Quantum Science and Technology

OPEN ACCESS

RECEIVED
11 October 2024

REVISED
18 December 2024

ACCEPTED FOR PUBLICATION
14 January 2025

PUBLISHED
3 February 2025

PAPER

Security of hybrid BB84 with heterodyne detection

Jasminder S Sidhu[1,*], Rocco Maggi[2,3,4], Saverio Pascazio[3,4] and Cosmo Lupo[2,3,4,*]

[1] SUPA Department of Physics, The University of Strathclyde, Glasgow G4 0NG, United Kingdom
[2] Dipartimento Interateneo di Fisica, Politecnico di Bari, 70126 Bari, Italy
[3] Dipartimento Interateneo di Fisica, Università di Bari, 70126 Bari, Italy
[4] INFN, Sezione di Bari, 70126 Bari, Italy
[*] Authors to whom any correspondence should be addressed.

E-mail: jsmdrsidhu@gmail.com and cosmo.lupo@poliba.it

Keywords: quantum communications, quantum networking, security proofs, quantum key distribution

Abstract

Quantum key distribution (QKD) promises everlasting security based on the laws of physics. Most common protocols are grouped into two distinct categories based on the degrees of freedom used to carry information, which can be either discrete or continuous, each presenting unique advantages in either performance, feasibility for near-term implementation, and compatibility with existing telecommunications architectures. Recently, hybrid QKD protocols have been introduced to leverage advantages from both categories. In this work we provide a rigorous security proof for a protocol introduced by Qi in 2021, where information is encoded in discrete variables as in the widespread Bennett Brassard 1984 protocol but decoded continuously via heterodyne detection. Security proofs for hybrid protocols inherit the same challenges associated with continuous-variable protocols due to unbounded dimensions. Here we successfully address these challenges by exploiting symmetry. Our approach enables truncation of the Hilbert space with precise control of the approximation errors and lead to a tight, semi-analytical expression for the asymptotic key rate under collective attacks. As concrete examples, we apply our theory to compute the key rates under passive attacks, linear loss, and Gaussian noise.

1. Introduction

Quantum key distribution (QKD) exploits quantum optics to establish secret keys between distant users over an insecure communication channel [1]. Unlike software-based solutions such as the Rivest–Shamir–Adleman (RSA) protocol [2] and post-quantum cryptography [3], QKD promises informational-theoretical security under a well-defined set of assumptions [4]. This means that keys obtained through QKD protocols bear the property of everlasting security; they remain secure against any future development in algorithms, supercomputers, and quantum computers [5]. Most QKD protocols cluster into two categories: discrete-variable (DV) QKD and continuous-variable (CV) QKD, which differ in the degrees of freedom used to encode information. DV protocols, such as the celebrated (Bennett and Brassard, 1984 (BB84)) [6] use discrete degrees of freedom, such as polarisation or time-bin coding and decode information through direct detection [7, 8]. CV QKD protocols instead exploit the continuous amplitude and phase quadratures of the optical field to encode information, and coherent detection, such as homodyne and heterodyne detection, for decoding [9–11].

Both categories of QKD protocols have separate features that lend themselves to different applications [12]. DV protocols are generally more robust to channel losses, which permits their implementation in long-range ($\gtrsim$100 km) quantum communications such as satellite-based networks [13–16]. This has been showcased through recent landmark satellite-based QKD experiments and quantum networking demonstrations [17], with the current state of the art for entanglement distribution being over 1200 km [18]. However, DV protocols rely on high-efficiency photon detectors, which are currently costly and bulky owing to their need for cryogenics [19]. CV QKD protocols find more widespread implementation in terrestrial networks ($\lesssim$100 km) given their compatibility with existing telecommunication infrastructures and tolerance to co-propagation with classical signals [20]. While the feasibility of CV protocols on greater ranges have been explored [21], distances with CV protocols are typically shorter than with DV protocols since security requires very low noise during transmission and detection [22].

With DV and CV protocols offering distinct advantages, a hybrid protocol that merges the salient features of both may offer a promising route to enable longer-range quantum networking. Specifically, this hybrid protocol would operate with low-cost photodiodes at room temperature and improved compatibility with existing telecommunication architectures. Additionally, by benefiting from mature security proofs, hybrid protocols could contribute to advancing the state-of-the-art in networked quantum communications over global scales. Developing such hybrid protocols for QKD has recently gained traction, where information is encoded in discrete variables of light and decoded through coherent detection [23, 24].

The asymptotic key rate, obtained after a large number of transmitted signals, is regularly used as a proxy for upper bounding the performance of QKD protocols and to provide straightforward comparison between protocols. A severe bottleneck is that security proofs require a theoretical model that precisely matches the physical devices used in an implementation. Hybrid protocols additionally inherit technical challenges associated with CV protocols due to an infinite-dimensional Hilbert space. There have been a number of approaches to overcome these challenges to simplify security analyses and the key rate calculations. First, by coarse-graining measurement outcomes from heterodyne detection, the DVs encoded in the input signals can be inferred at the expense of increased noise [23]. Heterodyne detection also enables full reconstruction of the photon number distribution of received signals, which can be exploited to bound the number of bits leaked to the environment [25, 26]. Second, lower bounds have been exploited to reduce the key-rate calculation to a semi-definite program [24], an approach also suitable to encompass decoy states [27–29].

Hybrid QKD has been explored with single photons, employing either polarisation or time bin encoding [23], decoy states [24], and discrete modulation phase-shift keying [30]. In this work, we explore the potential of single-photon-based hybrid QKD for practical implementation and deployment across quantum-secured networks. Specifically, we improve the security analysis within the collective attack framework to establish a tight lower bound on the asymptotic key rate. The tightness of our method enables higher key rates and increased robustness to noise over the previous single-photon based hybrid protocol. We quantify this improvement within an experimentally feasible parameter space, providing insights into the current readiness for implementation. Additionally, we compare the performance of hybrid protocols with DV and CV protocols to discuss their current viability for applications in quantum networking, which remains an open question in the field. Section 1.1 provides an executive summary of our results, with an outline of the paper provided in section 1.2.

1.1. Summary of results

In this work, we provide the first rigorous security proof that yields a tight lower bound on the key rate. We obtain a semi-analytical expression for the asymptotic key rate under collective attacks, where attacks from an eavesdropper on transmitted signals are identical and statistically independent. It is likely that methods developed in the context of DV or CV QKD [30–35] can be adapted and applied to hybrid protocols too.

To explore the performance of hybrid QKD, we outline a general approach to exploit state symmetries to establish invariant states with reduced parameterisation. Note that security proofs against general attacks often introduce a symmetrisation step to endow composite systems with permutation invariance. CV QKD protocols have been shown to additionally exhibit Lie group invariance. The symmetry we appeal to is the invariance of two-party composite states under $(U \otimes U^*)$ transformations, where U belongs to the SU(2) Lie group that physically represents a linear-optics passive (LOP) unitary acting on the two polarisation modes. The resulting invariant states we derive have a significantly reduced parameterisation; one that scales linearly with the Hilbert space dimension, compared with the quadratic scaling of the original composite states. This reduced parameterisation permits efficient numerical calculation of the secret key rate.

Inspired by the numerical approach developed in [36–38], we use our invariant states to construct a constrained key rate optimisation that is closely aligned to an experimental implementation of the protocol. In particular, we constrain the optimisation according to error parameters that can be directly measured, including the gain Q and the quantum bit error rate (QBER). Our work therefore provides a route towards an experimental realisation of the hybrid QKD analysed in this work. Most notably, this procedure allows us to perform an exact numerical optimisation with full control of the error due to finite-dimensional cut-off of the otherwise infinite-dimensional Hilbert space that characterises CV QKD systems.

By exploring the performance of a pure loss channel, we find the asymptotic key rate for our hybrid protocol scale as $O(\eta^2)$, where η is the attenuation factor. Most DV and CV protocols are characterised by a linear scaling $O(\eta)$. The worse scaling of hybrid protocols than DV ones is due to decreasing gain with increasing range, and is the penalty to pay for improved compatibility with terrestrial networks. This work is the first to quantify this tradeoff that would be instrumental in guiding future research into the use of hybrid protocols for quantum networking.

For passive attacks, our theory provides higher rates and can tolerate higher channel losses than what estimated by previous security analyses. When Gaussian noise is introduced the key rate decreases rapidly, highlighting high sensitivity of hybrid protocols to excess noise in the detector; a feature inherited from CV protocols. For an excess noise variance of $N = 10^{-4}$ (in shot-noise units), we demonstrate our hybrid scheme can tolerate losses up to ∼17 dB, making it suitable to deliver high-rate QKD in terrestrial or free-space quantum networks over metropolitan scales. However, the key rates are lower than those achieved with CV protocols. This suggests that the hybrid approach is not always advantageous in terms of robustness to noise.

Before concluding, we note that our hybrid QKD protocol significantly eases implementation over DV and CV protocols. First, in contrast to DV QKD, our hybrid protocol allows for the use of faster receivers and does not require sifting since a single decoding measurement applies to both encoding bases. Second, in contrast to CV QKD, our hybrid protocol does not require a shared local oscillator or a pilot tone. This significantly reduces transmitter and receiver complexity and the potential for side-channel attacks [39, 40]. Combined with a key rate optimiser that is closely aligned to an experimental implementation, our work provides a feasible route towards practical implementation of the protocol.

1.2. Outline of paper

The paper develops as follows. In section 2 we review the protocol introduced in [23] based on independent detection of two polarisation modes. In section 3 we lay the foundation of our security analysis, which is inspired by the work in [36–38]. A first case study is presented in section 4, which explores a pure-loss communication channel. Section 5 extends our approach to most general collective attacks. Here we introduce symmetry in the protocol and exploit it to simplify the security analysis. In section 6 we show how symmetry allows us to control the error introduced by the truncation of the Hilbert space in view of the numerical optimisation. This approach is developed in section 7 to study in detail the case of Gaussian noise. This noise model may be used to describe electronic noise in heterodyne detection. Conclusions and discussions are presented in section 8, where we summarise the motivations for our work and the most important take-home messages. Further details and a number of technical results are reported in the appendix.

2. BB84 with heterodyne detection—independent detection

The subject of our analysis is one of the hybrid protocols introduced by Qi in [23]; one that is based on *independent detection* of the two optical modes used to encode quantum information. To make the presentation more concrete, we assume that these modes represent polarisation, though other degrees of freedom could be equivalently considered.

We first start with a review of the hybrid protocol in the prepare-and-measure (PM) representation. The schematic setup of our protocol is shown in figure 1 and the protocol is as follows:

1. *State preparation.* First, as in BB84, the sender (Alice) encodes one bit of information by preparing a single-photon state with either horizontal (H) or vertical (V) polarisation. Alternatively, Alice may use diagonal (D) or anti-diagonal (A) polarisation. The choice of polarisation basis is random; without loss of generality we assume equal probabilities. For each transmission round, Alice sends her prepared states to Bob through an insecure quantum channel.
2. *Measurement.* The hybrid protocol differs from standard BB84 in the measurement procedure. In standard BB84 the receiver (Bob) applies photon-detection to decode received signals. Instead, we assume coherent decoding by heterodyne detection, which is a CV measurement defined on a single mode of the quantum electromagnetic field [41]. Bob receives two optical modes, characterised by the canonical bosonic annihilation and creation operators $\{b_H, b_H^\dagger\}$ and $\{b_V, b_V^\dagger\}$, which corresponds to H/V polarisation. The canonical operators for the D/A polarisation are obtained from the latter as

$$b_D = (b_H + b_V)/\sqrt{2}, \tag{1}$$

$$b_A = (b_H - b_V)/\sqrt{2}. \tag{2}$$

Bob performs a heterodyne measurement on the state, which is described by a continuous family of positive operator-valued measurement (POVM) elements

$$\Lambda(\beta) = \frac{1}{\pi}|\beta\rangle\langle\beta|, \tag{3}$$

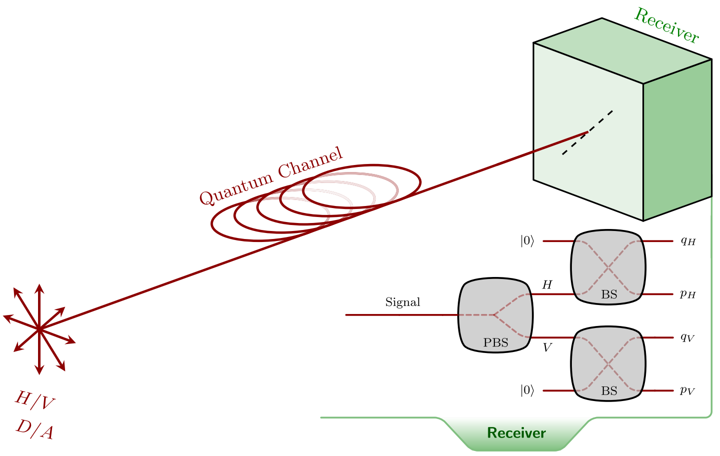

Figure 1. Schematic setup of the protocol: the transmitter (Alice) prepares polarisation states in the rectilinear (H/V) or diagonal (D/A) bases. After the quantum channel, the receiver (Bob) performs a heterodyne measurement on received states. The inset illustrates the receiver in detail: a polarising beam splitter (PBS) sorts the beam according to polarisation, then each beam is measured using heterodyne detection.

where $|\beta\rangle$ is the coherent state of amplitude $\beta = (q + ip)/\sqrt{2}$ of the optical mode being measured. Recall that the coherent states satisfy the completeness relation, from which we obtain

$$\int \mathrm{d}^2\beta \Lambda(\beta) = I, \tag{4}$$

where I is the identity operator and $\mathrm{d}^2\beta := \mathrm{d}q\mathrm{d}p/2$.
Alice and Bob repeat the state preparation and measurement stage m times.

3. *Basis announcement.* Alice announces her choices for the polarisation basis. According to this information Bob will adapt his inference strategy. However, as remarked below, no sifting is necessary.
4. *Inference.* To infer the bit value encoded by Alice, Bob compares the output of mode-wise heterodyne to a given threshold value $\tau > 0$ that is decided before executing the protocol. Consider the operators

$$R_0 = \int_{|\beta|^2 \leqslant \tau} \mathrm{d}^2\beta\, \Lambda(\beta)\,, \tag{5}$$

$$R_1 = \int_{|\beta|^2 > \tau} \mathrm{d}^2\beta\, \Lambda(\beta)\,. \tag{6}$$

Bob then establishes a *key map* through a threshold detection obtained by combining these operators on the two modes. For example, to discriminate between H and V polarisation, we need to combine the above operators applied to each mode of polarisation, denoted as R_0^H, R_1^H and R_0^V, R_1^V. The threshold detection corresponds to the POVM elements

$$M_H = R_1^H \otimes R_0^V\,, \tag{7}$$

$$M_V = R_0^H \otimes R_1^V\,. \tag{8}$$

To obtain a complete set, one also needs to introduce the null operator

$$M_0 = I - M_H - M_V\,, \tag{9}$$

in such a way that $M_H + M_V + M_0 = I$. Successful detection is associated to measurement outcomes M_H (in which case Bob infers a horizontally polarised photon) or M_V (Bob infers vertical polarisation). Events corresponding to the null outcome M_0 are discarded. The analogous construction applied to D/A polarisation leads to the definition of the operator M_D, M_A.

The above describes the quantum part of the QKD protocol. Alice and Bob use the data collected to determine the secret key rate by solving the optimisation problem in equation (32). The protocol is aborted if no secret key can be generated, otherwise, they proceed. The raw keys are finally post-processed for parameter estimation, error correction, and privacy amplification. The post-processing procedures are equivalent to standard BB84.

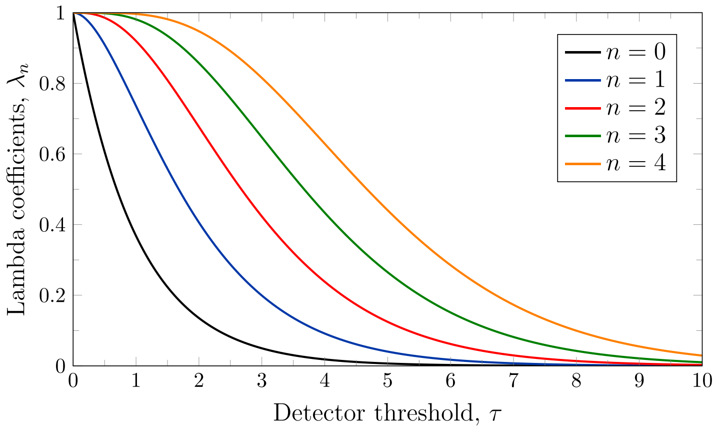

Figure 2. Eigenvalues of R_1 operator: the coefficients λ_n in equation (14) plotted vs the threshold value τ, from bottom to top, $n = 0,1,2,3,4$.

Remark 1. One interesting feature of this hybrid protocol is that Bob only needs to apply heterodyne detection to infer both the H/V and D/A modes of polarisation. This is because from equations (1) and (2) the outcomes β_D, β_A of heterodyne detection in the D/A polarisation modes can be obtained exactly from the outcomes β_H, β_V of heterodyne detection in the H/V modes,

$$\beta_D = (\beta_H + \beta_V)/\sqrt{2}\,, \tag{10}$$

$$\beta_A = (\beta_H - \beta_V)/\sqrt{2}\,. \tag{11}$$

This implies that no data is discarded, in contrast to the sifting phase in standard BB84. The price to pay, as highlighted in [23], is an additional error in the inference compared to direct detection.

We conclude this section by presenting the expansion of the operators R_0, R_1 in the number basis. From the expression of the coherent state, $|\beta\rangle = \mathrm{e}^{-|\beta|^2/2}\sum_{n=0}^{\infty}\beta^n/\sqrt{n!}|n\rangle$, we obtain

$$R_0 = \sum_{n=0}^{\infty}(1-\lambda_n)\,|n\rangle\langle n|\,, \tag{12}$$

$$R_1 = \sum_{n=0}^{\infty}\lambda_n\,|n\rangle\langle n|\,, \tag{13}$$

where

$$\lambda_n := \frac{\Gamma[1+n,\tau]}{n!} \tag{14}$$

and Γ is the incomplete gamma function. Figure 2 shows a plot of these coefficients versus the threshold value τ.

3. Security analysis

The security of our hybrid protocol is better assessed using its equivalent entanglement-based (EB) representation. We emphasise that the EB representation provides a useful mathematical tool but the physical implementation of the protocol in general follows the PM representation.

In the EB representation Alice prepares a pair of photons that are entangled in polarisation,

$$|\phi\rangle_{AA'} = (|H\rangle_A|H\rangle_{A'} + |V\rangle_A|V\rangle_{A'})/\sqrt{2}\,. \tag{15}$$

Alice sends photon A' to Bob and keeps photon A for herself. Alice eventually measures photon A' in either the H/V basis or in the conjugate D/A basis, thus conditionally preparing the other photon in the same state of polarisation.

A noisy communication channel $\mathcal{N}_{A'\to B}$ maps the state $|\phi\rangle_{AA'}$ into

$$\rho_{AB} = I_A \otimes \mathcal{N}_{A'\to B}(|\phi\rangle\langle\phi|)\,, \tag{16}$$

where I_A is the identity channel acting on photon A. In this work, we consider collective attacks, where the eavesdropper applies i.i.d. noise to each signal transmission. Hence, for m photons sent by Alice, the state shared with Bob is simply given by the tensor power $\rho_{AB}^{\otimes m}$. In the limit of $m \to \infty$, the asymptotic secret key rate rate, expressed in secret bits per photon sent can be expressed as [36–38]

$$r(\rho_{AB}) = D[\mathcal{G}(\rho_{AB}) \| \mathcal{Z}(\mathcal{G}(\rho_{AB}))] - \mathrm{leak}_{\mathrm{EC}}, \tag{17}$$

where $D[\rho\|\sigma] = \mathrm{Tr}(\rho\log\rho) - \mathrm{Tr}(\rho\log\sigma)$ is the quantum relative entropy (log denotes the logarithm in base 2, whereas ln is used for natural logarithm), and the maps $\mathcal{G}$ and $\mathcal{Z}$ will be defined below. The relative entropy term quantifies the number of secret bits per photons that can be extracted from the raw key after privacy amplification. The final secret key rate is then determined by subtracting the term $\mathrm{leak}_{\mathrm{EC}}$, which is the number of bits per photon leaked for error correction. Here we assume reverse reconciliation.

The map $\mathcal{G}$ in equation (17), dubbed *key map*, is a partial isometry that gives a coherent representation of the measurement and decoding applied by the receiver. It takes as input a state of the B system and outputs a state of the composite system BB_1, where B_1 is an auxiliary qubit:

$$\mathcal{G}(\rho_{AB}) = (I\otimes K)\rho_{AB}\left(I\otimes K^\dagger\right), \tag{18}$$

where

$$K = |H\rangle_{B_1}\otimes\sqrt{M_H} + |V\rangle_{B_1}\otimes\sqrt{M_V}, \tag{19}$$

with M_H and M_V as in equations (7) and (8). The state $\mathcal{G}(\rho_{AB})$ is in general not normalised. Its trace determines the gain Q such that

$$\begin{aligned} Q = \mathrm{Tr}[\mathcal{G}(\rho_{AB})] &= \mathrm{Tr}\left[\left(I\otimes K^\dagger K\right)\rho_{AB}\right] & (20)\\ &= \mathrm{Tr}[(M_H + M_V)\rho_B]. & (21)\end{aligned}$$

The gain is the probability that Bob obtains a valid measurement output and can be estimated in an experimental implementation of the protocol.

The map $\mathcal{Z}$ in equation (17) applies the *pinching map* to the auxiliary system B_1, inducing complete dephasing in the basis $\{|H\rangle_{B_1}, |V\rangle_{B_1}\}$,

$$\mathcal{Z}(\mathcal{G}(\rho_{AB})) = |H\rangle_{B_1}\langle H|\mathcal{G}(\rho_{AB})|H\rangle_{B_1}\langle H| + |V\rangle_{B_1}\langle V|\mathcal{G}(\rho_{AB})|V\rangle_{B_1}\langle V|. \tag{22}$$

An analogous definition may be introduced for the D/A polarisation modes. However, as in our discussion we will only consider symmetric states, it is sufficient to consider the H/V basis.

The calculation of the relative entropy is simplified using proposition:

Proposition 1. *The relative entropy equals the difference of two entropies:*

$$D[\mathcal{G}(\rho_{AB}) \| \mathcal{Z}(\mathcal{G}(\rho_{AB}))] = S[\mathcal{Z}(\mathcal{G}(\rho_{AB}))] - S[\mathcal{G}(\rho_{AB})], \tag{23}$$

where $S[\sigma] = -\mathrm{Tr}(\sigma\log\sigma)$ *is the von Neumann entropy.*

Proof. Note that equation (22) implies

$$\log[\mathcal{Z}(\mathcal{G}(\rho_{AB}))] = |H\rangle_{B_1}\langle H|\log[\mathcal{Z}(\mathcal{G}(\rho_{AB}))]|H\rangle_{B_1}\langle H| + |V\rangle_{B_1}\langle V|\log[\mathcal{Z}(\mathcal{G}(\rho_{AB}))]|V\rangle_{B_1}\langle V|. \tag{24}$$

Therefore

$$\begin{aligned} &\mathrm{Tr}\{\mathcal{G}(\rho_{AB})\log[\mathcal{Z}(\mathcal{G}(\rho_{AB}))]\} & \\ &= \mathrm{Tr}\{(|H\rangle_{B_1}\langle H|\mathcal{G}(\rho_{AB})|H\rangle_{B_1}\langle H| + |V\rangle_{B_1}\langle V|\mathcal{G}(\rho_{AB})|V\rangle_{B_1}\langle V|)\log[\mathcal{Z}(\mathcal{G}(\rho_{AB}))]\} & (25)\\ &= \mathrm{Tr}\{\mathcal{Z}(\mathcal{G}(\rho_{AB}))\log[\mathcal{Z}(\mathcal{G}(\rho_{AB}))]\}. & (26)\end{aligned}$$

□

To simplify the notation for the rest of the paper, we denote

$$D[\rho_{AB}] := D[\mathcal{G}(\rho_{AB}) \| \mathcal{Z}(\mathcal{G}(\rho_{AB}))]. \tag{27}$$

Besides the gain Q, another parameter that can be estimated experimentally is the QBER E. First consider the quantity

$$c := \frac{1}{2}\mathrm{Tr}\left[\left(|H\rangle\langle H| \otimes M_V + |V\rangle\langle V| \otimes M_H\right)\rho_{AB}\right] . \tag{28}$$

From c and Q we obtain the QBER

$$E = \frac{2c}{Q} = \frac{\mathrm{Tr}\left[\left(|H\rangle\langle H| \otimes M_V + |V\rangle\langle V| \otimes M_H\right)\rho_{AB}\right]}{\mathrm{Tr}\left[\left(M_H + M_V\right)\rho_B\right]} , \tag{29}$$

such that $QE = 2c$. In turn, from the QBER we estimate the error correction term in the key rate,

$$\mathrm{leak}_{\mathrm{EC}} = Qh_2\left(E\right) , \tag{30}$$

where $h_2(x) = -x\log x - (1-x)\log(1-x)$ is the binary Shannon entropy. This expression follows from the model of symmetric binary channel [42].

Finally, we remark that in QKD we do not assume complete knowledge of the state ρ_{AB}, therefore one should consider the worst-case scenario that is compatible with the experimental data. In our setup, the experimental data allows Alice and Bob to estimate the parameters Q and c. Furthermore, as discussed in [25], heterodyne detection allows Bob to estimate the photon-number distribution of the unknown state ρ_{AB},

$$P_j := \sum_{a=0}^{j} \mathrm{Tr}\left[\left(|a\rangle_H\langle a| + |j-a\rangle_V\langle j-a|\right)\rho_B\right] . \tag{31}$$

In conclusion, the asymptotic key rate is obtained by solving the following constrained minimisation problem

$$\min_{\rho_{AB}\in\mathcal{S}} D\left[\rho_{AB}\right] - Qh_2\left(E\right) , \tag{32}$$

given experimental estimates for Q and E, and the set $\mathcal{S}$ of feasible states defined through the following conditions:

1. The reduced state of Alice photon is maximally mixed:

$$\rho_A = \mathrm{Tr}_B\left(\rho_{AB}\right) = I/2 = \frac{|H\rangle\langle H| + |V\rangle\langle V|}{2} . \tag{33}$$

2. The experimentally estimated error parameter c. In full generality, one should distinguish between errors in the H/V basis and those in the D/A basis. Here, for simplicity we assume that they are independent of the polarisation direction. We will use and expand this symmetry assumption below.

$$\begin{aligned} &\mathrm{Tr}\left[\left(|H\rangle\langle H| \otimes M_V\right)\rho_{AB}\right] = \mathrm{Tr}\left[\left(|V\rangle\langle V| \otimes M_H\right)\rho_{AB}\right] \\ &= \mathrm{Tr}\left[\left(|D\rangle\langle D| \otimes M_A\right)\rho_{AB}\right] = \mathrm{Tr}\left[\left(|A\rangle\langle A| \otimes M_D\right)\rho_{AB}\right] \\ &= c . \end{aligned} \tag{34}$$

3. The experimental estimated gain Q. As for c, we should make a distinction between the two polarisation bases. For simplicity we assume equal value for both.

$$\mathrm{Tr}\left[\left(M_H + M_V\right)\rho_B\right] = \mathrm{Tr}\left[\left(M_D + M_A\right)\rho_B\right] = Q . \tag{35}$$

4. The experimental estimates P_j for the photon number distribution, up to a certain photon number k. For $j = 0, \ldots, k$:

$$\sum_{a=0}^{j} \mathrm{Tr}\left[\left(|a\rangle_H\langle a| + |j-a\rangle_V\langle j-a|\right)\rho_B\right] = P_j . \tag{36}$$

Note the final three constraints originate from experimental informed parameters, providing a route to physical implementation of the protocol. In addition, the asymptotic key rate in equation (32) can be further maximised by optimising over the detector threshold $\tau > 0$.

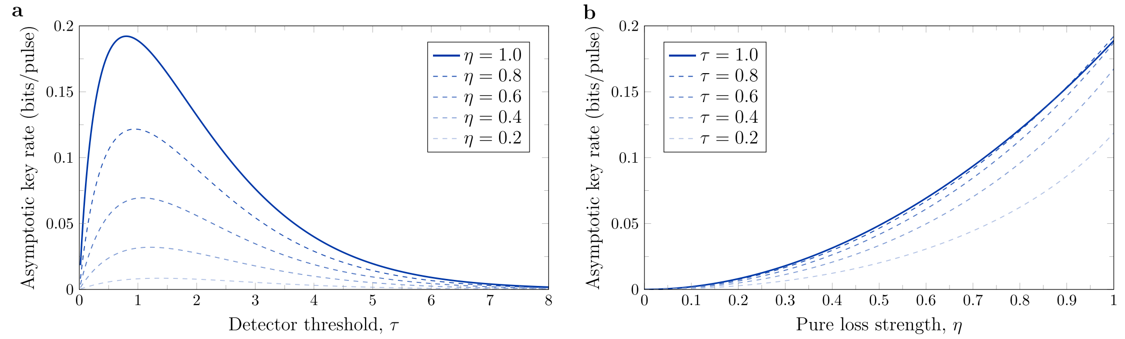

Figure 3. Asymptotic key rate for pure loss: (a) asymptotic rate as a function of the detector threshold τ for independent detection scheme, computed from equation (42). Solid line corresponds to lossless transmission, dashed to loss case with strength η, from bottom to top $\eta = 0.2, 0.4, 0.6, 0.8$. The optimal values for the detector threshold depend on the noise: For transmissivity $\eta = 1$, $\tau_{\text{opt}} = 0.8012$, $\eta = 0.8$, $\tau_{\text{opt}} = 0.9458$, $\eta = 0.6$, $\tau_{\text{opt}} = 1.0779$, $\eta = 0.4$, $\tau_{\text{opt}} = 1.2159$, and $\eta = 0.2$, $\tau_{\text{opt}} = 1.3768$. (b) Asymptotic rate as a function of the pure loss strength η, computed for different values of τ.

4. Pure-loss channel

As a first example, here we determine the asymptotic secret key rate for a pure-loss channel. The communication channel $\mathcal{N}$ is a wiretap channel that induces polarisation-independent loss with transmissivity factor $\eta \in [0,1]$. In the Heisenberg picture, the canonical operators are transformed as follows

$$b_H \to \sqrt{\eta}\, b_H + \sqrt{1-\eta}\, e_H \,, \tag{37}$$

$$b_V \to \sqrt{\eta}\, b_V + \sqrt{1-\eta}\, e_V \,, \tag{38}$$

where e_H, e_V are auxiliary vacuum modes.

In the Schrödinger picture, the input state (15) is transformed according to equation (16) into

$$\rho_{AB} = \eta |\phi\rangle_{AB}\langle\phi| + \frac{(1-\eta)}{2} I_A \otimes |0\rangle_B\langle 0| \,. \tag{39}$$

where $|0\rangle_B$ is the vacuum state on Bob's side. From this expression we compute

$$D[\rho_{AB}] = 2(1-\eta)(1-\lambda_0)\lambda_0 + \eta(\lambda_0 + \lambda_1 - 2\lambda_0\lambda_1) \,, \tag{40}$$

$$c = \frac{\lambda_0}{2}\left[1 - (1-\eta)\lambda_0 - \eta\lambda_1\right] . \tag{41}$$

As expected for a pure-loss channel, all qubits that reach to Bob are secure, therefore we also obtain $Q = D[\rho_{AB}]$.

Finally, the asymptotic secret key rate is obtained using equations (17) and (30):

$$r = Q(1 - h_2(E)) \,, \tag{42}$$

with

$$E = \frac{2c}{Q} = \frac{\lambda_0\left[1 - (1-\eta)\lambda_0 - \eta\lambda_1\right]}{2(1-\eta)\lambda_0(1-\lambda_0) + \eta(\lambda_0 + \lambda_1 - 2\lambda_0\lambda_1)} \,. \tag{43}$$

The key rate is illustrated in figure 3(a) as a function of the threshold value τ for various transmissivity η. Note that the optimal detector threshold has a weak dependency on η. These optimal values are summarised in the caption to figure 3. In figure 3(b) we illustrate the dependence of the key rate on η, taking different values for τ.

It is interesting to investigate the limit of large communication distance, i.e. when $\eta \ll 1$. We obtain

$$r \simeq \frac{\eta^2(\lambda_0 - \lambda_1)^2}{4\lambda_0(1-\lambda_0)\ln 2} = \frac{\eta^2\tau^2}{(e^\tau - 1)\ln 16} \,. \tag{44}$$

This shows that the key rate is of order $O(\eta^2)$. The ultimate repeaterless Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound scales as $O(\eta)$ [43]. The same $O(\eta)$ scaling is commonly achieved by both DV and CV protocols. The sub-optimal scaling of the hybrid protocol is attributed to a decrease in the rate as the distance increases, which is driven by two independent mechanisms. First, it becomes increasingly unlikely that Bob receives transmitted photons, leading to a decrease in the gain Q. Second, the QBER E increases with the distance even for a pure-loss channel. Use of hybrid protocols must therefore address the tradeoff between sub-optimal scaling and increased compatibility. Finally, from equation (44) we obtain that in the limit of long distance the optimal threshold value is $\tau \simeq 1.59$.

5. General collective attacks: exploiting symmetry

To assess the security of the hybrid protocol beyond the pure-loss channel, we must address two challenges:

1. The Hilbert space associated with the receiver is infinite-dimensional. To implement the optimisation in equation (32) numerically, a cutoff into a finite-dimensional subspace is required, together with a method to control the cutoff error introduced.
2. For a Hilbert space cutoff of up to k photons on Bob side, the joint state ρ_{AB} would lives in a space of dimensions $(k+1)(k+2)$ [44]. This quadratic scaling with k presents a bottleneck for efficient numerical optimisation.

Here we solve both issues by exploiting symmetry. Symmetry allows us to reduce the number of free parameters from quadratic to linear in the cutoff photon number k, also providing a way to control the error introduced by the Hilbert-space truncation.

The symmetry group is of the form $U\otimes U^*$, where the unitary U is applied on Alice's system, and U^* on Bob's. Here U denotes a LOP unitary [45] acting on the two polarisation modes, and U^* is its complex-conjugate. Note that the Bell state in equation (15) is invariant under $U\otimes U^*$ transformations.

LOP unitaries are defined as unitary transformations that, in the Heisenberg picture, act linearly on the canonical bosonic operators, without mixing the creation and the annihilation operators. Consider for example Alice's system, which is associated to the bosonic operators $\{a_H, a_H^\dagger\}$, $\{a_V, a_V^\dagger\}$ for horizontal and vertical polarisation respectively. A LOP unitary transforms the operators as follows

$$a_H \to U a_H U^\dagger = \alpha\, a_H + \beta\, a_V\,, \tag{45}$$

$$a_V \to U a_V U^\dagger = -\beta^*\, a_H + \alpha^*\, a_V\,, \tag{46}$$

where α, β are complex number such that $|\alpha|^2 + |\beta^2| = 1$. On Bob side, the application of U^* yields

$$b_H \to U^* b_H (U^*)^\dagger = \alpha^*\, b_H + \beta^*\, b_V\,, \tag{47}$$

$$b_V \to U^* b_V (U^*)^\dagger = -\beta\, b_H + \alpha\, b_V\,. \tag{48}$$

We remark that LOP unitaries preserve the total photon number, i.e.

$$U\left(a_H^\dagger a_H + a_V^\dagger a_V\right) U^\dagger = a_H^\dagger a_H + a_V^\dagger a_V\,, \tag{49}$$

$$U^*\left(b_H^\dagger b_H + b_V^\dagger b_V\right) U^\intercal = b_H^\dagger b_H + b_V^\dagger b_V\,. \tag{50}$$

This implies that states that are invariant under the action of the symmetry group $U\otimes U^*$ are block-diagonal in the total photon number both on Alice and on Bob side.

Note that in our protocol there is only one photon on Alice side, whereas for a generic attack there could be an arbitrary distribution of photon number on Bob side. This leads to the following form for a state that is invariant under the symmetry group:

$$\rho_{AB}^{(\mathrm{inv})} = \sum_{j=0}^{\infty} P_j \rho_{1:j}^{(\mathrm{inv})}\,, \tag{51}$$

where $\rho_{1:j}^{(\mathrm{inv})}$ is an invariant state with one photon on Alice side and j photons on Bob side, and P_j is the probability of having j photons on Bob side.

In appendix A we derive explicit expressions for the invariant states $\rho_{1:j}^{(\mathrm{inv})}$. We show that for each $j>0$ there exists a one-parameter family of invariant states, $\rho_{1:j}^{(\mathrm{inv})}(f_j)$, with $f_j \in [0,1]$, whereas for $j=0$ the invariant state is unique. Note that for any $j \neq j'$ the states $\mathcal{G}(\rho_{1:j}^{(\mathrm{inv})})$ and $\mathcal{G}(\rho_{1:j'}^{(\mathrm{inv})})$ have orthogonal support, as well as $\mathcal{Z}(\mathcal{G}(\rho_{1:j}^{(\mathrm{inv})}))$ and $\mathcal{Z}(\mathcal{G}(\rho_{1:j'}^{(\mathrm{inv})}))$. This implies that the relative entropy in equation (17) reads

$$D\left[\rho_{AB}^{(\mathrm{inv})}\right]=P_0 D\left[\rho_{1:0}^{(\mathrm{inv})}\right]+\sum_{j=1}^{\infty}P_j D\left[\rho_{1:j}^{(\mathrm{inv})}\left(f_j\right)\right]. \tag{52}$$

For each j we can define the corresponding parameter $c_j(f_j)$. By linearity, we have

$$c=P_0 c_0+\sum_{j=1}^{\infty}P_j c_j\left(f_j\right). \tag{53}$$

An analogous decomposition holds for the gain Q, i.e.

$$Q=\sum_{j=0}^{\infty}Q_j\,, \tag{54}$$

where Q_j is the gain subject to Bob receiving exactly j photons. Following [23], for each j we write

$$Q_j=P_j Y_j\,, \tag{55}$$

where Y_j is the yield for given j. The feasible range and expressions for Y_j, c_j are computed explicitly in appendices B and C, where we also note that Y_j does not depend on f_j. By combining these parameters we obtain the QBER conditioned on Bob receiving j photons,

$$E_j=\frac{2c_j}{Y_j}\,, \tag{56}$$

such that

$$E=\frac{\sum_j Q_j E_j}{Q}. \tag{57}$$

5.1. A modified protocol

Symmetry is commonly exploited to assess the security of QKD protocols. Examples are found in the literature for both DV [46–49] and CV [31, 32, 50–52] systems.

To justify our use of the $U\otimes U^*$ symmetry, we introduce a modified protocol that includes an *active symmetrisation* step. First we note that the hybrid BB84 protocol requires Alice and Bob to share a reference frame in order to agree on the orientation of the H/V and D/A polarisation states. In the original protocol it is implicitly assumed that this reference frame is fixed. To make the protocol explicitly invariant under $U\otimes U^*$ symmetry we need to modify it in such a way that Alice and Bob randomly change the shared reference frame at each photon transmission. In the EB representation, this invariance is equivalent to applying a random local LOP transformation of the form $U\otimes U^*$, mapping any joint state ρ_{AB} into an invariant state,

$$\rho_{AB}\to\rho_{AB}^{(\mathrm{inv})}=\int \mathrm{d}\mu_U\,(U\otimes U^*)\,\rho_{AB}\,(U\otimes U^*)^{\dagger}\,, \tag{58}$$

where $\mathrm{d}\mu_U$ is the Haar measure on the group.

Remark 2. It was proven in [49] (see also [32]) that if a QKD protocol is invariant under a symmetry group, then one can assume without loss of generality that the state shared by Alice and Bob in the EB representation of the protocol is also invariant under the very same symmetry group. By applying this result in our setup to the modified protocol, we can restrict the minimisation of the relative entropy in equation (32) to states that are invariant under transformations of the form $U\otimes U^*$. This restriction comes with no loss of generality because the modified protocol is indeed invariant under $U\otimes U^*$ transformations. The advantage we gain in doing this is that the invariant states are block-diagonal in the number basis and can be decomposed as in equation (51).

Note that in fact only Alice needs to physically apply the unitary U. For Bob it is sufficient to always apply the same measurements and simply modify the inference strategy according to the unitary U (and to the basis choice communicated by Alice). It may be possible to prove that invariant states are optimal even without introducing the active symmetrisation on Alice side, in a way similar to [51]. However, we do not address this question here leaving it to future work.

5.2. Passive attacks

In this section, we apply our modified protocol to passive attacks, where the eavesdropper does not add photons into the channel. This limits the minimisation of the relative entropy to the vacuum and the sector of the Hilbert space with one photon:

$$\rho_{AB}^{(\mathrm{inv})} = (1-\eta)\,\rho_{1:0}^{(\mathrm{inv})} + \eta\rho_{1:1}^{(\mathrm{inv})}(f_1)\,, \tag{59}$$

where η is the channel transmissivity. The explicit form of the states $\rho_{1:j}^{(\mathrm{inv})}$ and of the parameters Y_j, $c_{1:j}$ are presented in appendix C. We obtain

$$Q = 2(1-\eta)\,\lambda_0(1-\lambda_0) + \eta(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\,. \tag{60}$$

This sets the range of feasibility for the gain,

$$Q \in [Q_{\mathrm{min}}, Q_{\mathrm{max}}]\,, \tag{61}$$

with

$$Q_{\mathrm{min}} = \min\{2\lambda_0(1-\lambda_0), \lambda_0+\lambda_1-2\lambda_0\lambda_1\}\,, \tag{62}$$

$$Q_{\mathrm{max}} = \max\{2\lambda_0(1-\lambda_0), \lambda_0+\lambda_1-2\lambda_0\lambda_1\}\,. \tag{63}$$

In an experimental implementation, Q can be estimated from the data, from which one in turn determines η,

$$\eta = \frac{Q-2\lambda_0(1-\lambda_0)}{(1-2\lambda_0)(\lambda_1-\lambda_0)} \tag{64}$$

Similarly, the parameters c reads

$$c = (1-\eta)\frac{1}{2}\lambda_0(1-\lambda_0) + \eta\left(\frac{2f+1}{6}(1-\lambda_1)\lambda_0 + \frac{1-f}{3}(1-\lambda_0)\lambda_1\right)\,. \tag{65}$$

Given η, the range of c is given by

$$c \in [c_{\mathrm{min}}, c_{\mathrm{max}}]\,, \tag{66}$$

with

$$c_{\mathrm{min}} = (1-\eta)\frac{\lambda_0(1-\lambda_0)}{2} + \eta\frac{\lambda_0(1-\lambda_1)}{2}\,, \tag{67}$$

$$c_{\mathrm{max}} = (1-\eta)\frac{\lambda_0(1-\lambda_0)}{2} + \eta\left(\frac{\lambda_0(1-\lambda_1)}{6} + \frac{\lambda_1(1-\lambda_0)}{3}\right)\,. \tag{68}$$

The feasible region for key rates compatible with our protocol is illustrated (for different values of the threshold τ) by the shaded regions in the Q-c plane in figure 4.

Note that the error parameter c can be estimated from the experimental data, which in turn determines the parameter f_1 uniquely,

$$f_1 = \frac{3(1-\eta)\lambda_0(1-\lambda_0)}{2\eta(\lambda_1-\lambda_0)} + \frac{\lambda_0+2\lambda_1-3\lambda_0\lambda_1}{2(\lambda_1-\lambda_0)} - \frac{3c}{\eta(\lambda_1-\lambda_0)}\,. \tag{69}$$

In conclusion, the experimental estimates of c and Q completely determine the state with no minimisation required to compute the key rate. It remains to compute the relative entropy and hence the rate for given values of these two parameters. The asymptotic rate can then be written as

$$r = (1-\eta)D\left[\rho_{1:0}^{(\mathrm{inv})}\right] + \eta D\left[\rho_{1:1}^{(\mathrm{inv})}(f_1)\right] - Qh_2(E)\,, \tag{70}$$

with $E = 2c/Q$. By using the above expressions for η and f_1, the key rate is entirely determined by the experimental estimates of Q and c. In figure 4, the blue line at the bottom boundary corresponds to the pure-loss channel, in which case the key rate reduces to equation (42).

Our results can be directly compared with those of Qi in [23]. We first need to recall that Qi introduced a model of virtual detectors to provide an upper bound on the key rate as a function of the detector

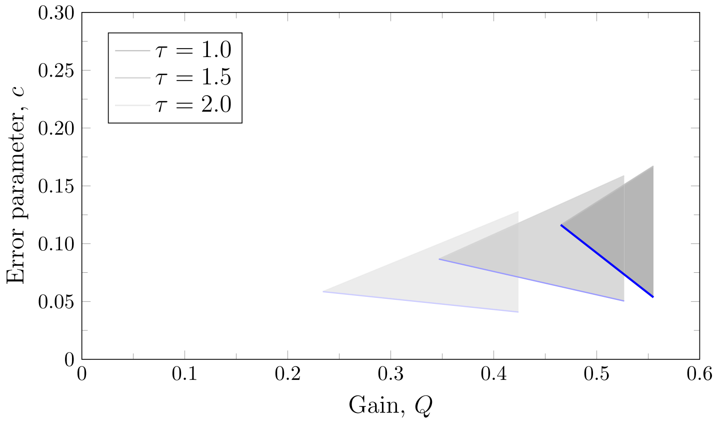

Figure 4. Feasible key rate region: the shaded regions illustrates feasible values for Q and c that are compatible with our model with up to one photon on Bob side for different detector threshold values τ. The feasible region for $\tau = 1$ is illustrated in darkest gray. Lighter shades of gray are for $\tau = 1.5$ and $\tau = 2.0$. The blue lines on the bottom boundaries correspond to passive attacks (for varying values of the loss factor η), in which case the key rate reduces to equation (42).

misalignment, quantified by the parameter E_d. Leveraging this virtual detection model, the QBER corresponding to Bob detecting a single-photon is [23]

$$E_1^{\mathrm{Qi}} = \frac{(E_d\tau + 1)\,\mathrm{e}^{-\tau} - (\tau + 1)\,\mathrm{e}^{-2\tau}}{(\tau + 2)\,e^{-\tau} - 2(\tau + 1)\,e^{-2\tau}}. \tag{71}$$

The key rate in [23] can then be written using our notation,

$$r_{\mathrm{Qi}} = Q_0 + Q_1(1 - h_2(E_d)) - Qh_2(E), \tag{72}$$

with

$$Q_0 = 2(1-\eta)\lambda_0(1-\lambda_0), \tag{73}$$
$$Q_1 = \eta(\lambda_0 + \lambda_1 - 2\lambda_0\lambda_1), \tag{74}$$
$$Q = Q_0 + Q_1, \tag{75}$$
$$E = \frac{Q_0E_0 + Q_1E_1^{\mathrm{Qi}}}{Q} = \frac{Q_0/2 + Q_1E_1^{\mathrm{Qi}}}{Q}. \tag{76}$$

Now, to compare the key rate in equation (72) with our formalism in equation (70), we determine an expression for f_1 using our expression for the QBER conditioned on Bob receiving a single photon

$$E_1 = \frac{2c_1}{Y_1} = \frac{1}{3}\frac{\lambda_0 + 2\lambda_1 - 3\lambda_0\lambda_1 - 2f_1(\lambda_1 - \lambda_0)}{\lambda_0 + \lambda_1 - 2\lambda_0\lambda_1}. \tag{77}$$

By equating this to E_1^{Qi}, we find

$$f_1 = 1 - \frac{3E_d}{2}, \tag{78}$$

which is independent of the detector threshold, τ. Note that for $E_d = 0$ we obtain $f_1 = 1$ and our key rate recovers the rate for passive attacks and matches the result of Qi. For non-zero E_d, figure 5 illustrates a comparison of the rates achieved with our formalism with [23]. Our theory provides higher rates and can tolerate higher channel losses.

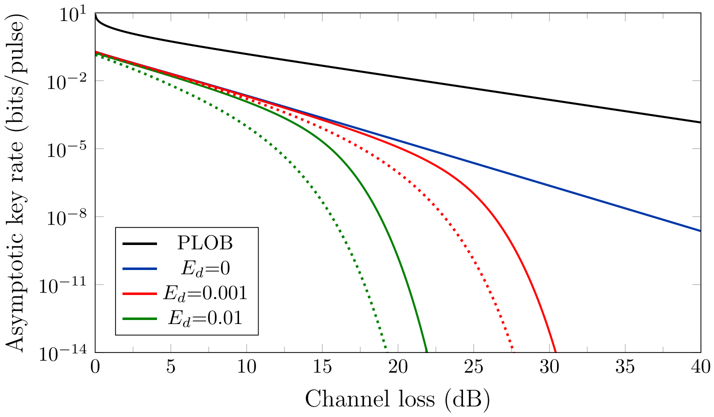

Figure 5. Protocol comparison: comparison of asymptotic rates (bits/pulse) vs loss (dB) according to our theory (solid lines) and to the theory of Qi [23] (dotted lines), for different values of the error probability, E_d. The black line on the top of the figure corresponds to the PLOB repeaterless bound [43].

6. Controlled minimisation of the relative entropy

In general, there is no guarantee that the state obtained by Bob involves only one photon or even a bounded number of photons. However, Bob can estimate the photon number distribution using the output of heterodyne detection [25]. In practice, only a few parameters P_j in the expansion (51) will be realistically estimated with a reasonable small error, say from $j = 0$ up to $j = k$. The limited information on the parameters P_j is still useful to obtain a lower bound on the relative entropy. In fact from equation (52) we obtain

$$D\left[\rho_{AB}^{(\mathrm{inv})}\right] \geqslant P_0 D\left[\rho_{1:0}^{(\mathrm{inv})}\right] + \sum_{j=1}^{k} P_j D\left[\rho_{1:j}^{(\mathrm{inv})}\left(f_j\right)\right] . \tag{79}$$

Since Alice and Bob can estimate the parameters Q, c, and P_j for j between 0 and k from their experimental data, a lower bound on the relative entropy is obtained by solving the constrained minimisation:

$$D\left[\rho_{AB}^{(\mathrm{inv})}\right] \geqslant P_0 D\left[\rho_{1:0}^{(\mathrm{inv})}\right] + \min_{f_1,\ldots,f_k} \sum_{j=1}^{k} P_j D\left[\rho_{1:j}^{(\mathrm{inv})}\left(f_j\right)\right] , \tag{80}$$

where the minimisation is subject to the constraint

$$P_0 c_0 + \sum_{j=1}^{k} P_j c_j\left(f_j\right) \leqslant c . \tag{81}$$

Since we expect the relative entropy to decrease monotonically with increasing c, we may replace this inequality with an equality. Note that the optimisation in equation (80) is over k parameters $f_j \in [0,1]$, for $j = 1,\ldots,k$. Therefore, the complexity of the optimisation is reduced from quadratic to linear in the photon number cutoff.

Alternatively, one can use the estimated QBER in the constrained minimisation instead of the parameter c, yielding

$$2\,\frac{P_0 c_0 + \sum_{j=1}^{k} P_j c_j\left(f_j\right)}{Q_{(k)}} \leqslant E , \tag{82}$$

where $Q_{(k)}$ is an upper bound for Q. As shown in appendix B, a suitable upper bound is

$$Q_{(k)} = \sum_{j=0}^{k} P_j Y_j + \left(1 - \sum_{j=0}^{k} P_j\right) Y_{k+1} . \tag{83}$$

7. Application: assessing the robustness to electronic noise

We apply our theory to assess the robustness of the hybrid protocol against electronic noise in heterodyne detection. Electronic noise is one of the most significant challenges for QKD protocols based on coherent detection. We model the electronic noise as Gaussian noise with zero mean and variance N, with the following representation as a quantum channel acting on each mode of the field:

$$\rho \to \int \frac{d^2\alpha}{\pi N} e^{-|\alpha|^2/N} \mathcal{D}(\alpha) \rho \mathcal{D}(\alpha)^\dagger , \tag{84}$$

where $\mathcal{D}(\alpha)$ is the displacement operator. Note that when applied to the two modes received by Bob, this map preserves the $U \otimes U^*$ symmetry.

Overall, we model the communication channel from Alice to Bob as a Gaussian channel obtained by first applying a pure-loss channel of transmissivity η, followed by mode-wise application of the channel in equation (84). In the Heisenberg picture, this is described by the map

$$b_H \to \sqrt{\eta}\, b_H + \sqrt{1-\eta}\, e_H + z , \tag{85}$$

$$b_V \to \sqrt{\eta}\, b_V + \sqrt{1-\eta}\, e_V + z^* , \tag{86}$$

where z is a circularly symmetric, complex-valued Gaussian random variable with zero mean and variance N.

Using the expansion of the displacement operator in the number bases [53] (for $m \geqslant n$)

$$\langle m|\mathcal{D}(\alpha)|n\rangle = \sqrt{\frac{n!}{m!}}\, \alpha^{m-n} e^{-|\alpha|^2/2} L_n^{(m-n)}\left(|\alpha|^2\right) , \tag{87}$$

where $L_n^{(m-n)}$ denotes the Laguerre polynomials, we are able to compute the invariant states. We truncate the Hilbert space to three photons on Bob side. By repeated applications of equation (87) we obtain (details in appendix D)

$$\rho_{AB}^{(\mathrm{inv})} = P_0 \rho_{1:0}^{(\mathrm{inv})} + \sum_{j=1}^{3} P_j \rho_{1:j}^{(\mathrm{inv})}\left(f_j\right) , \tag{88}$$

with

$$f_1 = \frac{2\eta + N^2 - \eta N + N}{2\left(\eta + 2N^2 - 2\eta N + 2N\right)} , \tag{89}$$

$$f_2 = \frac{3\eta + N^2 - \eta N + N}{3\left(\eta + N^2 - \eta N + N\right)} , \tag{90}$$

$$f_3 = \frac{3\left(4\eta + N^2 - \eta N + N\right)}{4\left(3\eta + 2N^2 - 2\eta N + 2N\right)} , \tag{91}$$

and P_0, P_1, P_2, P_3 are given by the formula

$$\begin{aligned} P_j = {} & \frac{\eta}{N+1} \sum_{m=0}^{j} p_m \left(\frac{N}{N+1}\right)^{j-m} \\ & + (j+1) \frac{1-\eta}{(N+1)^2} \left(\frac{N}{N+1}\right)^{j} \end{aligned} \tag{92}$$

where

$$p_m := \begin{cases} \frac{N}{(N+1)^2} & \text{if} \quad m = 0 \\ \frac{1}{N+1}\left(\frac{N}{N+1}\right)^m \frac{m+N^2}{N(N+1)} & \text{if} \quad m \geqslant 1 \end{cases} \tag{93}$$

From this we obtain a lower bound on the relative entropy:

$$D\left[\rho_{AB}^{(\mathrm{inv})}\right] \geqslant P_0 D\left[\rho_{1:0}^{(\mathrm{inv})}\right] + \sum_{j=1}^{3} P_j D\left[\rho_{1:j}^{(\mathrm{inv})}\left(f_j\right)\right] . \tag{94}$$

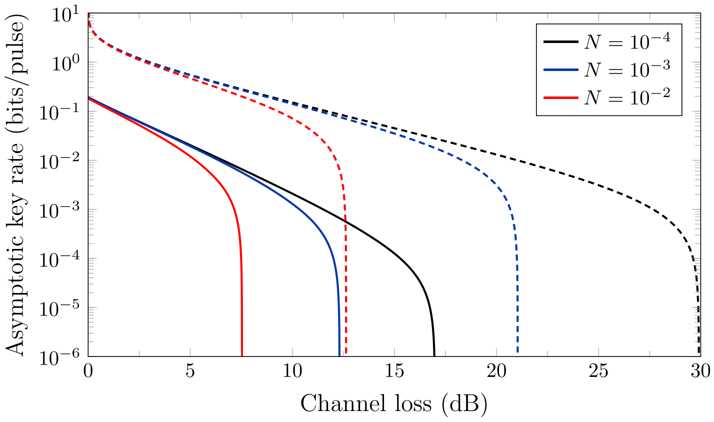

Figure 6. Comparison of asymptotic key rates as a function of loss (dB) for different excess noise variance N. Solid lines: our lower bound for the hybrid protocol, computed using equation (97) after optimisation of the threshold value τ. Dashed lines: upper bound for continuous-modulation CV QKD, obtained from the reverse coherent information in equation (98).

Note that the function $Qh_2[2c/Q]$ is monotonically increasing with both Q and c. Therefore, an upper bound on the error correction leak is obtained from upper bounds on Q and c (these upper bounds are needed only for our numerical simulation; in any experimental implementation the values of Q and c can be directly estimated from the data).

As discussed in appendix B, suitable upper bounds are

$$Q_{(3)} = \sum_{j=0}^{3} P_j Y_j + \left(1 - \sum_{j=0}^{3} P_j\right) Y_4 \,, \tag{95}$$

$$c_{(3)} = P_0 c_0 + \sum_{j=1}^{3} P_j c_j \left(f_j\right) + \left(1 - \sum_{j=0}^{3} P_j\right) \frac{1-\lambda_0}{2} \,. \tag{96}$$

In conclusion, we obtain the following lower bound on the asymptotic key rate:

$$r \geqslant P_0 D\left[\rho_{1:0}^{(\mathrm{inv})}\right] + \sum_{j=1}^{3} P_j D\left[\rho_{1:j}^{(\mathrm{inv})}\left(f_j\right)\right] - Q_{(3)} h_2\left[\frac{2c_{(3)}}{Q_{(3)}}\right] \,, \tag{97}$$

this rate is expected to be tight if the variance N of the Gaussian noise is not too large, which in turn implies a small value for the probability $(1 - \sum_{j=0}^{3} P_j)$.

The key rate is illustrated in figure 6. The hybrid protocol is sensitive to excess noise in the detector with $N = 10^{-6}$ closely approximating the ideal scenario of no electronic noise. Suppression of excess noise down to the 10^{-4} regime in CV-QKD is possible through carrier frequency switching [54]. In figure 6 we compare the performance of our hybrid protocol with CV QKD. Following [55], an upper bound on the key rate achievable in CV QKD with heterodyne detection and reverse reconciliation is given by the *reverse coherent information*,

$$r_{\mathrm{CV}} \leqslant \log\left(\frac{1}{1-\eta}\right) - g(N) \,, \tag{98}$$

where $g(N) := (N+1)\log(N+1) - N\log N$. Note that for an excess noise of $N = 10^{-4}$, our scheme can tolerate losses up to ∼17 dB, corresponding to an optical fibre transmission of 85 km. The protocol can therefore deliver high-rate QKD in terrestrial or free-space quantum networks over metropolitan scales.

8. Conclusions

Security proofs in quantum cryptography are often limited to a specific protocol and generally require a theoretical model that precisely matches the physical devices used in their implementation. Closing the disparity between theory and implementation of DV and CV QKD has therefore been the subject of significant effort [24, 51, 56]. Recent numerical approaches have provided easier implementation by enabling reliable calculation of key rates that are robust to both device imperfections and changes in protocol structure [36–38]. An alternative research direction that offers a promising route towards implementation is the development of hybrid QKD protocols that strive to assimilate the best features of both DV and CV protocols [23, 24]. Most notable of these features is better range performance and mature security proofs inherited from DV protocols and the scalability and compatibility with existing telecommunication infrastructures inherited from CV protocols due to the use of coherent detection.

We explore the security of hybrid BB84 with heterodyne detection proposed by Qi in [23], where information is encoded is in discrete variables (e.g. polarisation), and decoding is by heterodyne detection. This variant offers two additional advantages. First, in contrast to DV QKD, it does not require sifting, as a single decoding measurement applies to both encoding bases. Second, in contrast to CV QKD, it does not require a shared local oscillator. However, this proposal requires a shared reference frame (though a reference-frame free version could be envisaged along the lines of [57]). One outstanding challenge for implementation is that our scheme requires multiple low-noise homodyne detectors.

Compared to the protocol of Qi, we add a symmetrisation step to make the protocol invariant under local LOP transformations of the form $U \otimes U^*$, such that Alice and Bob can randomly change the reference frame at each photon transmission. By exploiting symmetry, our modified protocol takes advantage of invariant states that are block-diagonal in the number basis with reduced complexity. Our modified protocol therefore offers several advantages over previous protocols. First, it enables a simplified security analysis. Second, our use of symmetry allows for semi-analytical expressions for the asymptotic key rate under collective attacks. Finally, it enables an efficient numerical procedure to optimise the secret key rate with quadratic speedup. In particular, we are able to perform an exact numerical optimisation with full control of the error due to finite-dimensional cut-off of the otherwise infinite-dimensional Hilbert space typical of CV QKD protocols.

We apply our theory to a few examples of quantum channels connecting Alice to Bob, including linear loss, passive attacks, and Gaussian noise. Our analysis sheds light on the salient features of hybrid QKD: (1) the study of linear loss shows that the key rate scale as $O(\eta^2)$, where η is the attenuation factor, instead of the linear scaling that characterises most DV and CV protocols; (2) when Gaussian noise is introduced the key rate decreases rapidly, even when compared with CV protocols, this suggests that the hybrid approach is not necessarily advantageous in terms of robustness to noise.

Returning to the original motivation of improving the implementation of QKD protocols, our work achieves this by introducing a symmetrised hybrid QKD protocol. Our results pave the way for a number of interesting research questions that may further improve the performance of hybrid protocols. First, our theory can be directly extended to include decoy states. Second, it may be possible to prove that invariant states are optimal without introducing active symmetrisation. Third, it would be interesting to introduced post-selection in the protocol, which may increase the achievable distance, and to explore the *differential detection mode* of [23]. Finally, our approach may be extended to reference-frame-independent QKD [57], hence removing the need of maintaining a shared reference frame and paving the way to satellite-based applications. In a broader context, our framework to establish invariant states provides a general utility that can be applied to other use cases, such as semi-device-independent communication protocols.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

JSS acknowledges the support of the UKNQTP and the Quantum Technology Hub in Quantum Communications (EPSRC Grant EP/T001011/1). This work has received funding from the: European Union's Horizon Europe research and innovation programme under the Project 'Quantum Secure Networks Partnership' (QSNP, Grant Agreement No. 101114043); European Union's Next Generation EU: PNRR MUR Project PE0000023-NQSTI; INFN through the Project 'QUANTUM'. We warmly thank Marco Lucamarini for inspiring discussions.

Appendix A. $(U \otimes U^*)$-invariant states

Suppose that both Alice's and Bob's Hilbert spaces are endowed with SU(2) representations. For $U \in \mathrm{SU}(2)$, Alice's space transforms under U, and Bob's space under U^*. *Are there any states of the composite system that are left invariant by these transformations?* If yes, *what is their most general form?* We will informally refer to such states as $(U \otimes U^*)$-invariant. The purpose of this appendix is to answer some variations on the theme of the previous questions.

A.1. Preliminaries

In this section we will recall some basic notions, allowing us to give meaning to the problem in different contexts, and study it in the framework of the representation theory of SU(2).

Addition of two spin angular momenta—Let $\boldsymbol{J}_\alpha$ $(\alpha = A, B)$ be a spin-j_α angular momentum, with basis $|j_\alpha, m_\alpha\rangle_\alpha$, generating a unitary irreducible representation $\mathscr{D}_\alpha$ of SU(2). The addition of the two angular momenta, denoted by $\boldsymbol{J}_A + \boldsymbol{J}_B$, is an angular momentum, generating the $j_A \times j_B$ representation $\mathscr{D}_A \otimes \mathscr{D}_B \colon U \mapsto \mathscr{D}_A(U) \otimes \mathscr{D}_B(U)$, which is unitary and (completely) reducible.

The irreducible invariant subspaces—i.e. invariant subspaces with no invariant proper subspace; any invariant subspace is a direct sum of irreducible ones—of $\boldsymbol{J}_A + \boldsymbol{J}_B$, or, which is the same, of $\mathscr{D}_A \otimes \mathscr{D}_B$, are precisely the eigenspaces of $(\boldsymbol{J}_A + \boldsymbol{J}_B)^2$. The whole space is decomposed into $\min(2j_A, 2j_B) = j_A + j_B - |j_A - j_B|$ eigenspaces of $(\boldsymbol{J}_A + \boldsymbol{J}_B)^2$, labelled by the quantum number j, which varies by decreasing integer steps from $j_A + j_B$ to $|j_A - j_B|$. On each such eigenspace, $\boldsymbol{J}_A + \boldsymbol{J}_B$ is a spin-j angular momentum, and there is an orthonormal basis $|j, m\rangle$, with m (the eigenvalue of $J_{A,z} + J_{B,z}$) varying by decreasing integer steps from j to $-j$. The vectors $|j, m\rangle$, with all possible values of j and m, form an orthonormal basis of the whole space.

A particular basis of this kind is singled out by the following conditions [58]:

$$|j, m\rangle = \sqrt{\frac{(j+m)!}{(j-m)!\,(2j)!}}\, J_-^{j-m} |j, j\rangle \,, \tag{A1}$$

$$_A\langle j_A, m_A|_B\langle j_B, m_B|j, m\rangle > 0\,. \tag{A2}$$

Condition (A1), often called *Condon–Shortley phase convention*, yields the standard action of the ladder operators, where the relative phase between $|j, m \pm 1\rangle$ and $J_\pm |j, m\rangle$ is 1. If $|j, m\rangle$ is a basis for a spin-j angular momentum, and equation (A1) holds, the matrix elements of the associated representation are the corresponding coefficients of the Wigner matrix $D^{(j)}$—hereafter, whenever we choose an arbitrary basis for a spin angular momentum, the phase convention (A1) will always be assumed. In the present context, condition (A1) allows us to obtain each j-multiplet $|j, m\rangle$ by repeated applications of the destruction operator on $|j, j\rangle$, hence determining a basis up to an overall phase for each multiplet, and such phase is singled out by condition (A2). The two conditions together ensure the reality of the Fourier coefficients of the basis vectors, with respect to the product basis. In other words, the transition matrices between the two bases are not only unitary but also orthogonal. The basis vectors determined by the above prescriptions are denoted as $|j_A, j_B; j, m\rangle$, and their Fourier coefficients are called Clebsch–Gordan (CG) coefficients, and denoted by $C(j_A, m_A; j_B, m_B; j, m)$,

$$|j_A, j_B; j, m\rangle = \sum_{m_A, m_B} C(j_A, m_A; j_B, m_B; j, m)\, |j_A, m_A\rangle_A |j_B, m_B\rangle_B. \tag{A3}$$

It's easy to see that the nontrivial CG coefficients must satisfy the selection rule $m_A + m_B = m$, hence the sum on the right-hand side of equation (A3) has only one free index.

The irreducible invariant subspaces of $\mathscr{D}_A \otimes \mathscr{D}_B$—the $(U \otimes U)$-invariant subspaces—can be expressed in terms of the basis vectors (A3) as

$$V^{(2j+1)}_{2j_A:2j_B} = \mathrm{Span}\,\{\, |j_A, j_B; j, m\rangle \mid m = -j, \ldots, j \,\}\,, \tag{A4}$$

for integer $j = j_A + j_B, \ldots, |j_A - j_B|$. The irreducible components of $\mathscr{D}_A \otimes \mathscr{D}_B$ are obtained by restricting its action to each irreducible invariant subspace,

$$\mathscr{D}_A(U) \otimes \mathscr{D}_B(U)\, |j_A, j_B; j, m\rangle = \sum_{m'} D^{(j)}_{m'm}(U)\, |j_A, j_B; j, m'\rangle. \tag{A5}$$

Complex conjugation in SU(2)—Complex conjugation is an automorphism (i.e. an isomorphism of the group to itself) of SU(2). Actually, this is true for all special unitary groups, since identities $(AB)^* = A^* B^*$, $(A^*)^* = A$, $(A^*)^\dagger = (A^\dagger)^*$, $\det A^* = (\det A)^*$, hold for square matrices A, B, of arbitrary order. Crucially, complex conjugation is an *inner* automorphism of SU(2) [59],

$$U^* = \left(-\mathrm{i}\sigma_y\right) U \left(-\mathrm{i}\sigma_y\right)^{-1}, \tag{A6}$$

that is, taking the complex conjugate of a SU(2) matrix is the same as taking its adjoint with respect to $-\mathrm{i}\sigma_y$, an element of the group. Observe that the SO(3) representation of $-\mathrm{i}\sigma_y$ is a rotation of 180 degrees around the y axis, i.e. an inversion of the xz plane.

These considerations extend to representations. If $\mathscr{D}$ is a SU(2) representation,

$$\tilde{\mathscr{D}}\colon U \mapsto \mathscr{D}(U^*) \tag{A7}$$

is in turn a SU(2) representation, which is unitary if $\mathscr{D}$ is. These statements hold for all special unitary groups. However, if $\mathscr{D}$ is a representation of SU(2), $\mathscr{D}$ and $\tilde{\mathscr{D}}$ are isomorphic by equation (A6),

$$\tilde{\mathscr{D}}(U) = \mathscr{D}\left(-\mathrm{i}\sigma_y\right)\mathscr{D}(U)\left(\mathscr{D}\left(-\mathrm{i}\sigma_y\right)\right)^{-1}, \tag{A8}$$

and, in particular, unitarily equivalent if $\mathscr{D}$ is unitary.

If $\mathscr{D}$ is generated by a spin-j angular momentum $\boldsymbol{J}$, by equation (A8), $\tilde{\mathscr{D}}$ is generated by

$$\tilde{\boldsymbol{J}} = \mathscr{D}\left(-\mathrm{i}\sigma_y\right)\boldsymbol{J}\left(\mathscr{D}\left(-\mathrm{i}\sigma_y\right)\right)^{\dagger} = \exp\left(\mathrm{i}\pi J_y\right)\boldsymbol{J}\exp\left(-\mathrm{i}\pi J_y\right) = \left(-J_x, J_y, -J_z\right), \tag{A9}$$

in turn a spin-j angular momentum, related to $\boldsymbol{J}$ by a rotation of 180 degrees around the y axis. Moreover, if $|j,m\rangle$ is a basis for $\boldsymbol{J}$, $\mathscr{D}(-\mathrm{i}\sigma_y)|j,m\rangle$ is a basis for $\tilde{\boldsymbol{J}}$.

Schwinger angular momentum—Let $\mathscr{H}$ be a Hilbert space of two independent bosonic modes, that is, with creation and destruction operators $a_k^\dagger$ and a_k, such that $(k,\ell = 1,2)$

$$[a_k, a_\ell] = 0, \qquad \left[a_k^\dagger, a_\ell^\dagger\right] = 0, \qquad \left[a_k, a_\ell^\dagger\right] = \delta_{k\ell}\mathbb{1}, \tag{A10}$$

with number operators $N_k = a_k^\dagger a_k$, and total number operator $N = N_1 + N_2$. The vectors

$$|(n_1,n_2)\rangle = \frac{a_1^{\dagger n_1} a_2^{\dagger n_2}}{\sqrt{n_1! n_2!}}|0\rangle \tag{A11}$$

form an orthonormal basis of joint eigenstates of the number operators, where $|0\rangle = |(0,0)\rangle$ is the vacuum state, $a_k|0\rangle = 0$.

The Jordan map [58],

$$(M_{k\ell})_{k,\ell=1}^2 \mapsto \sum_{k,\ell=1}^{2} M_{k\ell}\, a_k^\dagger a_\ell, \tag{A12}$$

is a Lie-algebra homomorphism, mapping matrices of order 2 to operators on $\mathscr{H}$, that are bilinear in the creation and destruction operators. Since the Hermitian conjugate of a matrix is mapped to the adjoint of the corresponding operator, Hermitian matrices are mapped to observables. In particular, the spin-$\frac{1}{2}$ angular momentum $\boldsymbol{\sigma}/2$, with ladder operators $\sigma_\pm/2 = (\sigma_x \pm \mathrm{i}\sigma_y)/2$, is mapped to the *Schwinger angular momentum* [58, 60] $\boldsymbol{J} = (J_x, J_y, J_z)$, with ladder operators $J_\pm = J_x \pm \mathrm{i}J_y$, where

$$J_+ = a_1^\dagger a_2, \qquad J_- = a_2^\dagger a_1, \qquad J_z = \frac{a_1^\dagger a_1 - a_2^\dagger a_2}{2} = \frac{N_1 - N_2}{2}. \tag{A13}$$

Remarkably, $\boldsymbol{J}$ yields all the irreducible representations of the Lie algebra su(2), and generates a representation $\mathscr{D}$ yielding all the irreducible representations of the Lie group SU(2) [58]. Indeed, the square of the angular momentum is related to the total number operator (corresponding to the image, through the Jordan map, of the identity matrix) by

$$\boldsymbol{J}^2 = \frac{N}{2}\left(\frac{N}{2} + \mathbb{1}\right). \tag{A14}$$

As a consequence, the eigenspace of $\boldsymbol{J}^2$ relative to the quantum number j coincides with the eigenspace $\mathscr{H}_{2j}$ of the total number operator N relative to the eigenvalue $2j$, which is spanned by $|(n_1,n_2)\rangle$, with $n_1 + n_2 = 2j$. Moreover, by equations (A13) and (A14), joint eigenvectors of N_1 and N_2, and joint eigenvectors of $\boldsymbol{J}^2$ and J_z coincide, and the corresponding quantum numbers are related by

$$j = \frac{n_1 + n_2}{2}, \qquad m = \frac{n_1 - n_2}{2}. \tag{A15}$$

Therefore, $\mathscr{H}_{2j}$ is invariant under $\boldsymbol{J}$, and the restriction of $\boldsymbol{J}$ to $\mathscr{H}_{2j}$ is a spin-j angular momentum, with basis

$$|j,m\rangle = \frac{a_1^{\dagger j+m} a_2^{\dagger j-m}}{\sqrt{(j+m)!(j-m)!}}|0\rangle, \tag{A16}$$

with $m = -j, \ldots, j$, automatically satisfying the phase convention (A1). Then SU(2) can act on $\mathscr{H}$ under the unitary representation $\mathscr{D}$ generated by $\boldsymbol{J}$. In particular, its action on $\mathscr{H}_{2j}$ is

$$\mathscr{D}(U)|j,m\rangle = \sum_{m'} D^{(j)}_{m'm}(U)|j,m'\rangle. \tag{A17}$$

In other words, the subrepresentation $\mathscr{D}^{(j)}: U \mapsto \mathscr{D}(U)|_{\mathscr{H}_{2j}}$, restricting the action of $\mathscr{D}$ to $\mathscr{H}_{2j}$, is a spin-j representation on $\mathscr{H}_{2j}$, generated by the restriction of $\boldsymbol{J}$ to $\mathscr{H}_{2j}$.

As to complex conjugation, the representation $\tilde{\mathscr{D}}$ defined by equation (A7) is generated by the rotated angular momentum $\tilde{\boldsymbol{J}} = (-J_x, J_y, -J_z)$, the Schwinger angular momentum associated to the rotated spin-$^1/_2$ angular momentum $\tilde{\boldsymbol{\sigma}}/2 = (-\sigma_x/2, \sigma_y/2, -\sigma_z/2)$. Then $\mathscr{H}_{2j}$ is invariant under $\tilde{\mathscr{D}}$, and the spin-j subrepresentations of $\mathscr{D}$ and $\tilde{\mathscr{D}}$ on $\mathscr{H}_{2j}$ are related by

$$\tilde{\mathscr{D}}^{(j)}(U) = \mathscr{D}^{(j)}(U^*). \tag{A18}$$

A.2. Abstract problem

Let us consider the simple case in which Alice's and Bob's representations are both irreducible, namely, let $\boldsymbol{J}_\alpha$ $(\alpha = A, B)$ be a spin-j_α angular momentum on a Hilbert space $\mathscr{H}_\alpha$, with basis $|j_\alpha, m_\alpha\rangle_\alpha$, generating a representation $\mathscr{D}_\alpha$ of SU(2). Let us also keep in mind that the relevant case to our actual problem will be $j_A = 1/2$. While theoretical considerations will generally be carried out for a generic j_A, we will generally look for explicit expressions only for $j_A = 1/2$.

A.2.1. General considerations

We know that $\mathscr{D}_A \otimes \mathscr{D}_B$ and $\mathscr{D}_A \otimes \tilde{\mathscr{D}}_B$ are unitary representations of SU(2), acting on $\mathscr{H}_A \otimes \mathscr{H}_B$, generated by the angular momenta $\boldsymbol{J}_A + \boldsymbol{J}_B$ and $\boldsymbol{J}_A + \tilde{\boldsymbol{J}}_B$, respectively, and unitarily equivalent by equation (A8),

$$\mathscr{D}_A(U) \otimes \tilde{\mathscr{D}}_B(U) = \left(\mathbb{1}_A \otimes \mathscr{D}_B(-\mathrm{i}\sigma_y)\right)\left(\mathscr{D}_A(U) \otimes \mathscr{D}_B(U)\right)\left(\mathbb{1}_A \otimes \mathscr{D}_B(-\mathrm{i}\sigma_y)\right)^\dagger. \tag{A19}$$

$(U \otimes U^*)$-invariant subspaces from $(U \otimes U)$-invariant subspaces—Since $\mathscr{D}_A \otimes \mathscr{D}_B$ and $\mathscr{D}_A \otimes \tilde{\mathscr{D}}_B$ are related by a unitary transformation, the $(U \otimes U^*)$-invariant subspaces are all and only the images of the $(U \otimes U)$-invariant subspace through the unitary operator $\mathbb{1}_A \otimes \mathscr{D}_B(-\mathrm{i}\sigma_y)$. Moreover, we are free to multiply this unitary, on the left, by any unitary of the kind $\mathscr{D}_A(U_0) \otimes \mathscr{D}_B(U_0^*)$, with $U_0 \in \mathrm{SU}(2)$. Since we are essentially interested to $j_A = 1/2$, a suitable choice, allowing us to move the action of the identity map on the higher spin, is $\mathscr{U} = \mathscr{D}_A(-\mathrm{i}\sigma_y) \otimes \mathbb{1}_B$. Incidentally, $\mathscr{U}$ is the precise analogue of $\mathbb{1}_A \otimes \mathscr{D}_B(-\mathrm{i}\sigma_y)$ for $\tilde{\mathscr{D}}_A \otimes \mathscr{D}_B$. This fact should not come as a surprise: $(U \otimes U^*)$-invariance and $(U^* \otimes U)$-invariance coincide, after all.

By equation (A4), the whole space is decomposed into the irreducible $(U \otimes U^*)$-invariant subspaces

$$W^{(2j+1)}_{2j_A:2j_B} = \mathscr{U}\, V^{(2j+1)}_{2j_A:2j_B} = \mathrm{Span}\left\{\mathscr{U}|j_A, j_B; j, m\rangle \mid m = -j, \ldots, j\right\}, \tag{A20}$$

with $j = j_A + j_B, \ldots, |j_A - j_B|$.

Invariant states from invariant subspaces—We say that a density operator ρ of the bipartite system is a $(U \otimes U^*)$-invariant state if

$$\rho = \mathscr{D}_A(U) \otimes \mathscr{D}_B(U^*)\, \rho\, \left(\mathscr{D}_A(U) \otimes \mathscr{D}_B(U^*)\right)^\dagger, \tag{A21}$$

for all $U \in \mathrm{SU}(2)$, that is, if ρ commutes with $\mathscr{D}_A \otimes \tilde{\mathscr{D}}_B$, or, which is the same, with each component of $\boldsymbol{J}_A + \tilde{\boldsymbol{J}}_B$. Now, if ρ is an invariant state, each invariant subspace of $\mathscr{D}_A \otimes \tilde{\mathscr{D}}_B$ must be invariant under ρ. Consequently, ρ is decomposed into a convex combination of states, each living in a different irreducible invariant subspace of $\mathscr{D}_A \otimes \tilde{\mathscr{D}}_B$. But then each such state is a scalar by Schur's lemma [61]. As a result, the following states are $(U \otimes U^*)$-invariant:

$$\rho^{(2j+1)}_{2j_A:2j_B} = \frac{1}{2j+1} P^{(2j+1)}_{2j_A:2j_B}, \tag{A22}$$

where $P^{(2j+1)}_{2j_A:2j_B}$ is the orthogonal projection onto $W^{(2j+1)}_{2j_A:2j_B}$, and the most general invariant state is a convex combination of states of the kind (A22).

A.2.2. Discussion of the case $\frac{1}{2}\times j_B$

Let us assign the role of 'computational basis' to the product basis $|j_A,m_A\rangle_A|j_B,m_B\rangle_B$, and look for explicit expressions of the $(U\otimes U^*)$-invariant states. Since an invariant state is a linear combination of orthogonal projections onto irreducible invariant subspaces, and, by equation (A20), such subspaces are spanned by orthonormal vectors in the form $\mathscr{U}|j_A,j_B;j,m\rangle$, all we have to do is decompose these vectors on the product basis. To this end, we need the matrix elements of $\mathscr{U}=\mathscr{D}_A(-\mathrm{i}\sigma_y)$, and the CG coefficients for $j_A\times j_B$.

Hereafter we will show how to handle this problem in the case of our concern, $j_A=1/2$. First of all, our notation for a spin-$^1/_2$ can be simplified by setting $|\pm\rangle=|\frac{1}{2},\pm\frac{1}{2}\rangle$. We know that the whole space is decomposed as

$$\mathscr{H}_A\otimes\mathscr{H}_B=V^{(2j_B+2)}_{1:2j_B}\oplus V^{(2j_B)}_{1:2j_B}=W^{(2j_B+2)}_{1:2j_B}\oplus W^{(2j_B)}_{1:2j_B}\,, \tag{A23}$$

that is, into two irreducible $(U\otimes U)$-invariant subspaces, as well as two irreducible $(U\otimes U^*)$-invariant subspaces, of dimension $2j_B+2$ and $2j_B$, related by

$$W^{(2j_B+2)}_{1:2j_B}=\mathscr{U}\,V^{(2j_B+2)}_{1:2j_B}\,,\qquad\qquad W^{(2j_B)}_{1:2j_B}=\mathscr{U}\,V^{(2j_B)}_{1:2j_B}\,. \tag{A24}$$

The basis vectors of the irreducible $(U\otimes U)$-invariant subspaces are precisely the two j-multiplets for $\frac{1}{2}\times j_B$ $(j=j_B\pm1/2)$, and are linear combinations of at most two product basis vectors,

$$\begin{aligned}|\tfrac{1}{2},j_B;j_B\pm\tfrac{1}{2},m\rangle=&\,C\big(\tfrac{1}{2},\tfrac{1}{2};j_B,m-\tfrac{1}{2};j_B\pm\tfrac{1}{2},m\big)\,|+\rangle_A\,|j_B,m-\tfrac{1}{2}\rangle_B\\&+C\big(\tfrac{1}{2},-\tfrac{1}{2};j_B,m+\tfrac{1}{2};j_B\pm\tfrac{1}{2},m\big)\,|-\rangle_A\,|j_B,m+\tfrac{1}{2}\rangle_B.\end{aligned} \tag{A25}$$

In our settings, $\mathscr{D}_A$ can be identified with the defining representation. In particular, $\mathscr{D}_A(-\mathrm{i}\sigma_y)|\pm\rangle_A=\pm|\mp\rangle_A$. As a result, the basis vectors of the irreducible $(U\otimes U^*)$-invariant subspaces read

$$\begin{aligned}\mathscr{U}\,|\tfrac{1}{2},j_B;j_B\pm\tfrac{1}{2},m\rangle=&\,C\big(\tfrac{1}{2},\tfrac{1}{2};j_B,m-\tfrac{1}{2};j_B\pm\tfrac{1}{2},m\big)\,|-\rangle_A\,|j_B,m-\tfrac{1}{2}\rangle_B\\&-C\big(\tfrac{1}{2},-\tfrac{1}{2};j_B,m+\tfrac{1}{2};j_B\pm\tfrac{1}{2},m\big)\,|+\rangle_A\,|j_B,m+\tfrac{1}{2}\rangle_B.\end{aligned} \tag{A26}$$

The calculation the CG coefficients for $\frac{1}{2}\times j_B$ is also rather straightforward, and will be shown below, in order to make this appendix as self-consistent as possible. Actually, this task will be carried out by first computing the CG coefficients, with the two highest values of j, for $j_A\times j_B$, and then specializing the results to $j_A=1/2$. Indeed, there would be no advantage in assuming $j_A=1/2$ right from the start; on the contrary, while our math would not get any simpler, the resulting notation would become quite cumbersome.

Clebsch–Gordan coefficients for $j_A\times j_B, j=j_A+j_B$—Throughout this paragraph, and the next one, j_A and j_B are fixed; therefore we will write $|m_A\rangle|m_B\rangle$ instead of $|j_A,m_A\rangle_A|j_B,m_B\rangle_B$, and $|j,m\rangle$ instead of $|j_A,j_B;j,m\rangle$. We will also set $\hat{\jmath}=j_A+j_B$.

Let us start with the $\hat{\jmath}$-multiplet. The eigenspace of $J_{A,z}+J_{B,z}$ relative to $m=\hat{\jmath}$ is spanned by $|j_A\rangle|j_B\rangle$. Then, by condition (A2) we must set

$$|\hat{\jmath},\hat{\jmath}\rangle=|j_A\rangle|j_B\rangle, \tag{A27}$$

and, by condition (A1),

$$|\hat{\jmath},m\rangle=\sqrt{\frac{(\hat{\jmath}+m)!}{(\hat{\jmath}-m)!\,(2\hat{\jmath})!}}\,J_-^{\hat{\jmath}-m}|j_A\rangle|j_B\rangle. \tag{A28}$$

We first compute

$$\begin{aligned}J_-^{\hat{\jmath}-m}|j_A\rangle|j_B\rangle&=(J_{A,-}+J_{B,-})^{\hat{\jmath}-m}\,|j_A\rangle|j_B\rangle\\&=\sum_{\substack{m_A,m_B\\m_A+m_B=m}}\frac{(\hat{\jmath}-m)!}{(j_A-m_A)!\,(j_B-m_B)!}\,J_{A,-}^{j_A-m_A}|j_A\rangle J_{B,-}^{j_B-m_B}|j_B\rangle\\&=\sum_{\substack{m_A,m_B\\m_A+m_B=m}}\left[\frac{(\hat{\jmath}-m)!^2\,(2j_A)!\,(2j_B)!}{(j_A-m_A)!\,(j_A+m_A)!\,(j_B-m_B)!\,(j_B+m_B)!}\right]^{\frac{1}{2}}|m_A\rangle|m_B\rangle,\end{aligned} \tag{A29}$$

and then plug the result into equation (A28), to obtain the whole multiplet,

$$
\begin{aligned}
|\hat{\jmath}, m\rangle &= \sum_{\substack{m_A, m_B \\ m_A + m_B = m}} \left[\frac{(\hat{\jmath}+m)!\,(\hat{\jmath}-m)!\,(2j_A)!\,(2j_B)!}{(2\hat{\jmath})!\,(j_A-m_A)!\,(j_A+m_A)!\,(j_B-m_B)!\,(j_B+m_B)!}\right]^{\frac{1}{2}} |m_A\rangle|m_B\rangle \\
&= \sum_{\substack{m_A, m_B \\ m_A + m_B = m}} \left[\frac{\binom{2j_A}{j_A-m_A}\binom{2j_B}{j_B-m_B}}{\binom{2\hat{\jmath}}{\hat{\jmath}-m}}\right]^{\frac{1}{2}} |m_A\rangle|m_B\rangle. \qquad \text{(A30)}
\end{aligned}
$$

Observe that the coefficients with $j = j_A + j_B - 1$ are all non negative.

Clebsch–Gordan coefficients for $j_A \times j_B, j = j_A + j_B - 1$—As to the $(\hat{\jmath}-1)$-multiplet, the eigenspace of $J_{A,z} + J_{B,z}$, relative to $m = \hat{\jmath} - 1$, is spanned by $|j_A\rangle|j_B - 1\rangle$ and $|j_A - 1\rangle|j_B\rangle$, and, by equation (A30),

$$
|\hat{\jmath}, \hat{\jmath}-1\rangle = \sqrt{\frac{j_B}{j_A + j_B}}\,|j_A\rangle|j_B - 1\rangle + \sqrt{\frac{j_A}{j_A + j_B}}\,|j_A - 1\rangle|j_B\rangle. \qquad \text{(A31)}
$$

is one of the eigenstates. Therefore, by condition (A2), we must set

$$
|\hat{\jmath}-1, \hat{\jmath}-1\rangle = \sqrt{\frac{j_A}{j_A + j_B}}\,|j_A\rangle|j_B - 1\rangle - \sqrt{\frac{j_B}{j_A + j_B}}\,|j_A - 1\rangle|j_B\rangle, \qquad \text{(A32)}
$$

and, by condition (A1),

$$
|\hat{\jmath}-1, m\rangle = \sqrt{\frac{(\hat{\jmath}-1+m)!}{(\hat{\jmath}-1-m)!\,(2\hat{\jmath}-2)!\hat{\jmath}}}\left[\sqrt{j_A}\,J_-^{\hat{\jmath}-m-1}|j_A\rangle|j_B-1\rangle - \sqrt{j_B}\,J_-^{\hat{\jmath}-m-1}|j_A-1\rangle|j_B\rangle\right]. \qquad \text{(A33)}
$$

The generic state of the multiplet is the sum of two terms. We first compute

$$
\begin{aligned}
J_-^{\hat{\jmath}-m-1}|j_A\rangle|j_B-1\rangle &= (J_{A,-} + J_{B,-})^{\hat{\jmath}-m-1}\,|j_A\rangle|j_B-1\rangle \\
&= \sum_{\substack{m_A, m_B \\ m_B \leqslant j_B - 1 \\ m_A + m_B = m}} \frac{(\hat{\jmath}-m-1)!}{(j_A-m_A)!\,(j_B-m_B-1)!}\,J_{A,-}^{j_A-m_A}|j_A\rangle J_{B,-}^{j_B-m_B-1}|j_B-1\rangle \\
&= \sum_{\substack{m_A, m_B \\ m_B \leqslant j_B - 1 \\ m_A + m_B = m}} \left[\frac{(\hat{\jmath}-m-1)!^2\,(2j_A)!\,(2j_B-1)!\,(j_B-m_B)}{(j_A-m_A)!\,(j_A+m_A)!\,(j_B-m_B-1)!\,(j_B+m_B)!}\right]^{\frac{1}{2}} |m_A\rangle|m_B\rangle \\
&= \sum_{\substack{m_A, m_B \\ m_A + m_B = m}} \left[\frac{(\hat{\jmath}-m-1)!^2\,(2j_A)!\,(2j_B-1)!\,(j_B-m_B)^2}{(j_A-m_A)!\,(j_A+m_A)!\,(j_B-m_B)!\,(j_B+m_B)!}\right]^{\frac{1}{2}} |m_A\rangle|m_B\rangle, \qquad \text{(A34)}
\end{aligned}
$$

so that the term in $J_-^{\hat{\jmath}-m-1}|j_A\rangle|j_B-1\rangle$ is

$$
\begin{aligned}
&\sqrt{\frac{(\hat{\jmath}-1+m)!j_A}{(\hat{\jmath}-1-m)!\,(2\hat{\jmath}-2)!\hat{\jmath}}}\,J_-^{\hat{\jmath}-m-1}|j_A\rangle|j_B-1\rangle \\
&= \sum_{\substack{m_A, m_B \\ m_A + m_B = m}} \left[\frac{(\hat{\jmath}-m-1)!\,(\hat{\jmath}-m+1)!\,(2j_A)!\,(2j_B-1)!j_A\,(j_B-m_B)^2}{(2\hat{\jmath}-2)!\,(j_A-m_A)!\,(j_A+m_A)!\,(j_B-m_B)!\,(j_B+m_B)!\hat{\jmath}}\right]^{\frac{1}{2}} |m_A\rangle|m_B\rangle \\
&= \sum_{\substack{m_A, m_B \\ m_A + m_B = m}} \left[\frac{\binom{2j_A}{j_A-m_A}\binom{2j_B}{j_B-m_B}}{\binom{2\hat{\jmath}-2}{\hat{\jmath}-m-1}}\right]^{\frac{1}{2}} \frac{j_A\,(j_B-m_B)}{\sqrt{2j_Aj_B\hat{\jmath}}}\,|m_A\rangle|m_B\rangle. \qquad \text{(A35)}
\end{aligned}
$$

The term in $J_-^{\hat{\jmath}-m-1}|j_A-1\rangle|j_B\rangle$ is obtained by substituting $A \leftrightarrow B$ in the coefficients of the above linear combination. Plugging these results into equation (A33) yields the whole multiplet,

$$
|\hat{\jmath}-1, m\rangle = \sum_{\substack{m_A, m_B \\ m_A + m_B = m}} \left[\frac{\binom{2j_A}{j_A-m_A}\binom{2j_B}{j_B-m_B}}{\binom{2\hat{\jmath}-2}{\hat{\jmath}-m-1}}\right]^{\frac{1}{2}} \frac{j_Bm_A - j_Am_B}{\sqrt{2j_Aj_B\hat{\jmath}}}\,|m_A\rangle|m_B\rangle. \qquad \text{(A36)}
$$

The coefficients with $j = j_A + j_B - 1$ have the sign of $m_A/j_A - m_B/j_B$, hence can be negative.

Clebsch–Gordan coefficients for $\frac{1}{2} \times j_B$—By equation (A30), the nontrivial CG coefficients with $j = j_B + 1/2$ are in the form

$$\begin{aligned} C\left(\tfrac{1}{2}, \pm\tfrac{1}{2}; j_B, m \mp \tfrac{1}{2}; j_B + \tfrac{1}{2}, m\right) &= \binom{1}{\frac{1}{2} \mp \frac{1}{2}}^{\frac{1}{2}} \binom{2j_B}{j_B - m \pm \frac{1}{2}}^{\frac{1}{2}} \binom{2j_B + 1}{j_B - m + \frac{1}{2}}^{-\frac{1}{2}} \\ &= \sqrt{\frac{1}{2} \pm \frac{m}{2j_B + 1}}, \end{aligned} \tag{A37}$$

for $m = j_B + 1/2, \ldots, -j_B - 1/2$. They are all non negative; for $m = \pm(j_B + 1/2)$ one sign choice yields 0 (and the other 1, as it should be); for any other value of m, both choices lead to nontrivial coefficients. Likewise, by equation (A36), the nontrivial CG coefficients with $j = j_B - 1/2$ are in the form

$$\begin{aligned} C\left(\tfrac{1}{2}, \pm\tfrac{1}{2}; j_B, m \mp \tfrac{1}{2}; j_B - \tfrac{1}{2}, m\right) &= \pm \binom{1}{\frac{1}{2} \mp \frac{1}{2}}^{\frac{1}{2}} \binom{2j_B}{j_B - m \pm \frac{1}{2}}^{\frac{1}{2}} \binom{2j_B - 1}{j_B - m - \frac{1}{2}}^{-\frac{1}{2}} \frac{j_B \mp m + \frac{1}{2}}{\sqrt{2j_B\left(2j_B + 1\right)}} \\ &= \pm \sqrt{\frac{1}{2} \mp \frac{m}{2j_B + 1}}, \end{aligned} \tag{A38}$$

for $m = j_B - 1/2, \ldots, -j_B + 1/2$. They are all non vanishing, and have the sign of $m_A = \pm 1/2$.

As a result, the $(j_B + 1/2)$-multiplet is made up of two separable states,

$$\left|\tfrac{1}{2}, j_B; j_B + \tfrac{1}{2}, \pm\left(j_B + \tfrac{1}{2}\right)\right\rangle = |\pm\rangle_A |j_B, \pm j_B\rangle_B, \tag{A39}$$

corresponding to the highest and lowest values of $J_{A,z} + J_{B,z}$, and the $2j_B$ entangled states

$$\left|\tfrac{1}{2}, j_B; j_B + \tfrac{1}{2}, m\right\rangle = \sqrt{\frac{1}{2} + \frac{m}{2j_B + 1}}\, |+\rangle_A |j_B, m - \tfrac{1}{2}\rangle_B + \sqrt{\frac{1}{2} - \frac{m}{2j_B + 1}}\, |-\rangle_A |j_B, m + \tfrac{1}{2}\rangle_B, \tag{A40}$$

with $m = j_B - 1/2, \ldots, -j_B + 1/2$. These $2j_B + 2$ states together generate $V_{1:2j_B}^{(2j_B+2)}$. On the other hand, the $(j_B - 1/2)$-multiplet is made up of

$$\left|\tfrac{1}{2}, j_B; j_B - \tfrac{1}{2}, m\right\rangle = \sqrt{\frac{1}{2} - \frac{m}{2j_B + 1}}\, |+\rangle_A |j_B, m - \tfrac{1}{2}\rangle_B - \sqrt{\frac{1}{2} + \frac{m}{2j_B + 1}}\, |-\rangle_A |j_B, m + \tfrac{1}{2}\rangle_B, \tag{A41}$$

with $m = j_B - 1/2, \ldots, -j_B + 1/2$. These $2j_B$ entangled states generate $V_{1:2j_B}^{(2j_B)}$.

If $|j, \pm(j+1)\rangle = 0$ is understood, equations (A39)–(A40) and (A41) can be put together, by saying that $V_{1:2j_B}^{(2j_B+1\pm1)}$ is spanned by the $2j_B + 1 \pm 1$ orthonormal vectors

$$\left|\tfrac{1}{2}, j_B; j_B \pm \tfrac{1}{2}, m\right\rangle = \sqrt{\frac{1}{2} \pm \frac{m}{2j_B + 1}}\, |+\rangle_A |j_B, m - \tfrac{1}{2}\rangle_B \pm \sqrt{\frac{1}{2} \mp \frac{m}{2j_B + 1}}\, |-\rangle_A |j_B, m + \tfrac{1}{2}\rangle_B, \tag{A42}$$

with $m = j_B \pm 1/2, \ldots, -j_B \mp 1/2$.

Irreducible $(U \otimes U^*)$-invariant subspaces for $\frac{1}{2} \times j_B$—By equations (A24) and (A42), $W_{1:2j_B}^{(2j_B+1\pm1)}$ is generated by the $2j_B + 1 \pm 1$ orthonormal vectors

$$\mathscr{U}\left|\tfrac{1}{2}, j_B; j_B \pm \tfrac{1}{2}, m\right\rangle = \sqrt{\frac{1}{2} \pm \frac{m}{2j_B + 1}}\, |-\rangle_A |j_B, m - \tfrac{1}{2}\rangle_B \mp \sqrt{\frac{1}{2} \mp \frac{m}{2j_B + 1}}\, |+\rangle_A |j_B, m + \tfrac{1}{2}\rangle_B, \tag{A43}$$

with $m = j_B \pm 1/2, \ldots, -j_B \mp 1/2$. Specifically, $W^{(2j_B+2)}_{1:2j_B}$ is spanned by the $2j_B + 2$ vectors

$$\begin{gathered}
|-\rangle_A |j_B, j_B\rangle_B, \\
\sqrt{\frac{2j_B}{2j_B+1}}|-\rangle_A|j_B, j_B-1\rangle_B - \sqrt{\frac{1}{2j_B+1}}|+\rangle_A|j_B, j_B\rangle_B, \\
\vdots \\
\sqrt{\frac{1}{2j_B+1}}|-\rangle_A|j_B, -j_B\rangle_B - \sqrt{\frac{2j_B}{2j_B+1}}|+\rangle_A|j_B, -j_B+1\rangle_B, \\
-|+\rangle_A|j_B, -j_B\rangle_B,
\end{gathered} \tag{A44}$$

and $W^{(2j_B)}_{1:2j_B}$ by the $2j_B$ vectors

$$\begin{gathered}
\sqrt{\frac{1}{2j_B+1}}|-\rangle_A|j_B, j_B-1\rangle_B + \sqrt{\frac{2j_B}{2j_B+1}}|+\rangle_A|j_B, j_B\rangle_B, \\
\vdots \\
\sqrt{\frac{2j_B}{2j_B+1}}|-\rangle_A|j_B, -j_B\rangle_B + \sqrt{\frac{1}{2j_B+1}}|+\rangle_A|j_B, -j_B+1\rangle_B.
\end{gathered} \tag{A45}$$

The above expressions allow us to write the orthogonal projection over each invariant subspace, hence, by equation (A22), the corresponding invariant state.

A.3. Actual problem

Let us now consider two systems, each of two independent photonic modes, namely, the horizontal and the vertical polarization. Alice's system is described by a Hilbert space $\mathscr{H}_A$, with canonical bosonic annihilation and creation operators $\{a_k, a_k^\dagger\}$ for the optical modes $k = H, V$, determining the number operators N_A^k, the total number operator $N_A = N_A^H + N_A^V$, and the standard basis $|(n_A^H, n_A^V)\rangle_A$, as well as the Schwinger angular momentum $\boldsymbol{J}_A$, with basis $|j_A, m_A\rangle_A$, and generating the SU(2) representation $\mathscr{D}_A$. Likewise for Bob.

We look for the $(U \otimes U^*)$-invariant states—defined as in equation (A21)—of the composite system, such that Alice's total number is 1, and Bob's is n (an arbitrary, but fixed number).

A.3.1. General considerations

This problem is just a special case of the one we studied in section A.2. Indeed, in a Hilbert space of two independent bosonic modes, eigenstates and eigenvalues of the number operators correspond to eigenstates and eigenvalues of the Schwinger angular momentum. In particular, equations (A11) and (A15)–(A16) yield $j = n/2$, $m = n^H - n/2$, and $|j, m\rangle = |(n^H, n - n^H)\rangle$ (entailing $|+\rangle = |H\rangle$, and $|-\rangle = |V\rangle$). With this in mind, a bipartite state such that Alice's total number is 1, and Bob's is n, lives in the finite-dimensional tensor product space $\mathscr{H}_{A,1} \otimes \mathscr{H}_{B,n}$, where Alice's and Bob's representations are both irreducible, with spin $1/2$ and $n/2$, respectively. But then such space is decomposed into two $(U \otimes U^*)$-irreducible invariant subspaces,

$$\mathscr{H}_{A,1} \otimes \mathscr{H}_{B,n} = W^{(n+2)}_{1:n} \oplus W^{(n)}_{1:n}, \tag{A46}$$

and the most general invariant state is in the form of a convex combination, with one real parameter $f \in [0, 1]$, of the corresponding invariant states,

$$\rho^{(\mathrm{inv})}_{1:n}(f) = (1-f)\,\rho^{(n+2)}_{1:n} + f\rho^{(n)}_{1:n} = \frac{1-f}{n+2}P^{(n+2)}_{1:n} + \frac{f}{n}P^{(n)}_{1:n}, \tag{A47}$$

where $W^{(2j+1)}_{2j_A:2j_B}$, $\rho^{(2j+1)}_{2j_A:2j_B}$, and $P^{(2j+1)}_{2j_A:2j_B}$ have the same meaning as in equations (A20) and (A22).

Let us now turn our attention to the problem of expressing the irreducible invariant subspaces on the product basis,

$$|H\rangle_A|(n,0)\rangle_B, \ldots, |H\rangle_A|(0,n)\rangle_B, |V\rangle_A|(n,0)\rangle_B, \ldots, |V\rangle_A|(0,n)\rangle_B. \tag{A48}$$

By equation (A44), the subspace $W_{1:n}^{(n+2)}$ is spanned by the $n+2$ orthonormal states

$$\begin{gathered}|V\rangle_A|(n,0)\rangle_B,\\ \sqrt{\frac{n}{n+1}}|V\rangle_A|(n-1,1)\rangle_B-\sqrt{\frac{1}{n+1}}|H\rangle_A|(n,0)\rangle_B,\\ \vdots\\ \sqrt{\frac{1}{n+1}}|V\rangle_A|(0,n)\rangle_B-\sqrt{\frac{n}{n+1}}|H\rangle_A|(1,n-1)\rangle_B,\\ -|H\rangle_A|(0,n)\rangle_B.\end{gathered}\tag{A49}$$

And by equation (A45) the subspace $W_{1:n}^{(n)}$ is spanned by the n orthonormal states

$$\begin{gathered}\sqrt{\frac{1}{n+1}}|V\rangle_A|(n-1,1)\rangle_B+\sqrt{\frac{n}{n+1}}|H\rangle_A|(n,0)\rangle_B,\\ \vdots\\ \sqrt{\frac{n}{n+1}}|V\rangle_A|(0,n)\rangle_B+\sqrt{\frac{1}{n+1}}|H\rangle_A|(1,n-1)\rangle_B.\end{gathered}\tag{A50}$$

A.3.2. Explicit solutions for the simplest cases

Hereafter, we will give a glance at the cases in which Bob has 1, 2, or 3 photons. Tensor products will be written as Kronecker products. Matrix representations for linear operators on $\mathscr{H}_{A,1}\otimes\mathscr{H}_{B,n}$ shall always be understood with respect to the product basis, ordered as in equation (A48)—i.e. first by decreasing values of n_A^H, then by decreasing values of n_B^H. We will also emphasize the block structure brought about by the Kronecker product with respect to the ordered basis $(|H\rangle_A,|V\rangle_A)$ of $\mathscr{H}_{A,1}$. In this way, the density matrix is partitioned into four square blocks, of order $n+1$, and its partial trace on Bob's system is obtained by replacing each block with its own trace.

Case $n=1$—The 4-dimensional space $\mathcal{H}_{A,1}\otimes\mathcal{H}_{B,1}$, corresponding to the case with one photon in each system, is decomposed into invariant subspaces of dimension 3 and 1,

$$\mathscr{H}_{A,1}\otimes\mathscr{H}_{B,1}=W_{1:1}^{(3)}\oplus W_{1:1}^{(1)}.\tag{A51}$$

The subspace $W_{1:1}^{(3)}$ is spanned by the orthonormal states

$$|V\rangle_A|H\rangle_B,\qquad \frac{1}{\sqrt{2}}\left(|V\rangle_A|V\rangle_B-|H\rangle_A|H\rangle_B\right),\qquad -|H\rangle_A|V\rangle_B,\tag{A52}$$

and corresponds to the invariant state

$$\rho_{1:1}^{(3)}=\frac{1}{3}\left(\begin{array}{cc|cc}1/2&0&0&-1/2\\0&1&0&0\\\hline 0&0&1&0\\-1/2&0&0&1/2\end{array}\right).\tag{A53}$$

The invariant pure state spanning $W_{1:1}^{(1)}$, $(|HH\rangle+|VV\rangle)/\sqrt{2}$, yields the density matrix

$$\rho_{1:1}^{(1)}=\left(\begin{array}{cc|cc}1/2&0&0&1/2\\0&0&0&0\\\hline 0&0&0&0\\1/2&0&0&1/2\end{array}\right).\tag{A54}$$

A generic invariant state is a convex combination of $\rho_{1:1}^{(3)}$ and $\rho_{1:1}^{(1)}$, depending on $f\in[0,1]$,

$$\rho_{1:1}^{(\mathrm{inv})}(f)=(1-f)\,\rho_{1:1}^{(3)}+f\,\rho_{1:1}^{(1)}=\frac{1}{6}\left(\begin{array}{cc|cc}2f-1&0&0&4f-1\\0&2(1-f)&0&0\\\hline 0&0&2(1-f)&0\\4f-1&0&0&2f-1\end{array}\right).\tag{A55}$$

Case $n=2$—The 6-dimensional space $\mathscr{H}_{A,1}\otimes\mathscr{H}_{B,2}$, corresponding to the case with one photon in Alice's system, and two in Bob's, is decomposed into invariant subspaces of dimension 4 and 2,

$$\mathscr{H}_{A,1}\otimes\mathscr{H}_{B,2}=W^{(4)}_{1:2}\oplus W^{(2)}_{1:2} \tag{A56}$$

The subspace $W^{(4)}_{1:2}$ has orthonormal basis

$$\begin{gathered}|V\rangle_A|(2,0)\rangle_B,\\ \sqrt{\frac{2}{3}}|V\rangle_A|(1,1)\rangle_B-\frac{1}{\sqrt{3}}|H\rangle_A|(2,0)\rangle_B,\\ \frac{1}{\sqrt{3}}|V\rangle_A|(0,2)\rangle_B-\sqrt{\frac{2}{3}}|H\rangle_A|(1,1)\rangle_B,\\ -|H\rangle_A|(0,2)\rangle_B,\end{gathered} \tag{A57}$$

and determines the invariant state

$$\rho^{(4)}_{1:2}=\frac{1}{4}\left(\begin{array}{ccc|ccc}1/3&0&0&0&-\sqrt{2}/3&0\\0&2/3&0&0&0&-\sqrt{2}/3\\0&0&1&0&0&0\\\hline 0&0&0&1&0&0\\-\sqrt{2}/3&0&0&0&2/3&0\\0&-\sqrt{2}/3&0&0&0&1/3\end{array}\right). \tag{A58}$$

The subspace $W^{(2)}_{1:2}$ has orthonormal basis

$$\begin{gathered}\frac{1}{\sqrt{3}}|V\rangle_A|(1,1)\rangle_B+\sqrt{\frac{2}{3}}|H\rangle_A|(2,0)\rangle_B,\\ \sqrt{\frac{2}{3}}|V\rangle_A|(0,2)\rangle_B+\frac{1}{\sqrt{3}}|H\rangle_A|(1,1)\rangle_B,\end{gathered} \tag{A59}$$

and determines the invariant state

$$\rho^{(2)}_{1:2}=\frac{1}{2}\left(\begin{array}{ccc|ccc}2/3&0&0&0&\sqrt{2}/3&0\\0&1/3&0&0&0&\sqrt{2}/3\\0&0&0&0&0&0\\\hline 0&0&0&0&0&0\\\sqrt{2}/3&0&0&0&1/3&0\\0&\sqrt{2}/3&0&0&0&2/3\end{array}\right). \tag{A60}$$

A generic invariant state is a convex combination of $\rho^{(4)}_{1:2}$ and $\rho^{(2)}_{1:2}$, depending on $f\in[0,1]$,

$$\begin{aligned}\rho^{(\mathrm{inv})}_{1:2}(f)&=f\rho^{(2)}_{1:2}+(1-f)\,\rho^{(4)}_{1:2}\\&=\frac{1}{12}\left(\begin{array}{ccc|ccc}3f+1&0&0&0&\sqrt{2}\,(3f-1)&0\\0&2&0&0&0&\sqrt{2}\,(3f-1)\\0&0&3\,(1-f)&0&0&0\\\hline 0&0&0&3\,(1-f)&0&0\\\sqrt{2}\,(3f-1)&0&0&0&2&0\\0&\sqrt{2}\,(3f-1)&0&0&0&3f+1\end{array}\right).\end{aligned} \tag{A61}$$

Case $n=3$ —The 6-dimensional space $\mathscr{H}_{A,1}\otimes\mathscr{H}_{B,3}$, corresponding to the case with one photon in Alice's system, and three in Bob's, is the direct sum of a 5- and a 3-dimensional invariant subspaces, namely,

$$\mathscr{H}_{A,1}\otimes\mathscr{H}_{B,3}=W^{(5)}_{1:3}\oplus W^{(3)}_{1:3}\,. \tag{A62}$$

The subspace $W^{(5)}_{1:3}$ is spanned by the orthonormal vectors

$$\begin{gathered}
|V\rangle_A|(3,0)\rangle_B, \\
\frac{\sqrt{3}}{2}|V\rangle_A|(2,1)\rangle_B - \frac{1}{2}|H\rangle_A|(3,0)\rangle_B, \\
\frac{1}{\sqrt{2}}\left(|V\rangle_A|(1,2)\rangle_B - |H\rangle_A|(2,1)\rangle_B\right), \\
\frac{1}{2}|V\rangle_A|(0,3)\rangle_B - \frac{\sqrt{3}}{2}|H\rangle_A|(1,2)\rangle_B, \\
-|H\rangle_A|(0,3)\rangle_B,
\end{gathered} \tag{A63}$$

and yields the invariant state

$$\rho^{(5)}_{1:3} = \frac{1}{5}\left(\begin{array}{cccc|cccc}
1/4 & 0 & 0 & 0 & 0 & -\sqrt{3}/4 & 0 & 0 \\
0 & 1/2 & 0 & 0 & 0 & 0 & -1/2 & 0 \\
0 & 0 & 3/4 & 0 & 0 & 0 & 0 & -\sqrt{3}/4 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
-\sqrt{3}/4 & 0 & 0 & 0 & 0 & 3/4 & 0 & 0 \\
0 & -1/2 & 0 & 0 & 0 & 0 & 1/2 & 0 \\
0 & 0 & -\sqrt{3}/4 & 0 & 0 & 0 & 0 & 1/4
\end{array}\right). \tag{A64}$$

The subspace $W^{(3)}_{1:3}$, spanned by the orthonormal vectors

$$\begin{gathered}
\frac{1}{2}|V\rangle_A|(2,1)\rangle_B + \frac{\sqrt{3}}{2}|H\rangle_A|(3,0)\rangle_B, \\
\frac{1}{\sqrt{2}}\left(|V\rangle_A|(1,2)\rangle_B + |H\rangle_A|(2,1)\rangle_B\right), \\
\frac{\sqrt{3}}{2}|V\rangle_A|(0,3)\rangle + \frac{1}{2}|H\rangle_A|(1,2)\rangle_B,
\end{gathered} \tag{A65}$$

determines the invariant state

$$\rho^{(3)}_{1:3} = \frac{1}{3}\left(\begin{array}{cccc|cccc}
3/4 & 0 & 0 & 0 & 0 & \sqrt{3}/4 & 0 & 0 \\
0 & 1/2 & 0 & 0 & 0 & 0 & 1/2 & 0 \\
0 & 0 & 1/4 & 0 & 0 & 0 & 0 & \sqrt{3}/4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\sqrt{3}/4 & 0 & 0 & 0 & 0 & 1/4 & 0 & 0 \\
0 & 1/2 & 0 & 0 & 0 & 0 & 1/2 & 0 \\
0 & 0 & \sqrt{3}/4 & 0 & 0 & 0 & 0 & 3/4
\end{array}\right). \tag{A66}$$

A generic invariant state is a convex combination of $\rho^{(5)}_{1:3}$ and $\rho^{(3)}_{1:3}$, depending on $f \in [0,1]$,

$$\begin{aligned}
&\rho^{(\mathrm{inv})}_{1:3}(f) = f\rho^{(3)}_{1:3} + (1-f)\,\rho^{(5)}_{1:3} \\
&= \frac{1}{60}\left(\begin{array}{cccc|cccc}
12f+3 & 0 & 0 & 0 & 0 & \sqrt{3}(8f-3) & 0 & 0 \\
0 & 4f+6 & 0 & 0 & 0 & 0 & 16f-6 & 0 \\
0 & 0 & 9-4f & 0 & 0 & 0 & 0 & \sqrt{3}(8f-3) \\
0 & 0 & 0 & 12(1-f) & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 12(1-f) & 0 & 0 & 0 \\
\sqrt{3}(8f-3) & 0 & 0 & 0 & 0 & 9-4f & 0 & 0 \\
0 & 16f-6 & 0 & 0 & 0 & 0 & 4f+6 & 0 \\
0 & 0 & \sqrt{3}(8f-3) & 0 & 0 & 0 & 0 & 12f+3
\end{array}\right).
\end{aligned} \tag{A67}$$

Appendix B. Feasibility ranges and bounds for the parameters Y and c

In this section we study in more details the properties of the parameters Q and c. In particular, we characterise their range and values on the invariant states.

Recall the definition of the gain Q,

$$Q := \mathrm{Tr}\left[\left(R_1^H \otimes R_0^V + R_0^H \otimes R_1^V\right)\rho_B\right] . \tag{B1}$$

Therefore, the values of Q depends on the eigenvalues of the operator $R_1^H \otimes R_0^V + R_0^H \otimes R_1^V$. As shown in equations (12) and (13), this operator is diagonal in the number basis,

$$R_1^H \otimes R_0^V + R_0^H \otimes R_1^V = \sum_{a,b=0}^{\infty} \left[\lambda_a (1-\lambda_b) + (1-\lambda_a)\lambda_b\right] |a\rangle_H\langle a| \otimes |b\rangle_V\langle b| \tag{B2}$$

$$= \sum_{a,b=0}^{\infty} (\lambda_a + \lambda_b - 2\lambda_a\lambda_b) |a\rangle_H\langle a| \otimes |b\rangle_V\langle b| . \tag{B3}$$

Recall that eigenvalues depends on the threshold value τ. To make our analysis more concrete we assume $\tau = 1$, which is close to the optimal value that maximises the asymptotic key rate. By inspection of the eigenvalues $\lambda_a + \lambda_b - 2\lambda_a\lambda_b$, we find that the smallest eigenvalue is zero, and is obtained when both $a = b \to \infty$. The largest eigenvalues is $1 - \lambda_0$ obtained when $a = 0$ and $b \to \infty$. This implies the following range for the gain:

$$Q \in (0, 1 - \lambda_0) . \tag{B4}$$

Recall that $Q_j = P_j Y_j$. We now consider the value of Y_j on the invariant state $\rho_{1:j}^{(\mathrm{inv})}$, with j photons on Bob side. Since the invariant states commute with the photon number, the reduced state on Bob side is proportional to the projector $\mathbb{P}_j$ into the subspace with j photons:

$$\mathrm{Tr}_A\left(\rho_{1:j}^{(\mathrm{inv})}\right) = \frac{\mathbb{P}_j}{\mathrm{Tr}\left(\mathbb{P}_j\right)} , \tag{B5}$$

where

$$\mathbb{P}_j = \sum_{a=0}^{j} |a\rangle_H\langle a| \otimes |j-a\rangle_V\langle j-a| , \tag{B6}$$

and

$$\mathrm{Tr}\left(\mathbb{P}_j\right) = j + 1 . \tag{B7}$$

We thus have

$$Y_j = \frac{1}{j+1} \sum_{a=0}^{j} \lambda_a + \lambda_{j-a} - 2\lambda_a\lambda_{j-a} . \tag{B8}$$

The behaviour of Y_j as a function of j is determined by the threshold value τ. If τ is sufficiently small, it is a decreasing function of j. For example, if we put $\tau = 1$, Y_j is decreasing for any $j \geqslant 1$. If instead we put $\tau = 2$, Y_j is decreasing for any $j \geqslant 4$. This means that with a careful choice of τ (not too large) and k (not too small), we can bound the gain Q as follows,

$$\sum_{j=0}^{k} P_j Y_j \leqslant Q \leqslant \sum_{j=0}^{k} P_j Y_j + \left(1 - \sum_{j=0}^{k} P_j\right) Y_{k+1} . \tag{B9}$$

Consider now the parameter c, defined in equation (28) as

$$c := \frac{1}{2}\mathrm{Tr}\left[\left(|H\rangle\langle H| \otimes R_0^H \otimes R_1^V + |V\rangle\langle V| \otimes R_1^H \otimes R_0^V\right)\rho_{AB}\right] . \tag{B10}$$

If we restrict to invariant states, we have

$$c = \mathrm{Tr}\left[\left(|H\rangle\langle H| \otimes R_0^H \otimes R_1^V\right)\rho_{AB}^{(\mathrm{inv})}\right] . \tag{B11}$$

Using the fact that $\mathrm{Tr}_B \rho_{AB} = I/2$ this further simplifies to

$$c = \frac{1}{2}\mathrm{Tr}\left[\left(R_0^H \otimes R_1^V\right)\rho_B^{(\mathrm{inv})}(H)\right], \tag{B12}$$

where $\rho_B^{(\mathrm{inv})}(H) = \langle H|\rho_{AB}^{(\mathrm{inv})}|H\rangle$.

To bound the range of feasibility of the parameter c on invariant state we shall look at the eigenvalues of the operator $R_0^H \otimes R_1^V$. We have

$$R_0^H \otimes R_1^V = \sum_{a,b=0}^{\infty} (1-\lambda_a)\,\lambda_b |a\rangle_H\langle a| \otimes |b\rangle_V\langle b|. \tag{B13}$$

As above, we assume $\tau = 1$. The smallest eigenvalues is zero and obtained in the limit $a \to \infty$. The largest eigenvalues is $1-\lambda_0$ and is obtained in the limit of $b \to \infty$. In conclusion, this yields the following feasibility interval for the parameter c on invariant states:

$$c \in \left(0, \frac{1-\lambda_0}{2}\right). \tag{B14}$$

Similarly, if we consider the invariant state $\rho_{1:j}^{(\mathrm{inv})}$ with j photons on Bob side, we obtain the following bounds on the attainable values of $c_{1:j}$:

$$\frac{1}{2}(1-\lambda_j)\,\lambda_0 \leqslant c_j\left(f_j\right) \leqslant \frac{1}{2}(1-\lambda_0)\,\lambda_j. \tag{B15}$$

We observe that with increasing j, the lower bound becomes smaller and the upper bound becomes larger, yielding the interval (B14) in the limit of $j \to \infty$.

This observation allows us to bound the value of c using a finite number of parameters $c_{1:j}$. We have

$$P_0 c_0 + \sum_{j=1}^{k} P_j c_j\left(f_j\right) \leqslant c \leqslant P_0 c_0 + \sum_{j=1}^{k} P_j c_j\left(f_j\right) + \left(1 - \sum_{j=1}^{k} P_j\right)\frac{1-\lambda_0}{2}. \tag{B16}$$

Appendix C. Properties of the invariant states

In this section we present in details the invariant states $\rho_{1:j}^{(\mathrm{inv})}$ such that there is one photon on Alice side, and j photons on Bob side. We compute the coefficients Y_j, c_j and the relative entropy $D[\rho_{1:j}^{(\mathrm{inv})}]$.

C.1. Vacuum sector: the invariant state $\rho_{1:0}^{(\mathrm{inv})}$

The simplest state corresponds to that with one photon on Alice side and zero photons on Bob side. The unique invariant state is

$$\rho_{1:0}^{(\mathrm{inv})} = \frac{I}{2} \otimes |0\rangle\langle 0| = \frac{|H\rangle\langle H| + |V\rangle\langle V|}{2} \otimes |0\rangle\langle 0|. \tag{C1}$$

For this subspace we have

$$Y_0 = 2\lambda_0(1-\lambda_0), \tag{C2}$$

$$c_0 = \frac{1}{2}\lambda_0(1-\lambda_0), \tag{C3}$$

and the QBER is, as one would have expected, $E_0 = 2c_0/Y_0 = 1/2$.

The relative entropy for the vacuum sector is

$$D[\rho_{1:0}] = 2\lambda_0(1-\lambda_0). \tag{C4}$$

C.2. One-photon sector: the invariant states $\rho_{1:1}^{(\mathrm{inv})}(f_1)$

Using the expression for the invariant state in equation (A55) we compute

$$\begin{aligned}
Y_1 &= \lambda_0 + \lambda_1 - 2\lambda_0\lambda_1\,, &\text{(C5)}\\
c_1 &= \mathrm{Tr}\big(|H\rangle\langle H| \otimes R_0^H \otimes R_1^V\big)\,\rho_{1:1}^{(\mathrm{inv})} &\text{(C6)}\\
&= \frac{2f_1+1}{6}\mathrm{Tr}\big(R_0^H \otimes R_1^V\big)\,|H\rangle\langle H| + \frac{1-f_1}{3}\mathrm{Tr}\big(R_0^H \otimes R_1^V\big)\,|V\rangle\langle V| &\text{(C7)}\\
&= \frac{2f_1+1}{6}\,(1-\lambda_1)\,\lambda_0 + \frac{1-f_1}{3}\,(1-\lambda_0)\,\lambda_1\,. &\text{(C8)}
\end{aligned}$$

Defining

$$A_1 := \frac{2f_1+1}{6}, \quad B_1 := \frac{4f_1-1}{6}, \quad C_1 := \frac{1-f_1}{3}, \tag{C9}$$

we compute the entropic quantities

$$\begin{aligned}
\mathrm{Tr}\left[\mathcal{G}\left(\rho_{1:1}^{(\mathrm{inv})}\right)\log\mathcal{G}\left(\rho_{1:1}^{(\mathrm{inv})}\right)\right] &= (A_1-B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log\left[(A_1-B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\right]\\
&\quad + (A_1+B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log\left[(A_1+B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\right]\\
&\quad + 2C_1\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log\left[C_1\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\right] &\text{(C10)}\\
&= (A_1-B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log(A_1-B_1)\\
&\quad + (A_1+B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log(A_1+B_1)\\
&\quad + 2\,(A_1+C_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\\
&\quad + 2C_1\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log C_1 &\text{(C11)}
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{Tr}\left[\mathcal{Z}\left(\mathcal{G}\left(\rho_{1:1}^{(\mathrm{inv})}\right)\right)\log\mathcal{Z}\left(\mathcal{G}\left(\rho_{1:1}^{(\mathrm{inv})}\right)\right)\right] &= F_-\log\frac{F_-}{2} + F_+\log\frac{F_+}{2} + 2C_1\lambda_0\,(1-\lambda_1)\log\left[C_1\lambda_0\,(1-\lambda_1)\right]\\
&\quad + 2C_1\lambda_1\,(1-\lambda_0)\log\left[C_1\lambda_1\,(1-\lambda_0)\right]\\
&= F_-\log F_- + F_+\log F_+ - 2A_1\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\\
&\quad + 2C_1\lambda_0\,(1-\lambda_1)\log\left[\lambda_0\,(1-\lambda_1)\right] + 2C_1\lambda_1\,(1-\lambda_0)\log\left[\lambda_1\,(1-\lambda_0)\right]\\
&\quad + 2C_1\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log C_1\,, &\text{(C12)}
\end{aligned}$$

where

$$F_\pm = A_1\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1) \pm \sqrt{A_1^2\,(\lambda_0-\lambda_1)^2 + 4B_1^2\lambda_0\lambda_1\,(1-\lambda_0)\,(1-\lambda_1)}\,. \tag{C13}$$

From them we finally obtain the relative entropy for the single-photon sector:

$$\begin{aligned}
D_{1;1} &= -F_+\log F_+ - F_-\log F_-\\
&\quad - 2C_1\lambda_0\,(1-\lambda_1)\log\left[\lambda_0\,(1-\lambda_1)\right] - 2C_1\lambda_1\,(1-\lambda_0)\log\left[\lambda_1\,(1-\lambda_0)\right]\\
&\quad + (A_1-B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log(A_1-B_1)\\
&\quad + (A_1+B_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log(A_1+B_1)\\
&\quad + 2A_1\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\\
&\quad + 2\,(A_1+C_1)\,(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\log(\lambda_0+\lambda_1-2\lambda_0\lambda_1)\,. &\text{(C14)}
\end{aligned}$$

C.3. Two-photon sector: the invariant states $\rho_{1:2}^{(\mathrm{inv})}(f_2)$

Consider the explicit form for the invariant state in equation (A61). Let us put

$$A_2 := \frac{3f_2+1}{12}\,,\ B_2 := \sqrt{2}\frac{3f_2-1}{12}\,,\ C_2 := \frac{1}{6}\,,\ D_2 := \frac{1-f_2}{4}\,. \tag{C15}$$

The first term in the expression of relative entropy is

$$\mathrm{Tr}\left[\mathcal{G}\left(\rho_{1:2}^{(\mathrm{inv})}\right)\log\mathcal{G}\left(\rho_{1:2}^{(\mathrm{inv})}\right)\right] = 2D_2\,(\lambda_0+\lambda_2-2\lambda_0\lambda_2)\log\left[D_2\,(\lambda_0+\lambda_2-2\lambda_0\lambda_2)\right] + G_+\log\frac{G_+}{2} + G_-\log\frac{G_-}{2} \tag{C16}$$

where

$$\begin{aligned} G_{\pm} = {} & A_2\left(\lambda_0+\lambda_2-2\lambda_0\lambda_2\right)+2C_2\lambda_1\left(1-\lambda_1\right) \\ & \pm\sqrt{\left[A_2\left(\lambda_0+\lambda_2-2\lambda_0\lambda_2\right)-2C_2\lambda_1\left(1-\lambda_1\right)\right]^2+8B_2^2\lambda_1\left(1-\lambda_1\right)\left(\lambda_0+\lambda_2-2\lambda_0\lambda_2\right)} \end{aligned} \tag{C17}$$

The second term in the expression of relative entropy is

$$\begin{aligned} \mathrm{Tr}\left[\mathcal{Z}\left(\mathcal{G}\left(\rho_{1:2}^{(\mathrm{inv})}\right)\right)\log\mathcal{Z}\left(\mathcal{G}\left(\rho_{1:2}^{(\mathrm{inv})}\right)\right)\right] = {} & 2D_2\lambda_0\left(1-\lambda_2\right)\log\left[D_2\lambda_0\left(1-\lambda_2\right)\right]+2D_2\lambda_2\left(1-\lambda_0\right)\log\left[D_2\lambda_2\left(1-\lambda_0\right)\right] \\ & +H_+\log\frac{H_+}{2}+H_-\log\frac{H_-}{2}+I_+\log\frac{I_+}{2}+I_-\log\frac{I_-}{2}\,, \end{aligned} \tag{C18}$$

where

$$H_{\pm}=A_2\left(1-\lambda_0\right)\lambda_2+C_2\lambda_1\left(1-\lambda_1\right)\pm\sqrt{\left[A_2\left(1-\lambda_0\right)\lambda_2-C_2\lambda_1\left(1-\lambda_1\right)\right]^2+4B_2^2\left(1-\lambda_0\right)\lambda_1\left(1-\lambda_1\right)\lambda_2}\,, \tag{C19}$$

$$I_{\pm}=A_2\left(1-\lambda_2\right)\lambda_0+C_2\lambda_1\left(1-\lambda_1\right)\pm\sqrt{\left[A_2\left(1-\lambda_2\right)\lambda_0-C_2\lambda_1\left(1-\lambda_1\right)\right]^2+4B_2^2\left(1-\lambda_2\right)\lambda_1\left(1-\lambda_1\right)\lambda_0}\,. \tag{C20}$$

We then have

$$\begin{aligned} D\left[\rho_{1:2}^{(\mathrm{inv})}\right] = {} & 2D_2\left[\left(\lambda_0+\lambda_2\left(1-2\lambda_0\right)\right)\log\left[\lambda_0+\lambda_2\left(1-2\lambda_0\right)\right]-\lambda_0\left(1-\lambda_2\right)\log\left[\lambda_0\left(1-\lambda_2\right)\right]\right. \\ & \left.-\lambda_2\left(1-\lambda_0\right)\log\left[\lambda_2\left(1-\lambda_0\right)\right]\right]+G_+\log G_++G_-\log G_- \\ & -H_+\log H_+-H_-\log H_--I_+\log I_+-I_-\log I_-\,. \end{aligned} \tag{C21}$$

For the two-photon sector we obtain

$$Y_2=\mathrm{Tr}\left[\mathcal{G}\left(\rho_{1:2}^{(\mathrm{inv})}\right)\right]=\frac{2}{3}\left(\lambda_0+\lambda_1+\lambda_2-2\lambda_0\lambda_2-\lambda_1^2\right), \tag{C22}$$

$$c_2=\mathrm{Tr}\big(|H\rangle\langle H|\otimes R_0^H\otimes R_1^V\big)\,\rho_{1:2}^{(\mathrm{inv})}=A_2\lambda_0\left(1-\lambda_2\right)+C_2\left(1-\lambda_1\right)\lambda_1+D_2\left(1-\lambda_0\right)\lambda_2\,. \tag{C23}$$

C.4. Three-photon sector: the invariant states $\rho_{1:3}^{(\mathrm{inv})}(f_3)$

Consider the invariant state in equation (A67). Defining

$$A_3:=\frac{12f_3+3}{60}\,,\;B_3:=\frac{\sqrt{3}\left(8f_3-3\right)}{60}\,,\;C_3:=\frac{4f_3+6}{60}\,,\;D_3:=\frac{16f_3-6}{60}\,,\;E_3:=\frac{9-4f_3}{60}\,,\;F_3:=\frac{12\left(1-f_3\right)}{60}\,. \tag{C24}$$

(note that $D_3=2B_3/\sqrt{3}$ and $F_3=3C_3-2A_3$) such a state reads

$$\rho_{1:3}^{(\mathrm{inv})}=\left(\begin{array}{cccc|cccc} A_3 & 0 & 0 & 0 & 0 & B_3 & 0 & 0 \\ 0 & C_3 & 0 & 0 & 0 & 0 & D_3 & 0 \\ 0 & 0 & E_3 & 0 & 0 & 0 & 0 & B_3 \\ 0 & 0 & 0 & F_3 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & F_3 & 0 & 0 & 0 \\ B_3 & 0 & 0 & 0 & 0 & E_3 & 0 & 0 \\ 0 & D_3 & 0 & 0 & 0 & 0 & C_3 & 0 \\ 0 & 0 & B_3 & 0 & 0 & 0 & 0 & A_3 \end{array}\right). \tag{C25}$$

From this expression we compute the relative entropy,

$$D\left[\rho_{1:3}^{(\mathrm{inv})}\right]=\left(\lambda_1\left(1-2\lambda_2\right)+\lambda_2\right)\left[\left(C_3-D_3\right)\log\left(C_3-D_3\right)+\left(C_3+D_3\right)\log\left(C_3+D_3\right)+2C_3\left(1+\log\left(\lambda_1\left(1-2\lambda_2\right)+\lambda_2\right)\right)\right] \tag{A66}$$

$$+2F_3\left[\left(\lambda_0+\lambda_3-2\lambda_0\lambda_3\right)\log\left(\lambda_0+\lambda_3-2\lambda_0\lambda_3\right)-\lambda_0\left(1-\lambda_3\right)\log\left(\lambda_0\left(1-\lambda_3\right)\right)-\lambda_3\left(1-\lambda_0\right)\log\left(\lambda_3\left(1-\lambda_0\right)\right)\right] \tag{A66}$$

$$+P_-\log P_-+P_+\log P_+-Q_-\log Q_--Q_+\log Q_+-R_-\log R_--R_+\log R_+-S_-\log S_--S_+\log S_+\,, \tag{C26}$$

where

$$
\begin{aligned}
P_{\pm} &= A_3\left(\lambda_0+\lambda_3-2\lambda_0\lambda_3\right)+E_3\left(\lambda_1+\lambda_2\left(1-2\lambda_1\right)\right)\\
&\quad \pm\sqrt{\left[A_3\left(\lambda_0+\lambda_3\left(1-2\lambda_0\right)\right)-E_3\left(\lambda_1+\lambda_2\left(1-2\lambda_1\right)\right)\right]^2+4B_3^2\left(\lambda_3+\lambda_0\left(1-2\lambda_3\right)\right)\left(\lambda_2+\lambda_1\left(1-2\lambda_2\right)\right)},\\
Q_{\pm} &= C_3\left(\lambda_1+\lambda_2\left(1-2\lambda_1\right)\right)\pm\sqrt{C_3^2\left(\lambda_1-\lambda_2\right)^2+4D_3^2\lambda_1\lambda_2\left(1-\lambda_1\right)\left(1-\lambda_2\right)},\\
R_{\pm} &= A_3\lambda_0\left(1-\lambda_3\right)+E_3\lambda_1\left(1-\lambda_2\right)\pm\sqrt{\left[A_3\lambda_0\left(1-\lambda_3\right)-E_3\lambda_1\left(1-\lambda_2\right)\right]^2+4B^2\lambda_0\lambda_1\left(1-\lambda_2\right)\left(1-\lambda_3\right)},\\
S_{\pm} &= A_3\left(1-\lambda_0\right)\lambda_3+E_3\left(1-\lambda_1\right)\lambda_2\pm\sqrt{\left[A_3(1-\lambda_0)\lambda_3-E_3(1-\lambda_1)\lambda_2\right]^2+4B^2(1-\lambda_0)(1-\lambda_1)\lambda_2\lambda_3}\,.
\end{aligned}
\tag{C27}
$$

Finally, for the three-photon sector we obtain

$$
Y_3=\mathrm{Tr}\left[\mathcal{G}\left(\rho_{1:3}^{(\mathrm{inv})}\right)\right]=\frac{1}{2}\left(\lambda_0+\lambda_1+\lambda_2+\lambda_3-2\lambda_0\lambda_3-2\lambda_1\lambda_2\right), \tag{C28}
$$

$$
c_3=\mathrm{Tr}\big(|H\rangle\langle H|\otimes R_0^H\otimes R_1^V\big)\,\rho_{1:3}^{(\mathrm{inv})}=A_3\lambda_0\left(1-\lambda_3\right)+C_3\lambda_1\left(1-\lambda_2\right)+E_3\left(1-\lambda_1\right)\lambda_2+F_3\left(1-\lambda_0\right)\lambda_3\,. \tag{C29}
$$

Appendix D. Invariant states under Gaussian noise

In this appendix we derive the invariant states for a communication channel characterised by loss η and Gaussian noise with variance N.

In the EB representation, first the lossy channel is applied to state (15), yielding

$$
\frac{\eta}{2}\left(|H\rangle\langle H|\otimes|H\rangle\langle H|+|V\rangle\langle V|\otimes|V\rangle\langle V|+|H\rangle\langle V|\otimes|H\rangle\langle V|+|V\rangle\langle H|\otimes|V\rangle\langle H|\right)+\frac{(1-\eta)}{2}I\otimes|0\rangle\langle 0|\otimes|0\rangle\langle 0|\,. \tag{D1}
$$

Second, a Gaussian-noise channel is applied to each mode belonging to Bob. Recall the action on each mode of this noise:

$$
\rho\to\int\frac{\mathrm{d}^2\alpha}{\pi N}\mathrm{e}^{-|\alpha|^2/N}\mathcal{D}\left(\alpha\right)\rho\mathcal{D}\left(\alpha\right)^{\dagger}, \tag{D2}
$$

where $\mathcal{D}(\alpha)$ is the displacement operator.

To compute the effect of this noise, we first apply independent displacements on the H and V modes, obtaining the state

$$
\begin{aligned}
&\frac{\eta}{2}\Big(|H\rangle\langle H|\otimes\mathcal{D}\left(\alpha\right)|H\rangle\langle H|\mathcal{D}\left(\alpha\right)^{\dagger}+|V\rangle\langle V|\otimes\mathcal{D}\left(\beta\right)|V\rangle\langle V|\mathcal{D}\left(\beta\right)^{\dagger}\\
&+|H\rangle\langle V|\otimes\mathcal{D}\left(\alpha\right)|H\rangle\langle V|\mathcal{D}\left(\beta\right)^{\dagger}+|V\rangle\langle H|\otimes\mathcal{D}\left(\beta\right)|V\rangle\langle H|\mathcal{D}\left(\alpha\right)^{\dagger}\Big)\\
&+\frac{(1-\eta)}{2}I\otimes\mathcal{D}\left(\alpha\right)|0\rangle\langle 0|\mathcal{D}\left(\alpha\right)^{\dagger}\otimes\mathcal{D}\left(\beta\right)|0\rangle\langle 0|\mathcal{D}\left(\beta\right)^{\dagger}\,.
\end{aligned}
\tag{D3}
$$

Finally, we will average over the displacement amplitudes α and β.

The result of the average is immediate for the terms of the kind $\mathcal{D}(\beta)|0\rangle\langle 0|\mathcal{D}(\beta)^{\dagger}$, where the displacement is applied on the vacuum state. These terms yield thermal states with N mean photon number,

$$
\rho_N=\frac{1}{N+1}\sum_{k=0}^{\infty}\left(\frac{N}{N+1}\right)^k. \tag{D4}
$$

Below we use the notation $\rho_N^{(H)}$ and $\rho_N^{(V)}$ to indicate a thermal state in horizontal or vertical mode of polarisation.

To compute the other terms, we exploit the expansion in number basis of the displacement operator:

$$
\langle m|\mathcal{D}\left(\alpha\right)|n\rangle=\sqrt{\frac{m!}{n!}}\left(-\alpha^*\right)^{n-m}e^{-|\alpha|^2/2}L_m^{(n-m)}\left(|\alpha|^2\right)\quad\text{for } m<n\,. \tag{D5}
$$

The only non-zero terms are:

$$\int \frac{d^2\alpha}{\pi N} e^{-|\alpha|^2/N} \langle 0|D(\alpha)|1\rangle\langle 1|D(\alpha)^\dagger|0\rangle = \frac{N}{(N+1)^2} \tag{D6}$$

and

$$\int \frac{d^2\alpha}{\pi N} e^{-|\alpha|^2/N} \langle m|D(\alpha)|1\rangle\langle 1|D(\alpha)^\dagger|m\rangle = \frac{1}{N+1}\left(\frac{N}{N+1}\right)^m \frac{m+N^2}{N(N+1)}. \tag{D7}$$

From this we define a probability distribution

$$p_m := \begin{cases} \frac{N}{(N+1)^2} & \text{if} \quad m = 0 \\ \frac{1}{N+1}\left(\frac{N}{N+1}\right)^m \frac{m+N^2}{N(N+1)} & \text{if} \quad m \geqslant 1 \end{cases} \tag{D8}$$

For the off-diagonal terms, the only non-zero contributions come from

$$\int \frac{\mathrm{d}^2\alpha}{\pi N} \mathrm{e}^{-|\alpha|^2/N} \langle m+1|D(\alpha)|1\rangle\langle 0|D(\alpha)^\dagger|n\rangle = \frac{1}{N+1}\left(\frac{N}{N+1}\right)^m \frac{\sqrt{m+1}}{N+1}. \tag{D9}$$

From this we define the coefficients

$$t_m := \frac{1}{N+1}\left(\frac{N}{N+1}\right)^m \frac{\sqrt{m+1}}{N+1}. \tag{D10}$$

In conclusion, the state after averaging over the noise realisation is

$$\begin{aligned} \rho_{AB}^{(\mathrm{inv})} = \frac{\eta}{2} \Bigg(& |H\rangle\langle H| \otimes \sum_m p_m |m_H\rangle\langle m_H| \otimes \rho_N^{(V)} + |V\rangle\langle V| \otimes \rho_N^{(H)} \otimes \sum_m p_m |m_V\rangle\langle m_V| \\ & + |H\rangle\langle V| \otimes \sum_m t_m |m+1\rangle\langle m| \otimes \sum_{m'} t_{m'} |m'\rangle\langle m'+1| + \mathrm{h.c.} \Bigg) \\ & + (1-\eta)\frac{I}{2} \otimes \rho_N^{(H)} \otimes \rho_N^{(V)}. \end{aligned} \tag{D11}$$

D.1. Invariant state in the vacuum sector for Gaussian noise

From equation (D11) we obtain the (not-normalised) invariant state with one photon on Alice side and the vacuum on Bob side:

$$P_0 \rho_{1:0}^{(\mathrm{inv})} = \frac{I}{2} \otimes \left(\eta \frac{p_0}{N+1} + (1-\eta)\left(\frac{1}{N+1}\right)^2 \right) |0\rangle\langle 0|. \tag{D12}$$

By computing the trace we obtain

$$P_0 = \eta \frac{p_0}{N+1} + (1-\eta)\left(\frac{1}{N+1}\right)^2. \tag{D13}$$

D.2. Invariant state in the one-photon sector for Gaussian noise

From equation (D11) we obtain the (not-normalised) invariant state with one photon on Alice side and one photon on Bob side.

In the basis $\{|HH\rangle, |HV\rangle, |VH\rangle, |VV\rangle\}$, it reads

$$P_1 \rho_{1:1}^{(\mathrm{inv})} \equiv \frac{\eta}{2} \left(\begin{array}{cc|cc} \frac{p_1}{N+1} & 0 & 0 & t_0^2 \\ 0 & \frac{p_0}{N+1}\frac{N}{N+1} & 0 & 0 \\ \hline 0 & 0 & \frac{p_0}{N+1}\frac{N}{N+1} & 0 \\ t_0^2 & 0 & 0 & \frac{p_1}{N+1} \end{array} \right) + \frac{1-\eta}{2}\left(\frac{1}{N+1}\right)^2 \frac{N}{N+1} \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right). \tag{D14}$$

The trace gives

$$P_1 = \frac{\eta}{N+1}\left(p_0 \frac{N}{N+1} + p_1 \right) + 2(1-\eta)\left(\frac{1}{N+1}\right)^2 \frac{N}{N+1}. \tag{D15}$$

D.3. Invariant state in the two-photon sector for Gaussian noise

From equation (D11) we obtain the (not-normalised) invariant state with one photon on Alice side and two photons on Bob side.

In the basis

$$\{|H;(2,0)\rangle, |H;(1,1)\rangle, |H;(0,2)\rangle, |V;(2,0)\rangle, |V;(1,1)\rangle, |V;(0,2)\rangle\} , \tag{D16}$$

the (not-normalised) invariant state has the following matrix representation:

$$P_2\rho_{1:2}^{(\mathrm{inv})} \equiv \frac{\eta}{2}\left(\begin{array}{ccc|ccc} \frac{p_2}{N+1} & 0 & 0 & 0 & t_0t_1 & 0 \\ 0 & \frac{p_1}{N+1}\frac{N}{N+1} & 0 & 0 & 0 & t_0t_1 \\ 0 & 0 & \frac{p_0}{N+1}\left(\frac{N}{N+1}\right)^2 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \frac{p_0}{N+1}\left(\frac{N}{N+1}\right)^2 & 0 & 0 \\ t_0t_1 & 0 & 0 & 0 & \frac{p_1}{N+1}\frac{N}{N+1} & 0 \\ 0 & t_0t_1 & 0 & 0 & 0 & \frac{p_2}{N+1} \end{array}\right) + \frac{1-\eta}{2}\left(\frac{1}{N+1}\frac{N}{N+1}\right)^2 I_6 , \tag{D17}$$

where I_6 is the 6×6 identity matrix.

By computing the trace we obtain

$$P_2 = \eta\left(\frac{p_0}{N+1}\left(\frac{N}{N+1}\right)^2 + \frac{p_1}{N+1}\frac{N}{N+1} + \frac{p_2}{N+1}\right) + 3\left(1-\eta\right)\left(\frac{1}{N+1}\frac{N}{N+1}\right)^2 . \tag{D18}$$

D.4. Invariant state in the three-photon sector for Gaussian noise

From equation (D11) we obtain the (not-normalised) invariant state with one photon on Alice side and three photons on Bob side.

In the basis

$$\{|H;(3,0)\rangle, |H;(2,1)\rangle, |H;(1,2)\rangle, |H;(0,3)\rangle, |V;(3,0)\rangle, |V;(2,1)\rangle, |V;(1,2)\rangle, |V;(0,3)\rangle\} , \tag{D19}$$

we have

$$\begin{aligned} P_3\rho_{1:3}^{(\mathrm{inv})} \equiv \frac{\eta}{2}&\left(\begin{array}{cccc|cccc} \frac{p_3}{N+1} & 0 & 0 & 0 & 0 & t_0t_2 & 0 & 0 \\ 0 & \frac{p_2}{N+1}\frac{N}{N+1} & 0 & 0 & 0 & 0 & t_1^2 & 0 \\ 0 & 0 & \frac{p_1}{N+1}\left(\frac{N}{N+1}\right)^2 & 0 & 0 & 0 & 0 & t_0t_2 \\ 0 & 0 & 0 & \frac{p_0}{N+1}\left(\frac{N}{N+1}\right)^3 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \frac{p_0}{N+1}\left(\frac{N}{N+1}\right)^3 & 0 & 0 & 0 \\ t_0t_2 & 0 & 0 & 0 & 0 & \frac{p_1}{N+1}\left(\frac{N}{N+1}\right)^2 & 0 & 0 \\ 0 & t_1^2 & 0 & 0 & 0 & 0 & \frac{p_2}{N+1}\frac{N}{N+1} & 0 \\ 0 & 0 & t_0t_2 & 0 & 0 & 0 & 0 & \frac{p_3}{N+1} \end{array}\right) \\ &+ \frac{1-\eta}{2}\left(\frac{1}{N+1}\right)^2\left(\frac{N}{N+1}\right)^3 I_8 , \end{aligned} \tag{D20}$$

where I_8 is the 8×8 identity matrix.

From the trace we obtain

$$P_3 = \eta\left(\frac{p_0}{N+1}\left(\frac{N}{N+1}\right)^3 + \frac{p_1}{N+1}\left(\frac{N}{N+1}\right)^2 + \frac{p_2}{N+1}\frac{N}{N+1} + \frac{p_3}{N+1}\right) + 4\left(1-\eta\right)\left(\frac{1}{N+1}\right)^2\left(\frac{N}{N+1}\right)^3 . \tag{D21}$$

This concludes all the properties for each invariant state up to the three-photon subspace.

ORCID iDs

Jasminder S Sidhu https://orcid.org/0000-0002-6167-8224
Saverio Pascazio https://orcid.org/0000-0002-7214-5685
Cosmo Lupo https://orcid.org/0000-0002-5227-4009

References

[1] Pirandola S *et al* 2020 *Adv. Opt. Photon.* **12** 1012

[2] Rivest R L, Shamir A and Adleman L 1978 *Commun. ACM* **21** 120

[3] Bernstein D 2009 Introduction to post-quantum cryptography *Post-Quantum Cryptography* (Springer) pp 1–14 (https://doi.org/10.1007/978-3-540-88702-7_1)

[4] Mosca M, Stebila D and Ustaoğlu B 2013 *Post-Quantum Cryptography* ed P Gaborit (Springer) pp 136–54

[5] Stebila D, Mosca M and Lütkenhaus N 2010 *Quantum Communication and Quantum Networking* ed A Sergienko, S Pascazio and P Villoresi (Springer) pp 283–96

[6] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* p 175 (available at: www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf)

[7] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[9] Ralph T C 1999 *Phys. Rev.* A **61** 010303

[10] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[11] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621

[12] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 *npj Quantum Inf.* **2** 16025

[13] Sidhu J S *et al* 2021 *IET Quantum Commun.* **2** 182

[14] Sidhu J S, Brougham T, McArthur D, Pousa R G and Oi D K L 2021 *Proc. SPIE* **11881** 1–8

[15] Wallnöfer J, Hahn F, Gündoğan M, Sidhu J S, Krüger F, Walk N, Eisert J and Wolters J 2022 *Commun. Phys.* **5** 169

[16] Islam T, Sidhu J S, Higgins B L, Brougham T, Vergoossen T, Oi D K L, Jennewein T and Ling A 2022 *PRX Quantum* **5** 030101

[17] Lu C-Y, Cao Y, Peng C-Z and Pan J-W 2022 *Rev. Mod. Phys.* **94** 035001

[18] Yin J *et al* 2017 *Science* **356** 1140

[19] Holzman I and Ivry Y 2019 *Adv. Quantum Technol.* **2** 1800058

[20] Karinou F *et al* 2018 *IEEE Photonics Technol. Lett.* **30** 650

[21] Dequal D, Vidarte L T, Rodriguez V R, Vallone G, Villoresi P, Leverrier A and Diamanti E 2021 *npj Quantum Inf.* **7** 3

[22] Jain N *et al* 2022 *Nat. Commun.* **13** 4740

[23] Qi B 2021 *Phys. Rev.* A **103** 012606

[24] Primaatmaja I W, Liang C C, Zhang G, Haw J Y, Wang C and Lim C C-W 2022 *Quantum* **6** 613

[25] Qi B, Lougovski P and Williams B P 2020 *Opt. Express* **28** 2276

[26] Chapman J C, Lukens J M, Qi B, Pooser R C and Peters N A 2022 *Opt. Express* **30** 15184

[27] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901

[28] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503

[29] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[30] Lin J, Upadhyaya T and Lütkenhaus N 2019 *Phys. Rev.* X **9** 041064

[31] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501

[32] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501

[33] Kanitschar F, George I, Lin J, Upadhyaya T and Lütkenhaus N 2023 *PRX Quantum* **4** 040306

[34] Lupo C and Ouyang Y 2022 *PRX Quantum* **3** 010341

[35] Bäuml S, García C P, Wright V, Fawzi O and Acín A 2022 arXiv:2303.09255

[36] Coles P J 2012 *Phys. Rev.* A **85** 042103

[37] Coles P J, Metodiev E M and Lütkenhaus N 2016 *Nat. Commun.* **7** 11712

[38] Winick A, Lütkenhaus N and Coles P J 2018 *Quantum* **2** 77

[39] Ma X-C, Sun S-H, Jiang M-S and Liang L-M 2013 *Phys. Rev.* A **88** 022339

[40] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev.* A **87** 062313

[41] Ferraro A, Olivares S and Paris M G A 2005 Gaussian states in continuous variable quantum information (Bibliopolis, Napoli) (arXiv:quant-ph/0503237)

[42] Cover T M and Thomas J A 2006 *Elements of Information Theory* vol 11, 2nd edn (Wiley)

[43] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043

[44] There are $j+1$ ways to distribute j photons on two polarisation modes. Therefore, the dimensions of Bob's Hilbert space are $\sum_{j=0}^{k}(j+1)=\frac{1}{2}(k+1)(k+2)$. Finally we need to multiply by 2, which is the dimension of Alice's Hilbert space.

[45] Aniello P, Lupo C and Napolitano M 2006 *Open Syst. Inf. Dyn.* **13** 415

[46] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501

[47] Renner R, Gisin N and Kraus B 2005 *Phys. Rev.* A **72** 012332

[48] Renner R 2007 *Nat. Phys.* **3** 645

[49] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504

[50] Leverrier A 2018 *J. Math. Phys.* **59** 042202

[51] Ghorai S, Diamanti E and Leverrier A 2019 *Phys. Rev.* A **99** 012311

[52] Kaur E, Guha S and Wilde M M 2021 *Phys. Rev.* A **103** 012412

[53] Cahill K E and Glauber R J 1969 *Phys. Rev.* **177** 1857

[54] Dong J, Wang T, He Z, Shi Y, Li L, Huang P and Zeng G 2023 *Entropy* **25** 1286

[55] Pirandola S, García-Patrón R, Braunstein S L and Lloyd S 2009 *Phys. Rev. Lett.* **102** 050503

[56] Matsuura T, Maeda K, Sasaki T and Koashi M 2021 *Nat. Commun.* **12** 252

[57] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev.* A **82** 012304

[58] Biedenharn L and Van Dam H 1965 *Quantum Theory of Angular Momentum: A Collection of Reprints and Original Papers* (*Perspectives in Physics: A Series of Reprint Collections*) (Academic)

[59] Artin M 2011 *Algebra* (Pearson Education)

[60] Sakurai J and Napolitano J 2017 *Modern Quantum Mechanics* (Cambridge University Press)

[61] Hall B 2016 *Lie Groups, Lie Algebras and Representations: An Elementary Introduction* (*Graduate Texts in Mathematics*) (Springer)