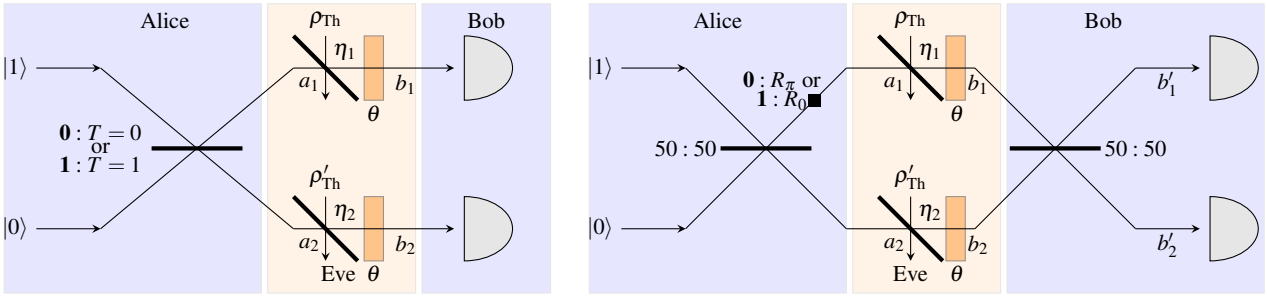


Figure 1: Dual-rail BB84 protocol in the thermal-loss channel. a) and b) show the rectilinear and diagonal polarization bases as the dual-rail equivalent of the BB84 discrete-variable QKD protocol, respectively. The phase θ of either bases are affected independently by randomly distributed phase noise σ_θ^2. In a), based on which mode (top or bottom) Alice chooses to send a single photon determines the logical bit $\mathbf{0}$ or $\mathbf{1}$. In b), based on the phase 0 or π of the rotation R (black square), Alice prepares a logical bit $\mathbf{0}$ or $\mathbf{1}$, respectively.

accepting single-photon events at b_1 or b_2 corresponding to logical $\mathbf{0}$ or $\mathbf{1}$. Any other detector events are not counted towards the final key. In the diagonal basis (see Fig. 1 b)), Alice interferes with a single-photon with the vacuum using a balanced $50:50$ beamsplitter to generate the superposition state $|+\rangle = \frac{1}{\sqrt{2}}(|1\rangle_{a_1}|0\rangle_{a_2} + |0\rangle_{a_1}|1\rangle_{a_2})$ which corresponds to a logical $\mathbf{1}$ state. A logical $\mathbf{0}$ corresponds to Alice placing a π-phase shifter after the beamsplitter and generating the state $|-\rangle = \frac{1}{\sqrt{2}}(|1\rangle_{a_1}|0\rangle_{a_2} - |0\rangle_{a_1}|1\rangle_{a_2})$ to send to Bob. Bob, having randomly decided to measure in the X-basis by placing a balanced beamsplitter, measures only single-photon events at b'_1 or b'_2 corresponding to logical $\mathbf{0}$ or $\mathbf{1}$. We assume the modes pass through the thermal-loss channels with $\eta_1 = \eta_2 = \eta$ and thermal noise N_{Th} and no correlations between the two thermal environments. In the final step of the protocol, Bob sends information to Alice about which basis he used. In this reconciliation phase, Alice discards the data that does not match the basis she used to encode her qubits.

The key rate (per channel use) for the BB84 protocol with perfect reconciliation efficiency in the asymptotic limit is [21, 22, 23]

$$K_{\text{BB84}} = \frac{P_S}{2}(1 - h(Q_Z) - h(Q_X)), \qquad (1)$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, P_S is the success probability of single-photon events, Q_Z and Q_X are the quantum bit error rates (QBERs) of the measurement bases Z and X respectively. Unlike the usual normalization preserving DV channels, the success probability P_S is necessary because the thermal environment adds Gaussian noise, and only single-photon events are counted towards the secret key rate. Here, we assume perfect number-resolving detectors as opposed to click detectors that count all non-vacuum $n > 0$ events.

To calculate Q_Z, we consider the probability of a bit-flip if Alice sends a logical $\mathbf{0}$ (i.e. $|1\rangle_{a_1}|0\rangle_{a_2}$) and Bob detects a logical $\mathbf{1}$ (i.e. simultaneously detects $|0\rangle_{b_1}$ and $|1\rangle_{b_2}$) with probability given by (see Appendix A for full calculations):

$$\begin{aligned} P_{Z,\mathbf{0}\to\mathbf{1}} &= P_{Z,|0\rangle_{a_1}\to|1\rangle_{b_1}} P_{Z,|1\rangle_{a_2}\to|0\rangle_{b_2}} \\ &= \frac{N_{\text{Th}}(1+N_{\text{Th}})(1-\eta)^2}{\gamma^4}, \end{aligned} \qquad (2)$$

where $\gamma = 1 + N_{\text{Th}} - N_{\text{Th}}\eta$.

Bob only accepts the correct bits and the flipped bits using photon-number resolving detectors. Therefore, we normalize by considering the total probability Bob only detects the logical bits in the Z-basis. Since we assume the channels are symmetric, $P_{Z,\mathbf{1}\to\mathbf{0}} = P_{Z,\mathbf{0}\to\mathbf{1}}$, the QBER is

$$Q_Z = \frac{P_{Z,\mathbf{0}\to\mathbf{1}}}{P_{Z,\mathbf{0}\to\mathbf{1}} + P_{Z,\mathbf{0}\to\mathbf{0}}} = \frac{P_{Z,\mathbf{1}\to\mathbf{0}}}{P_{Z,\mathbf{1}\to\mathbf{0}} + P_{Z,\mathbf{1}\to\mathbf{1}}}, \qquad (3)$$

where $P_{Z,\mathbf{0}\to\mathbf{0}} = P_{Z,|1\rangle_{a_1}\to|1\rangle_{b_1}} P_{Z,|0\rangle_{a_2}\to|0\rangle_{b_2}}$ and $P_{Z,\mathbf{1}\to\mathbf{1}} = P_{Z,|0\rangle_{a_1}\to|0\rangle_{b_1}} P_{Z,|1\rangle_{a_2}\to|1\rangle_{b_2}}$ are the probabilities of Bob detecting the same bits that Alice sent after passing through the channel. The

probability of an event (or success) is given by:

$$\begin{aligned} P_S &= P_{Z,\mathbf{0}\to\mathbf{1}} + P_{Z,\mathbf{0}\to\mathbf{0}} \\ &= \frac{\eta + 2\,N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}{\gamma^4}. \end{aligned} \tag{4}$$

To calculate Q_X, we consider the bit-flips in the X basis. In this case, the modes a_1 and a_2 are entangled because of the balanced beamsplitter (see Fig. 1 b)). Similar to above, we obtain the QBER, for the X bases as

$$Q_X = \frac{P_{X,\mathbf{0}\to\mathbf{1}}}{P_{X,\mathbf{0}\to\mathbf{1}} + P_{X,\mathbf{0}\to\mathbf{0}}}. \tag{5}$$

We find due to symmetry that the probabilities for the diagonal basis are the same as for the rectilinear basis and it follows that $Q_X = Q_Z$, simplifying the key rate equation. We make use of Eqs. (1), (5), and (4) to calculate the key rate in the asymptotic limit.

Conditioned on the outcome with probability P_S, it can be shown that the density matrix after the thermal-loss channel is, in fact, a depolarized state (see Appendix B):

$$\begin{aligned} \tilde{\rho}^B := \frac{\rho^B}{P_S} &= \frac{\eta}{\eta + 2\,N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}\rho^A \\ &+ \frac{N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}{\eta + 2\,N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}\mathbb{I}, \end{aligned} \tag{6}$$

where ρ^A is Alice's initial density matrix. This represents a depolarizing channel [24]

$$\rho \to (1-\lambda)\rho + \frac{\lambda}{2}\mathbb{I} \tag{7}$$

with depolarizing parameter

$$\lambda = \frac{2\,N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}{\eta + 2\,N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}, \tag{8}$$

which tends to 1 as $\eta \to 0$ or $N_{\rm Th} \to \infty$, as expected.

A property of the depolarizing channel is that the error rate is the same in all bases:

$$Q_{X,Y,Z} = \frac{\lambda}{2} = \frac{N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}{\eta + 2N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}, \tag{9}$$

which can be seen from Eq. (7). In establishing this equivalence between the thermal-loss and depolarizing channel, we extend our analysis to the six-state protocol which makes use of an additional basis Y with QBER Q_Y. The key rate for the 6S protocol is given by [23]:

$$K_{\rm 6S} = \frac{P_S}{2}(1 - H(\Lambda_{00}) - H(\Lambda_{01}) - H(\Lambda_{10}) - H(\Lambda_{11})), \tag{10}$$

where $H(x) = -x\log_2 x$, and

$$\begin{aligned} \Lambda_{00} &= 1 - \frac{Q_X + Q_Y + Q_Z}{2}, \\ \Lambda_{01} &= \frac{Q_X + Q_Y - Q_Z}{2}, \\ \Lambda_{10} &= \frac{-Q_X + Q_Y + Q_Z}{2}, \\ \Lambda_{11} &= \frac{Q_X - Q_Y + Q_Z}{2}, \end{aligned} \tag{11}$$

where the factor of $1/2$ is to normalize the key-rate to per channel use. In the thermal-loss channel, the QBER $Q_X = Q_Y = Q_Z$ is symmetric. However, as we will see when phase noise is introduced, the QBER of the three bases can be asymmetric.

Lower bounds of BB84 and 6S protocols in the thermal-loss channel

Introducing random bit flips at Alice before the error processing increases the performance of BB84 in a noisy channel and sets a tighter lower bound on the key rate [25]. In this extension of the BB84 protocol which we denote as NBB84, the key rate equation depends on Alice's added bit-flip probability q (or trusted bit-flips). Following Ref. [25], we make use of the QBER for the thermal-loss channel in Eq. (58) and maximize the key rate with respect to q. We note that the six-state protocol (with and without trusted bit-flips) can tolerate higher QBER than the BB84 protocol [25]. Similarly, the lower bound on the secret key rate of the 6S protocol is likewise calculated by introducing bit-flips at Alice which increases the QBER tolerance of the channel [25].

1.2 Thermal-loss in the squeezed state protocol

In the squeezed-state protocol in a prepare-and-measure (PM) scheme presented in Fig. 2 a), Alice introduces a modulation signal in either the $\hat{X} = \hat{a} + \hat{a}^\dagger$ or $\hat{P} = -i(\hat{a} - \hat{a}^\dagger)$ quadrature (randomly chosen) a squeezed state with $V_{\rm sq}$ with

a) b)

Figure 2: Squeezed-state protocol with homodyne detection in the thermal-loss channel. The phase shifter θ represents the phase noise σ_θ^2. Shown in a) is the equivalent prepare and measure squeezed-state protocol and in b) is the entanglement-based version of the squeezed-state protocol.

Gaussian distribution centered at 0 with variance V_{sig}. In the equivalent entanglement-based (EB) scheme presented in Fig. 2 b), Alice performs a homodyne measurement on one mode of a shared two-mode squeezed vacuum state (TMSV) where the other mode passes through the channel $\mathcal{E}$, and Bob performs a homodyne measurement [26]. The parameter transformation between the PM and EB schemes is:

$$\begin{aligned} V_{\text{sq}} &= 1/\mu, \\ V_{\text{sig}} &= \frac{\mu^2-1}{\mu}, \end{aligned} \tag{12}$$

where $\mu = V_{\text{sq}} + V_{\text{sig}}$ is the quadrature variance of $\hat{X}$ and $\hat{P}$ of the TMSV source in EB scheme. The following key rate calculations are in the EB scheme. In the asymptotic regime of infinite keys, Eve's most powerful attack is a collective attack. Security proofs in this regime for this protocol are based on reduction of coherent attacks to collective attacks for infinite dimensions and on the optimality of Gaussian attacks [27, 28, 29]. The secret key rate against collective attacks in the asymptotic regime with reverse reconciliation is given by [30]

$$K_{\text{RR}} = \beta I_{\text{AB}} - \chi_{\text{EB}}, \tag{13}$$

where β is the reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{EB} is the Holevo information between Bob and Eve. In a Gaussian channel, the quadrature covariance matrix between Alice and Bob is [26]:

$$\begin{aligned} \gamma_{\text{AB}} &= \begin{pmatrix} a\mathbb{I} & c\sigma_z \\ c\sigma_z & b\mathbb{I} \end{pmatrix} = \begin{pmatrix} \gamma_{\text{A}} & \sigma_{\text{AB}} \\ \sigma_{\text{AB}} & \gamma_{\text{B}} \end{pmatrix} = \\ &\begin{pmatrix} (V_{\text{A}}+1)\mathbb{I} & \sqrt{\eta(V_{\text{A}}^2+2V_{\text{A}})}\sigma_z \\ \sqrt{\eta(V_{\text{A}}^2+2V_{\text{A}})}\sigma_z & V_B\mathbb{I} \end{pmatrix}, \end{aligned} \tag{14}$$

where $V_{\text{A}} = \mu - 1$ and $V_B = \eta(V_{\text{A}} + 1 + \chi)$ are the TMSV variances measured by Alice and Bob (respectively), $\chi = \frac{(1-\eta)(2N_{\text{Th}}+1)}{\eta}$ is the noise of the thermal-loss channel, $\mathbb{I} = \text{diag}(1,1)$ is the unity matrix and $\sigma_z = \text{diag}(1,-1)$ is the Pauli-Z matrix. We choose homodyne detection (also known as "switching") at Bob, in which Bob switches between $\hat{X}$ or $\hat{P}$ quadrature measurements.

In the squeezed state protocol with homodyne detection, the mutual information is given by:

$$I_{\text{AB}}^{\text{hom}} = \frac{1}{2}\log_2\left(\frac{V_{\text{B}}}{V_{\text{B|A}}}\right), \tag{15}$$

where $V_{\text{B|A}} = b - \frac{c^2}{a}$. The Holevo information between Bob and Eve for the collective attack is given by

$$\chi_{\text{EB}} = S(\text{E}) - S(\text{E|B}), \tag{16}$$

where $S(\text{E})$ is Eve's information and $S(\text{E|B})$ is Eve's information conditioned on Bob's measurement. In Eve's collective attack, Eve holds a purification of the state between Alice and Bob with entropy given by

$$S(\text{E}) = S(\text{AB}) = G[(\lambda_1 - 1)/2] + G[(\lambda_2 - 1)/2], \tag{17}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix γ_{AB} given by $\lambda_{1,2}^2 = \frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4\mathcal{D}^2}]$, where $\Delta = \text{Det}(\gamma_{\text{A}}) + \text{Det}(\gamma_{\text{B}}) + 2\text{Det}(\sigma_{\text{AB}})$, and $\mathcal{D} = \text{Det}(\gamma_{\text{AB}})$. The conditional covariance matrix of Alice's mode after the homodyne detection by Bob is

$$\Gamma_{\text{A}|b} = \begin{pmatrix} \mu - \frac{\eta(\mu^2-1)}{\eta\mu+(1-\eta)(2N_{\text{Th}}+1)} & 0 \\ 0 & \mu \end{pmatrix}. \tag{18}$$

Therefore, Eve's entropy conditioned on Bob's measurement $S(\text{E|B}) = S(\text{A}|b)$ is given by $G[(\lambda_3 - 1)/2]$ where λ_3 is the symplectic eigenvalue of $\Gamma_{A|b}$.

Introducing trusted noise before Bob's homodyne measurement can help extend a high-noise thermal-loss channel. In this extension of the

squeezed-state protocol which we denote NSqz-Hom, trusted Gaussian noise ξ_B is added before post-processing on Bob's homodyne measurement data [26]. The effect is that Eve's information decreases more than the mutual information between Alice and Bob (see Appendix C for calculations), thus increasing the secret key rate of the protocol. Similarly, heterodyne detection at Bob has the same effect of introducing additional noise, thereby extending secure communication distance in a thermal-loss channel [31].

2 Phase noise in QKD

We consider a standard model of bosonic phase noise, known also as dephasing, phase-diffusion, or phase-damping. This channel represented by θ on the right of Fig. 1 applies rotation by a random angle θ to the bosonic state according to a classical distribution $f(\theta)$, giving the transformation

$$\hat{\rho} \longmapsto \int_{-\pi}^{\pi} d\theta f(\theta) e^{i\hat{a}^\dagger \hat{a}\theta} \hat{\rho} e^{-i\hat{a}^\dagger \hat{a}\theta}. \tag{19}$$

Since $\hat{a}^\dagger \hat{a}$ is the number operator, a given rotation θ applies a phase $e^{in\theta}$ to each Fock state $|n\rangle$, equivalently described by the transformation

$$\hat{a}^\dagger \longmapsto e^{i\theta} \hat{a}^\dagger. \tag{20}$$

The canonical phase distribution is the *wrapped normal distribution*, which models the random diffusion of an angle and accurately represents the physical process of phase diffusion [24]. Birefringence may produce this behaviour in polarisation-based implementations of the six-state and BB84 protocols or in time-bin implementations, phase drift in between the interferometers at either end [32].

The phase shift θ (assumed here to have mean zero) is normally distributed over the whole real line:

$$\tilde{f}_{WN}(\theta) = \frac{1}{\sigma_\theta \sqrt{2\pi}} e^{-\theta^2/2\sigma_\theta^2} : \qquad \theta \in \mathbb{R}, \tag{21}$$

which we can 'wrap' into a single 2π interval by summing the contributions from equivalent angles:

$$f_{WN}(\theta) = \frac{1}{\sigma_\theta \sqrt{2\pi}} \sum_{k=-\infty}^{\infty} e^{-(\theta+2\pi k)^2/2\sigma_\theta^2} : \theta \in [-\pi, \pi]. \tag{22}$$

The variance σ_θ^2 of θ over the whole real line is in general *not* its variance when wrapped; however, the two distributions approach each other in the limit of small variance.

The corresponding qubit transformation of the phase noise ignoring the thermal-loss ($\eta = 1$) is $\rho_{jk} \mapsto e^{i\theta_j} e^{-i\theta_k} \rho_{jk}$, which may be expressed as $\hat{\rho} \to \hat{U}_{\boldsymbol{\theta}} \hat{\rho} \hat{U}_{\boldsymbol{\theta}}^\dagger$ where $\hat{U}_{\boldsymbol{\theta}} = \mathrm{diag}(e^{i\theta_i}, e^{i\theta_j})$. If $\boldsymbol{\theta}$ is drawn from a distribution $f(\boldsymbol{\theta})$, the qubit channel becomes

$$\hat{\rho} \to \langle \hat{U}_{\boldsymbol{\theta}} \hat{\rho} \hat{U}_{\boldsymbol{\theta}}^\dagger \rangle = \int_{\boldsymbol{\theta}} f(\boldsymbol{\theta}) \hat{U}_{\boldsymbol{\theta}} \hat{\rho} \hat{U}_{\boldsymbol{\theta}}^\dagger \, d\boldsymbol{\theta} \tag{23}$$

where $\langle \cdot \rangle$ denotes expected value. If $\{\theta_j\}$ are independent, the corresponding transformation of off-diagonal terms ($i \neq j$) is

$$\rho_{jk} \longmapsto \langle e^{i\theta_j} e^{-i\theta_k} \rangle \rho_{jk} = \langle e^{i\theta_j} \rangle \langle e^{-i\theta_k} \rangle \rho_{jk} = \bar{r}_j \bar{r}_k^* \rho_{jk} \tag{24}$$

where $\bar{r}_j := \langle e^{i\theta_j} \rangle$ is the so-called 'circular mean' of θ_j, given for the wrapped normal distribution:

$$\bar{r}_j = e^{-\sigma_\theta^2/2}. \tag{25}$$

Diagonal entries remain unchanged:

$$\rho_{jj} \longmapsto \langle e^{i\theta_j} e^{-i\theta_j} \rangle \rho_{jj} = \rho_{jj}.$$

If $\{\theta_j\}$ are identically distributed then all have the same (real) circular mean $\bar{r}$ and we obtain a (generalised) dephasing channel

$$\hat{\rho} \longmapsto \hat{\rho}_{\text{dephased}} = \begin{bmatrix} \rho_{00} & \bar{r}^2 \rho_{01} \\ \bar{r}^2 \rho_{10} & \rho_{11} \end{bmatrix} \tag{26}$$

which always sends single-photon inputs to single-photon outputs, unlike the thermal-loss channel. By leaving diagonal entries unchanged, Eq. (26) introduces *no error* in the Z basis. Common DV-QKD protocols such as the (generalised) BB84 and six-state protocols make use of additional bases (X and Y) which are *unbiased* with respect to the Z basis.

The extension to the combined thermal-loss phase-noise rail presented in Fig. 1 can be obtained by composing the separate depolarization and dephasing channels described in Eqs. (7) and (26), giving

$$\hat{\rho} \longrightarrow (1-\lambda) \begin{bmatrix} \rho_{00} & \bar{r}^2 \rho_{01} \\ \bar{r}^2 \rho_{10} & \rho_{11} \end{bmatrix} + \frac{\lambda}{2} \mathbb{I}.$$

The corresponding error rates are thus $(1-\lambda)\hat{\rho}_{\text{dephased}} + \frac{\lambda}{2}\mathbb{I}$, i.e.

$$Q_Z = \left(\frac{\lambda}{2}\right), \qquad Q_{X,Y} = \left(\frac{1}{2}\right)\left[(1-\lambda)(1-\bar{r}^2)+\lambda\right], \tag{27}$$

with $\bar{r}^2$ and λ given by Eqs. (25) and (8) respectively. The probability of success P_S remains the same as for the thermal-loss channel in Eq. (4), as the subsequent dephasing does not affect which states are discarded. The key rate for the BB84 and 6S protocols are straightforward to calculate from these QBERs and using Eqs. (1) and (10), respectively.

Turning to CV-QKD, the phase noise channel is given by the same random rotation $\hat{a} \to \hat{U}\hat{a}\hat{U}^\dagger = e^{-i\theta}\hat{a}$, with θ drawn from a distribution as in Eq. (23). This models statistical error in the phase, regardless of the chosen CV-QKD implementation scheme. For a given θ, a coherent state $|\alpha\rangle$ becomes $|\alpha e^{-i\theta}\rangle$.

For the squeezed-state protocol, the combined thermal-loss and phase noise channel leads to the following covariance matrix:

$$\begin{aligned}\gamma_{\text{AB}} &= \begin{pmatrix} a\mathbb{I} & c\sigma_z \\ c\sigma_z & b\mathbb{I}\end{pmatrix} \\ &= \begin{pmatrix} \mu\mathbb{I} & \sqrt{\eta_{\text{I}}(\mu^2-1)}\sigma_z \\ \sqrt{\eta_{\text{I}}(\mu^2-1)}\sigma_z & (\eta_{\text{I}}(\mu+\chi_{\text{I}})\mathbb{I}\end{pmatrix} \\ &= \begin{pmatrix} \mu\mathbb{I} & \bar{r}\sqrt{\eta(\mu^2-1)}\sigma_z \\ \bar{r}\sqrt{\eta(\mu^2-1)}\sigma_z & (\eta\mu+(1-\eta)(2N_{\text{Th}}+1))\mathbb{I}\end{pmatrix},\end{aligned} \tag{28}$$

where the inferred transmittance $\eta_I = \eta\bar{r}^2 = \eta e^{-\sigma_\theta^2}$ and noise $\chi_I = \frac{(1-e^{-\sigma_\theta^2})\eta\mu+(1-\eta)(2N_{\text{Th}}+1)}{\eta e^{-\sigma_\theta^2}}$ are derived in Appendix E. Since phase noise wraps squeezed states around the axis, the average state of modulated squeezed states remains a thermal state but the correlations $\langle X_A X_B\rangle$ are now reduced by the factor $\bar{r} = e^{-\sigma_\theta^2/2}$. It is straightforward to calculate the SKR using Eq. (28) and the equations in the previous section.

We note that in the regime where σ_θ^2 is large, the phase diffusion channel becomes non-Gaussian [33]. Since we are considering the squeezed-state protocol with coherent detection, we make use of Eq. (16) to calculate a lower bound on the key rate. It is left for future work to determine the optimal protocol in the non-Gaussian phase diffusion channel.

3 Comparison of QKD protocols

3.1 Without phase noise $\sigma_\theta^2 = 0$

In CV-QKD, information is encoded in the $\hat{X}$ and/or $\hat{P}$ quadratures in one polarization with access to an infinite Hilbert space. Conversely, in DV-QKD, information is encoded in one or more polarization basis in a 2-dimensional Hilbert space. To make a fair comparison, we assume that Alice uses one polarization basis asymptotically close to 100% of the time (the "computational" basis). The other basis is only measured to characterize channel parameters and the QBER. We make a similar assumption for the squeezed state protocols in the sense that Bob rarely switches the quadrature he measures to characterize the anti-squeezing and determine whether Eve tampered with the shared EPR state, thus removing the usual sifting factor of 1/2 that comes with switching.

We also make the following ideal assumptions about the CV-QKD and DV-QKD protocols in the thermal-loss channel: (i) single-photon and laser sources are perfect (ii) detectors that are used are ideal with detector efficiencies $\eta_{\text{d}} = 1$ and detector noise $\xi_{\text{det}} = 0$ (except for intentionally adding *trusted* noise in the "fighting noise with noise" protocol) (iii) all channel parameters have been estimated with no statistical error (iv) all channel noise is attributed to Eve (v) reverse reconciliation efficiency is perfect with $\beta = 1$ and error correction efficiency is perfect for both CV-QKD and DV-QKD (vi) all security analysis is in the asymptotic limit. Our simplified analysis here is valid in the ideal situation where squeezed and coherent states are only affected by loss, thermal noise and (in the next section) phase noise.

A fundamental benchmark for QKD is the Pirandola, Laurenza, Ottaviani and Banchi (PLOB) bound of a quantum channel $\mathcal{E}$. The PLOB bound establishes upper bounds on two-way secret key capacities $C(\mathcal{E})$ and on point-to-point QKD protocols [34]. It is known that the PLOB bound in a *pure-loss* channel is tight and the squeezed-state protocol, under some conditions, saturates this bound in the limit of infinite squeezing [13]. However, there is a gap between the best lower bound and the best upper

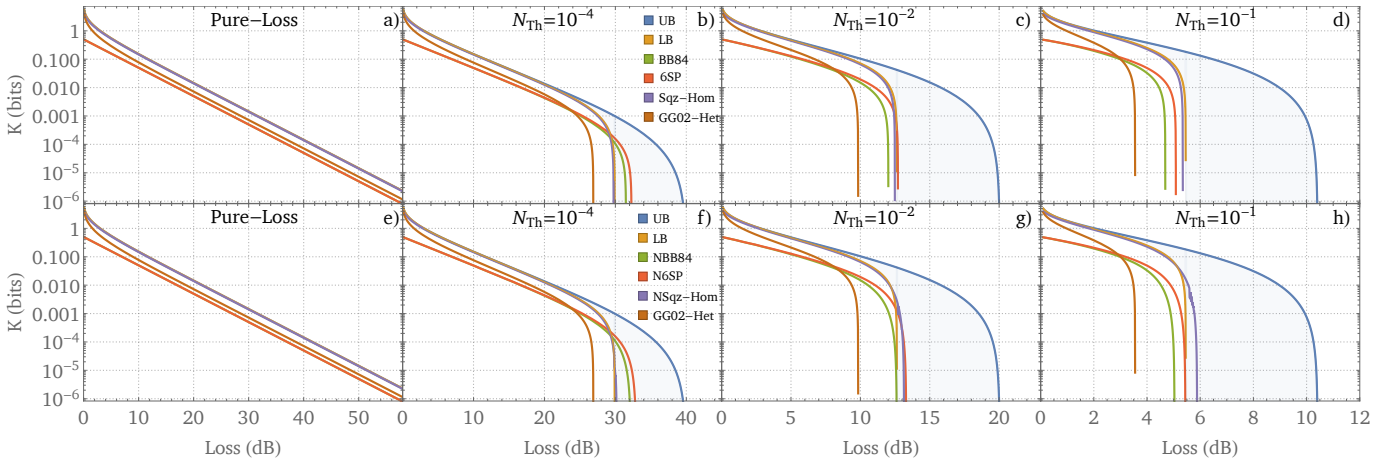


Figure 3: Secret key rate per polarization channel in a thermal-loss channel for increasing noise N_{Th}. Figures a)-d) and e)-h) show the QKD versions of the protocols without and with trusted noise, respectively. For comparison, we also include the GG02 in all figures. For the pure-loss channel, the Sqz-Hom and NSqz-Hom essentially overlap with the PLOB bound for the chosen squeezing of 15 dB. Next in b) and f) with some noise in the thermal-loss channel means that the BB84, NBB84, 6S and N6S protocols outperform the CV-QKD protocols. As shown in c), d), g) and h) as more thermal noise is present, the Sqz-Hom and NSqz-Hom outperform BB84, NBB84, 6S, and N6S. In particular, Sqz-Hom saturates the lower bound (LB). Lastly, NSqz-Hom is by far the best protocol in a high noise regime as shown in h) but far from the upper bound (UB).

bound of the secret key capacity of channels with thermal noise. Pirandola et. al determined lower bounds (LB) and upper bounds (UB) on the secret key capacity $C(\eta, N_{\text{Th}})$ of the thermal loss channel where N_{Th} is the thermal noise and η is the transmissivity of the thermal-loss channel [34, 35]. The lower bound is given by the reverse coherent information of the thermal-loss channel and the upper bound by the Gaussian relative entropy of entanglement (of the Choi state in the thermal-loss channel):

$$\begin{aligned} C(\eta, N_{\text{Th}}) &\geq -\log_2[1-\eta] - G(N_{\text{Th}}) = K_{\text{Lower}}, \\ C(\eta, N_{\text{Th}}) &\leq -\log_2[(1-\eta)\eta^{N_{\text{Th}}}] - G(N_{\text{Th}}) \\ &= K_{\text{Upper}}, \end{aligned} \tag{29}$$

given for non-entanglement breaking channels $N_{\text{Th}} < \eta/(1-\eta)$ and where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$.

We present our results in Fig. 3 a)-d) for the secret key rate per polarization channel based on calculations of the BB84 protocol, the 6S protocol, the GG02 protocol (see Appendix G calculations), and the squeezed state with homodyne (Sqz-Hom) protocols in the thermal-loss channel for various thermal noise parameters. We note that since we make use of the dual-rail BB84 protocol which is one possible implementation of the BB84 protocol, the key rate equation for the DV-QKD protocols has been divided by 2 into units of symbols per polarization channel. For the Sqz-Hom protocol, we choose a practically achievable squeezing V_{sq} of 15 dB [36]. We note that adding more squeezing only adds a very small improvement to the key rates (see Appendix H for more details). In the limit of infinite squeezing, the secret key rate of the Sqz-Hom would approach the lower bound (LB) of the secret key capacity in the thermal-loss channel as shown most clearly in Fig. 3 b) and in a pure-loss channel as shown in Fig. 3 a). The BB84 and 6S protocols surpass the lower bound in an intermediate thermal-noise regime as shown in Fig. 3 b). In Fig. 3 e)-h), we present the "fighting noise with noise" versions of the protocols. For the squeezed state protocol with homodyne detection (NSqz-Hom) with 15 dB squeezing we optimized with respect to the trusted noise ξ_B. As shown in Fig. 3 g) and h) surpasses the LB for high thermal noise. In addition, the secret key rate of the "fighting noise with noise" versions of the DV-QKD protocols, the NBB84 and N6S protocols are optimized with respect to the added bit-flips by Alice q and a slight advantage is obtained as shown in Fig. 3 c). In Fig. 4, to benchmark the performance of the different protocols, we normalized the key rate to the upper bound of the secret key capac-

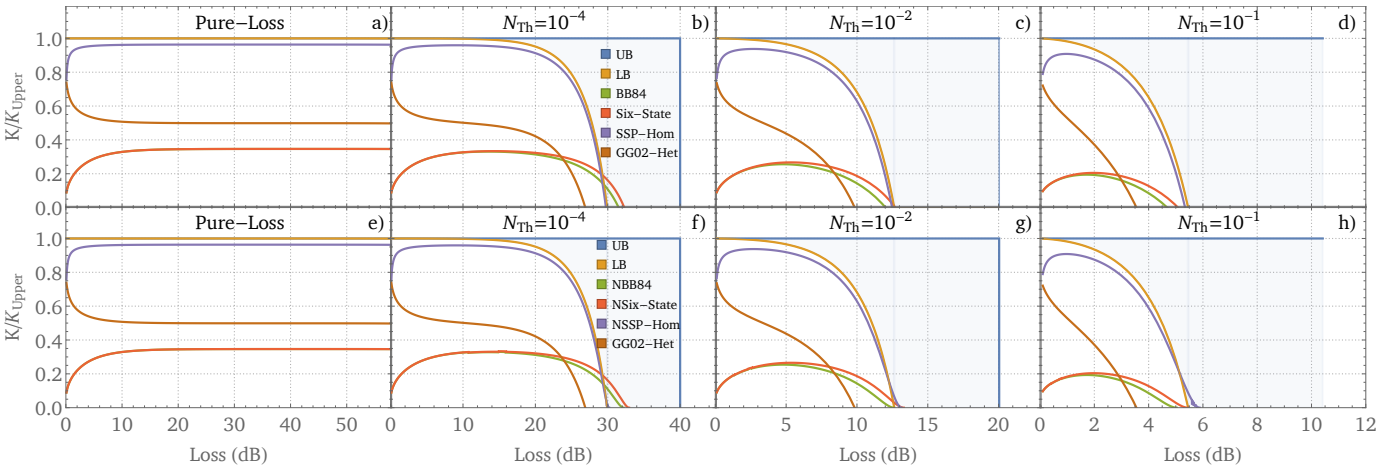


Figure 4: Same as Fig. 3 but to benchmark the performance of the different protocols, we normalise the key rates by the upper bound K_{Upper}. We note that the Sqz-Hom protocol is very close to the LB bound. For clarity in the pure-loss channel, from top to bottom is UB=LB, SSP-Hom, GG02-Het, Six-State=BB84.

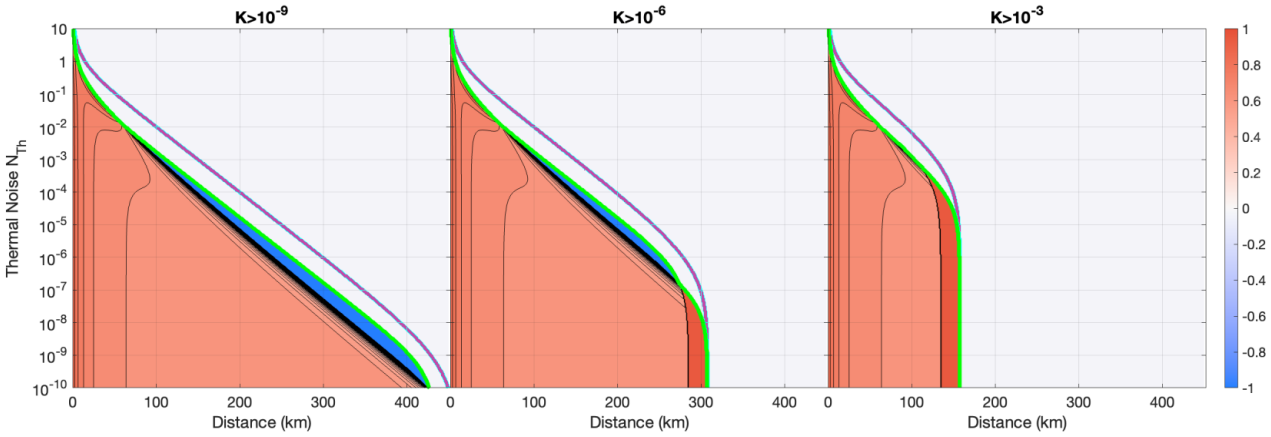


Figure 5: Comparison of $\tilde{K}^{\text{CV:DV}}$ for protocols for a set of thermal-loss channel parameters. Blue regions indicate where the 6S protocol has a higher key rate than Sqz-Hom and conversely, red regions are where the Sqz-Hom has higher key rates than the 6S protocol. Given a minimum key rate requirement, we compare the protocols which operate the best for single-channel use QKD. The 6S protocol covers a small region of intermediate noise and loss as seen in the first two subfigures. The green line indicates where the QKD protocols can operate up to the minimum key rate. The rest of the parameter space is covered by the squeezed state protocol. For high key rates in the rightmost subfigure, the 6S protocol always performs worse than Sqz-Hom. The purple line is the upper bound (UB) of the key capacity in the thermal-loss channel. The red region in the middle and right subfigures are regions where only the Sqz-Hom can achieve the minimum key rate.

ity.

We compare the protocols by plotting the parameter:

$$\tilde{K}^{\text{CV:DV}} = \frac{K_{\text{Sqz-Hom}} - K_{\text{6S}}}{\text{Max}[K_{\text{Sqz-Hom}}, K_{\text{6S}}]}, \qquad (30)$$

for channel parameters of standard optical fibre of loss 0.2 dB/km with distance $D = -50\log_{10}(\eta)$ km and N_{Th} in Fig. 5. The key rate $(K_{\text{Sqz-Hom}}, K_{\text{6S}}) > K_0$ where K_0 is the minimum required key rate. When the squeezed-state protocol is significantly higher in key rates $\tilde{K} = 1$, and conversely, when the 6S protocol is best, $\tilde{K} = -1$.

In Fig. 5, from left to right, the protocols are operated at increasingly higher key rates. Given a minimum key rate requirement, we compare the protocols which operate the best in bits per channel use. The main observation here is that the channel parameter space where the 6S protocol dominates shrinks for increasingly higher key rates and CV-QKD is at an advantage. It can also be seen that for higher minimum key-rate requirements, only the Sqz-Hom protocol can operate

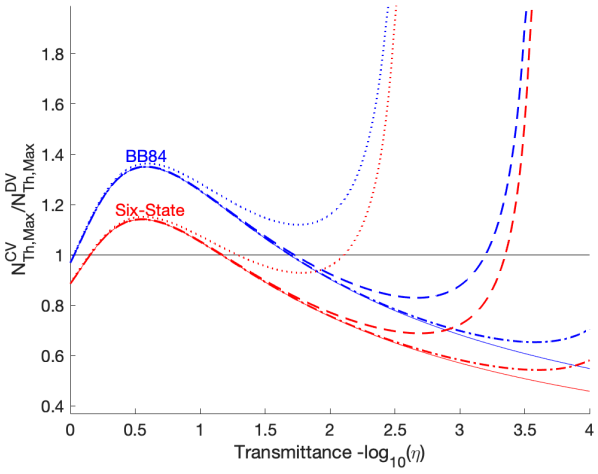


Figure 6: Ratio of maximum noise tolerance of the Sqz-Hom protocol with BB84 (blue) and Six-State (red) protocols. Shown are numerical results for K_0 of 10^{-3} (dotted line), 10^{-4} (dashed line), 10^{-5} (dotted-dashed line) and 10^{-10} (solid line). The protocol parameters of CV-QKD and DV-QKD are the same as those in Fig. 3.

(see red regions in the middle and right subfigures). However, the 6S protocol can be operated in an intermediate-noise regime at low-key rates where CV-QKD cannot (left and centre subfigure). In Fig. 6, we plot the ratio of maximum noise tolerance of the Sqz-Hom protocol with the BB84 and the Six-State protocol for various K_0. Here it can be seen that DV-QKD performs better for low SKR requirements and at low transmittance values.

Our results indicate that common QKD protocols are far from the upper bound secret key capacity in a thermal-loss channel. We also find that the NSqz-Hom protocol has the best excess noise tolerance in very noisy channels in agreement with Ref. [37] but we find that the BB84 and 6S protocols perform better in an intermediate noise regime. However, we note that Ref. [17] arrives at different conclusions regarding the noise tolerance of DV-QKD compared to CV-QKD. The difference can be explained by the model for the thermal-loss channel in DV-QKD in Ref. [17] which assumes that the signal and noise photons can be distinguished (see Appendix D for more detail).

3.2 With phase noise $\sigma_\theta^2 > 0$

In the following section, we quantify the performance of the 6S and Sqz-Hom (with optimized modulation variance V_A) protocols in the combined thermal-loss and phase noise channel. We note that we assume the preparation noise of the Sqz-Hom attributed to the squeezing angle ϕ is zero i.e. the squeezed states are perfectly amplitude or phase squeezed. First, consider the maximum tolerable thermal noise given by:

$$N_{\mathrm{Th}}^{(\mathrm{Max})} = \arg N_{\mathrm{Th}} \begin{cases} 0, & \text{if } K(0,\sigma_\theta^2,D) < K_0. \\ K(N_{\mathrm{Th}},\sigma_\theta^2,D) = K_0, & \text{otherwise.} \end{cases} \tag{31}$$

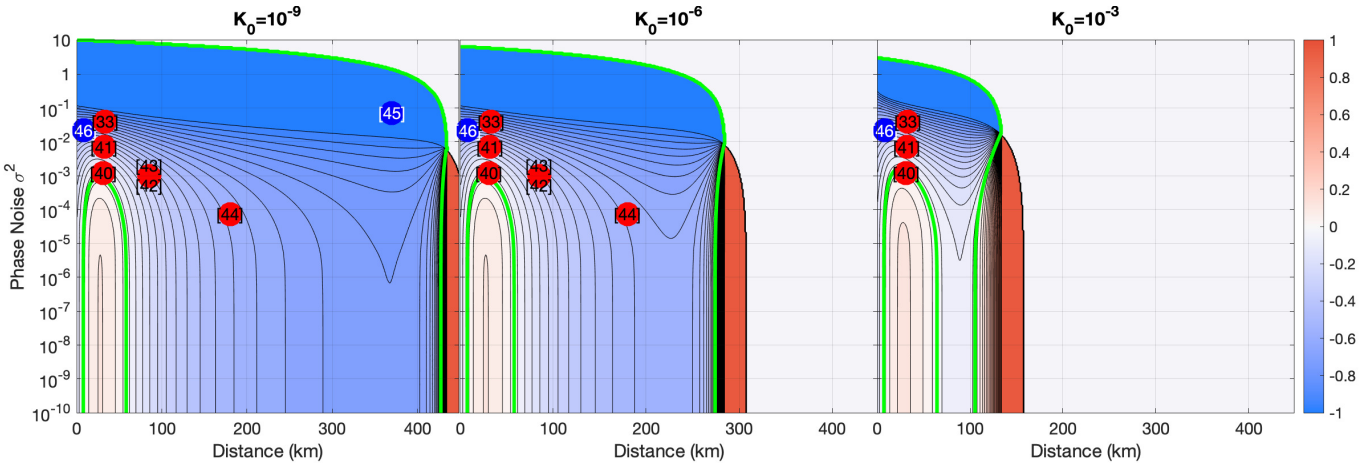
In other words, the maximum tolerable noise if the key rate is less than K_0 at $N_{\mathrm{Th}} = 0$ is 0. Otherwise, the maximum tolerable noise is N_{Th} when the key rate falls to K_0.

In Fig. 7 a), we plot the following quantity:

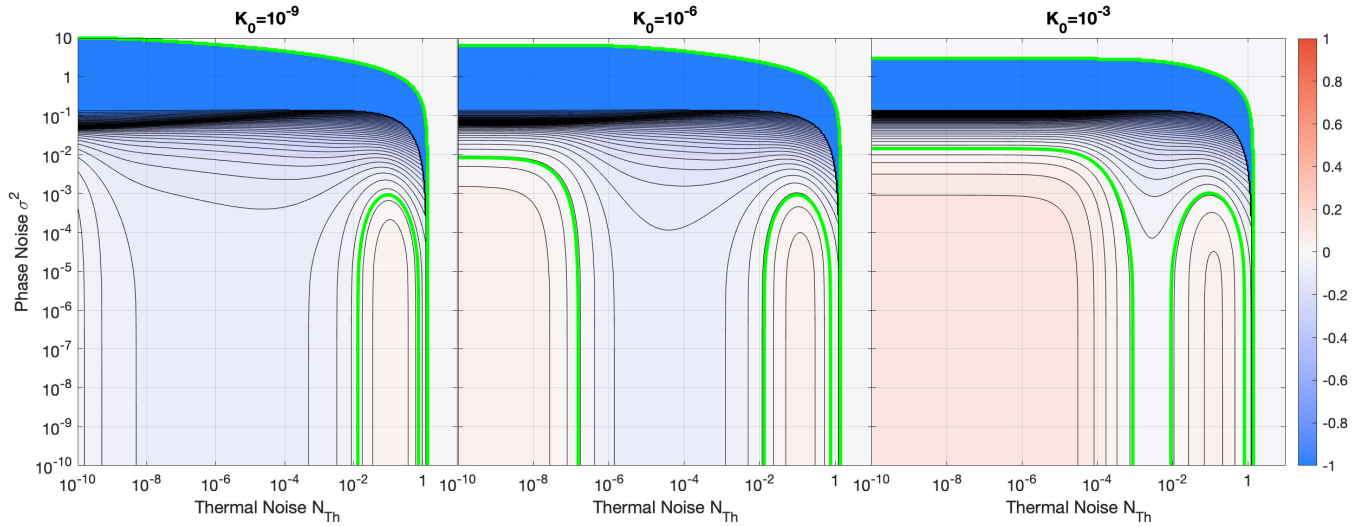
$$\tilde{N}_{\mathrm{Th}}^{\mathrm{CV:DV}}(\sigma_\theta^2, D) = \frac{N_{\mathrm{Th,Sqz\text{-}Hom}}^{(\mathrm{Max})} - N_{\mathrm{Th,6S}}^{(\mathrm{Max})}}{\mathrm{Max}[N_{\mathrm{Th,Sqz\text{-}Hom}}^{(\mathrm{Max})}, N_{\mathrm{Th,6S}}^{(\mathrm{Max})}]}, \tag{32}$$

which is the difference between the maximum tolerable thermal noise of the Sqz-Hom and the 6S protocols for a given phase noise σ_θ^2 and distance D to achieve a key rate K_0. Highlighted in the figure is the green contour where both protocols tolerate the same amount of thermal noise, i.e. $\tilde{N}_{\mathrm{Th}}^{\mathrm{CV:DV}} = 0$. For low key rates, it can be seen that the squeezed-state protocol tolerates more thermal noise than the 6S protocol in short channels and when $\sigma_\theta^2 < 10^{-3}$. The Sqz-Hom protocol also tolerates more thermal noise than the 6S protocol at longer distances. In this red region, the 6S protocol tolerates zero thermal noise, whereas the Sqz-Hom protocol tolerates some thermal noise. For higher key-rate requirements, although the region of noise tolerance shrinks for both protocols, the Sqz-Hom tolerates proportionally more thermal noise across the phase noise versus distance parameter space.

Next, we consider the maximum distance or maximum tolerable loss given by:



(a) Contour plot of $\tilde{N}_{\text{Th}}^{\text{CV:DV}}$ as a function of the phase noise and distance (or loss) for the Sqz-Hom and 6S protocol. The green line indicates the point at which both protocols tolerate the same amount of thermal noise. In the white regions to the right-hand side, neither one of the protocols tolerate any thermal noise. In the red region, only the Sqz-Hom protocol tolerates thermal noise. We also show current state-of-the-art CV-QKD (red circles) and DV-QKD (blue circles) protocols.



(b) Contour plot of $\tilde{L}^{\text{CV:DV}}$ or $\tilde{D}^{\text{CV:DV}}$ as a function of the phase noise and thermal noise for the Sqz-Hom and 6S protocol. The green line indicates the point at which both protocols tolerate the same amount of loss. In the white regions to the right-hand side, neither one of the protocols tolerate any loss.

Figure 7

$$D^{(\text{Max})} = \text{arg}D \begin{cases} 0, & \text{if } K(N_{\text{Th}}, \sigma_\theta^2, 0) < K_0. \\ K(N_{\text{Th}}, \sigma_\theta^2, D) = K_0, & \text{otherwise.} \end{cases} \tag{33}$$

In other words, the maximum distance if the key rate is less than K_0 at $D = 0$ is 0. Otherwise, the maximum distance is D when the key rate falls to K_0. In Fig. 7 b), we plot the following quantity:

$$\begin{aligned} &\tilde{L}^{\text{CV:DV}}(\sigma_\theta^2, N_{\text{Th}}) = \tilde{D}^{\text{CV:DV}}(\sigma_\theta^2, N_{\text{Th}}) \\ &= \frac{D_{\text{Sqz-Hom}}^{(\text{Max})} - D_{\text{6S}}^{(\text{Max})}}{\text{Max}[D_{\text{Sqz-Hom}}^{(\text{Max})}, D_{\text{6S}}^{(\text{Max})}]}, \end{aligned} \tag{34}$$

which is the difference between the maximum distance of the Sqz-Hom and the 6S protocols for a given phase noise σ_θ^2 and thermal noise N_{Th} to achieve a key rate K_0. The Sqz-Hom protocol can tolerate more loss than the 6S protocol at thermal noise between 10^{-2} and 0.9, and phase noise

$\sigma_\theta^2 < 10^{-3}$. As found in [17], at a small region of high thermal noise, the 6S protocol tolerates more loss than the Sqz-Hom protocol. At higher key-rate requirements, the Sqz-Hom protocol can tolerate more loss compared to the 6S protocol. In fact, it can tolerate as much as $\sigma_\theta^2 = 0.05$ for a $K > 10^{-3}$ key-rate requirement and $N_{\text{Th}} < 10^{-3}$ to perform at a longer distance than the 6S protocol.

From these results, we can conclude that for low key-rate requirements, the 6S protocol clearly dominates a larger region of parameters. However, for high key-rate requirements, the Sqz-Hom protocol dominates most of the parameter space for phase noise less than a phase noise of $\sigma_\theta^2 < 10^{-3}$.

CV-QKD

Reference	σ_θ^2
B. Qi et al. [38]	4×10^{-2}
T. Wang et al. [39]	1.2×10^{-3}
H. Wang et al. [40]	$\leq 7.0 \times 10^{-3}$
H.-M. Chin et al. [41] & A. A. Hajomer et al. [42]	$\leq 1.0 \times 10^{-3}$
Y. Zhang et al. [43]	7.4×10^{-5}

DV-QKD

Reference	σ_θ^2
A. Boaron et al. [44]	7.2×10^{-2}
W. Li et al. [45]	2.2×10^{-2}

Table 1: Residual phase noise of locally generated local oscillator Gaussian modulated CV-QKD schemes in the first table and phase noise due to timing jitter in DV-QKD schemes in the second table. With the exception of Ref. [38], [39] & [43], the phase noise is upper bounded from the total excess noise.

As a comparison, experimental values for the phase noise in CV-QKD protocols are shown in Table. 1. These are also shown in Fig. 7 a) along with current state-of-the-art DV-QKD protocols [44] & [45] (converted to equivalent distance in standard fibre). For DV-QKD implementations, we convert the time jitter Full Width at Half Maximum (FWHM) Δt_{FWHM}) to the phase noise using the following equation:

$$\sigma_\theta^2 = \frac{(2\pi\Delta t_{\text{FWHM}})^2}{(2\sqrt{2\ln 2}\Delta t)^2}, \tag{35}$$

where Δt is the timing between pulses. The fundamental limitation of timing jitter is from the uncertainty in the arrival time of the photon. It is usually quoted as a FWHM which is defined as "the difference between the two values of the independent variable at which the dependent variable is equal to half of its maximum value". This equation converts FWHM to a Gaussian width [46] and then to a phase noise (in radians squared). The timing between pulses in both experiments is inversely proportional to the repetition rate $\Delta t = 1/f$.

Discussion

We discuss our results with less-than-ideal experimental setups of QKD protocols. In optical fibre, the current distance record for DV-QKD is 421 km in ultralow-loss (ULL) fibre (0.17 dB/km) corresponding to 71.9 dB loss [44]. A secret key rate of 0.25 bps or equivalently $K = 10^{-10}$ bits per channel use was obtained using superconducting single-photon detectors at a repetition rate of 2.5 GHz. Most recently, a high key rate of $K = 4.4 \times 10^{-2}$ was demonstrated in 10 km of standard optical fiber for DV-QKD [45]. We plot these experimental points normalized to standard optical fiber loss (0.2 dB/km) in Fig. 7 a). Based on these results, for this similar key-rate requirement $K_0 = 10^{-3}$, CV-QKD would, in theory, be able to achieve the same high key rate and tolerate more noise if the same levels of phase noise are maintained as in [39] & [40]. Additionally, CV-QKD can extend up to 150 km as opposed to DV-QKD which cannot tolerate noise beyond 125 km. In the rightmost subfigure in Fig. 7 b), it can be seen that CV-QKD can tolerate more loss than DV-QKD for a large parameter region given a higher key rate requirement.

Nonetheless, in terms of distance, DV-QKD is currently leading the benchmark for QKD with the world record for CV-QKD being more than half the distance in ULL fibre at 202.81 km (or 32.4 dB) using the GG02 protocol where a key rate of $K \approx 10^{-6}$ was achieved [43]. On the other hand, the apparent advantage of CV-QKD is in the efficient encoding of keys per symbol and the faster generation and detection of coherent (or squeezed) states with a much larger block size. Post-processing codes at low signal-to-noise ratio were a bottleneck in CV-QKD until it was recently shown that Raptor-like LPDC codes can maintain a high key extraction rate and high rec-

onciliation efficiency, paving the way for practical and deployable CV-QKD [47].

We have also focused mainly on the squeezed-state protocol. Despite renewed interest in the squeezed-state protocol due to its robustness to noise [48, 49, 50], the difficulty of modulating and generating stable squeezed coherent states remains. However, entanglement-based versions have been demonstrated [51], and sources of highly entangled TMSV states are a promising pathway toward realizing the squeezed-state protocol [52].

Furthermore, one of the limitations of CV-QKD is currently the maintaining of phase reference using a local oscillator (LO), which needs to be practically solved without compromising unconditional security, in a real-world setting outside of the laboratory [43]. It can be seen from our results, that although CV-QKD performs well in a high-thermal noise regime, the introduction of phase noise destroys this advantage. For CV-QKD to maintain this advantage, the amount of phase noise must be less than $\sigma_\theta^2 < 10^{-3}$. However, we also find that CV-QKD performs best for high minimum key-rate requirements where it can tolerate more thermal noise at longer distances than DV-QKD. The physical reason behind this is that in CV-QKD, more symbols can be sent that will result in a shared key. Conversely, DV-QKD is limited to single photons.

Based on these results, we speculate that the consistent historical performance of DV-QKD protocols is mainly due to robustness to phase noise, which plagues CV-QKD protocols that rely on encoding information in phase as well as amplitude. However, with increasingly more robust carrier phase compensation schemes based on machine learning as in Ref. [41, 42], phase noise may no longer be a limiting factor in CV-QKD.

Although current upper bounds on the secret key capacity can serve as a benchmark for QKD protocols, no QKD protocol is currently known to saturate these bounds in the thermal-loss channel. In our analysis, we have only considered point-to-point QKD, but fundamental bounds on the secret key capacity using repeaters exist [53]. Recently, it was shown that an entanglement purification scheme could saturate the repeater bounds in a pure-loss channel [54] but this remains an open problem in the thermal-loss channel. We note that energy-constrained upper bounds in the thermal-loss channel have been recently determined, that would be comparable in energy to common DV-QKD protocols [55]. Additionally, identifying the optimal QKD protocol for the phase diffusion channel is a task for future research.

4 Conclusion

In this work, we compared DV-QKD and CV-QKD protocols on equal grounds in a thermal-loss channel and we assumed ideal sources and detector performances. We developed analytical formulas for the QBER of the BB84 and six-state protocols in a thermal-loss channel. We introduced the minimum key rate as a metric for QKD performance. We found the squeezed-state protocol dominates most of the channel parameter regimes when there is no phase noise, except for an intermediate-noise regime where the six-state protocol can tolerate more loss and surpasses the lower bound to the secret key capacity. With the addition of phase noise, we find that the overall landscape of the DV-QKD and CV-QKD comparison becomes more complex. Finally, we find DV-QKD is largely unaffected by phase noise, whilst CV-QKD is sensitive but performs better below a threshold phase noise only recently reached in experiments.

References

[1] Nedasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng, and Lajos Hanzo. Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook. *IEEE Communications Surveys Tutorials*, 21(1):881–919, 2019. DOI: 10.1109/COMST.2018.2864557.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560: 7–11, 2014. ISSN 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2014.05.025. URL https://www.sciencedirect.com/science/article/pii/S0304397514004241. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[3] Hong-Yi Su. Simple analysis of security of the BB84 quantum key distribution protocol. *Quantum Information Processing*, 19 (6):169, 2020. DOI: 10.1007/s11128-020-02663-z. URL https://doi.org/10.1007/s11128-020-02663-z.

[4] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61: 010303, Dec 1999. DOI: 10.1103/PhysRevA.61.010303. URL https://link.aps.org/doi/10.1103/PhysRevA.61.010303.

[5] T. C. Ralph. Security of continuous-variable quantum cryptography. *Phys. Rev. A*, 62: 062306, Nov 2000. DOI: 10.1103/PhysRevA.62.062306. URL https://link.aps.org/doi/10.1103/PhysRevA.62.062306.

[6] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61: 022309, Jan 2000. DOI: 10.1103/PhysRevA.61.022309. URL https://link.aps.org/doi/10.1103/PhysRevA.61.022309.

[7] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 63: 052311, Apr 2001. DOI: 10.1103/PhysRevA.63.052311. URL https://link.aps.org/doi/10.1103/PhysRevA.63.052311.

[8] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002. DOI: 10.1103/PhysRevLett.88.057902. URL https://link.aps.org/doi/10.1103/PhysRevLett.88.057902.

[9] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003. DOI: 10.1038/nature01289. URL https://doi.org/10.1038/nature01289.

[10] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93:170504, Oct 2004. DOI: 10.1103/PhysRevLett.93.170504. URL https://link.aps.org/doi/10.1103/PhysRevLett.93.170504.

[11] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002. DOI: 10.1103/PhysRevLett.89.167901. URL https://link.aps.org/doi/10.1103/PhysRevLett.89.167901.

[12] Xuyang Wang, Siyou Guo, Pu Wang, Wenyuan Liu, and Yongmin Li. Realistic rate-distance limit of continuous-variable quantum key distribution. *Opt. Express*, 27(9):13372–13386, Apr 2019. DOI: 10.1364/OE.27.013372. URL http://www.opticsexpress.org/abstract.cfm?URI=oe-27-9-13372.

[13] 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. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020. DOI: 10.1364/AOP.361502. URL http://aop.osa.org/abstract.cfm?URI=aop-12-4-1012.

[14] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*, 9(6):397–402, 2015. DOI: 10.1038/nphoton.2015.83. URL https://doi.org/10.1038/nphoton.2015.83.

[15] Feihu Xu, Marcos Curty, Bing Qi, Li Qian, and Hoi-Kwong Lo. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nature Photonics*, 9(12):772–773, 2015. DOI: 10.1038/nphoton.2015.206. URL https://doi.org/10.1038/nphoton.2015.206.

[16] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. Reply to 'discrete and continuous variables for measurement-device-independent quantum cryptography'. *Nature Photonics*, 9(12):773–775, Dec 2015. ISSN 1749-4893. DOI: 10.1038/nphoton.2015.207. URL https://doi.org/10.1038/nphoton.2015.207.

[17] Mikołaj Lasota, Radim Filip, and Vladyslav C. Usenko. Robustness of quantum key distribution with discrete and continuous variables to channel noise. *Phys. Rev. A*, 95:062312, Jun 2017. DOI: 10.1103/PhysRevA.95.062312. URL https://link.aps.org/doi/10.1103/PhysRevA.95.062312.

[18] Miao Er-long, Han Zheng-fu, Gong Shunsheng, Zhang Tao, Diao Da-sheng, and Guo Guang-can. Background noise of satellite-to-ground quantum key distribution. *New Journal of Physics*, 7(1): 215, oct 2005. DOI: 10.1088/1367-2630/7/1/215. URL https://dx.doi.org/10.1088/1367-2630/7/1/215.

[19] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1):16025, 2016. DOI: 10.1038/npjqi.2016.25. URL https://doi.org/10.1038/npjqi.2016.25.

[20] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, Sheng-Long Han, Qing Yu, Ken Liang, Fei Zhou, Xiao Yuan, Mei-Sheng Zhao, Tian-Yin Wang, Xiao Jiang, Liang Zhang, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Chao-Yang Lu, Rong Shu, Jian-Yu Wang, Li Li, Nai-Le Liu, Feihu Xu, Xiang-Bin Wang, Cheng-Zhi Peng, and Jian-Wei Pan. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841): 214–219, 2021. DOI: 10.1038/s41586-020-03093-8. URL https://doi.org/10.1038/s41586-020-03093-8.

[21] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000. DOI: 10.1103/PhysRevLett.85.441. URL https://link.aps.org/doi/10.1103/PhysRevLett.85.441.

[22] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 06(01):1–127, 2008. DOI: 10.1142/S0219749908003256. URL https://doi.org/10.1142/S0219749908003256.

[23] Gláucia Murta, Filip Rozpędek, Jérémy Ribeiro, David Elkouss, and Stephanie Wehner. Key rates for quantum key distribution protocols with asymmetric noise. *Phys. Rev. A*, 101:062321, Jun 2020. DOI: 10.1103/PhysRevA.101.062321. URL https://link.aps.org/doi/10.1103/PhysRevA.101.062321.

[24] Michael A. Nielsen and Isaac L. Chuang. Quantum computation and quantum information: 10th anniversary edition. 2010.

[25] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005. DOI: 10.1103/PhysRevA.72.012332. URL https://link.aps.org/doi/10.1103/PhysRevA.72.012332.

[26] R. Garcia-Patron Sańchez. Quantum information with optical continuous variables: from Bell tests to key distribution. 2007.

[27] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. Extremality of gaussian quantum states. *Phys. Rev. Lett.*, 96:080502, Mar 2006. DOI: 10.1103/PhysRevLett.96.080502. URL https://link.aps.org/doi/10.1103/PhysRevLett.96.080502.

[28] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006. DOI: 10.1103/PhysRevLett.97.190503. URL https://link.aps.org/doi/10.1103/PhysRevLett.97.190503.

[29] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502, Nov 2006. DOI: 10.1103/PhysRevLett.97.190502. URL https://link.aps.org/doi/10.1103/PhysRevLett.97.190502.

[30] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018. DOI: https://doi.org/10.1002/qute.201800011.

[31] Raúl García-Patrón and Nicolas J. Cerf. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.*, 102:130501, Mar 2009. DOI: 10.1103/PhysRevLett.102.130501. URL https://link.aps.org/doi/10.1103/PhysRevLett.102.130501.

[32] L.-P. Lamoureux, E. Brainis, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar. Experimental error filtration for quantum communication over highly noisy channels. *Phys. Rev. Lett.*, 94:230501, Jun 2005. DOI: 10.1103/PhysRevLett.94.230501. URL https://link.aps.org/doi/10.1103/PhysRevLett.94.230501.

[33] Ludovico Lami and Mark M. Wilde. Exact solution for the quantum and private capacities of bosonic dephasing channels. *Nature Photonics*, 17(6):525–530, 2023. DOI: 10.1038/s41566-023-01190-4. URL https://doi.org/10.1038/s41566-023-01190-4.

[34] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, 2017. DOI: 10.1038/ncomms15043. URL https://doi.org/10.1038/ncomms15043.

[35] Stefano Pirandola, Raul García-Patrón, Samuel L. Braunstein, and Seth Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.*, 102:050503, Feb 2009. DOI: 10.1103/PhysRevLett.102.050503. URL https://link.aps.org/doi/10.1103/PhysRevLett.102.050503.

[36] Henning Vahlbruch, Moritz Mehmet, Karsten Danzmann, and Roman Schnabel. Detection of 15 db squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency. *Phys. Rev. Lett.*, 117:110801, Sep 2016. DOI: 10.1103/PhysRevLett.117.110801. URL https://link.aps.org/doi/10.1103/PhysRevLett.117.110801.

[37] Stefano Pirandola, Samuel L Braunstein, Riccardo Laurenza, Carlo Ottaviani, Thomas P W Cope, Gaetana Spedalieri, and Leonardo Banchi. Theory of channel simulation and bounds for private communication. *Quantum Science and Technology*, 3(3):035009, may 2018. DOI: 10.1088/2058-9565/aac394. URL https://doi.org/10.1088/2058-9565/aac394.

[38] Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X*, 5:041009, Oct 2015. DOI: 10.1103/PhysRevX.5.041009. URL https://link.aps.org/doi/10.1103/PhysRevX.5.041009.

[39] Tao Wang, Peng Huang, Yingming Zhou, Weiqi Liu, Hongxin Ma, Shiyu Wang, and Guihua Zeng. High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt. Express*, 26(3):2794–2806, Feb 2018. DOI: 10.1364/OE.26.002794. URL https://opg.optica.org/oe/abstract.cfm?URI=oe-26-3-2794.

[40] Heng Wang, Yaodi Pi, Wei Huang, Yang Li, Yun Shao, Jie Yang, Jinlu Liu, Chenlin Zhang, Yichen Zhang, and Bingjie Xu. High-speed gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. *Opt. Express*, 28(22):32882–32893, Oct 2020. DOI: 10.1364/OE.404611. URL https://opg.optica.org/oe/abstract.cfm?URI=oe-28-22-32882.

[41] Hou-Man Chin, Nitin Jain, Darko Zibar, Ulrik L. Andersen, and Tobias Gehring. Machine learning aided carrier recovery in continuous-variable quantum key distribution. *npj Quantum Information*, 7 (1):20, 2021. DOI: 10.1038/s41534-021-00361-x. URL https://doi.org/10.1038/s41534-021-00361-x.

[42] Adnan A.E. Hajomer, Hossein Mani, Nitin Jain, Hou-Man Chin, Ulrik L. Andersen, and Tobias Gehring. Continuous-variable quantum key distribution over 60 km optical fiber with real local oscillator. In *European Conference on Optical Communication (ECOC) 2022*, page Th1G.5. Optica Publishing Group, 2022. URL https://opg.optica.org/abstract.cfm?URI=ECEOC-2022-Th1G.5.

[43] Yichen Zhang, Ziyang Chen, Stefano

Pirandola, Xiangyu Wang, Chao Zhou, Binjie Chu, Yijia Zhao, Bingjie Xu, Song Yu, and Hong Guo. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.*, 125:010502, Jun 2020. DOI: 10.1103/PhysRevLett.125.010502. URL https://link.aps.org/doi/10.1103/PhysRevLett.125.010502.

[44] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121:190502, Nov 2018. DOI: 10.1103/PhysRevLett.121.190502. URL https://link.aps.org/doi/10.1103/PhysRevLett.121.190502.

[45] Wei Li, Likang Zhang, Hao Tan, Yichen Lu, Sheng-Kai Liao, Jia Huang, Hao Li, Zhen Wang, Hao-Kun Mao, Bingze Yan, Qiong Li, Yang Liu, Qiang Zhang, Cheng-Zhi Peng, Lixing You, Feihu Xu, and Jian-Wei Pan. High-rate quantum key distribution exceeding 110 mb s–1. *Nature Photonics*, 2023. DOI: 10.1038/s41566-023-01166-4. URL https://doi.org/10.1038/s41566-023-01166-4.

[46] Misael Caloz, Matthieu Perrenoud, Claire Autebert, Boris Korzh, Markus Weiss, Christian Schönenberger, Richard J. Warburton, Hugo Zbinden, and Félix Bussières. High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors. *Applied Physics Letters*, 112(6), 02 2018. ISSN 0003-6951. DOI: 10.1063/1.5010102. URL https://doi.org/10.1063/1.5010102. 061103.

[47] Chao Zhou, XiangYu Wang, ZhiGuo Zhang, Song Yu, ZiYang Chen, and Hong Guo. Rate compatible reconciliation for continuous-variable quantum key distribution using raptor-like ldpc codes. *Science China Physics, Mechanics & Astronomy*, 64(6): 260311, Apr 2021. ISSN 1869-1927. DOI: 10.1007/s11433-021-1688-4. URL https://doi.org/10.1007/s11433-021-1688-4.

[48] Vladyslav C. Usenko. Unidimensional continuous-variable quantum key distribution using squeezed states. *Phys. Rev. A*, 98:032321, Sep 2018. DOI: 10.1103/PhysRevA.98.032321. URL https://link.aps.org/doi/10.1103/PhysRevA.98.032321.

[49] Ivan Derkach, Vladyslav C Usenko, and Radim Filip. Squeezing-enhanced quantum key distribution over atmospheric channels. *New Journal of Physics*, 22(5): 053006, may 2020. DOI: 10.1088/1367-2630/ab7f8f. URL https://dx.doi.org/10.1088/1367-2630/ab7f8f.

[50] Nedasadat Hosseinidehaj, Matthew S. Winnel, and Timothy C. Ralph. Simple and loss-tolerant free-space quantum key distribution using a squeezed laser. *Phys. Rev. A*, 105:032602, Mar 2022. DOI: 10.1103/PhysRevA.105.032602. URL https://link.aps.org/doi/10.1103/PhysRevA.105.032602.

[51] Lars S. Madsen, Vladyslav C. Usenko, Mikael Lassen, Radim Filip, and Ulrik L. Andersen. Continuous variable quantum key distribution with modulated entangled states. *Nature Communications*, 3(1):1083, 2012. DOI: 10.1038/ncomms2097. URL https://doi.org/10.1038/ncomms2097.

[52] Yajun Wang, Wenhui Zhang, Ruixin Li, Long Tian, and Yaohui Zheng. Generation of −10.7 dB unbiased entangled states of light. *Applied Physics Letters*, 118(13): 134001, 2021. DOI: 10.1063/5.0041289. URL https://doi.org/10.1063/5.0041289.

[53] Stefano Pirandola. End-to-end capacities of a quantum communication network. *Communications Physics*, 2(1):51, 2019. DOI: 10.1038/s42005-019-0147-3. URL https://doi.org/10.1038/s42005-019-0147-3.

[54] Matthew S. Winnel, Joshua J. Guanzon, Nedasadat Hosseinidehaj, and Timothy C. Ralph. Achieving the ultimate end-to-end rates of lossy quantum communication networks. *npj Quantum Information*, 8 (1):129, 2022. DOI: 10.1038/s41534-022-00641-0. URL https://doi.org/10.1038/s41534-022-00641-0.

[55] Noah Davis, Maksim E. Shirokov, and Mark M. Wilde. Energy-constrained two-way assisted private and quantum capacities of quantum channels. *Phys. Rev. A*, 97:062310, Jun 2018. DOI: 10.1103/Phys-

RevA.97.062310. URL https://link.aps.org/doi/10.1103/PhysRevA.97.062310.

[56] Adrien Marie and Romain Alléaume. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A*, 95:012316, Jan 2017. DOI: 10.1103/PhysRevA.95.012316. URL https://link.aps.org/doi/10.1103/PhysRevA.95.012316.

Acknowledgements

We wish to acknowledge Spyros Tserkis, and Matthew Winnel for their valuable discussions. We thank the reviewers for their valuable comments that led to the improvement of this article. This research was supported by the Australian Research Council (ARC) under the Centre of Excellence for Quantum Computation and Communication Technology (Grant No. CE110001027).

Author contributions statement

S. P. K. wrote the paper, and produced the majority of calculations and results. P. J. G. produced the DV phase-noise model in Sec 2, DV thermal-loss-to-depolarising derivation (Appendix B), and helped develop the squeezed-state phase-noise model. A. W. produced some of the calculations in the Appendix, S. M. A. and P. K. L. conceived the main idea and proofread the manuscript. All authors reviewed the manuscript.

Appendices

A Quantum Bit Error Rate (QBER)

To calculate Q_Z, we consider the probability of a bit-flip if Alice sends a logical **0** (i.e. $|1\rangle_{a_1}|0\rangle_{a_2}$) and Bob detects a logical **1** (i.e. simultaneously detects $|0\rangle_{b_1}$ and $|1\rangle_{b_2}$) given by,

$$\begin{aligned}P_{Z,\mathbf{0}\to\mathbf{1}} &= P_{Z,|1\rangle_{a_1}\to|0\rangle_{b_1}} P_{Z,|0\rangle_{a_2}\to|1\rangle_{b_2}} \\ &= \mathrm{Tr}(\hat{U}_{BS}(\eta)(|1\rangle_{a_1}\langle 1|_{a_1}\otimes\hat{\rho}_{\mathrm{Th}})\hat{U}^\dagger_{BS}(\eta)\,|0\rangle_{b_1}\langle 0|_{b_1}) \\ &\times \mathrm{Tr}(\hat{U}_{BS}(\eta)(|0\rangle_{a_2}\langle 0|_{a_2}\otimes\hat{\rho}_{\mathrm{Th}})\hat{U}^\dagger_{BS}(\eta)\,|1\rangle_{b_2}\langle 1|_{b_2}),\end{aligned} \tag{36}$$

where $\hat{\rho}_{\mathrm{Th}} = \sum_{n=0}^{\infty}[N_{\mathrm{Th}}^n/(N_{\mathrm{Th}}+1)^{n+1}]\,|n\rangle\langle n|$ is the thermal state with average thermal photon number N_{Th} and $\hat{U}_{BS}(\eta)$ is the unitary beamsplitter transformation mixing the thermal environment and the state sent by Alice. If Alice prepares a logical **1** and Bob measures **0**, the probability is

$$\begin{aligned}P_{Z,\mathbf{1}\to\mathbf{0}} &= P_{Z,|0\rangle_{a_1}\to|1\rangle_{b_1}} P_{Z,|1\rangle_{a_2}\to|0\rangle_{b_2}} \\ &= \mathrm{Tr}(\hat{U}_{BS}(\eta)(|0\rangle_{a_1}\langle 0|_{a_1}\otimes\hat{\rho}_{\mathrm{Th}})\hat{U}^\dagger_{BS}(\eta)\,|1\rangle_{b_1}\langle 1|_{b_1}) \\ &\times \mathrm{Tr}(\hat{U}_{BS}(\eta)(|1\rangle_{a_2}\langle 1|_{a_2}\otimes\hat{\rho}_{\mathrm{Th}})\hat{U}^\dagger_{BS}(\eta)\,|0\rangle_{b_2}\langle 0|_{b_2}),\end{aligned} \tag{37}$$

and since we assume the channels are symmetric, $P_{Z,\mathbf{1}\to\mathbf{0}} = P_{Z,\mathbf{0}\to\mathbf{1}}$. The total un-normalized probability of a bit-flip is $2P_{Z,\mathbf{0}\to\mathbf{1}}$.

Bob only accepts the correct bits and the flipped bits. Therefore, we normalize by considering the total probability Bob only detects the logical bits in the Z-basis. Hence

$$Q_Z = \frac{P_{Z,\mathbf{0}\to\mathbf{1}}}{P_{Z,\mathbf{0}\to\mathbf{1}}+P_{Z,\mathbf{0}\to\mathbf{0}}} = \frac{P_{Z,\mathbf{1}\to\mathbf{0}}}{P_{Z,\mathbf{1}\to\mathbf{0}}+P_{Z,\mathbf{1}\to\mathbf{1}}}, \tag{38}$$

where $P_{Z,\mathbf{0}\to\mathbf{0}} = P_{Z,|1\rangle_{a_1}\to|1\rangle_{b_1}} P_{Z,|0\rangle_{a_2}\to|0\rangle_{b_2}}$ and $P_{Z,\mathbf{1}\to\mathbf{1}} = P_{Z,|0\rangle_{a_1}\to|0\rangle_{b_1}} P_{Z,|1\rangle_{a_2}\to|1\rangle_{b_2}}$ are the probabilities of Bob detecting the same bits that Alice sent after passing through the channel. These probabilities are given by

$$\begin{aligned}P_{Z,\mathbf{0}\to\mathbf{0}} &= P_{Z,\mathbf{1}\to\mathbf{1}} \\ &= \mathrm{Tr}(\hat{U}_{BS}(\eta)(|1\rangle_{a_1}\langle 1|_{a_1}\otimes\hat{\rho}_{\mathrm{Th}})\hat{U}^\dagger_{BS}(\eta)\,|1\rangle_{b_1}\langle 1|_{b_1}) \\ &\times \mathrm{Tr}(\hat{U}_{BS}(\eta)(|0\rangle_{a_2}\langle 0|_{a_2}\otimes\hat{\rho}_{\mathrm{Th}})\hat{U}^\dagger_{BS}(\eta)\,|0\rangle_{b_2}\langle 0|_{b_2}).\end{aligned} \tag{39}$$

These probabilities are:

$$P_{Z,\mathbf{0}\to\mathbf{1}} = P_{Z,\mathbf{1}\to\mathbf{0}} = \frac{(1-\eta)^2(N_{\mathrm{Th}}+N_{\mathrm{Th}}^2)}{(1+(1-\eta)N_{\mathrm{Th}})^4} \tag{40}$$

$$P_{Z,\mathbf{0}\to\mathbf{0}} = P_{Z,\mathbf{1}\to\mathbf{1}} = \frac{\eta+(1-\eta)^2(N_{\mathrm{Th}}+N_{\mathrm{Th}}^2)}{(1+(1-\eta)N_{\mathrm{Th}})^4}. \tag{41}$$

To calculate Q_X, we consider the bit-flips in the X basis. In this case, the modes a_1 and a_2 are entangled because of the balanced beamsplitter (see Fig. 1 b)). Therefore, we consider the joint probability given by

$$
\begin{aligned}
&P_{X,\mathbf{0}\to\mathbf{1}} \\
&= \mathrm{Tr}[\hat{U}_{50/50,b_1b_2}\hat{U}_{BS,a_1}(\eta)\hat{U}_{BS,a_2}(\eta)(|-\rangle_{a_1,a_2}\langle -|_{a_1,a_2}\otimes\hat{\rho}_{a_1,\mathrm{Th}}\otimes\hat{\rho}_{a_2,\mathrm{Th}})\hat{U}^\dagger_{BS,a_1}(\eta)\hat{U}^\dagger_{BS,a_2}(\eta)\hat{U}^\dagger_{50/50,b_1b_2}M_{\mathbf{1}}], \\
&P_{X,\mathbf{1}\to\mathbf{0}} \\
&= \mathrm{Tr}[\hat{U}_{50/50,b_1b_2}\hat{U}_{BS,a_1}(\eta)\hat{U}_{BS,a_2}(\eta)(|+\rangle_{a_1,a_2}\langle +|_{a_1,a_2}\otimes\hat{\rho}_{a_1,\mathrm{Th}}\otimes\hat{\rho}_{a_2,\mathrm{Th}})\hat{U}^\dagger_{BS,a_1}(\eta)\hat{U}^\dagger_{BS,a_2}(\eta)\hat{U}^\dagger_{50/50,b_1b_2}M_{\mathbf{0}}],
\end{aligned}
\tag{42}
$$

where $\hat{U}_{50/50,b_1b_2}$ is the second balanced beamsplitter unitary, $|-\rangle_{a_1,a_2}\langle -|_{a_1,a_2} = R_{\pi,a_1}|+\rangle_{a_1,a_2}\langle +|_{a_1,a_2}R^\dagger_{\pi,a_1}$ is obtained by applying a π-phase shifter to the state $|+\rangle$, $M_{\mathbf{1}} = |0\rangle_{b_1'}\langle 0|_{b_1'}\otimes|1\rangle_{b_2'}\langle 1|_{b_2'}$ is the logical $\mathbf{1}$ measurement outcome and $M_{\mathbf{0}} = |1\rangle_{b_1'}\langle 1|_{b_1'}\otimes|0\rangle_{b_2'}\langle 0|_{b_2'}$. Similar to above, we also renormalize to obtain the QBER,

$$
Q_X = \frac{P_{X,\mathbf{0}\to\mathbf{1}}}{P_{X,\mathbf{0}\to\mathbf{1}}+P_{X,\mathbf{0}\to\mathbf{0}}}. \tag{43}
$$

We find due to symmetry that the probabilities for the diagonal basis are the same as for the rectilinear basis and it follows that $Q_X = Q_Z$, simplifying the key rate equation.

B Thermal-loss to depolarized state

Using the model of thermal noise from the previous section we identify Alice's input mode A, Bob's output mode B, and the environmental input and output modes E and F (see Fig. 8), with corresponding creation and annihilation operators (lowercase). A photon-number (Fock) state of a bosonic mode may be expressed as $|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle$; in this representation, the action of the beamsplitter is given entirely by the transformation

$$
\begin{aligned}
\hat{a} &\mapsto \sqrt{\eta}\,\hat{b} + \sqrt{1-\eta}\,\hat{f} \\
\hat{e} &\mapsto \sqrt{1-\eta}\,\hat{b} - \sqrt{\eta}\,\hat{f}.
\end{aligned}
\tag{44}
$$

If the beamsplitter receives no photon from Alice and exactly n photons from the environment,

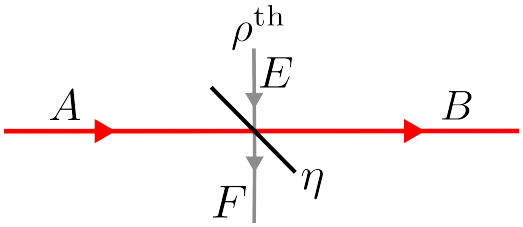


Figure 8: A thermal noise rail with modes labeled for Alice, Bob, and the environment.

then under action (44) the combined input state $|0,n\rangle_{AE}$ transforms as

$$
\begin{aligned}
|0,n\rangle_{AE} = \frac{(\hat{e}^\dagger)^n}{\sqrt{n!}}|0,0\rangle_{AE} &\longmapsto \frac{(\sqrt{1-\eta}\,\hat{b}^\dagger - \sqrt{\eta}\,\hat{f}^\dagger)^n}{\sqrt{n!}}|0,0\rangle_{BF} \\
&= \frac{1}{\sqrt{n!}}\left(\sum_{k=0}^{n}\binom{n}{k}(\sqrt{1-\eta}\,\hat{b}^\dagger)^{n-k}(-\sqrt{\eta}\,\hat{f}^\dagger)^k\right)|0,0\rangle \\
&= \frac{1}{\sqrt{n!}}\sum_{k=0}^{n}\frac{n!}{k!(n-k)!}(\sqrt{1-\eta})^{n-k}(-\sqrt{\eta})^k\sqrt{(n-k)!}\sqrt{k!}\,|n-k,k\rangle \\
&= \sum_{k=0}^{n}\sqrt{\binom{n}{k}}(\sqrt{1-\eta})^{n-k}(-\sqrt{\eta})^k\,|n-k,k\rangle \\
&:= |\psi_n\rangle
\end{aligned}
$$

which is a coherent superposition of Fock states, with n total photons split across rails B and F according to a binomial distribution. If Alice instead sends a single photon we obtain

$$
\begin{aligned}
|1,n\rangle_{AE} = \hat{a}^\dagger\,|0,n\rangle_{AE} &\longmapsto (\sqrt{\eta}\,\hat{b}^\dagger + \sqrt{1-\eta}\,\hat{f}^\dagger)\,|\psi_n\rangle \\
&= \sqrt{\eta}\sum_{k=0}^{n}\sqrt{\binom{n}{k}}(-\sqrt{\eta})^k(\sqrt{1-\eta})^{n-k}\sqrt{n-k+1}\,|n-k+1,k\rangle \\
&\quad + \sqrt{1-\eta}\sum_{k=0}^{n}\sqrt{\binom{n}{k}}(-\sqrt{\eta})^k(\sqrt{1-\eta})^{n-k}\sqrt{k+1}\,|n-k,k+1\rangle \\
&:= |\phi_n\rangle
\end{aligned}
$$

where the first term corresponds with Alice's photon reaching Bob, and the second with it escaping to the environment.

It follows that Alice's input can be considered a 2×2 density matrix $\hat{\rho}^A$ with terms of form $\rho^A_{ij}\,|\mathbf{i}\rangle\langle\mathbf{j}|$. The collective input AE to the beamsplitter system is therefore

$$
\hat{\rho}^{\text{in}} = \hat{\rho}^A \otimes \hat{\rho}^E = \sum_{i,j,\mathbf{n}} \hat{\rho}^A_{ij} p_{\mathbf{n}}\,|\mathbf{i},\mathbf{n}\rangle\langle\mathbf{j},\mathbf{n}|\,.
$$

Since quantum channels are linear, the collective output BF is determined by the action of the channel on each $|\mathbf{i},\mathbf{n}\rangle\langle\mathbf{j},\mathbf{n}|$ term (despite $|\mathbf{i}\rangle\langle\mathbf{j}|$ individually representing a nonphysical state whenever $i\neq j$). Since $|\mathbf{i},\mathbf{n}\rangle$ represents an independent input to each beamsplitter, the output is a direct tensor product of the independent single-rail outputs derived above, i.e.

$$
\begin{aligned}
|\mathbf{i},\mathbf{n}\rangle_{AE} \longmapsto\; & |\psi_{n_0}\rangle_{B_0F_0}\,|\psi_{n_1}\rangle_{B_1F_1}\cdots \\
& |\phi_{n_0}\rangle_{B_0F_0}\cdots|\psi_{n_1}\rangle_{B_{n_1}F_{n_1}} := |\omega_{\mathbf{i},\mathbf{n}}\rangle_{BF}
\end{aligned}
$$

where only rail i has output $|\phi_n\rangle$, the symbol ω was chosen for no particular reason. The Hermitian conjugate of Eq. (44) transforms the corresponding bra in the same way, giving $\langle\mathbf{j},\mathbf{n}| \longmapsto \langle\omega_{\mathbf{j},\mathbf{n}}|$ and hence $|\mathbf{i},\mathbf{n}\rangle\langle\mathbf{j},\mathbf{n}| \mapsto |\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{j},\mathbf{n}}|$. Bob's final state is

$$
\hat{\rho}^B = \text{Tr}_F(\hat{\rho}^{\text{out}}) = \text{Tr}_F\left(\sum_{i,j,\mathbf{n}} \rho^A_{ij} p_{\mathbf{n}}\,|\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{j},\mathbf{n}}|\right) = \sum_{i,j}\rho^A_{ij}\sum_{\mathbf{n}} p_{\mathbf{n}}\,\text{Tr}_F\,|\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{j},\mathbf{n}}| \tag{45}
$$

obtained by tracing over the environmental modes in the collective output $\hat{\rho}^{\text{out}}$.

We assume that Bob may perform a perfect photon-number-resolving (PNR) measurement in any desired basis, and that like Alice he is interested only in single-photon states $|\boldsymbol{\beta}\rangle = \sum_i \beta_i\,|\mathbf{i}\rangle$ and will discard all others. With perfect measurement, Bob's outcome probabilities are given by projection:

$$
P(|\boldsymbol{\beta}\rangle) = \langle\boldsymbol{\beta}|\hat{\rho}^B|\boldsymbol{\beta}\rangle = \text{Tr}\Big(|\boldsymbol{\beta}\rangle\langle\boldsymbol{\beta}|\,\hat{\rho}^B\Big) \tag{46}
$$

where only terms of form $|\mathbf{i}\rangle\langle\mathbf{j}|$ in Bob's state $\hat{\rho}^B$ contribute to this expression if $|\boldsymbol{\beta}\rangle$ is a single-photon state. Like $\hat{\rho}^A$, Bob's state $\hat{\rho}^B$ may therefore be effectively considered a 2×2 matrix ρ^B_{ij}, which we now compute. Discarding terms which contain multiple photons in any single one of Bob's rails leaves

$$
\begin{aligned}
|\psi_n\rangle &\longrightarrow |\psi'_n\rangle = (-\sqrt{\eta})^{n-1}\left(-\sqrt{\eta}\,|0,n\rangle + \sqrt{n(1-\eta)}\,|1,n-1\rangle\right) \\
|\phi_n\rangle &\longrightarrow |\phi'_n\rangle = (-\sqrt{\eta})^{n-1}\left([n-\eta n-\eta]\,|1,n\rangle - \sqrt{\eta(1-\eta)(n+1)}\,|0,n+1\rangle\right).
\end{aligned} \tag{47}
$$

Next, to compute

$$
\text{Tr}_F\,|\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{j},\mathbf{n}}| = \sum_{\mathbf{n}}\langle\mathbf{n}\rangle\,\omega_{\mathbf{i},\mathbf{n}}\,\langle\omega_{\mathbf{j},\mathbf{n}}\rangle\,\mathbf{n}
$$

we need only consider components of $|\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{j},\mathbf{n}}|$

with diagonal environmental mode $|\mathbf{n}\rangle\langle\mathbf{n}|$, as all others vanish. Discarding these nondiagonal terms in each of our single-rail outer products gives

$$|\psi'_n\rangle\langle\psi'_n| \longrightarrow \eta^{n-1}(\eta\,|0,n\rangle\langle 0,n| + n(1-\eta)\,|1,n-1\rangle\langle 1,n-1|) \tag{48}$$

$$|\phi'_n\rangle\langle\phi'_n| \longrightarrow \eta^{n-1}([n-\eta n-\eta]^2\,|1,n\rangle\langle 1,n| + \eta(1-\eta)(n+1)\,|0,n+1\rangle\langle 0,n+1|) \tag{49}$$

$$|\phi'_n\rangle\langle\psi'_n| \longrightarrow -\eta^{n-1}\sqrt{\eta}\,[n-\eta n-\eta]\,|1,n\rangle\langle 0,n| \tag{50}$$

$$|\psi'_n\rangle\langle\phi'_n| \longrightarrow -\eta^{n-1}\sqrt{\eta}\,[n-\eta n-\eta]\,|0,n\rangle\langle 1,n|\,. \tag{51}$$

We can decompose $|\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{j},\mathbf{n}}|$ in the collective Fock basis as a sum of terms corresponding with each different combination of photon numbers from Eqs. (48) and/or (49). However, we keep only those terms with a photon in exactly one of Bob's modes; if $i \neq j$, terms (50) and (51) provide these photons (albeit in a different rail on each side of the outer product) and hence all other rails must be empty. After simultaneously tracing out the environment, this gives

$$\mathrm{Tr}_F\,|\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{j},\mathbf{n}}| = \frac{1}{\eta}\left(\eta^{n_i}[n_i-\eta n_i-\eta]\right)\left(\eta^{n_j}[n_j-\eta n_j-\eta]\right)\left(\prod_{k\neq i,j}\eta^{n_k}\right)|\mathbf{i}\rangle\langle\mathbf{j}|\,.$$

If $i=j$, the photon is received either in the original rail i or an erroneous rail $j\neq i$, giving

$$\mathrm{Tr}_F\,|\omega_{\mathbf{i},\mathbf{n}}\rangle\langle\omega_{\mathbf{i},\mathbf{n}}| = \eta^{n_i-1}(n_i-\eta n_i-\eta)\left(\prod_{k\neq i}\eta^{n_k}\right)|\mathbf{i}\rangle\langle\mathbf{i}|$$
$$+\sum_{j\neq i}(1-\eta)^2\,\eta^{n_i}(n_i+1)\,n_j\eta^{n_j-1}\left(\prod_{k\neq i,j}\eta^{n_k}\right)|\mathbf{j}\rangle\langle\mathbf{j}|\,.$$

Returning to Eq. (45), we now sum over all $\mathbf{n}$. This is done analytically, and can also be done with the aid of Mathematica. The resulting action of the channel is defined by

$$|\mathbf{i}\rangle\langle\mathbf{j}|_A \longmapsto \frac{\eta}{\gamma^4}\,|\mathbf{i}\rangle\langle\mathbf{j}|_B : \qquad i\neq j,$$

$$|\mathbf{i}\rangle\langle\mathbf{i}|_A \longmapsto \frac{\eta}{\gamma^4}\,|\mathbf{i}\rangle\langle\mathbf{i}| + \frac{N_{\mathrm{Th}}(1+N_{\mathrm{Th}})(1-\eta)^2}{\gamma^4}\mathbb{I}$$

where $\gamma = 1+N_{\mathrm{Th}}-N_{\mathrm{Th}}\eta$ and $\mathbb{I}$ is the identity, i.e. $\mathbb{I}/2$ is the maximally-mixed state. Noting that $\mathrm{Tr}\,\hat{\rho}^A = \sum_i \rho^A_{ii} = 1$, we can thus express this as the qubit transformation $\hat{\rho}^A \to \hat{\rho}^B$ (see Eq. (45)):

$$\hat{\rho}^A \longmapsto \frac{\eta}{\gamma^4}\hat{\rho}^A + \frac{N_{\mathrm{Th}}(1+N_{\mathrm{Th}})(1-\eta)^2}{\gamma^4}\left(\sum_i \hat{\rho}^A_{ii}\right)\mathbb{I} \tag{52}$$

$$= \frac{\eta}{\gamma^4}\hat{\rho}^A + \frac{N_{\mathrm{Th}}(1+N_{\mathrm{Th}})(1-\eta)^2}{\gamma^4}\mathbb{I}. \tag{53}$$

The trace of this un-normalised output now represents the probability P_s of successfully receiving a valid qubit:

$$P_S = \mathrm{Tr}\,\hat{\rho}^B = \frac{\eta + 2\,N_{\mathrm{Th}}(1+N_{\mathrm{Th}})(1-\eta)^2}{\gamma^4}. \tag{54}$$

Conditional on success, we obtain the normalised state

$$\tilde{\hat{\rho}}^B := \frac{\hat{\rho}^B}{P_S} = \frac{\eta}{\eta + 2\,N_{\mathrm{Th}}(1+N_{\mathrm{Th}})(1-\eta)^2}\hat{\rho}^A$$
$$+\frac{N_{\mathrm{Th}}(1+N_{\mathrm{Th}})(1-\eta)^2}{\eta + 2\,N_{\mathrm{Th}}(1+N_{\mathrm{Th}})(1-\eta)^2}\mathbb{I}. \tag{55}$$

This represents a depolarizing channel [24]

$$\hat{\rho} \to (1-\lambda)\hat{\rho} + \frac{\lambda}{2}\mathbb{I} \tag{56}$$

with depolarizing parameter

$$\lambda = \frac{2\,N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}{\eta + 2\,N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}, \tag{57}$$

which tends to 1 as $\eta \to 0$ or $N_{\rm Th} \to \infty$, as expected.

A property of the depolarizing channel is that the error rate is the same in all bases:

$$Q = \frac{\lambda}{2} = \frac{N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}{\eta + 2N_{\rm Th}(1+N_{\rm Th})(1-\eta)^2}, \tag{58}$$

which can be seen from Eq. (56). In this article, we only focus on the dual-rail case of $d = 2$. It is left for future work to consider the high-dimensional QKD protocols in-depth.

C Fighting noise with noise squeezed state protocol

Introducing trusted Gaussian noise $\xi_{\rm B}$ before Bob's detection modifies the mutual information:

$$I_{\rm AB}^{\rm noise} = \frac{1}{2}\log_2\left(\frac{V_{\rm B}+\xi_{\rm B}}{V_{\rm B|A}+\xi_{\rm B}}\right), \tag{59}$$

The conditional entropy is:

$$S({\rm E}|x_{\rm B}) = S({\rm BC}|x_{\rm B}) = G((\lambda_3-1)/2)+G((\lambda_4-1)/2), \tag{60}$$

where the symplectic eigenvalues are given by:

$$\lambda_{3,4}^2 = \frac{1}{2}[A \pm \sqrt{A^2-4B}], \tag{61}$$

where

$$\begin{aligned} A &= \frac{1}{V_{\rm B}+\xi_{\rm B}}(V_{\rm B}+V_{\rm A}D+\xi_{\rm B}\Delta), \\ B &= \frac{D}{V_{\rm B}+\xi_{\rm B}}(V_{\rm A}+\xi_{\rm B}D), \end{aligned} \tag{62}$$

where for $\xi_{\rm B} = 0$ and $\xi_{\rm B} = 1$, we obtain the squeezed protocol with homodyne and heterodyne detection, respectively.

D Thermal-loss channel treatment in Ref. [17]

In Fig. 9, we plot the numerical results of the noise tolerance ratio between CV and DV for comparison with Ref. [17]. We find that the Sqz-Hom protocol tolerates thermal noise for a wider range of transmittance values for high secret key rate requirements. The numerical results from Ref. [17] are different for $\eta = 10^{-1}$ to $\eta = 1$ which showed the ratio $N_{\rm Th,Max}^{CV}/N_{\rm Th,Max}^{DV} = 0.4$

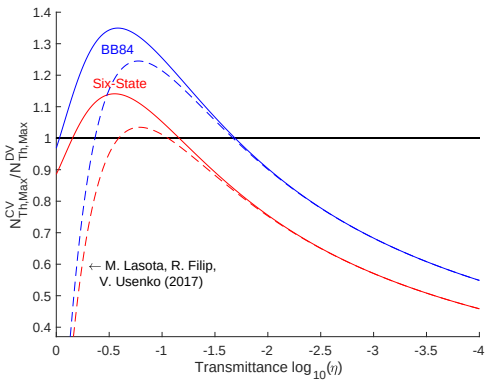


Figure 9: Ratio of maximum noise tolerance of the squeezed state protocol with BB84 (blue) and Six-State (red) protocols. Shown are numerical results for K_0 of 10^{-10} (solid line), compared with the noise tolerance from Ref. [17] (dashed lines). The protocol parameters of CV and DV are the same as those in Fig. 3.

as $\eta \to 1$ from $\eta = 10^{-0.5} = 0.32$. Our results show a much less dramatic noise tolerance drop-off of the ratio compared to Ref. [17]. The difference can be explained by the model for the thermal-loss channel in DV-QKD in Ref. [17] which assumes that the signal and noise photons can be distinguished. The probabilities are calculated as a classical conditional probability rather than quantum as we will show below. In our model, we do not make this assumption, as the dual-rail protocol in the thermal-loss channel is completely controlled by Eve and consequently the QBER in our model is higher. In this Appendix, we derive the equations that give the same QBER as in Ref. [17]. The difference between our model in the main text and Ref. [17] are

1. The treatment of the thermal noise model is different. Ref. [17] treats the thermal-loss channel as a conditional photon-loss channel and a thermal noise channel.

2. In their initial analysis they make use of ON/OFF detectors rather than photon-number resolving detectors. Nonetheless, these were shown to be equivalent for the noise tolerance.

The first point of difference is the most important as this impacts the noise tolerance.

With this model of noise, the accepted probability for the ON/OFF detector is given by [17]:

$$p_{\text{exp}} = \sum_{k=0}^{n_+=\infty} p_+(k,0) + \sum_{k=1}^{n_-=\infty} p_-(k,0) + \sum_{l=1}^{n_-=\infty} p_-(0,l), \tag{63}$$

where the first term represents the following:

$$p_+(k,0) = [p_\eta(1,1)p_{\eta,N_{\text{Th}}}(0,k)]p_{\eta,N_{\text{Th}}}(0,0), \tag{64}$$

where $p_\eta(1,1)$ is the probability that a photon is not lost by the pure-loss channel multiplied by the probability $p_{\eta,N_{\text{Th}}}(0,k)$ that a noise photon is added in the RIGHT detector (inside of brackets) and multiplied by the probability $p_{\eta,N_{\text{Th}}}(0,0)$ no noise photon is added in the WRONG detector (outside of brackets). The middle term is:

$$p_-(k,0) = [p_\eta(1,0)p_{\eta,N_{\text{Th}}}(0,k)]p_{\eta,N_{\text{Th}}}(0,0), \tag{65}$$

where $p_\eta(1,0)$ is the probability that a photon is lost by the pure-loss channel multiplied by the probability $p_{\eta,N_{\text{Th}}}(1,k)$ that a noise photon is added in the RIGHT detector and as before, multiplied by the probability $p_{\eta,N_{\text{Th}}}(0,0)$ no noise photon is added in the WRONG detector. Finally the last term is

$$p_-(0,l) = [p_\eta(1,0)p_{\eta,N_{\text{Th}}}(0,0)]p_{\eta,N_{\text{Th}}}(0,l), \tag{66}$$

where a photon is lost by the pure-loss channel and no noise photon is added in the RIGHT detector and a noise photon is added in the WRONG detector. Evidently this last term is the only term that contributes to the QBER:

$$Q = \frac{\sum_{l=1}^{n=\infty} p_-(0,l)}{p_{\text{exp}}}. \tag{67}$$

For a photon number resolving detector (PNRD) the summations terminate at $n_+ = 0$ and $n_- = 1$. Evaluating this expression for PNRDs and using the calculations from Appendix A that $p_{\eta,N_{\text{Th}}}(1,0) = (1-\eta)(N_{\text{Th}}+1)/\gamma^2$, $p_{\eta,N_{\text{Th}}}(0,1) = (1-\eta)N_{\text{Th}}/\gamma^2$, $p_{\eta,N_{\text{Th}}}(0,0) = 1/\gamma$ and $p_{\eta,N_{\text{Th}}}(1,1) = (\eta + (1-\eta)^2(N_{\text{Th}}^2 + N_{\text{Th}}))/\gamma^3$ where it is reminded that $\gamma = 1 + (1-\eta)N_{\text{Th}}$. The probability of the bit-flip error is

$$p_-(0,l) = \frac{N_{\text{Th}}(1-\eta)^2}{\gamma^3}. \tag{68}$$

Comparing this probability of a bit-flip with that of Appendix A:

$$P_{Z,\mathbf{0}\to\mathbf{1}} = \frac{N_{\text{Th}}(1+N_{\text{Th}})(1-\eta)^2}{\gamma^4}. \tag{69}$$

Therefore, not being able to distinguish signal photons and noise photons increases the probability of a bit-flip error by the factor $(1+N_{\text{Th}})/(1+(1-\eta)N_{\text{Th}}) > 1$. The difference is that in the RIGHT detector the probability $p_\eta(1,0)p_{\eta,N_{\text{Th}}}(0,0) = (1-\eta)/\gamma \neq p_{\eta,N_{\text{Th}}}(1,0) = (1-\eta)(N_{\text{Th}}+1)/\gamma^2$. The probability of success is $p_{\text{exp}} = \frac{\eta + N_{\text{Th}}(1-\eta)(2-\eta)}{\gamma^3}$.

Comparing the QBER of this "distinguishable" approach:

$$Q_{\text{D}} = \frac{N_{\text{Th}}(1-\eta)^2}{\eta + N_{\text{Th}}(1-\eta)(2-\eta)}, \tag{70}$$

with calculations in Appendix A for indistinguishable noise and signal photons:

$$Q_{\text{I}} = \frac{N_{\text{Th}}(1+N_{\text{Th}})(1-\eta)^2}{\eta + 2N_{\text{Th}}(1+N_{\text{Th}})(1-\eta)^2}. \tag{71}$$

We remark that Q_{D} for ON/OFF detectors are exactly the same as for PNRDs for this approach. We can evaluate the sums $\sum_{m=0}^{n=\infty} p_{\eta,N_{\text{Th}}}(0,m) = 1$ and $\sum_{m=1}^{n=\infty} p_{\eta,N_{\text{Th}}}(0,m) = 1 - p_{\eta,N_{\text{Th}}}(0,0) = \frac{\gamma-1}{\gamma}$ leading to the probability of bit-flip errors $\sum_{l=1}^{n=\infty} p_-(0,l) = N_{\text{Th}}(1-\eta)^2/\gamma^2$ and $p_{\text{exp}} = \frac{\eta + N_{\text{Th}}(1-\eta)(2-\eta)}{\gamma^2}$.

In Fig. 9, we plot the ratio of the maximum noise tolerance of the SS-Hom protocol with the BB84 and 6S protocols, comparing the two approaches. As illustrated in Fig. 9, distinguishable photons seem to tolerate more thermal noise than indistinguishable photons in the limit of $\eta \to 1$. Setting $Q_{\text{D}} = Q_{\text{I}} = 0.1262$ for the highest QBER tolerance of the 6S protocol, the maximum tolerable noises are:

$$N_{\text{Th,D,Max}} = \frac{631\eta}{3738 - 8107\eta + 4369\eta^2}, \tag{72}$$

implies that at $\eta \to 0.8556$, the tolerable noise approaches ∞. For $\eta > 0.8556$ the QBER never reaches 0.1262 for any value of N_{Th}. And for indistinguishable:

$$N_{\text{Th,I,Max}} = \frac{\sqrt{1 - \frac{2476\eta}{1869} + \eta^2}}{2(1-\eta)} - \frac{1}{2}, \tag{73}$$

where we note that $N_{\mathrm{Th}} < \eta/(1-\eta)$ for non-entanglement breaking channels. Clearly, Eq. (72) violates this condition whereas Eq. (73) does not. We note the difference with the results of Ref. [17] which determine the noise tolerance numerically. We believe that with high enough dimensions, this behaviour can be seen and will match the analytical expression for the QBER of Eq. (70).

In the high loss limit $\eta \ll 1$, the maximum tolerable noises are:

$$N_{\mathrm{Th,D,Max}} \approx \frac{0.1688\eta}{1-2.1688\eta}, \tag{74}$$

and

$$N_{\mathrm{Th,I,Max}} \approx \frac{0.1688\eta}{1-\eta}. \tag{75}$$

These results show that for $\eta \ll 10^{-2}$ as seen in Fig. 9, the ratio of CV to DV noise tolerances are both approaching the same limits i.e. 0.1688η. As loss increases and tolerable noise decreases, the ability to distinguish signal photons from noise photons is no longer an advantage.

E Squeezed-state protocol with phase noise

In this section, we derive the covariance matrix of the squeezed-state protocol in the combined thermal-loss and phase noise channel. Consider the squeezed-state protocol where Alice's modulation variance is $V_{\mathrm{sig}} = e^{2r} - e^{-2r}$. This state passes through a thermal-loss channel with η and N_{Th} followed by a phase noise channel with circular variance $V_\theta = \sigma_\theta^2$. Since Bob's average state is thermal, the phase noise does not affect the variance of Bob's data. Modeling the phase following the wrapped normal distribution as done for the DV case, Bob's received variance in the EB scheme is $V_B = \eta\mu + (1-\eta)(2N_{\mathrm{Th}}+1)$ where $\mu = V_{\mathrm{sig}} + V_{\mathrm{sqz}} = e^{2r}$.

The inferred transmittance η_{I} is found by first considering the Gaussian integrals of the correlations $\langle X_A X_B|\theta\rangle$ in the PM scheme for a fixed value of θ:

$$\begin{aligned}&\langle X_A X_B|\theta\rangle \\ &= \int\int dx_A dx_B f_{B|A}(x_A,x_B) f_A(x_A) x_A x_B \\ &= V_{\mathrm{sig}}\sqrt{\eta}\cos\theta,\end{aligned} \tag{76}$$

where for a fixed θ, x_A follows a Gaussian distribution (centered at zero) with modulation variance V_{sig} and $x_B = \sqrt{\eta}x_A\cos\theta$ with variance Ξ due to channel noise. The correlations are reduced as expected, due to the wrapping of the squeezed state around phase space, by a factor of $\cos\theta$. Next, we integrate over the wrapped normal distribution of θ which is also known as the circular mean as in Eq. (25). Therefore,

$$\langle X_A X_B\rangle = \int d\theta V_{\mathrm{sig}}\sqrt{\eta} f_{WN}(\theta)\cos\theta = V_{\mathrm{sig}}\sqrt{\eta}\bar{r}, \tag{77}$$

where $\bar{r} = e^{-\sigma_\theta^2/2}$. In the entanglement-based scheme, the correlations are $\langle X_A X_B\rangle_{\mathrm{EB}} = \sqrt{\eta\bar{r}^2(\mu^2-1)}$. The inferred transmittance is therefore

$$\eta_{\mathrm{I}} = \eta e^{-\sigma_\theta^2}. \tag{78}$$

The effective Gaussian channel is:

$$V_B = \eta_{\mathrm{I}}(\mu + \chi_I), \tag{79}$$

where χ_{I} is the inferred noise. Rearranging,

$$\begin{aligned}\chi_{\mathrm{I}} &= \frac{V_B - \eta_I\mu}{\eta_{\mathrm{I}}} \\ &= \frac{(1-e^{-\sigma_\theta^2})\eta\mu + (1-\eta)(2N_{\mathrm{Th}}+1)}{\eta e^{-\sigma_\theta^2}}.\end{aligned} \tag{80}$$

We can also define the excess noise w.r.t. Alice due to phase noise ξ_θ by

$$V_B = \eta_I\mu + (1-\eta)(2N_{\mathrm{Th}}+1) + \eta\xi_\theta, \tag{81}$$

implying that $\xi_\theta = (1-e^{-\sigma_\theta^2})\mu$.

For the squeezed-state protocol, the combined thermal-loss and phase noise channel leads to the following covariance matrix in the EB scheme:

$$\begin{aligned}\gamma_{\mathrm{AB}} &= \begin{pmatrix} a\mathbb{I} & c\sigma_z \\ c\sigma_z & b\mathbb{I}\end{pmatrix} \\ &= \begin{pmatrix} \mu\mathbb{I} & \sqrt{\eta_{\mathrm{I}}(\mu^2-1)}\sigma_z \\ \sqrt{\eta_{\mathrm{I}}(\mu^2-1)}\sigma_z & (\eta_{\mathrm{I}}(\mu+\chi_{\mathrm{I}})\mathbb{I}\end{pmatrix} \\ &= \begin{pmatrix} \mu\mathbb{I} & \bar{r}\sqrt{\eta(\mu^2-1)}\sigma_z \\ \bar{r}\sqrt{\eta(\mu^2-1)}\sigma_z & (\eta\mu+(1-\eta)(2N_{\mathrm{Th}}+1))\mathbb{I}\end{pmatrix},\end{aligned} \tag{82}$$

where the inferred transmittance $\eta_I = \eta\bar{r}^2 = \eta e^{-\sigma_\theta^2}$ and noise $\chi_I = \frac{(1-e^{-\sigma_\theta^2})\eta\mu + (1-\eta)(2N_{\mathrm{Th}}+1)}{\eta e^{-\sigma_\theta^2}}$.

The phase noise channel is a non-Gaussian channel. To estimate the channel parameters, Alice and Bob evaluate the covariance matrices between their measurement results and infer the effective transmittance (η_I) and effective noise (χ_I) of an equivalent Gaussian channel. The phase

noise reduces the effective transmittance, and increases the effective noise.

We note that the phase noise model in Eq. (82) is different from previous treatments, for example, as in [56] for the GG02 protocol (see Appendix F) which only considers the effect of the phase noise on $\langle \Delta X_B^2 \rangle$. The implicit assumption is that the estimate for η (or G defined in [56] as the intensity transmission of the channel) is unchanged and an excess noise ξ_θ is added by the phase noise channel. Without the attenuation in transmittance by the factor $\bar{r}^2$, this leads to a model that is inaccurate in the high phase noise regime where the noise $\chi = \xi_\theta + \frac{(1-\eta)(2N_{\mathrm{Th}}+1)}{\eta}$ would be underestimated compared to χ_I.

F GG02 protocol phase noise

For the coherent state Gaussian modulated protocols, Alice prepares coherent states in the phase space with θ phase.

As in [56], we consider the residual phase noise after estimating the phase. The quadratures after homodyne or heterodyne measurements are:

$$\begin{pmatrix} x_m \\ p_m \end{pmatrix} = \sqrt{\frac{G}{2}} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x_A + x_0 \\ p_A + p_0 \end{pmatrix}, \tag{83}$$

where Alice sends a coherent state that follows a Gaussian distribution with $x_A \sim \mathcal{N}(0, V_x)$ and $p_A \sim \mathcal{N}(0, V_p)$ centered at $x_0 = 0$ and $p_0 = 0$ measured with a coherent detector with total intensity transmission G of the channel.

Bob then estimates the phase with the estimator $\hat{\theta} \sim \mathcal{N}(\theta, V_\theta)$. Bob then sends his phase estimates to Alice who makes corrections and estimates Bob's measurements. The excess noise due to the phase noises would then be:

$$\begin{aligned} \xi_x &= \mathrm{var}(x_m - \tilde{x}_m) \\ \xi_p &= \mathrm{var}(p_m - \tilde{p}_m). \end{aligned} \tag{84}$$

where var is the variance, and $\tilde{x}_m$ and $\tilde{p}_m$ are the estimated quadratures as a function of the estimator $\hat{\theta}$. The excess noise depends on the remaining phase noise $\Theta = \theta - \hat{\theta}$ which we assume is a normally distributed variable $\Theta \sim \mathcal{N}(0, \sigma_\Theta^2)$. Then it is straightforward to calculate the excess noise:

$$\begin{aligned} \xi_x &= 2V_A(1 - e^{-\tilde{\sigma}_\Theta^2/2}) \\ \xi_p &= 2V_A(1 - e^{-\tilde{\sigma}_\Theta^2/2}), \end{aligned} \tag{85}$$

where $\tilde{\sigma}_\Theta^2 = V_\theta$. For small phase noise $\tilde{\sigma}_\Theta^2 < 0.1$, $\xi_x = \xi_p \approx \tilde{\sigma}_\Theta^2 V_A$.

G GG02 protocol with heterodyne detection

For heterodyne detection by Bob, the mutual information I_{AB} in a thermal-loss channel is [26]

$$\begin{aligned} I_{\mathrm{AB}} &= \log_2\left(\frac{V_{\mathrm{B}}+1}{V_{\mathrm{B|A}^M}+1}\right) \\ &= \log_2\left(\frac{\eta V_{\mathrm{A}} + (1-\eta)(2N_{\mathrm{Th}}+1)}{\eta + (1-\eta)(2N_{\mathrm{Th}}+1)}\right), \end{aligned} \tag{86}$$

where V_{B} is Bob's variance and $V_{\mathrm{B|A}^M} = b - c^2/(a+1)$ is Bob's variance conditioned on Alice's heterodyne measurement. $S(\mathrm{E|B}) = S(\mathrm{A}|x_B, p_D)$ is the information obtained by Eve conditioned on Bob's heterodyne measurement result x_{B} and the auxiliary mode p_{D} [26]. The covariance matrix of Alice after a projective measurement by Bob's heterodyne detection is

$$\gamma_{\mathrm{A}}^{\mathrm{out}} = \gamma_{\mathrm{A}} - \sigma_{\mathrm{AB}}(\gamma_{\mathrm{B}} + \mathbb{I})^{-1}\sigma_{\mathrm{AB}}^T, \tag{87}$$

where $\sigma_{\mathrm{AB}} = c\sigma_Z$. The conditional Von Neumann entropy is

$$S(\mathrm{A}|x_{\mathrm{B}}, p_{\mathrm{D}}) = G[(\lambda_3 - 1)/2], \tag{88}$$

where the symplectic eigenvalue λ_3 is

$$\lambda_3 = a - c^2/(b+1). \tag{89}$$

H Squeezing required for the Sqz-Hom protocol

In Fig. 10, we compare the performance of the Sqz-Hom protocol for the amount of squeezing used to the BB84 protocol and GG02 with heterodyne (GG02) protocol. In a pure-loss channel (see Fig. 10 a)), Sqz-Hom protocols with more than 10 dB of squeezing are sufficient to be equal to or better than the GG02 protocol for all loss parameters (where the key rate is greater than $K = 10^{-10}$). However, for an intermediate-noise region (i.e. Fig. 10 b)), the BB84 protocol is robust at higher channel losses. We find that for very noisy thermal-loss channels shown in Fig. 10 c) and d), more than 9 dB of squeezing is required to surpass BB84.

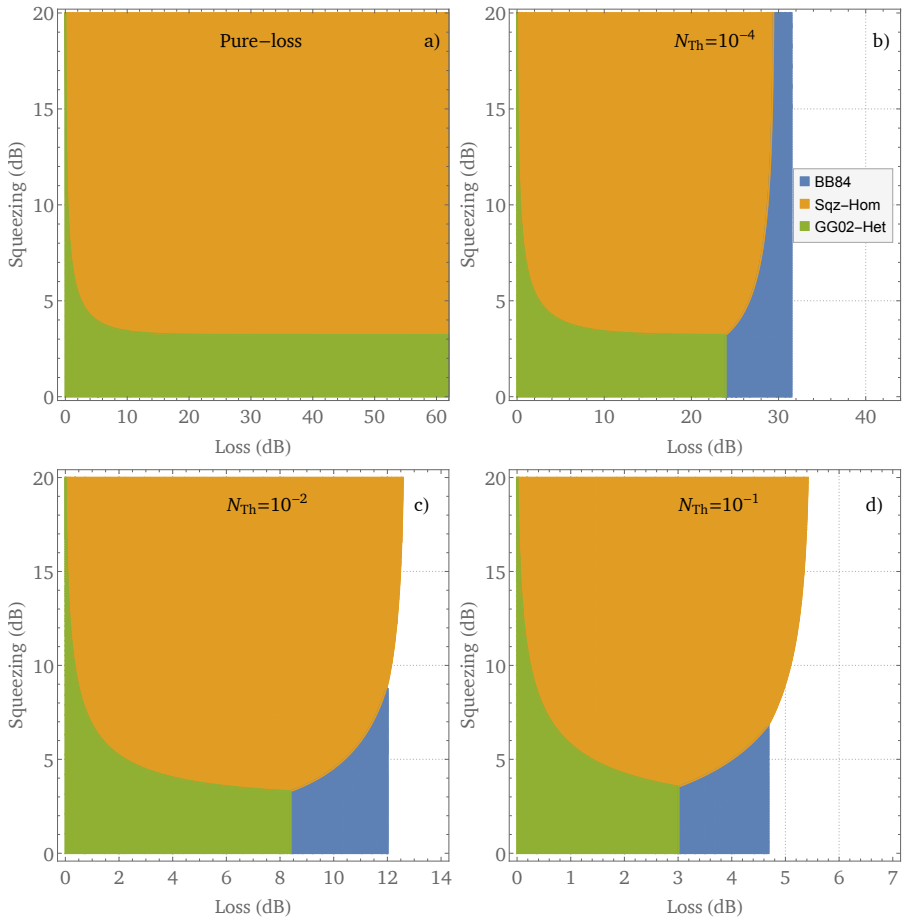


Figure 10: Regions where QKD protocols give the highest secret key rate greater than $K = 10^{-10}$ based on the amount of squeezing V_{sq} prepared by Alice for the squeezed-state protocol with homodyne detection. In the unshaded regions, K is less than 10^{-10} for all protocols. Comparison of the squeezed-state protocol with homodyne detection in a pure-loss channel based on the amount of squeezing prepared by Alice. Above 9 dB of squeezing, the Sqz-Hom protocol performs better than GG02 and BB84 protocols.