Asymmetric twin-field quantum key distribution

Federico Grasselli 1,3, Álvaro Navarrete 2 and Marcos Curty 3

1 Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225, Düsseldorf, Germany
2 El Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo, E-36310, Spain
3 Author to whom any correspondence should be addressed.

E-mail: federico.grasselli@hhu.de and anavarrete@com.uvigo.es

Keywords: asymmetric loss, twin-field quantum key distribution (QKD), analytical yields bounds, single-photon interference, decoy state, asymmetric QKD, intensity fluctuations

1. Introduction

Quantum Key Distribution (QKD) [1–5] allows two separated parties (typically called Alice and Bob) to generate identical bit strings with information-theoretic security. Due to the loss in the quantum channel connecting the parties, the performance of point-to-point QKD generally decreases with the distance, being unpractical for far-distance applications. Nonetheless, there have been remarkable efforts towards improving its range of applicability, such as the recent QKD experiments performed over 421 km of optical fiber [6] and over 1000 km of free space in satellite-to-ground links [7, 8]. However, even for the most outstanding far-distance experiments, the secret key rate turns out to be probably too low for commercial purposes. In fact, it has been proven that there exist fundamental limits on the secret key rate that can be extracted from such point-to-point configurations. These limits say that the secret key rate scales linearly with the transmittance of the quantum channel linking the parties, or in other words, that it decreases exponentially with the channel length [9, 10].

Quantum repeaters [11–13] and measurement-device-independent QKD (MDI-QKD) protocols with either quantum memories [14, 15] or with quantum non-demolition measurements [16] are possible theoretical solutions to overcome these limits. Unfortunately, in practice they require a technology that seems to be far from available in the near future. A more realistic solution was proposed recently by Lucamarini et al [17]. They devised an MDI-QKD type protocol—called twin-field QKD (TF-QKD)—in which the untrusted central node performs a single-photon interference measurement on the two incoming pulses, causing the key rate to scale with the square-root of the channel transmittance by using simple optical devices. Since the original proposal, several variants of the TF-QKD protocol were proven to be secure [18–23] and some of them were experimentally implemented [24–27].

Here we focus on the TF-QKD scheme proposed in [19]. In this protocol, Alice and Bob use the decoy-state technique to upper bound the detection probabilities associated to various photon-number states (called yields),...
which are subsequently used to obtain a bound on the phase error rate. Importantly, and in contrast to other solutions [18, 20, 22] which use a post-selection step based on the matching of a global phase, the scheme in [19] pre-selects the value of the global phase and thus it can provide a higher secret key rate. Moreover, the practical feasibility of this scheme has been recently demonstrated in [24, 25, 27]. A complete analysis of the symmetric scenario where both users use the same signal intensities and analytically estimate the yields using the same decoy intensity settings was performed recently in [28]. However, using the same set of intensities is an optimal strategy only when the quantum channels connecting the users to the central node have approximately the same transmittance. Thus, the bounds derived in [28] are not suitable for several real-world situations in optical networks where the distances between the users and the central node can be notoriously different. Furthermore, assuming that the parties employ exactly the same intensities is problematic even when the losses are symmetric. This is due to the fact that, typically, neither Alice nor Bob can ensure that their lasers emit pulses with a perfectly locked intensity. Instead, their intensities are typically fluctuating randomly and independently from the other party. For these reasons, the use of independent signal intensities and the derivation of yields bounds based on asymmetric decoy intensities is crucial for the protocol’s security in the presence of intensity fluctuations and for addressing asymmetric-loss scenarios. This idea has already been used to optimize the early MDI-QKD protocols based on two-photon interference in asymmetric-loss scenarios [29] and has recently been applied to another type of TF-QKD protocol in [30]. Moreover, decoy-state based protocols affected by intensity fluctuations have already been studied in [31–34].

In this paper, we address the above-mentioned problems by analyzing the performance of the TF-QKD scheme proposed in [19] in the presence of asymmetric losses and independent laser intensity fluctuations. For this, we derive new analytical bounds on the yields when Alice and Bob use asymmetric intensity settings. In particular, we consider the practical cases where each of Alice and Bob uses two, three and four decoy intensity settings, which are the most efficient solutions for covering long distances. In doing so, we show that the protocol can tolerate highly-asymmetric loss scenarios and is quite robust against intensity fluctuations, thus demonstrating its practicality for realistic network configurations.

The paper is organized as follows. In section 2 we summarize the TF-QKD protocol introduced in [19]. Then, in section 3 we analyze the performance of the aforementioned protocol under the assumption that Alice and Bob use the same signal and decoy intensities. In section 4 we present analytical bounds on the yields when the parties are allowed to use three independent decoy intensity settings. With the derived bounds, we investigate the protocol’s performance in section 5 when using independent signal and decoy intensities and in the presence of uncorrelated intensity fluctuations affecting the users’ lasers. Finally, in section 6 we present our conclusions. The paper includes also a few Appendixes with additional calculations, including the analytical bounds on the yields when each of Alice and Bob uses either two or four independent decoy intensity settings.

2. TF-QKD

2.1. Protocol description

In this section we briefly summarize the considered TF-QKD protocol [19]. As shown in figure 1, it consists in both Alice and Bob sending optical pulses through a quantum channel to an untrusted third party, Charles, who is in charge of performing joint measurements on the incoming pulses and announcing the results. The protocol is composed of the following seven steps.

![Figure 1. Scheme of the TF-QKD protocol proposed in [19]. After selecting the X or Z basis randomly, Alice and Bob send optical pulses through a quantum channel to an intermediate node controlled by the untrusted party Charles. In an honest implementation, Charles makes the incoming pulses interfere in a 50:50 beam splitter (BS) and publicly announces which of the two threshold detectors placed at the beam splitter output ports clicks. For the X basis, Alice and Bob send coherent states |±αa⟩ and |±αb⟩, respectively. For the Z basis, they send PRCS whose intensities are chosen at random from predefined sets.](image-url)
(i) Alice (Bob) chooses the X basis with probability \( p_x^A (p_x^B) \) and the Z basis with probability \( p_z^A = 1 - p_x^A \) (\( p_z^B = 1 - p_x^B \)). For the X basis, Alice (Bob) prepares an optical pulse in a coherent state \((-\bar{y}^{\kappa_A} \alpha_{\kappa_A}, \bar{y}^{\kappa_B} \alpha_{\kappa_B})\)), with \( \alpha_{\kappa_A}, \alpha_{\kappa_B} \) being a randomly chosen bit and \( \kappa_A, \kappa_B \in \mathbb{R} \), for simplicity. For the Z basis, Alice (Bob) prepares an optical pulse in a phase-randomized coherent state (PRCS) \( \rho_{\mu_k} (\nu_k) \) whose intensity \( \mu_k \) (\( \nu_k \)) is chosen from a set \( S_k = \{ \mu_k \} \), with probability \( p_k (p_k) \).

(ii) Both Alice and Bob send their pulses to an intermediate untrusted node, Charles, through optical channels with transmittances \( \eta_A \) and \( \eta_B \), respectively, in a synchronized manner.

(iii) Charles interferes the incoming pulses in a 50:50 beam splitter, followed by two threshold detectors associated with the constructive (detector \( D_c \)) and destructive (detector \( D_d \)) interference, respectively.

(iv) Charles announces the measurement outcomes \( k_c \) and \( k_d \) of the detectors \( D_c \) and \( D_d \), respectively, with \( k_c = 1 \) (\( k_d = 1 \)) corresponding to a click event and \( k_c = 0 \) (\( k_d = 0 \)) corresponding to a no-click event.

(v) Alice and Bob reveal a small fraction of the bits \( b_A (b_B) \) collected from those events when both parties chose the X basis and Charles reported a click only in one detector \( (k_c + k_d = 1) \) to estimate the bit error rate. Their raw keys consist on the remaining undisclosed bits. Also, Bob flips all the bits \( b_B \) collected when the click occurred in \( D_d \).

(vi) Alice and Bob publicly announce the intensities used in all the events when both chose the Z basis, and they use that information to estimate the phase error rate.

(vii) Alice and Bob apply error correction and privacy amplification techniques to their raw keys to distill two identical secret keys.

2.2. Secret key rate

The asymptotic secret key rate of the protocol described above is lower bounded by [19]

\[
R \geq \max \{ R_{\alpha}^\Omega, 0 \} + \max \{ R_{\beta}^\Omega, 0 \},
\]

(1)

where \( R_{\alpha}^\Omega \) is a lower bound on the secret key rate that Alice and Bob obtain from the event \( \Omega \in \{ \Omega_\alpha, \Omega_\beta \} \), being \( \Omega_\alpha \equiv (k_c = 1 \land k_d = 0) \) and \( \Omega_\beta \equiv (k_c = 0 \land k_d = 1) \). This lower bound is given by

\[
R_{\alpha}^\Omega = p_x^A p_x^B p_X (\Omega) [1 - \eta_x (e_{\alpha,\Omega,\alpha}) - \eta_\beta (e_{\alpha,\Omega,\beta})],
\]

(2)

where \( p_X (\Omega) = \sum_X \sum_{b_A} \sum_{b_B} p_X (\Omega |b_A, b_B) \) is the conditional probability that the event \( \Omega \) occurs given that Alice and Bob select the X basis, \( e_{\alpha,\Omega,\alpha} \) is an upper bound on the phase error rate, \( e_{\alpha,\Omega,\alpha} \) is the bit error rate, \( \eta_x(x) = -x \log_2(x) - (1 - x) \log_2(1 - x) \) is the binary entropy function. Note that in the asymptotic scenario, which is the scenario we consider in this work, we assume for simplicity that \( p_x^A = p_x^B = 1 \). The upper bound on the phase error rate, \( e_{\alpha,\Omega,\alpha} \), is given by [19]:

\[
e_{\alpha,\Omega,\alpha} = X_x \times p_X (\Omega) = \left\{ \sum_{n,m \in \mathbb{Z}^2} e_{n,m}(Y_{nm}) \right\} + \left\{ \sum_{n,m \in \mathbb{Z}^2+1} e_{n,m}(Y_{nm}) \right\}.
\]

(3)

where \( Y_{nm} = p_{\Omega}(\Omega | n, m) \) is the conditional probability of the event \( \Omega \) given that Alice and Bob sent \( n \) and \( m \) photons, respectively, \( e_{n,m} = e^{-\frac{1}{2} e_{\alpha,\Omega,\alpha} \alpha_n \alpha_m} \) and \( \mathbb{Z}^2 \) denotes the set of non-negative integers. The yields \( Y_{nm} \) are not experimentally observed but can be estimated through the decoy-state method [35–37] (see section 4). The bit error rate is given by

\[
e_{x,\Omega_\alpha} = X_x \times p_X (b_A = b_B | \Omega_\alpha) = \frac{1}{4} \sum_{b_A = b_B} p_X (\Omega | b_A, b_B),
\]

(4)

\[
e_{x,\Omega_\beta} = X_x \times p_X (b_A = b_B | \Omega_\beta) = \frac{1}{4} \sum_{b_A = b_B} p_X (\Omega | b_A, b_B).\]

(5)

The values of the bit error rate \( e_{x,\Omega} \) and of the probability \( p_X (\Omega) \) for a typical channel model are given in appendix A. These are the values we use in our simulations.

3. Symmetric intensities

When analyzing QKD protocols based on a central-node architecture, it is common to consider the symmetric scenario where the transmittances of the channels Alice–Charles and Bob–Charles are equal. This is, however, an
unrealistic assumption. In a practical scenario, the loss introduced by the quantum channel Alice-Charles could significantly differ from the loss in the channel Bob-Charles. In this case, the yields bounds obtained by using the decoy-state technique with the same intensity settings for Alice and Bob are not optimal anymore, i.e. they are looser than those obtained when the channel losses are instead symmetric.

Indeed, as already shown in MDI-QKD [29, 38–40], if Alice and Bob use the same intensity settings, they might be in a situation where it is convenient for them to symmetrize the channels losses by increasing the loss in one of the channels, in order to enhance the key rate. In doing so, the intensities of the pulses arriving at the central node are now of similar magnitude, which results in an improvement of the key rate. However, if they use different intensity settings, that is no longer the case [29, 38–40]. The same happens in the TF-QKD scheme introduced in [19]. This is clear from figure 2, where we plot the secret key rate assuming that Alice and Bob use the same set of two, three and four decoy intensities. The plots are obtained by using the analytical yields bounds for the symmetric-intensities scenario derived in [28]. The experimental parameters used for the simulations are given in table 1.

In figure 2, the key rate is optimized over the signal intensity $s_A = s_B$ and over the strongest decoy intensity (assumed to be equal for the two parties), while the other decoy intensities are fixed to the same values for both parties. As a matter of fact, after having observed that in the asymptotic scenario the optimal values of the weaker decoy intensities tend to be as small as possible regardless of the losses in the two channels, we fixed them to reasonably low values in the key rate optimization. More precisely: the weakest decoy intensities of Alice and Bob in the two-, three- and four-decoy case are fixed to $10^{-5}$; the second-to-the-weakest decoy intensities in the three- and four-decoy case are both fixed to $10^{-4}$; and the third-to-the-weakest decoy intensities in the four-decoy case are fixed to $10^{-3}$. The resulting key rate in both the three- and four-decoy case basically reproduces the rate one would obtain when optimizing even on the weaker decoy intensities [28]. In the two-decoy case, however, the key rate can be enhanced further by decreasing the value of the weakest decoy intensity, as explained in appendix E. The disadvantage of using symmetric signal and decoy intensity settings is clear in all the two-, three- and four-decoy cases, since increasing the loss in one of the channels can lead to an increase of the key rate in asymmetric-loss scenarios.

Furthermore, as already mentioned in the introduction, assuming that Alice and Bob are using exactly the same intensities is not realistic in most experimental implementations [25–27] due to the intensity fluctuations on the transmitters’ lasers. The effect of intensity fluctuations was already considered in [28] under the

![Figure 2. Contour lines for the secret key rate of the TF-QKD protocol introduced in [19] as a function of the channel loss in Alice’s and Bob’s sides, assuming that both Alice and Bob use the same signal and decoy intensities. Specifically, in (a)–(c) they use two, three and four decoy intensities each, respectively. The black dashed line encloses the loss region where the key rate overcomes the repeaterless bound [10]. We note that for several combinations of losses, it might be beneficial for the parties to increase the loss in one of the channels in order to make them more symmetric, thus maximizing the key rate. The experimental parameters used in the simulations are given in table 1.]
assumption that the fluctuations are correlated among the two parties, which is satisfied in the experiment reported in [24], but does not hold in general.

4. Asymmetric intensities

In order to enhance the protocol’s performance in the presence of asymmetric losses and to investigate uncorrelated intensity fluctuations, in this work we derive analytical upper bounds on the yields for the two-, three- and four-decoy scenarios with independent intensity settings for Alice and Bob. We note that the use of three or four decoy intensity settings is already enough to obtain a secret key rate close to the one that could be achieved with infinite decoy intensity settings [19, 28]. The derivation of the yields bounds for different decoy intensity settings is presented in appendix F (two-decoy scenario), appendix G (three-decoy scenario) and appendix H (four-decoy scenario). However, for illustration purposes, we present in this section the resulting upper bounds for the three-decoy case.

According to the TF-QKD protocol [19] summarized in section 2—when both parties choose the Z basis—Alice prepares a PRCS whose intensity belongs to the set \{\mu_0, \mu_1, \mu_2\}, with \mu_0 > \mu_1 > \mu_2. Analogously, Bob prepares a state whose intensity is instead drawn from the set \{\nu_0, \nu_1, \nu_2\}, with \nu_0 > \nu_1 > \nu_2. The key assumption of the decoy-state method is that the yields are independent of the chosen intensities and are thus subjected to the following four equality constraints:

\[
\tilde{Q}^{k,l} \equiv e^{i\nu_l + i\nu_l}Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \mu_k^k \nu_l^m \quad k, l \in \{0, 1, 2\},
\]

where \(Q^{k,l}\) is the gain in the Z basis given that Alice and Bob choose intensities \(\mu_k\) and \(\nu_l\), respectively. Note that we omit here and in what follows, for readability, the dependency of the variables with \(\Omega\). Being probabilities, the yields are additionally subjected to the inequality constraints:

\[
0 \leq Y_{nm} \leq 1 \quad \forall n, m.
\]

By properly combining the constraints (6) with a procedure similar to Gaussian elimination, we can obtain analytical upper bounds on the yields \(Y_{00}, Y_{11}, Y_{02}, Y_{12}, Y_{20}, Y_{21}, Y_{22}\) and \(Y_{31}\). The other yields are trivially upper bounded by one. The upper bounds are then inserted in the expression for the phase error rate (3), which can be rewritten as

\[
e_{z,11}^{\text{upper}} \times p_x(\Omega) = (c_{0,0} \sqrt{Y_{00}} + c_{0,2} \sqrt{Y_{02}} + c_{2,0} \sqrt{Y_{20}} + c_{2,2} \sqrt{Y_{22}} + c_{0,4} \sqrt{Y_{04}} + c_{4,0} \sqrt{Y_{40}} + \Delta_{\text{even}})^2
\]

\[
+ (c_{1,1} \sqrt{Y_{11}} + c_{1,3} \sqrt{Y_{13}} + c_{3,1} \sqrt{Y_{31}} + \Delta_{\text{odd}})^2,
\]

where \(\Delta_{\text{even}} = \sum_{(n,m) \in S_0} c_{n,m} \Delta_{\text{odd}} = \sum_{(n,m) \in S_0} c_{n,m}\), being \(S_0, S_1\) the subset of \(2\mathbb{N}^0, (2\mathbb{N}^0 + 1)\) which only includes the \((n, m)\) pairs of those yields that are being trivially upper bounded by one. In doing so, we can obtain a fully analytical expression of the asymptotic secret key rate (1). In what follows, we present the resulting upper bounds on the aforementioned yields (we refer the reader to appendix G for their derivation). For this, let’s consider the most general combination of the nine constraints (6):

\[
G_{av} = \sum_{i,j=0}^{2} c_{ij} \tilde{Q}^{ij}.
\]

For simplicity, in (9) and also below, we omit the explicit dependence of the coefficients \(c_{ij}\) with the value of \(\mu\) and \(\nu\). Then, we can obtain an upper bound on the yield \(Y_{00}\) by appropriately choosing the coefficients \(c_{ij}\) that appear in (9).

4.1. Upper bound on \(Y_{00}\)

An upper bound on the yield \(Y_{00}\) is given by

\[
Y_{00}^{U} = \frac{\mu_1 \mu_2 \nu_1 \nu_2 G_{00}}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)},
\]

where \(G_{00}\) is given by (9) by fixing the \(c_{ij}\) coefficients to those given in (G.54).
4.2. Upper bound on $Y_{11}$

An upper bound on the yield $Y_{11}$ is given by

$$Y_{11}^U = \frac{G_{11}(\mu_1 + \mu_2)(\nu_1 + \nu_2)}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)} + \frac{Y_{13}^U}{6}(\nu_1\nu_2 + \nu_0\nu_1 + \nu_2\nu_0) + \frac{Y_{13}^U}{12}(\mu_1\mu_2 + \mu_6\mu_1 + \mu_2\mu_0)
$$

$$= \left(\epsilon^{\nu_1} - \epsilon^{\nu_2} - \frac{\nu_1^2}{2} + \frac{\nu_2^2}{2}\right)(\nu_0^2 - \nu_2^2) + \left(\epsilon^{\nu_2} - \epsilon^{\nu_1} - \frac{\nu_1^2}{2} + \frac{\nu_2^2}{2}\right)(\nu_0^2 - \nu_0^2)
$$

$$- \left(\epsilon^{\nu_1} - \epsilon^{\nu_2} - \frac{\nu_1^2}{2} + \frac{\nu_2^2}{2}\right)(\mu_0^2 - \mu_2^2) + \left(\epsilon^{\nu_2} - \epsilon^{\nu_1} - \frac{\nu_1^2}{2} + \frac{\nu_2^2}{2}\right)(\mu_0^2 - \mu_0^2)
$$

$$= \frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}
$$

(11)

where $G_{11}$ is given by (9) by fixing the $c_{ij}$ coefficients to those given in (G.16), and where the upper bounds $Y_{13}^U$ and $Y_{13}$ are provided below.

4.3. Upper bound on $Y_{22}$

An upper bound on the yield $Y_{22}$ is given by

$$Y_{22}^U = \frac{4G_{22}}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}
$$

(12)

where $G_{22}$ is given by (9) by fixing the $c_{ij}$ coefficients to those given in (G.6).

4.4. Upper bounds on $Y_{02}$ and $Y_{04}$

The upper bounds on the yields $Y_{02}$ and $Y_{04}$ are given by, respectively,

$$Y_{02}^U = \frac{2G_{02}\mu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}
$$

(13)

and

$$Y_{04}^U = \frac{24G_{02}\mu_1\mu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)} + \frac{\nu_0\nu_1 + \nu_0\nu_2 + \nu_1\nu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}
$$

(14)

where $G_{02}$ is given by (9) by fixing the $c_{ij}$ coefficients to those given in (G.28).

4.5. Upper bounds on $Y_{20}$ and $Y_{40}$

The upper bounds on the yields $Y_{20}$ and $Y_{40}$ are given by, respectively,

$$Y_{20}^U = \frac{2G_{20}\nu_1\nu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}
$$

(15)

and

$$Y_{40}^U = \frac{24G_{20}\nu_1\nu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)} + \frac{\mu_0\mu_1 + \mu_0\mu_2 + \mu_1\mu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}
$$

(16)

where $G_{20}$ is given by (9) by fixing the $c_{ij}$ coefficients to those given in (G.36).

4.6. Upper bound on $Y_{13}$

An upper bound on the yield $Y_{13}$ is given by

$$Y_{13}^U = \frac{-6(\mu_1 + \mu_2)G_{13}}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)} + \frac{6\epsilon^{\nu_1}(\nu_0 - \nu_0) + \epsilon^{\nu_1}(\nu_0 - \nu_2) + \epsilon^{\nu_1}(\nu_2 - \nu_0)}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}
$$

$$\times \left[\epsilon^{\nu_2}(\mu_0^2 - \mu_2^2) + \epsilon^{\nu_1}(\mu_0^2 - \mu_2^2) + \epsilon^{\nu_1}(\mu_0^2 - \mu_0^2) - (\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)\right]
$$

(17)

where $G_{13}$ is given by (9) by fixing the $c_{ij}$ coefficients to those given in (G.43).
4.7. Upper bound on $Y_{31}$

An upper bound on the yield $Y_{31}$ is given by

$$Y_{31}^u = \frac{-6(\nu_1 + \nu_2)G_{31}}{(\mu_0 - \mu_2)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\mu_0 + \mu_1 + \mu_2) + 6[\epsilon \mu_2(\mu_0 - \mu_2) + \epsilon_0(\mu_0 - \mu_2)]}$$

$$\times [\epsilon_0(\nu_0^2 - \nu_0^2) + \epsilon_0(\nu_2^2 - \nu_2^2) - (\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_1 - \nu_2)]$$

where $G_{31}$ is given by (9) by fixing the $c_{ij}$ coefficients to those given in (G,47).

5. Simulations

In order to obtain the optimal secret key rate in the asymptotic-key regime, one needs to optimize it over the $X$ basis intensities $\epsilon_i^X$ and $\epsilon_i^G$, and over four, six or eight decoy intensities, depending on the number of decoys used by Alice and Bob. The key rate depends on the decoy intensities through the yields bounds derived in appendices F, H. For instance, for the three-decoy case analyzed in the previous section, we have that the vector $\mu$ depends on the decoy intensities through the yields bounds derived in appendices F, H. In order to fairly compare the simulation results with those of the symmetric scenario (figure 2), we use the same experimental parameters given by table 1 and we again fix the weaker decoy intensities to the same symmetric values for Alice and Bob, namely: $\mu_1 = \nu_1 = 10^{-5}$ for the two-decoy case, $\mu_1 = \nu_1 = 10^{-4}$ and $\mu_2 = \nu_2 = 10^{-5}$ for the three-decoy case, $\mu_0 = \nu_0 = 10^{-3}, \mu_1 = \nu_1 = 10^{-4}$ and $\mu_2 = \nu_2 = 10^{-5}$ for the four-decoy case. Thus the key rate is actually optimized over $\vec{\mu} = (\epsilon_0, \epsilon_0, \mu_0, \nu_0, \nu_1, \nu_2)$ in the two and three-decoy case, and over $\vec{\mu} = (\epsilon_0, \epsilon_0, \mu_0, \nu_0, \nu_1, \nu_2, \nu_3)$ in the four-decoy case. As explained in appendix H, note that in the four-decoy case, for convenience of our notation, $\mu_3$ and $\nu_3$ denote the strongest decoy intensities, i.e. we use the ordering $\mu_3 > \mu_0 > \mu_1 > \mu_2$ and $\nu_3 > \nu_0 > \nu_1 > \nu_2$. Although having fixed the weaker decoy intensities to the same values for both parties might seem restrictive in the asymmetric-loss scenario considered here, it is not as a matter of fact, we observed that the optimal values of the weaker decoy intensities (i.e. $\mu_1$ and $\nu_1$ in the two-decoy case, $\mu_1, \mu_2$ and $\nu_1, \nu_2$ in the three-decoy case, $\mu_0, \mu_1, \mu_2$ and $\nu_0, \nu_1, \nu_2$ in the four-decoy case) tend to be as low as possible, independently of the losses in Alice and Bob’s channels. We thus fixed them to symmetric low values that are reasonable from an experimental point of view [24, 25]. We additionally required every non-fixed decoy intensity to be at least one order of magnitude greater than any other fixed decoy intensity of the same scenario, due to practicality reasons in an experiment.

Fixing the decoy intensities reduces the computation complexity of the simulations, which is important since, in contrast to the MDI-QKD scenario [41], the key rate is not, in general, a convex function of $\vec{\mu}$ (see appendix C). This means that it is not possible to safely use time-efficient optimization methods, such as, for instance, the coordinate descent algorithm [42]. Our optimization is thus carried out by using the built-in global optimization algorithms of Wolfram Mathematica 11.0 [43].

In figure 3 we plot the asymptotic secret key rate as a function of the loss when the parties employ independent signal and decoy intensities, and each party uses either two (figure 3(a)), three (figure 3(b)) or four (figure 3(c)) decoy intensities. In all plots we observe that the improvement given by the use of independent intensities in the asymmetric-loss regions is significant. That is, introducing extra losses in one of the channels does not enhance the key rate any longer, in contrast to figures 2(a)–(c), where the intensities are instead symmetric for the two parties. Interestingly, this substantial improvement is mainly due to the independence of Alice’s and Bob’s signal intensities, while the independence of the decoy intensities plays a secondary role. In fact, the weaker dependence of the secret key rate on the asymmetry of Alice’s and Bob’s decoy intensities was recently investigated for specific scenarios and under some approximations in [44]. Nevertheless, allowing Alice and Bob to independently optimize both their signal and decoy intensities can almost double the secret key rate in extremely asymmetric-loss scenarios with respect to the case where only the signal intensities are independently optimized. This is particularly important when the estimation of the phase error rate is poor, like in the two-decoy case. It is also important to mention that, similarly to what happened in section 3, in the two-decoy scenario shown in figure 3(a) the secret key rate can be significantly enhanced by allowing the weakest decoy intensities of Alice and Bob to take lower values (see appendix E for further information). Additionally, by doing so, the trilobal pattern that can be observed in figure 3(a) almost disappears (see figure E1(a)), and the resulting figure looks similar to the three- and four-decoy cases.

The simulations suggest that in order to get a high key rate, it is important that the intensities of the pulses arriving at the central node are of similar magnitude (but not exactly the same), so that a cleaner interference occurs. This is clear from figure 4, where we plot the optimal signal and decoy intensities in the three-decoy scenario, as a function of the loss in the channel Alice-Charles and for fixed losses in the channel Bob-Charles.
We note that the optimal signal intensities \(a_A^2\) of Alice (solid lines) become greater than the correspondent ones \(a_B^2\) of Bob (dashed lines) as soon as the loss in Alice’s side is greater than in Bob’s side. The same happens for the decoy intensities \(\mu_0\) of Alice and \(\nu_0\) of Bob over which the key rate is optimized. Besides, when the losses at Alice’s and Bob’s sides are equal (symmetric scenario), the optimal values of both the signal and decoy intensities coincide for Alice and Bob, as expected. Moreover, the bottom plots in figure 4 show that the signal intensities arriving at the untrusted node, i.e. \(\eta_A a_A^2\) and \(\eta_B a_B^2\), are very similar to each other, while this is less pronounced in the case of the arriving decoy intensities. This is expected since the signal intensities are used to generate the raw keys. Thus it is optimal to minimize the bit error rate with a clean interference by tuning the signals so that the
arriving pulses have similar intensities. Conversely, the decoy pulses are used to indirectly estimate the phase error rate by upper bounding several yields. Because of the complex mathematical structure of such estimation problem, it is not true in general that the optimal phase error rate estimation is achieved by interfering arriving pulses of similar intensity. For completeness, the analogous figures with the optimal arrival intensities in the two- and four-decoy cases are shown in appendix D.

Apart from the general improvement in the secret key rate that the yields bounds derived in this work entail in asymmetric-loss scenarios, the bounds also allow to incorporate uncorrelated intensity fluctuations into the model, guaranteeing security in more realistic conditions. Figure 5 illustrates how taking into account the possible intensity fluctuations at the transmitters’ lasers affects the key rate. In particular, the dashed lines are obtained by optimizing the key rate over the signal and decoy intensities (we consider two, three and four decoy intensity settings) in the case of symmetric losses in the two quantum channels (figure 5(a)) and when Bob’s loss is fixed to 30 dB (figure 5(b)). We then apply uncorrelated fluctuations of fixed magnitudes (20%, 30% and 40%) on all the signal and decoy intensities of both parties and take the worst-case key rate (solid lines), i.e. the one minimized by letting each intensity independently fluctuate in its fluctuation range. For instance, by fixing the fluctuation magnitude to 30%, every signal and decoy intensities (\(\mu_A, \nu_A\) and \(\mu_0, \nu_0\)) intensities fluctuate independently in the following intervals centered on their optimal values (overlined terms): \(\mu_A, \nu_A \in [0.7 \, \mu_A, 1.3 \, \mu_A]\),

\(\mu_0, \nu_0 \in [0.7 \, \mu_0, 1.3 \, \mu_0]\).

Figure 5. Comparison between the secret key rate with optimal signal and decoys intensities (dashed lines) with the secret key rates affected by increasing intensity fluctuations (solid lines): 20%, 30% and 40% (brighter colors; right to left). The number of decoy intensity settings are two (green lines), three (red lines) and four (blue lines). In (a) the losses at Alice’s and Bob’s sides are equal (symmetric-loss scenario) while in (b) the loss in the channel Bob-Charles is fixed to 30 dB. We assume that the fluctuations affect each decoy intensity and each signal intensity of both parties in a independent way, i.e. the fluctuations are uncorrelated. The plots show that the TF-QKD protocol is quite robust against intensity fluctuations and that it can beat the repeaterless bound [10] even with 40% intensity fluctuations, when Alice and Bob use either three or four decoy intensities. The weaker decoy intensities have been fixed to the following values: \(\mu_1 = \nu_1 = 10^{-5}\) for two decoy intensity settings, \(\mu_2 = \nu_2 = 10^{-4}\) and \(\mu_3 = \nu_3 = 10^{-3}\) for three decoy intensity settings, and \(\mu_4 = \nu_4 = 10^{-2}\) for four decoy intensity settings. The other experimental parameters are given in table 1.
the abrupt change that the key rate suffers when considering intensity magnitude of 40% the decrease is still below 10 dB. Regarding the two-decoy case, it is important to mention against intensity the parties use either two, three or four decoy intensity settings. In contrast to previous results this, we have derived analytical bounds on the relevant yields that appear in the phase error rate expression when condition of asymmetric losses in the quantum channels linking Alice and Bob to the intermediate node. For this paper we have investigated the performance of the TF-QKD protocol proposed in

\[ \text{Figure 6. Optimal values of the signal intensities } \alpha_s^2 \text{ and } \alpha_d^2 \text{ (solid and dashed lines, respectively) as a function of the loss in the channel Alice–Charles for different levels of accuracy in the estimation of the yields, i.e. assuming that the parties have at their disposal two, three, four and infinite decoy intensity settings (bottom to top). The loss in the channel Bob–Charles is fixed to 30 dB. We observe that the optimal values of the signal intensities used to prepare states in the } X \text{ basis increase with the number of decoys used in the } Z \text{ basis. For the infinite decoy case, we assume that Alice and Bob can estimate the yields precisely and we used the theoretical values of the yields, which are given in appendix E. The experimental parameters used for the simulations are given in table 1.} \]

\[ \mu_s \in [0.7 \mu_s, 1.3 \mu_s] \text{ and } \nu_s \in [0.7 \nu_s, 1.3 \nu_s]. \] The secret key rate is then minimized over the fluctuations of all intensities constrained in their respective intervals. This effect has already been analyzed in [28] in the case of symmetric losses in the two quantum channels, where the fluctuations are, however, assumed to be perfectly correlated among the two users. This is a quite restrictive assumption, which only occurs in practice in certain experimental implementations based on the use of only one laser [24], but does not hold in general when two lasers are employed [25–27], even in a scenario with symmetric losses. In order to directly compare the effect of uncorrelated fluctuations with the results in [28], we fixed the weaker decoy intensities to exactly the same values used in the intensity fluctuations plots of [28], that is: \( \mu_1 = \nu_1 = 10^{-5} \) for two decoy intensity settings, \( \mu_2 = \nu_2 = 10^{-3} \) and \( \mu_1 = \nu_1 = 10^{-2} \) for three decoy intensity settings, and \( \mu_2 = \nu_2 = 10^{-3}, \mu_1 = \nu_1 = 10^{-2} \) and \( \mu_0 = \nu_0 = 10^{-1} \) for four decoy intensity settings. The figures suggest that the protocol is quite robust against intensity fluctuations even when the fluctuations are uncorrelated among the two parties. In fact, the maximal tolerable loss in the overall Alice–Bob channel for both the three and four-decoy scenarios decreases less than 2 dB for a 20% fluctuation of the signal and decoy intensities. Remarkably, even with a fluctuation magnitude of 40% the decrease is still below 10 dB. Regarding the two-decoy case, it is important to mention that the abrupt change that the key rate suffers when considering intensity fluctuations is due to a sudden change in the optimal decoy intensities (see appendix E). In particular, a sudden increase of the optimal decoy intensity directly implies a sudden increase of its fluctuation magnitude in absolute terms What concluded for figure 5(a) also applies to the asymmetric scenario shown in figure 5(b), where the loss in the channel Bob–Charles is fixed to 30 dB.

Finally, it is also interesting to observe how the optimal values for the signal intensities in the \( X \) basis depend on the estimation of the yields in the \( Z \) basis. Figure 6 shows the variation of the optimal \( \alpha_s^2 \) and \( \alpha_d^2 \) (\( X \) basis) as a function of the loss in the channel Alice–Charles (the loss in the channel Bob–Charles is fixed to 30 dB) for four different levels of accuracy in the estimation of the yields (\( Z \) basis). One can see that, when the yields’ estimation is not so tight, the \( X \) basis intensities \( \alpha_s^2 \) and \( \alpha_d^2 \) tend to be small in order to reduce the weights \( c_{n,m} \) of the yields appearing in (3) and compensate the yields’ loose upper bounds. By increasing the number of decoys in the \( Z \) basis and thus the tightness of the yields’ bounds as well as the number of relevant yields which are non-trivially upper bounded, the optimal values of the signal intensities in the \( X \) basis also increase, showing that the optimal signal intensities in the \( X \) basis depend on the number of decoy states used in the \( Z \) basis.

6. Conclusion

In this paper we have investigated the performance of the TF-QKD protocol proposed in [19] under the realistic condition of asymmetric losses in the quantum channels linking Alice and Bob to the intermediate node. For this, we have derived analytical bounds on the relevant yields that appear in the phase error rate expression when the parties use either two, three or four decoy intensity settings. In contrast to previous results [28], the bounds derived here are valid in the general scenario of independent intensity settings for the two parties, thus
optimizing the protocol’s performance in the presence of asymmetric losses in the two quantum channels. The simulations show a significant improvement on the secret key rate when using independent signal and decoy intensity settings in several asymmetric-loss scenarios. In particular, the secret key rate is never enhanced by adding fiber in one of the channels in order to symmetrize their losses. Furthermore, we have demonstrated the robustness of the protocol against uncorrelated intensity fluctuations on the transmitters’ lasers. These results clearly indicate the suitability of employing the considered TF-QKD protocol in practical QKD networks.

Acknowledgments

This work was supported by the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2017-88243-R, and the European Union’s Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 675662. AN gratefully acknowledges support from a FPU scholarship from the Spanish Ministry of Education.

Appendix A. Asymmetric channel model

Here, we present the expected values of the quantities required to calculate the lower bound on the secure key rate given by (1), in the case of the channel model described in [28]. The only difference is that here the losses in the channels Alice–Charles and Bob–Charles can differ and are modeled with a beamsplitter of transmittance \( \eta_A \) for Alice and \( \eta_B \) for Bob. Note that in this model the phase and polarization misalignments are independent from the channel’s transmittance. In order to model them, let \( \phi = \delta \pi \) be a phase shift at Bob’s side for some parameter \( \delta \) and let \( \theta_A (\theta_B) \) be the polarization shift angle at Alice’s (Bob’s) side. Finally, let \( p_d \) be the dark-count probability of Charles’ detectors, which we assume to be the same for both detectors. Let us define for convenience

\[
\gamma = \frac{\eta_A \alpha_A^2 + \eta_B \alpha_B^2}{2},
\]

\[
\chi (\phi, \theta) = \alpha_A \alpha_B \sqrt{\eta_A \eta_B} \cos(\phi) \cos(\theta),
\]

where \( \theta = \theta_A - \theta_B \). Then it can be shown that the bit error rate \( e_{X,\Omega} \) and the probability \( p_{X}(\Omega) \) are given by

\[
e_{X,\Omega} = \frac{e^{-\chi(\phi,\theta)} - (1 - p_d) e^{-\gamma}}{e^{-\chi(\phi,\theta)} + e^{\chi(\phi,\theta)} - 2(1 - p_d) e^{-\gamma}},
\]

and

\[
p_{X}(\Omega) = \frac{1}{2} (1 - p_d) (e^{-\chi(\phi,\theta)} + e^{\chi(\phi,\theta)}) e^{-\gamma} - (1 - p_d)^2 e^{-2\gamma}.
\]

Finally, the observed gains \( Q^{k,l} \) used by Alice and Bob to calculate the upper bounds on the yields \( Y_{nm} \) are just the probabilities that the event \( \Omega \) occurred when Alice and Bob chose intensities \( \mu_k \) and \( \nu_l \) for their PRCS. For this channel model it turns out that the gains read:

\[
Q^{k,l} = (1 - p_d) [e^{-\mu_k \eta_A + \nu_l \eta_B} I_0(\sqrt{\mu_k \nu_l \eta_A \eta_B} \cos(\theta))] - (1 - p_d) e^{-\mu_k \eta_A + \nu_l \eta_B}],
\]

where \( I_0(x) \) is the modified Bessel function of the first kind. Note that due to the balanced redistribution of the incoming photons in the central beam splitter, all the quantities presented here are actually independent of which detector clicked, i.e. they read the same for \( \Omega = \Omega_c, \Omega_d \).

In the simulations in the main text we assume that both the total polarization misalignment and phase mismatched are 2\%, that is, we select \( \theta = 2 \arcsin(\sqrt{0.02}) \) and \( \delta = 0.02 \).

Appendix B. Theoretical values for the yields

In order to check the quality of the analytical bounds on the yields, it is useful to compare them with their theoretical values, i.e. the values directly inferred from the channel model and that Alice and Bob would estimate when using an infinite number of decoy intensities. This is used, for instance, in figure 6. The theoretical values of the yields \( Y_{nm} \), according to the channel model presented in appendix A, are given by

\[
\text{New J. Phys.} 21 (2019) 113032
\]

F Grasselli et al
As one can notice from equations (1)–(5), the dependence of the key rate $R$ with its parameters is far from trivial. Here we numerically analyze the convexity of the key rate function $R(\vec{p})$, being $\vec{p}$ the vector of parameters to optimize by the users. It is well-known that this property is noticeably useful since convex functions permit to use efficient optimization methods, which are very important when the length of the vector $p$ increases. Unfortunately, it turns out that the key rate function is not convex in general, as shown in figure C1, therefore making many efficient optimization algorithms work poorly.

For instance, if we consider the coordinate descent algorithm [42], it is clear from the plots that it would not reach the optimal value if the starting point is any corner of the $\alpha_A$-$\alpha_B$ plane and the first variable to optimize is $\alpha_B$. Note that starting from a corner basically means that, in the first step, the algorithm has to optimize the darkest line in figure C1, for simplicity, we assume that Alice and Bob can estimate the yields precisely.

Note that the values of the yields are independent of the event $\Omega$.

Appendix C. Non-convexity of the secret key rate with respect to $\vec{p}$

As one can notice from equations (1)–(5), the dependence of the key rate $R$ with its parameters is far from trivial. Here we numerically analyze the convexity of the key rate function $R(\vec{p})$, being $\vec{p}$ the vector of parameters to optimize by the users. It is well-known that this property is noticeably useful since convex functions permit to use efficient optimization methods, which are very important when the length of $\vec{p}$ increases. Unfortunately, it turns out that the key rate function is not convex in general, as shown in figure C1, therefore making many efficient optimization algorithms work poorly.

For instance, if we consider the coordinate descent algorithm [42], it is clear from the plots that it would not reach the optimal value if the starting point is any corner of the $\alpha_A$-$\alpha_B$ plane and the first variable to optimize is $\alpha_B$. Note that starting from a corner basically means that, in the first step, the algorithm have to maximize the darkest line in figure C1, for simplicity, we assume that Alice and Bob can estimate the yields precisely.

That is, we assume they use efficient optimization algorithms, which are very important when the length of $\vec{p}$ increases. Unfortunately, it turns out that the key rate function is not convex in general, as shown in figure C1, therefore making many efficient optimization algorithms work poorly.

Note that the values of the yields are independent of the event $\Omega$.

Appendix D. Optimal signal and decoy intensities in the two- and four-decoy case

In figure D1 we show the arriving signal and decoy intensities for the two- and four-decoy case, corresponding to the optimal intensities employed in figures 3(a) and (c), respectively. Similarly to the three-decoy case (figure 4), it is optimal for the parties to prepare the intensities of their signal pulses such that the resulting intensities that arrive at Charles are of similar magnitude. This is true for both the two- and the four-decoy case.

Regarding the arriving strongest decoy intensity, the four-decoy scenario resembles again the three-decoy one, while the two-decoy case presents some differences. First of all, in contrast to the three- and four-decoy case, Bob’s optimal decoy intensity when the channel loss between Bob and Charles is fixed to 1 dB is constant and equal to the lowest allowed intensity value, i.e. $\nu_0 = 10^{-4}$ (see section 5 for the intensity range in which the...
key rate optimization is performed). Moreover, even Alice’s optimal decoy intensity is constant and equal to $10^{-4}$ at low losses, until it abruptly increases several orders of magnitude and behaves similarly to the three- and four-decoy case at higher losses. The reason for this peculiar behavior does not seem to lie in numerical optimization faults since it has been confirmed by different optimization routines. We also exclude that it is caused by suboptimal analytical bounds on the yields, since it remains present even when using linear programming in bounding the relevant yields. Instead, we believe that the effect of having an extremely low optimal decoy intensity at low losses followed by an abrupt increase at higher losses is inherent in the problem at hand. In particular, the fact that the parties have only two decoy intensity settings prevents them from obtaining sufficiently tight upper bounds on the yields. In other words, there exist relevant decoy intensities combinations for which the parties are unable to bound some yields in a non-trivial way, i.e. with a value strictly smaller than one. This is the reason why we explicitly present every yield upper bound, in the two-decoy case, as given by the minimum between the obtained analytical formula and 1 (see appendix F). The resulting yields bounds are non-smooth functions of the decoy intensities and so is the key rate. In turn, this can lead to discontinuities in the parameters over which the key rate is optimized, as observed.

Finally, we note that the loss thresholds where the discontinuities of the optimal decoy intensities take place, correspond to ‘crossing the border’ from one lobe to the other in the two-decoy contour plot (figure 3(a)), thus linking the peculiar shape of figure 3(a) to the above effect.

In order to have a better understanding of the special features arising in the two-decoy case discussed above, in appendix E we perform a further key rate optimization in this scenario, but allowing much smaller values for the intensity pulses.

**Appendix E. Allowing lower intensities in the two-decoy case**

In section 5 we observe a trilobal pattern affecting the two-decoy contour plot (figure 3(a)) and we then link it to the discontinuities affecting the optimal decoy intensities in appendix D. In particular, we observe that for both parties
the optimal strongest decoy intensity acquires the lowest possible value at low losses \((10^{-4})\), but then it experiences a sudden increase after a certain loss threshold. In appendix D we argue that such discontinuities are inherent in the problem of optimizing the key rate when the parties have only two decoy intensity settings at their disposal.

In order to check whether these effects are enhanced or caused by the experimentally-reasonable lower bound \((10^{-5})\) that we imposed on the decoy intensities, we rederive the same plots obtained for the two-decoy case in the main text, but this time we allow both the signal and the decoy intensities to acquire much smaller (but probably unpractical) values. In particular, we fix the lowest decoy intensities to \(\mu_1 = 10^{-10}\) for Alice and \(\nu_1 = 10^{-10}\) for Bob (opposed to \(\mu_1 = 10^{-5}\) and \(\nu_1 = 10^{-5}\) of the main text) and we optimize the key rate over the signal intensities \(\sigma_1^A \geq 10^{-10}\) and \(\sigma_1^B \geq 10^{-10}\) and over the decoy intensity \(\mu_0 > 10^{-10}\) for Alice and \(\nu_0 > 10^{-10}\) for Bob. In order to make a fair comparison, we use the same experimental parameters used in the main text, given in table 1. Because of the unpractical values allowed for both the signal and decoy intensities, this study is driven by theoretical interest and is not intended to replace the practical one presented in the main text and in appendix D.

In the new contour plots obtained in this scenario (figure E1) the trilobal pattern is barely visible. Indeed, figure E1 now resembles much more the correspondent figures of the three- and four-decoy case (figures 3(b) and (c)). This is readily explained by considering that now we perform the key rate optimization on a wider range of intensities, thus allowing the key rate contour lines to reach areas (i.e. loss combinations) where previously no positive key could be extracted.

Despite the trilobal shape being almost vanished, the optimal decoy intensities (figure E2) still show the same discontinuous behavior already observed in appendix D and acquire the lowest allowed value at low losses. This further confirms that this effect is not due to limits in the numerical optimization or in the analytical bounds, but it is rather inherent in the nature of the problem.

Finally, we also report the effect of intensity fluctuations on the optimized key rate (figure E3). Similarly to the contour plots, having a wider range of intensities in the key rate optimization not only allows one to obtain more non-zero key points, but also has the general effect of making the single plot points more robust to intensity fluctuations. For instance, the optimal values of the decoy intensities at low losses are—in this case—lower than those of the main text \((10^{-10} \text{ instead of } 10^{-4} \text{ and } 10^{-5})\), thus reducing the fluctuations in absolute terms.
Appendix F. Upper bounds on the yields with two decoy intensities

Here we derive analytical upper bounds on the yields for the two-decoy scenario with independent intensity settings for Alice and Bob. The three- and four-decoy cases follow a similar procedure and are presented in appendixes G and H, respectively.

In this scenario each party prepares PRCS with two possible intensities, namely \{μ₀, μ₁\} (with μ₀ > μ₁) for Alice and \{ν₀, ν₁\} (with ν₀ > ν₁) for Bob. The yields are subjected to the following four equality constraints:

\[ Q^{k,l} \equiv e^{\nu_l + \nu_k} Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \mu_k^{n} \nu_l^{m} \quad k, l \in \{0, 1\}, \]

and to the inequality constraints given in (7).

Below we derive analytical upper bounds on the yields \(Y_{00}, Y_{11}, Y_{02}\) and \(Y_{20}\), while the other yields are trivially upper bounded by one. This means that we can rewrite equation (3) as

\[ e^{\text{up}} \times p_\chi(\Omega) = (e_{0,0} \sqrt{Y_{00}} + e_{0,1} \sqrt{Y_{11}} + e_{0,2} \sqrt{Y_{20}} + \Delta_{\text{even}})^2 + (e_{1,1} \sqrt{Y_{11}} + \Delta_{\text{odd}})^2, \]

where \(\Delta_{\text{even}} = \sum_{(n,m) \in S_0} c_{n,m} \Delta_{\text{odd}} = \sum_{(n,m) \in S_1} c_{n,m}\), being \(S_0(S_1)\) the subset of \(2N_0(2N_0 + 1)\) which only includes the \((n, m)\) pairs of those yields that are being trivially upper bounded by one.

Figure E2. Arriving signal (a) and strongest decoy (b) intensity both for Alice (solid lines) and Bob (dashed lines). The lowest allowed signal and decoy intensities are set to \(10^{-10}\). The corresponding optimized key rate is given in figure E1(a), where each party has independently two decoy intensities. Like in the case with the higher allowed intensities (figure D1(a)), we still observe discontinuities for the arriving strongest decoy intensities, confirming that the effect is intrinsic to the optimization problem.

Figure E3. Comparison between the secret key rate with optimal signal and decoy intensities (dashed lines) with the secret key rates affected by increasing intensity fluctuations (solid lines): 20%, 30% and 40% (brighter colors; right to left), when the parties have two decoy intensity settings each. In (a) the losses at Alice’s and Bob’s sides are equal (symmetric-loss scenario) while in (b) the loss in the channel Bob-Charles is fixed to 30 dB. We assume that the fluctuations affect each decoy intensity and each signal intensity of both parties in an independent way, i.e. the fluctuations are uncorrelated. The lowest allowed signal and decoy intensities are set to \(10^{-10}\). The plots show that the robustness of the TF-QKD protocol is increased with respect to the case analyzed in the main text (figure 5, where instead the weakest decoy intensities are set to \(μ_1 = ν_1 = 10^{-5}\)).

Appendix F. Upper bounds on the yields with two decoy intensities

Here we derive analytical upper bounds on the yields for the two-decoy scenario with independent intensity settings for Alice and Bob. The three- and four-decoy cases follow a similar procedure and are presented in appendixes G and H, respectively.

In this scenario each party prepares PRCS with two possible intensities, namely \(\{μ_0, μ_1\}\) (with \(μ_0 > μ_1\)) for Alice and \(\{ν_0, ν_1\}\) (with \(ν_0 > ν_1\)) for Bob. The yields are subjected to the following four equality constraints:

\[ Q^{k,l} \equiv e^{\nu_l + \nu_k} Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \mu_k^{n} \nu_l^{m} \quad k, l \in \{0, 1\}, \]

and to the inequality constraints given in (7).

Below we derive analytical upper bounds on the yields \(Y_{00}, Y_{11}, Y_{02}\) and \(Y_{20}\), while the other yields are trivially upper bounded by one. This means that we can rewrite equation (3) as

\[ e^{\text{up}} \times p_\chi(\Omega) = (e_{0,0} \sqrt{Y_{00}} + e_{0,1} \sqrt{Y_{11}} + e_{0,2} \sqrt{Y_{20}} + \Delta_{\text{even}})^2 + (e_{1,1} \sqrt{Y_{11}} + \Delta_{\text{odd}})^2, \]

where \(\Delta_{\text{even}} = \sum_{(n,m) \in S_0} c_{n,m} \Delta_{\text{odd}} = \sum_{(n,m) \in S_1} c_{n,m}\), being \(S_0(S_1)\) the subset of \(2N_0(2N_0 + 1)\) which only includes the \((n, m)\) pairs of those yields that are being trivially upper bounded by one.
F.1. Upper bound on $Y_{11}$
Consider the following combination of gains:

$$G_{11} = \tilde{Q}_{1}^{0,0} + \tilde{Q}_{1}^{1,1} - (\tilde{Q}_{1}^{0,1} + \tilde{Q}_{1}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_0^n - \mu_0^n)(\nu_0^m - \nu_1^m). \quad (F.3)$$

The subscript in $G_{11}$ indicates the yield that is going to be bounded with this combination of gains, that is, $Y_{11}$ in this case. In (F.3) the coefficients of the yields $Y_{0m}$ and $Y_{m0}$ for any $n$ and $m$, are identically zero. Thus (F.3) can be rewritten as:

$$G_{11} = Y_1(\mu_0 - \mu_1)(\nu_0 - \nu_1) + \sum_{n+m=2}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_0^n - \mu_0^n)(\nu_0^m - \nu_1^m). \quad (F.4)$$

Note that $Y_{11}$ is now the yield with the ‘highest weight’ in (F.4) since it has the largest coefficient. All the yields’ bounds presented in this work follow the same philosophy. A valid upper bound for $Y_{11}$ is obtained considering the worst-case scenario for the other yields, taking into account that (7) holds. Since all the yields’ coefficients carry the same sign in (F.4), the yield $Y_{11}$ is maximal when all the other yields are minimal. Thus the upper bound on $Y_{11}$ is extracted by setting all the other yields to zero in (F.4):

$$Y_{11}^U = \min \left \{ \frac{G_{11}}{(\mu_0 - \mu_1)(\nu_0 - \nu_1)}, 1 \right \}, \quad (F.5)$$

where $G_{11}$ is defined in (F.3).

By taking the minimum between the analytical upper bound and 1 we enforce the validity of the inequality constraints (7). This is of particular importance in the two-decoys scenario since there exist relevant combinations of decoy intensities for which the analytical upper bounds would produce a value greater than one. As a consequence, we achieve a tighter estimation of the phase error rate (3) and thus a better performance of the key rate. However, the use of expressions like (F.5) can also affect the smoothness—i.e. the continuity of the first derivative—of the key rate as a function of the decoy intensities. This in turn can lead to discontinuities in the optimal decoy intensities as a function of the losses, as pointed out in appendices D and E.

F.2. Upper bound on $Y_{02}$
Consider the following combination of gains:

$$G_{02} = \mu_1 \tilde{Q}_{0}^{0,0} + \mu_0 \tilde{Q}_{1}^{1,1} - \mu_1 \tilde{Q}_{1}^{0,1} - \mu_0 \tilde{Q}_{1}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_1^n - \mu_0^n)(\nu_0^m - \nu_1^m). \quad (F.6)$$

In (F.6) the coefficients of the yields $Y_{00}$ and $Y_{1m}$ are identically zero. Thus (F.6) can be rewritten as:

$$G_{02} = \sum_{m=1}^{\infty} \frac{Y_{0m}}{m!} (\mu_1 - \mu_0)(\nu_0^m - \nu_1^m) + \sum_{m=1}^{\infty} \frac{Y_{nm}}{m!} \mu_0 \mu_1 (\mu_0^{n-1} - \mu_1^{n-1})(\nu_0^m - \nu_1^m). \quad (F.7)$$

Like in the derivation of the upper bound on $Y_{11}$ in the previous subsection, a valid upper bound for the generic $Y_{0m}$ (where $m \geq 1$ is fixed) is obtained by considering the worst-case scenario for the remaining yields in (F.7).

More specifically, $Y_{0m}$ is maximal when the yields whose coefficient has the same sign as the $Y_{0m}$’s coefficient are minimal, and the yields whose coefficient has opposite sign to the $Y_{0m}$’s coefficient are maximal. Recalling the constraint (7), this means setting all the yields of the form $Y_{0m}$ (for $m' = m$) to zero and $Y_{nm}$, with $n \geq 2$ and $m \geq 1$ to 1 in (F.7). In so doing, after summing the terms we obtain:

$$G_{02} = \frac{Y_{0m}^{Um}}{m!} (\mu_1 - \mu_0)(\nu_0^m - \nu_1^m) + (e^{\nu_0} - e^{\nu_1})(\mu_1 e^{\nu_0} - \mu_0 e^{\nu_1} - \mu_1 + \mu_0), \quad (F.8)$$

which leads to the following upper bound on $Y_{0m}$ for $m \geq 1$:

$$Y_{0m}^{U} = \min \left \{ \frac{m!}{(\mu_1 - \mu_0)(\nu_0^m - \nu_1^m)} [G_{02} - (e^{\nu_0} - e^{\nu_1})(\mu_0 - \mu_1 + \mu_1 e^{\nu_0} - \mu_0 e^{\nu_1})], 1 \right \}. \quad (F.9)$$

By fixing $m = 2$, one gets the desired upper bound on $Y_{02}$.

F.3. Upper bound on $Y_{20}$
In a similar fashion, we consider the following combination of gains:

$$G_{20} = \nu_1 \tilde{Q}_{0}^{0,0} + \nu_0 \tilde{Q}_{1}^{1,1} - \nu_1 \tilde{Q}_{1}^{0,1} - \nu_0 \tilde{Q}_{1}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\nu_1^n - \nu_0^n)(\nu_0^m - \nu_1^m). \quad (F.10)$$

In (F.10) the coefficients of the yields $Y_{01}$ and $Y_{m0}$ are identically zero. Thus (F.10) can be rewritten as:

$$G_{20} = \sum_{n=1}^{\infty} \frac{Y_{0n}}{n!} (\mu_0^n - \mu_0^n)(\nu_1 - \nu_0) + \sum_{n=1}^{\infty} \frac{Y_{n0}}{n!} \nu_0 \nu_1 (\mu_0^n - \mu_0^n)(\nu_0^{n-1} - \nu_1^{n-1}). \quad (F.11)$$
A valid upper bound on \( Y_{00} \) (with \( n \geq 1 \) fixed) is obtained by setting to zero the yields whose coefficient has the same sign as the \( Y_{00} \)’s coefficient, and by setting to 1 the yields whose coefficient has opposite sign to the \( Y_{00} \)’s coefficient. In the case of (F.11), this means setting \( Y_{i'0} \) (with \( n' = n \)) to zero and \( Y_{nm} \) with \( n \geq 1 \) and \( m \geq 2 \), to one. In this way we obtain:

\[
G_{20} = \frac{Y_{00}^{(m_0)}}{n!} (\mu_0 - \mu_1) (v_1 - v_0) + (e^{\nu_0} - e^{\nu_1}) (v_1 e^{\nu_0} - v_0 e^{\nu_1} - v_1 + v_0),
\]

which leads to the following upper bound on \( Y_{00} \), for \( n \geq 1 \):

\[
Y_{00}^U = \min \left\{ n! \left[ (v_1 - v_0) (\mu_0 - \mu_1) (v_0 - v_1) + (e^{\nu_0} - e^{\nu_1}) (v_1 e^{\nu_0} - v_0 e^{\nu_1} - v_1 + v_0) \right] \right\},
\]

By fixing \( n = 2 \), one gets the desired upper bound on \( Y_{20} \).

### F.4. Upper bound on \( Y_{00} \)

Consider the following combination of gains:

\[
G_{00} = \mu_1 v_1 Q_{00}^0 + \mu_0 v_0 Q_{00}^1 - \mu_1 v_0 Q_{00}^1 - \mu_0 v_1 Q_{00}^0 = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_0 - \mu_1) (v_0 - v_1). \tag{F.14}
\]

In (F.14) the coefficients of the yields \( Y_{nm} \) and \( Y_{n1} \), for any \( n \) and \( m \), are identically zero. Thus (F.14) can be rewritten as:

\[
G_{00} = Y_{00} (\mu_1 - \mu_0) (v_1 - v_0) + v_0 v_1 (\mu_1 - \mu_0) \sum_{m=2}^{\infty} \frac{Y_{0m}}{m!} (\nu_0^{m-1} - \nu_0^{m-1}) + \mu_0 \mu_1 (v_1 - v_0) \times \sum_{n=2}^{\infty} \frac{Y_{n0}}{n!} (\mu_0^{n-1} - \mu_1^{n-1}) + \mu_0 \mu_1 v_0 v_1 \sum_{n,m=2}^{\infty} \frac{Y_{nm}}{n!m!} (\nu_0^{m-1} - \nu_1^{m-1}). \tag{F.15}
\]

As usual we extract an upper bound on \( Y_{00} \) by setting to their lowest value the yields whose coefficient has the same sign as the \( Y_{00} \)’s coefficient (which correspond to the \( Y_{nm} \) with \( n, m \geq 2 \)), and by setting to their maximum value the yields whose coefficient has opposite sign to the \( Y_{00} \)’s coefficient (which correspond to \( Y_{0m} \) and \( Y_{0n} \)). We know that every yield is trivially bounded by (7). However, in order to derive a tighter bound on \( Y_{00} \) we employ non-trivial bounds for all the yields \( Y_{nm} \) with \( n + m \leq 4 \) in (F.15). The upper bound on \( Y_{00} \) thus reads:

\[
Y_{00}^U = \min \left\{ \frac{G_{00}}{\mu_0 - \mu_1} (v_0 - v_1) + \frac{1}{2} (Y_{00}^U v_0 v_1 + Y_{20}^U \mu_0 \mu_1) + \frac{1}{6} (Y_{00}^U v_0 v_1 (v_0 + v_1) + Y_{00}^U \mu_0 \mu_1 (\mu_0 + \mu_1)) \right\}
\]

\[
+ \frac{1}{24} [Y_{04}^U v_0 v_1 (v_0 + v_1 + v_0 + v_1) + Y_{00}^U \mu_0 \mu_1 (\mu_0 + \mu_1 + \mu_0 \mu_1 + \mu_0 \mu_1)]
\]

\[
- \frac{v_0}{v_1} \left( e^{\nu_0} - 1 - \frac{\nu_0^2}{2} \right) \left( \frac{\nu_0}{v_0} - \frac{\nu_0^2}{6} \right) + \frac{v_0}{v_1} \left( e^{\nu_1} - 1 - \frac{\nu_1^2}{2} \right) \left( \frac{\nu_1}{v_1} - \frac{\nu_1^2}{6} \right)
\]

\[
- \frac{v_0}{v_1} \left( e^{\nu_0} - 1 - \frac{\nu_0^2}{2} \right) \left( \frac{\nu_0}{v_0} - \frac{\nu_0^2}{6} \right) + \frac{v_0}{v_1} \left( e^{\nu_1} - 1 - \frac{\nu_1^2}{2} \right) \left( \frac{\nu_1}{v_1} - \frac{\nu_1^2}{6} \right)
\]

\[
= \left\{ 1 + \frac{4}{\mu_0^2 - \mu_1^2} (v_0^2 - v_1^2) [G_{11} - (e^{\nu_0} - e^{\nu_1}) (e^{\nu_0} - e^{\nu_1})] \right\}.
\]

We also note that the upper bounds derived on \( Y_{00} \) and \( Y_{04} \) in equations (F.9) and (F.13) could be used to improve the estimation of the phase error rate given in by (3). However, it can be shown that the resulting improvement in the secret key rate is very small in this case and we neglect it for simplicity.

### Appendix G. Upper bounds on the yields with three decoy intensities

Here we derive the upper bounds on the yields \( Y_{00} \), \( Y_{11}, Y_{02}, Y_{20} \), \( Y_{22}, Y_{13}, Y_{31}, Y_{04} \) and \( Y_{40} \) presented in section 4.
G.1. Upper bound on \( Y_{22} \)
We consider the most general combination of the nine constraints (6):
\[
G_{22} = \sum_{i,j=0}^{2} c_{ij} \mathcal{Q}_{ij} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \left[ \sum_{i,j=0}^{2} c_{ij} \mu_{i}^{n} \nu_{j}^{m} \right],
\]  
(G.1)
and require that the terms proportional to \( Y_{nm} \), \( Y_{m} \) and \( Y_{n} \) are removed in the combination. We achieve this by imposing proper conditions on the real coefficients \( c_{ij} \):

- **Y_{0} removed:**
  \[
  \sum_{i=0}^{2} \mu_{i}^{0} \left( \sum_{j=0}^{2} c_{ij} \right) = 0 \quad \forall n \iff c_{0,0} + c_{1,1} + c_{2,2} = 0 \quad \text{for } i = 0, 1, 2 \quad \text{(G.2)}
  \]

- **Y_{1} removed:**
  \[
  \sum_{i=0}^{2} \mu_{i}^{1} \left( \sum_{j=0}^{2} \nu_{j} c_{ij} \right) = 0 \quad \forall n \iff \nu_{0} c_{0,0} + \nu_{1} c_{1,1} + \nu_{2} c_{2,2} = 0 \quad \text{for } i = 0, 1, 2 \quad \text{(G.3)}
  \]

- **Y_{m} removed:**
  \[
  \sum_{j=0}^{2} \nu_{j}^{m} \left( \sum_{i=0}^{2} \mu_{i} c_{ij} \right) = 0 \quad \forall m \iff c_{0,j} + c_{1,j} + c_{2,j} = 0 \quad \text{for } j = 0, 1, 2 \quad \text{(G.4)}
  \]

- **Y_{n} removed:**
  \[
  \sum_{i=0}^{2} \mu_{i}^{n} \left( \sum_{j=0}^{2} \nu_{j} c_{ij} \right) = 0 \quad \forall m \iff \mu_{0} c_{0,j} + \mu_{1} c_{1,j} + \mu_{2} c_{2,j} = 0 \quad \text{for } j = 0, 1, 2 \quad \text{(G.5)}
  \]

The linear system of equations given by (G.2)–(G.5) has a unique solution in the variables \( c_{ij} \) (up to a global factor that we fix by imposing \( c_{0,0} = 1 \)), which reads as follows:

\[
\begin{align*}
c_{0,0} &= 1, \\
c_{0,1} &= \frac{\nu_{2} - \nu_{0}}{\nu_{1} - \nu_{2}}, \\
c_{0,2} &= \frac{\nu_{0} - \nu_{1}}{\nu_{1} - \nu_{2}}, \\
c_{1,0} &= \frac{\mu_{2} - \mu_{0}}{\mu_{1} - \mu_{2}}, \\
c_{1,1} &= \frac{(\mu_{0} - \mu_{2})(\nu_{0} - \nu_{2})}{(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}, \\
c_{1,2} &= \frac{(\mu_{0} - \mu_{2})(\nu_{0} - \nu_{1})}{(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}, \\
c_{2,0} &= \frac{\mu_{0} - \mu_{1}}{\mu_{1} - \mu_{2}}, \\
c_{2,1} &= \frac{(\mu_{0} - \mu_{1})(\nu_{0} - \nu_{2})}{(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}, \\
c_{2,2} &= \frac{(\mu_{0} - \mu_{1})(\nu_{0} - \nu_{1})}{(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}.
\end{align*}
\]  
(G.6)

By substituting the solution for the coefficients \( c_{ij} \) (G.6) back into (G.1) one gets:
\[
G_{22} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} A_{22}(\mu_{0}, \mu_{1}, \mu_{2}, n) A_{22}(\nu_{0}, \nu_{1}, \nu_{2}, m),
\]
where
\[
A_{22}(\mu_{0}, \mu_{1}, \mu_{2}, n) = (\mu_{0} - \mu_{2})(\mu_{2} - \mu_{0}) \sum_{k=0}^{n-1} \mu_{k}^{n-1-k} \mu_{n-1-k}^{k},
\]
(G.7)
is the function defined in [28] when obtaining the analogous bound on \( Y_{22} \) in the symmetric-intensities scenario (i.e. when the decay intensities of Alice and Bob are drawn from the same set). Thus we can employ the result from [28] and recast (G.8) as follows:
\[
A_{22}(\mu_{0}, \mu_{1}, \mu_{2}, n) = (\mu_{0} - \mu_{2})(\mu_{2} - \mu_{0}) \sum_{k=0}^{n-1} \mu_{k}^{n-1-k} \mu_{n-1-k}^{k},
\]
(G.9)
Of course we can employ this expression also for \( A_{22}(\nu_{0}, \nu_{1}, \nu_{2}, m) \) by making the proper substitutions. We will apply this consideration from now on to similar scenarios. By employing (G.9) into (G.7) one gets:
\[
G_{22} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_{0} - \mu_{2})(\nu_{0} - \nu_{2}) \sum_{k=0}^{n-1} \mu_{k}^{n-1-k} \mu_{n-1-k}^{k} \sum_{j=0}^{m-1} \nu_{j}^{m-1-j}(\nu_{0}^{m-1-j} - \nu_{1}^{m-1-j}).
\]  
(G.10)
From (G.10) we deduce that the sign of $Y_{nm}$’s coefficient is independent of $n$ and $m$ and it is the same for all terms in the sum. Thus a valid upper bound for $Y_{22}$ is obtained by setting all the other yields to zero in (G.10), except for $Y_{22}$. By doing this, we obtain (12).

### G.2. Upper bound on $Y_{11}$

We consider the most general combination of the nine equality constraints:

$$G_{11} = \sum_{i,j=0}^{2} c_{ij} Q^{ij} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \left[ \sum_{i,j=0}^{2} c_{ij} \nu^i_j \nu^m_j \right],$$

and require that the terms proportional to $Y_{nm}$, $Y_{m0}$, $Y_{n2}$ are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{ij}$:

1. $Y_{00}$ removed: $\sum_{i=0}^{2} \mu_i \left( \sum_{j=0}^{2} c_{ij} \right) = 0 \quad \forall n \iff c_{i0} + c_{i1} + c_{i2} = 0 \quad \text{for } i = 0, 1, 2$ (G.12)

2. $Y_{n2}$ removed: $\sum_{j=0}^{2} \nu^j \left( \sum_{i=0}^{2} c_{ij} \right) = 0 \quad \forall m \iff \nu^2_0 c_{i0} + \nu^2_1 c_{i1} + \nu^2_2 c_{i2} = 0 \quad \text{for } i = 0, 1, 2$ (G.13)

3. $Y_{0n}$ removed: $\sum_{i=0}^{2} \nu^i \left( \sum_{j=0}^{2} c_{ij} \right) = 0 \quad \forall m \iff c_{0,j} + c_{1,j} + c_{2,j} = 0 \quad \text{for } j = 0, 1, 2$ (G.14)

4. $Y_{2m}$ removed: $\sum_{j=0}^{2} \nu^j \left( \sum_{i=0}^{2} \mu_i^2 c_{ij} \right) = 0 \quad \forall m \iff \mu_0^2 c_{0,j} + \mu_1^2 c_{1,j} + \mu_2^2 c_{2,j} = 0 \quad \text{for } j = 0, 1, 2.$ (G.15)

The linear system of equations given by (G.12)–(G.15) has a unique solution in the variables $c_{ij}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:

$$c_{0,0} = 1,$$

$$c_{0,1} = \frac{\nu^2_0 - \nu^2_1}{\nu^2_1 - \nu^2_2},$$

$$c_{0,2} = \frac{\nu^2_0 - \nu^2_2}{\nu^2_1 - \nu^2_2},$$

$$c_{1,0} = \frac{\mu^2_0 - \mu^2_1}{\mu^2_1 - \mu^2_2},$$

$$c_{1,1} = \frac{(\nu^2_0 - \mu^2_2)(\nu^2_0 - \nu^2_2)}{(\mu^2_1 - \mu^2_2)(\nu^2_1 - \nu^2_2)},$$

$$c_{1,2} = \frac{(\nu^2_1 - \mu^2_2)(\nu^2_1 - \nu^2_2)}{(\mu^2_1 - \mu^2_2)(\nu^2_2 - \nu^2_2)},$$

$$c_{2,0} = \frac{\mu^2_0 - \mu^2_1}{\mu^2_1 - \mu^2_2},$$

$$c_{2,1} = \frac{(\mu^2_0 - \mu^2_2)(\nu^2_1 - \nu^2_2)}{(\mu^2_1 - \mu^2_2)(\nu^2_1 - \nu^2_2)},$$

$$c_{2,2} = \frac{(\mu^2_1 - \mu^2_2)(\nu^2_2 - \nu^2_2)}{(\mu^2_1 - \mu^2_2)(\nu^2_1 - \nu^2_2)}.$$ (G.16)

By substituting the solution for the coefficients $c_{ij}$ (G.16) back into (G.11) one gets:

$$G_{11} = Y_{11} \left( \frac{\mu_0 - \mu_1}(\mu_0 - \mu_2) (\nu_0 - \nu_1)(\nu_0 - \nu_2) \right) \frac{1}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} + \sum_{n=3}^{\infty} \frac{Y_{nm}}{n!} \frac{1}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} A_1(\nu_0, \nu_1, \nu_2, m) m!$$

$$+ \sum_{n=3}^{\infty} \frac{Y_{n1}}{n!} \frac{1}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} A_1(\mu_0, \mu_1, \mu_2, n) + \sum_{n,m=3}^{\infty} \frac{Y_{nm}}{n!m!} \frac{1}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} A_1(\mu_0, \mu_1, \mu_2, n) A_1(\nu_0, \nu_1, \nu_2, m).$$ (G.17)

The function $A_1(\mu_0, \mu_1, \mu_2, n)$ is defined in [28] when deriving the analogous bound in the symmetric-intensities scenario. It reads:
and can be recast as:

\[ A_11(\mu_0, \mu_1, \mu_2, n) = (\mu_0 - \mu_1)(\mu_1 - \mu_2)(\mu_1 - \mu_3)F(\mu_0, \mu_1, \mu_2, n) \quad \text{for} \quad n \geq 3, \]

with \( F(\mu_0, \mu_1, \mu_2, n) \) being a non-negative quantity independently of the intensities, defined as:

\[ F(\mu_0, \mu_1, \mu_2, n) \equiv \sum_{k=0}^{n-1} \mu_2^k \left( \mu_1 + \mu_2 \right) \sum_{j=0}^{n-k-1} \mu_1^{n-2-k-j} \mu_0^j + \mu_2 \mu_0^{n-2-k-j}. \]

By employing the expression (G.19) in (G.17) we obtain:

\[ G_{11} = Y_{11} \left( \frac{\mu_0 - \mu_1(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \right) + \sum_{m=3}^{\infty} \frac{Y_m}{m!} \left( \frac{\mu_0 - \mu_1(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \right) \left( \nu_1 - \nu_0 \right) F(\nu_0, \nu_1, \nu_2, m) + \sum_{m=3}^{\infty} \frac{Y_m}{n!} \left( \frac{\mu_0 - \mu_1(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \right) \left( \nu_1 - \nu_0 \right) F(\nu_0, \nu_1, \nu_2, m). \]

By looking at (G.21), we deduce that a valid upper bound on \( Y_{11} \) is obtained by setting the yields \( Y_{1m} \) and \( Y_{n1} \) to their maximum allowed value and by setting to zero the yields \( Y_{nm} \) for \( n, m \geq 3 \). In particular, we use the upper bounds derived in (G.5) and (G.6) to bound \( Y_{13} \) and \( Y_{31} \), respectively, while we set to 1 all the other yields \( Y_{1m} \) and \( Y_{n1} \), for \( n, m \geq 4 \). In so doing, we obtain:

\[ G_{11} = Y_{11} \left( \frac{\mu_0 - \mu_1(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \right) + \frac{Y_{13}}{6} \left( \frac{\mu_0 - \mu_1(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \right) \left( \nu_1 - \nu_0 \right) F(\nu_0, \nu_1, \nu_2, 3) + \frac{Y_{31}}{6} \left( \frac{\mu_0 - \mu_1(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \right) \left( \nu_1 - \nu_0 \right) F(\nu_0, \nu_1, \nu_2, 3) \]

By isolating the bound on \( Y_{11} \), and summing the series, we obtain (11).

### G.3. Upper bound on \( Y_{02} \) and \( Y_{04} \)

We consider the most general combination of the nine equality constraints:

\[ G_{02} = \sum_{i,j=0}^{2} c_{i,j} Q_{ij} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \left[ \sum_{i,j=0}^{2} c_{i,j} \mu_1^n \nu_1^m \right], \]

and require that the terms proportional to \( Y_{1m} \), \( Y_{2m} \), \( Y_{02} \) and \( Y_{04} \) are removed in the combination. We achieve this by imposing proper conditions on the real coefficients \( c_{i,j} \):

- \( Y_{00} \) removed:
  \[ \sum_{i=0}^{2} \mu_i^2 \sum_{j=0}^{2} c_{i,j} = 0 \quad \forall \quad n \quad \Leftrightarrow \quad c_{0,0} + c_{1,1} + c_{2,2} = 0 \quad \text{for} \quad i = 0, 1, 2 \]

- \( Y_{n1} \) removed:
  \[ \sum_{j=0}^{2} \mu_j^2 \sum_{i=0}^{2} c_{i,j} = 0 \quad \forall \quad n \quad \Leftrightarrow \quad \nu_0 c_{0,0} + \nu_1 c_{1,1} + \nu_2 c_{2,2} = 0 \quad \text{for} \quad i = 0, 1, 2 \]

- \( Y_{1m} \) removed:
  \[ \sum_{j=0}^{2} \mu_j^2 \sum_{i=0}^{2} c_{i,j} = 0 \quad \forall \quad m \quad \Leftrightarrow \quad \mu_0 c_{0,0} + \mu_1 c_{1,j} + \mu_2 c_{2,j} = 0 \quad \text{for} \quad j = 0, 1, 2 \]
Yields in and require that the terms proportional to

\[ \sum_{j=0}^{2} \nu_{j}^{m} \left( \sum_{i=0}^{2} \mu_{i}^{n} c_{i,j} \right) = 0 \quad \forall \ m \quad \Leftrightarrow \quad \mu_{0}^{n} c_{0,j} + \mu_{1}^{n} c_{1,j} + \mu_{2}^{n} c_{2,j} = 0 \quad \text{for } j = 0, 1, 2. \quad (G.27) \]

The linear system of equations given by (G.24)–(G.27) has a unique solution in the variables \( c_{i,j} \) (up to a global factor that we fix by imposing \( c_{0,0} = 1 \)), which reads as follows:

\[
\begin{align*}
   c_{0,0} & = 1, \\
   c_{0,1} & = \frac{\nu_{2} - \nu_{0}}{\nu_{1} - \nu_{2}}, \\
   c_{0,2} & = \frac{\nu_{0} - \nu_{1}}{\nu_{1} - \nu_{2}}, \\
   c_{1,0} & = \frac{\mu_{0}(\mu_{2} - \mu_{0})}{\mu_{1}(\mu_{1} - \mu_{2})}, \\
   c_{1,1} & = \frac{\mu_{0}(\mu_{0} - \mu_{2})(\nu_{0} - \nu_{2})}{\mu_{1}(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}, \\
   c_{1,2} & = \frac{\mu_{0}(\mu_{0} - \mu_{2})(\nu_{0} - \nu_{1})}{\mu_{1}(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}, \\
   c_{2,0} & = \frac{\mu_{0}(\mu_{0} - \mu_{1})}{\mu_{2}(\mu_{1} - \mu_{2})}, \\
   c_{2,1} & = \frac{\mu_{0}(\mu_{0} - \mu_{1})(\nu_{0} - \nu_{2})}{\mu_{2}(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}, \\
   c_{2,2} & = \frac{\mu_{0}(\mu_{0} - \mu_{1})(\nu_{0} - \nu_{1})}{\mu_{2}(\mu_{1} - \mu_{2})(\nu_{1} - \nu_{2})}.
\end{align*}
\]

(G.28)

By substituting the solution for the coefficients \( c_{i,j} \) back into (G.23) one gets:

\[
G_{02} = \sum_{m=4}^{\infty} \frac{Y_{0m}}{m!} (-1)^{m} \frac{(\mu_{0} - \mu_{1})(\mu_{0} - \mu_{2})A_{22}(\nu_{0}, \nu_{1}, \nu_{2}, m, \mu_{1}, \mu_{2})(\nu_{1} - \nu_{2})}{\mu_{1}\mu_{2}(\nu_{1} - \nu_{2})} + \sum_{n=3}^{\infty} \frac{Y_{nm}}{n!m!} (-1)^{m} \frac{B_{02}(\mu_{0}, \mu_{1}, \mu_{2}, n)(\mu_{0} - \mu_{2})A_{22}(\nu_{0}, \nu_{1}, \nu_{2}, m, \mu_{1}, \mu_{2})(\nu_{1} - \nu_{2})}{\mu_{1}\mu_{2}(\nu_{1} - \nu_{2})},
\]

(G.29)

where \( A_{22} \) is given in (G.8) and \( B_{02} \) can be written as follows for \( n \geq 3 \) [28]:

\[
B_{02}(\mu_{0}, \mu_{1}, \mu_{2}, n) = \mu_{0}\mu_{1}\mu_{2}(\mu_{1} - \mu_{2})(\mu_{0} - \mu_{2}) \sum_{k=0}^{n-2} \mu_{2}^{k}(\mu_{0}^{n-2-k} - \mu_{1}^{n-2-k}).
\]

(G.30)

We thus conclude that the sign of \( Y_{0m} \) and \( Y_{nm} \)'s coefficients are always equal in (G.29), regardless of the values of the intensities. Therefore a valid upper bound on \( Y_{0m} \)—for \( m = 2, 4 \)—is obtained by setting to zero all the other yields in (G.29). By doing so, we obtain the upper bounds on \( Y_{02} \) and \( Y_{04} \) given in equations (13) and (14).

G.4. Upper bound on \( Y_{20} \) and \( Y_{40} \)

We consider the most general combination of the nine equality constraints:

\[
G_{20} = \sum_{i,j=0}^{2} c_{i,j}Q_{i,j}^{2} = \sum_{m,n=0}^{\infty} \frac{Y_{nm}}{n!m!} \left[ \sum_{i,j=0}^{2} c_{i,j} \nu_{i}^{n} \nu_{j}^{m} \right],
\]

(G.31)

and require that the terms proportional to \( Y_{0m}, Y_{1m}, Y_{n1} \) and \( Y_{2n} \) are removed in the combination. We achieve this by imposing proper conditions on the real coefficients \( c_{i,j} \):

\[
\begin{align*}
   Y_{n1} \text{ removed: } \sum_{i=0}^{2} \mu_{i}^{n} \left( \sum_{j=0}^{2} \nu_{j}^{m} c_{i,j} \right) & = 0 \quad \forall \ m \quad \Leftrightarrow \quad \nu_{0}c_{i,0} + \nu_{1}c_{i,1} + \nu_{2}c_{i,2} = 0 \quad \text{for } i = 0, 1, 2 \quad (G.32) \\
   Y_{n2} \text{ removed: } \sum_{i=0}^{2} \nu_{i}^{n} \left( \sum_{j=0}^{2} \mu_{j}^{m} c_{i,j} \right) & = 0 \quad \forall \ m \quad \Leftrightarrow \quad \nu_{0}^{i}c_{i,0} + \nu_{1}^{i}c_{i,1} + \nu_{2}^{i}c_{i,2} = 0 \quad \text{for } i = 0, 1, 2 \quad (G.33) \\
   Y_{0m} \text{ removed: } \sum_{j=0}^{2} \nu_{j}^{m} \left( \sum_{i=0}^{2} c_{i,j} \right) & = 0 \quad \forall \ m \quad \Leftrightarrow \quad c_{0,j} + c_{1,j} + c_{2,j} = 0 \quad \text{for } j = 0, 1, 2 \quad (G.34)
\end{align*}
\]
Y\text{removed}: \sum_{j=0}^{2} \nu_j^m \left( \sum_{i=0}^{2} \mu_i c_{i,j} \right) = 0 \quad \forall \ m \quad \iff \quad \mu_0 c_{0,j} + \mu_1 c_{1,j} + \mu_2 c_{2,j} = 0 \quad \text{for} \ j = 0, 1, 2. \quad \text{(G.35)}

The linear system of equations given by (G.32)–(G.35) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:

\begin{align*}
c_{0,0} &= 1, \\
c_{0,1} &= \nu_0 (\nu_2 - \nu_0), \\
c_{0,2} &= \nu_0 (\nu_0 - \nu_1), \\
c_{1,0} &= \mu_2 - \mu_0, \\
c_{1,1} &= \nu_0 (\mu_0 - \mu_2)(\nu_0 - \nu_2), \\
c_{1,2} &= \nu_0 (\mu_0 - \mu_2)(\nu_0 - \nu_2), \\
c_{2,0} &= \mu_1 - \mu_2, \\
c_{2,1} &= -\nu_0 (\mu_0 - \mu_1)(\nu_0 - \nu_1), \\
c_{2,2} &= \nu_0 (\mu_0 - \mu_1)(\nu_0 - \nu_1).
\end{align*}

(G.36)

By substituting the solution for the coefficients $c_{i,j}$ (G.36) back into (G.31) one gets:

\begin{equation*}
G_{20} = \sum_{n=2}^{\infty} \frac{Y_{n0}}{n!} \frac{(-1)^n}{n!} \frac{(\nu_0 - \nu_2)(\nu_0 - \nu_2) A_{22}(\mu_0; \mu_1; \mu_2; n)}{\nu_1 \nu_2 (\mu_1 - \mu_2)}
+ \sum_{n=2}^{\infty} \frac{Y_{nm}}{n! m!} \frac{(-1)^n A_{22}(\mu_0; \mu_1; \mu_2; n) B_{02}(\nu_0, \nu_1, \nu_2, m)}{\nu_1 \nu_2 (\mu_1 - \mu_2)(\nu_1 - \nu_2)},
\end{equation*}

(G.37)

where $A_{22}$ is given in (G.8) and $B_{02}$ in (G.30). From (G.37) we observe that the sign of $Y_{n0}$ and $Y_{nm}$‘s coefficients are always the same, regardless of the values of the intensities. Therefore a valid upper bound on $Y_{n0}$—for $n = 2, 4$—is obtained by setting to zero all the other yields in (G.37). By doing so, we obtain the upper bounds on $Y_{20}$ and $Y_{40}$ given in equations (15) and (16).

G.5. Upper bound on $Y_{13}$

We consider the most general combination of the nine equality constraints:

\begin{equation*}
G_{13} = \sum_{j=0}^{2} c_{i,j} Q^i_j = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n! m!} \left[ \sum_{j=0}^{2} c_{i,j} \nu_j^m \nu_j^m \right],
\end{equation*}

(G.38)

and require that the terms proportional to $Y_{00}$, $Y_{20}$, $Y_{01}$, $Y_{02}$, $Y_{12}$, $Y_{22}$, $Y_{00}$, $Y_{11}$ and $Y_{12}$ are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

\begin{align*}
Y_{00}\text{removed:} \quad & \sum_{j=0}^{2} \nu_j^m \left( \sum_{i=0}^{2} c_{i,j} \right) = 0 \quad \forall \ n \quad \iff \quad c_{0,0} + c_{1,1} + c_{2,2} = 0 \quad \text{for} \ i = 0, 1, 2 \quad \text{(G.39)}
\end{align*}

\begin{align*}
Y_{11}\text{removed:} \quad & \sum_{j=0}^{2} \nu_j^m \left( \sum_{i=0}^{2} c_{i,j} \right) = 0 \quad \forall \ n \quad \iff \quad \nu_0 c_{0,0} + \nu_1 c_{1,1} + \nu_2 c_{2,2} = 0 \quad \text{for} \ i = 0, 1, 2 \quad \text{(G.40)}
\end{align*}

\begin{align*}
Y_{0m}\text{removed:} \quad & \sum_{j=0}^{2} \nu_j^m \left( \sum_{i=0}^{2} c_{i,j} \right) = 0 \quad \forall \ m \quad \iff \quad c_{0,j} + c_{1,j} + c_{2,j} = 0 \quad \text{for} \ j = 0, 1, 2 \quad \text{(G.41)}
\end{align*}
The linear system of equations given by (G.39)–(G.42) has a unique solution in the variables $c_{ij}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:

\[
\begin{align*}
\phi_{0,0} &= 1, \\
\phi_{0,1} &= \frac{\nu_2 - \nu_0}{\nu_1 - \nu_2}, \\
\phi_{0,2} &= \frac{\nu_0 - \nu_1}{\nu_1 - \nu_2}, \\
\phi_{1,0} &= \frac{\mu_2^2 - \mu_0^2}{\mu_1^2 - \mu_2^2}, \\
\phi_{1,1} &= \frac{(\mu_2^2 - \mu_0^2)(\nu_0 - \nu_2)}{(\mu_1^2 - \mu_2^2)(\nu_1 - \nu_2)}, \\
\phi_{1,2} &= \frac{(\mu_2^2 - \mu_0^2)(\nu_0 - \nu_1)}{(\mu_1^2 - \mu_2^2)(\nu_1 - \nu_2)}, \\
\phi_{2,0} &= \frac{\mu_0^2 - \mu_1^2}{\mu_1^2 - \mu_2^2}, \\
\phi_{2,1} &= \frac{(\mu_0^2 - \mu_1^2)(\nu_0 - \nu_2)}{(\mu_1^2 - \mu_2^2)(\nu_2 - \nu_1)}, \\
\phi_{2,2} &= \frac{(\mu_0^2 - \mu_1^2)(\nu_0 - \nu_1)}{(\mu_1^2 - \mu_2^2)(\nu_1 - \nu_2)}.
\end{align*}
\]  

By substituting the solution for the coefficients $\phi_{ij}$ (G.43) back into (G.38) one gets:

\[
G_{13} = \sum_{m=2}^{\infty} \frac{Y_m}{m!} \frac{\phi_{m-1}(\mu_0 - \mu_1)(\mu_0 - \mu_2)A_{12}(\nu_0, \nu_1, \nu_2, m)}{\phi_{m}(\nu_1 - \nu_2)} + \sum_{n=3}^{\infty} \sum_{m=2}^{\infty} \frac{Y_{nm}}{n!m!} \frac{A_{12}(\mu_0, \mu_1, \mu_2, n)A_{22}(\nu_0, \nu_1, \nu_2, m)}{(\mu_1^2 - \mu_2^2)(\nu_1 - \nu_2)},
\]

where $A_{22}$ is given in (G.9) and $A_{11}$ is given in (G.19). We thus conclude that $Y_{1m}$ and $Y_{nm}$’s coefficients have always opposite sign in (G.44), regardless of the values of the intensities. Therefore a valid upper bound on $Y_{13}$ is obtained by setting to zero all the yields of the form $Y_{1m}$ for $m = 3$ and by setting to 1 all the other yields of the form $Y_{nm}$ with $n \geq 3$ and $m \geq 2$. In so doing, we obtain the following expression:

\[
G_{13} = \frac{Y_{13}^{(1)}}{6} \frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_2)(\nu_2 - \nu_1)[\nu_0^2 - \nu_1^2 + \nu_2](\nu_0 - \nu_1)}{(\mu_1 + \mu_2)(\nu_1 - \nu_2)} + \sum_{n=3}^{\infty} \sum_{m=2}^{\infty} \frac{[\mu_0^2(\mu_1^2 - \mu_2^2) + \mu_2^2(\mu_1^2 - \mu_0^2) + \mu_0^2(\mu_2^2 - \mu_1^2)][\nu_0^m(\nu_0 - \nu_2) + \nu_2^m(\nu_1 - \nu_0) + \nu_0^m(\nu_2 - \nu_1)]}{n!m!(\mu_1^2 - \mu_2^2)(\nu_1 - \nu_2)},
\]

where we used in the series the original expressions of $A_{22}$ and $A_{11}$, that are given in (G.8) and (G.18), respectively. By summing and rearranging the terms, we obtain the upper bound on $Y_{13}$ given in (17).

**G.6. Upper bound on $Y_{31}$**

In a similar fashion to $Y_{13}$’s bound, one first removes the terms proportional to $Y_{0m}$, $Y_{1m}$, $Y_{n0}$ and $Y_{n2}$ from the general combination of the nine gains:

\[
G_{31} = \sum_{i,j=0}^{2} \phi_{ij}O_{ij} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \left[ \sum_{i,j=0}^{2} \phi_{ij}O_{ij} \right],
\]
by properly fixing the coefficients $c_{i,j}$ as follows:

$$
c_{0,0} = 1,
$$

$$
c_{0,1} = \frac{\nu_1^2 - \nu_0^2}{\nu_1^2 - \nu_2^2},
$$

$$
c_{0,2} = \frac{\nu_0^2 - \nu_1^2}{\nu_1^2 - \nu_2^2},
$$

$$
c_{1,0} = \frac{\mu_2 - \mu_0}{\mu_1 - \mu_2},
$$

$$
c_{1,1} = \frac{(\mu_0 - \mu_2)(\nu_0^2 - \nu_2^2)}{(\mu_1 - \mu_2)(\nu_1^2 - \nu_2^2)},
$$

$$
c_{1,2} = \frac{(\mu_0 - \mu_2)(\nu_0^2 - \nu_1^2)}{(\mu_1 - \mu_2)(\nu_1^2 - \nu_2^2)},
$$

$$
c_{2,0} = \frac{\mu_0 - \mu_1}{\mu_1 - \mu_2},
$$

$$
c_{2,1} = \frac{(\mu_0 - \mu_1)(\nu_0^2 - \nu_1^2)}{(\mu_1 - \mu_2)(\nu_1^2 - \nu_2^2)},
$$

$$
c_{2,2} = \frac{(\mu_0 - \mu_1)(\nu_0^2 - \nu_2^2)}{(\mu_1 - \mu_2)(\nu_1^2 - \nu_2^2)}.
$$

(G.47)

Then one substitutes the solution (G.47) back into (G.46) and gets:

$$
G_{31} = \sum_{n=2}^{\infty} \frac{Y_{11}}{n!} \frac{(\nu_0 - \nu_1)(\nu_0 - \nu_2)A_{22}(\mu_0, \mu_1, \mu_2, n)}{(\nu_1 + \nu_2)(\mu_1 - \mu_2)} + \sum_{m=3}^{\infty} \frac{Y_{nm}}{n!m!} \frac{A_{22}(\mu_0, \mu_1, \mu_2, n)A_{11}(\nu_0, \nu_1, \nu_2, m)}{(\nu_1^2 - \nu_2^2)(\mu_1 - \mu_2)},
$$

(G.48)

where $A_{22}$ and $A_{11}$ are given in (G.9) and (G.9), respectively. By noting that the coefficients of the $Y_{n1}$ terms have opposite sign to those of the $Y_{nm}$ terms, we derive an upper bound on $Y_{31}$ by setting to zero all the $Y_{n1}$ yields (for $n \neq 3$) and to 1 all the other ones. The upper bound on $Y_{31}$ is given in (18).

G.7. Upper bound on $Y_{00}$

We consider the most general combination of the nine equality constraints:

$$
G_{00} = \sum_{i,j=0}^{2} c_{i,j} Q_{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \left[ \sum_{i,j=0}^{2} c_{i,j} p_i^m p_j^n \right],
$$

(G.49)

and require that the terms proportional to $Y_{1m}, Y_{2m}, Y_{31}$ and $Y_{02}$ are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

$Y_{31}$ removed: $\sum_{i=0}^{2} \sum_{j=0}^{2} \nu_i c_{i,j} = 0 \quad \forall \ n \quad \Leftrightarrow \quad \nu_0 c_{i,0} + \nu_1 c_{i,1} + \nu_2 c_{i,2} = 0 \quad \text{for} \quad i = 0, 1, 2 \quad \text{(G.50)}$

$Y_{02}$ removed: $\sum_{j=0}^{2} \nu_j^2 c_{i,j} = 0 \quad \forall \ n \quad \Leftrightarrow \quad \nu_0^2 c_{0,0} + \nu_1^2 c_{1,1} + \nu_2^2 c_{2,2} = 0 \quad \text{for} \quad i = 0, 1, 2 \quad \text{(G.51)}$

$Y_{1m}$ removed: $\sum_{j=0}^{2} \nu_j^m c_{i,j} = 0 \quad \forall \ m \quad \Leftrightarrow \quad \mu_0 c_{0,j} + \mu_1 c_{1,j} + \mu_2 c_{2,j} = 0 \quad \text{for} \quad j = 0, 1, 2 \quad \text{(G.52)}$

$Y_{2m}$ removed: $\sum_{j=0}^{2} \nu_j^m c_{i,j} = 0 \quad \forall \ m \quad \Leftrightarrow \quad \mu_0^2 c_{0,j} + \mu_1^2 c_{1,j} + \mu_2^2 c_{2,j} = 0 \quad \text{for} \quad j = 0, 1, 2 \quad \text{(G.53)}$

The linear system of equations given by (G.50)–(G.53) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:
In this case each party prepares PRCS with four possible intensities, namely \( \nu_0, \nu_1, \nu_2, \nu_3 \) and notice that all the yields in Appendix H. Upper bounds on the yields with four decoy intensities are to be ordered within each set of intensities: 

\[
\mu_0 > \mu_1 > \mu_2 > \mu_3
\]

Thus, without loss of generality, we assume the following bounds presented here are not valid when two decoy intensities of the same party have the same value. This case would then reduce to the three decoy intensity case. Hence a valid upper bound on \( Y_{00} \) is obtained by setting all the other yields to zero (except for the yield to be bounded) in (G.55). The upper bound on \( Y_{00} \) is given in (10).

**Appendix H. Upper bounds on the yields with four decoy intensities**

In this case each party prepares PRCS with four possible intensities, namely \( \{\mu_0, \mu_1, \mu_2, \mu_3\} \) for Alice and \( \{\nu_0, \nu_1, \nu_2, \nu_3\} \) for Bob. The yields are then subjected to the following sixteen equality constraints:

\[
Q^{kl} \equiv e^{\nu_k + \nu_l} Q^{kl} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n! m!} \mu_k^n \nu_l^m \quad k, l \in \{0, 1, 2, 3\},
\]

and to the inequality constraints given in (7).

Below we derive tighter upper bounds on the yields \( Y_{04}, Y_{40}, Y_{13} \) and \( Y_{31}, \) since the bounds derived on the yields \( Y_{00}, Y_{11}, Y_{02}, Y_{20} \) and \( Y_{22} \) in appendix G are already good enough, i.e. bounding them with one additional decoy intensity would not result in a significant improvement of the performance of the protocol. Note that the bounds presented here are not valid when two decoy intensities of the same party have the same value. This case would then reduce to the three decoy intensity case. Thus, without loss of generality, we assume the following ordering within each set of intensities: \( \nu_3 > \nu_0 > \nu_1 > \nu_2 \) and \( \nu_3 > \nu_0 > \nu_1 > \nu_2 \).

### H.1. Upper bound on \( Y_{04} \)

We consider the combination of gains (G.29) that leads to the bound on \( Y_{04} \) in the case of three decoy intensity settings:

\[
C^{0.1,2}_{\nu_2} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n! m!} C^{0.1,2}_{\nu_2}(n, m),
\]

By substituting the solution for the coefficients \( c_{ij} \) (G.43) back into (G.38) one gets:

\[
G_{00} = Y_{00}(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2) + \sum_{m=1}^{\infty} \frac{Y_{0m}(\mu_0 - \mu_1)(\mu_0 - \mu_2) A_{00}(\nu_0, \nu_1, \nu_2, m)}{m! (\mu_0 - \mu_2) \nu_1 \nu_2 (\nu_0 - \nu_1)}
\]

\[
+ \sum_{n=3}^{\infty} \frac{Y_{0n}(\nu_0 - \nu_1)(\nu_0 - \nu_2) A_{00}(\mu_0, \mu_1, \mu_2, n)}{m! (\mu_0 - \mu_2) \nu_1 \nu_2 (\mu_0 - \mu_2)},
\]

where \( A_{00} \) is defined as [28]:

\[
A_{00}(\mu_0, \mu_1, \mu_2, n) = \mu_0^n (\mu_0 - \mu_2)^n + \mu_0^n (\mu_0 - \mu_1) \mu_1^n + \mu_0^n (\mu_1 - \mu_2) \mu_2^n + \mu_0^n (\mu_2 - \mu_1) \mu_1^n + \mu_0^n (\mu_2 - \mu_1) \mu_2^n + \mu_0^n (\mu_2 - \mu_1) \mu_2^n.
\]

Using the result in [28], one can recast the function \( A_{32} \) as follows:

\[
A_{00}(\mu_0, \mu_1, \mu_2, n) = \mu_0 \mu_1 \mu_2 (\mu_0 - \mu_2) (\mu_1 - \mu_2) \sum_{k=0}^{n-2} \mu_0^k (\mu_0 - \mu_2)^{n-2-k} (\mu_1 - \mu_2)^{n-2-k} (\mu_1 - \mu_2)^{n-2-k},
\]

and notice that all the yields in (G.55) have coefficients with equal sign, regardless of the intensities’ values. Hence a valid upper bound on \( Y_{00} \) is obtained by setting all the other yields to zero (except for the yield to be bounded) in (G.55). The upper bound on \( Y_{00} \) is given in (10).
where the function $C_{0,2}^{0,1,2}(n, m)$ is defined by the rhs of (G.29), while $C_{0,2}^{0,1,2}$ is the combination of gains given by (G.23), with the coefficients $c_{ij}$ of the combination given in (G.28). The subscript indicates the combination of gains to which it refers, while the superscript indicates the decoy intensities that are involved, namely $\{\mu_0, \mu_1, \mu_2\}$ for Alice and $\{\nu_0, \nu_1, \nu_2\}$ for Bob. From (G.3) we know that the terms $Y_{00}, Y_{01}, Y_{1m},$ and $Y_{2m}$ are removed in (H.2), i.e. $C_{0,2}^{0,1,2} (n, 0) = C_{0,2}^{0,1,2} (1, m) = C_{0,2}^{0,1,2} (2, m) = 0,$ for any $n, m$. Now that the parties have at their disposal the fourth decoy intensity $(\mu_2$ for Alice and $\nu_2$ for Bob), one can derive three additional combinations like (H.2) by simply replacing one of the first three intensities with the fourth one:

$$C_{0,2}^{0,1,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{0,2}^{0,1,3} (n, m),$$

(H.3)

$$C_{0,2}^{0,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{0,2}^{0,2,3} (n, m),$$

(H.4)

$$C_{0,2}^{0,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{0,2}^{0,2,3} (n, m).$$

(H.5)

For instance, the combination (H.3) is obtained by replacing $\mu_2 \rightarrow \mu_3$ and $\nu_2 \rightarrow \nu_3$ in the function $C_{0,2}^{0,1,2} (n, m)$, thus obtaining $C_{0,2}^{0,1,3} (n, m)$. Regarding the rhs, $C_{0,2}^{0,1,3}$ is obtained by replacing $\mu_2 \rightarrow \mu_3$ and $\nu_2 \rightarrow \nu_3$ in the coefficients $c_{ij}$ appearing in the combination $C_{0,2}^{0,1,2}$, and by making the substitution $Q^{2,1} \rightarrow Q^{3,1}$ and $Q^{2,2} \rightarrow Q^{3,2}$ on the gains in $G_{0,2}^{0,1,2}$. In so doing, we obtain three more combinations of gains (H.3)–(H.5) in which the terms $Y_{00}, Y_{01}, Y_{1m},$ and $Y_{2m}$ are removed.

At this point, we further combine the expressions (H.2), (H.3), (H.4), (H.5) with arbitrary real coefficients $d_{i,j,k}$:

$$H_{04} \equiv d_{0,1,2} C_{0,2}^{0,1,2} + d_{0,1,3} C_{0,2}^{0,1,3} + d_{0,2,3} C_{0,2}^{0,2,3} + d_{1,2,3} C_{0,2}^{0,2,3}$$

$$= \sum_{n,m} \frac{Y_{nm}}{n!m!} \left[ d_{0,1,2} C_{0,2}^{0,1,2} (n, m) + d_{0,1,3} C_{0,2}^{0,1,3} (n, m) + d_{0,2,3} C_{0,2}^{0,2,3} (n, m) + d_{1,2,3} C_{0,2}^{0,2,3} (n, m) \right].$$

(H.6)

and impose that even the terms $Y_{n2}$ and $Y_{3m}$ are removed:

$$\begin{cases} 
    d_{0,1,2} C_{0,2}^{0,1,2} (n, 2) + d_{0,1,3} C_{0,2}^{0,1,3} (n, 2) + d_{0,2,3} C_{0,2}^{0,2,3} (n, 2) + d_{1,2,3} C_{0,2}^{0,2,3} (n, 2) = 0 \quad \forall n \\
    d_{0,1,2} C_{0,2}^{0,1,2} (3, m) + d_{0,1,3} C_{0,2}^{0,1,3} (3, m) + d_{0,2,3} C_{0,2}^{0,2,3} (3, m) + d_{1,2,3} C_{0,2}^{0,2,3} (3, m) = 0 \quad \forall m \\
    d_{0,1,2} = 1 
\end{cases}$$

(H.7)

where we fixed the remaining degree of freedom (global factor on all the $d_{i,j,k}$) by requiring that $d_{0,1,2} = 1$. The solution of the linear system (H.7) reads:

$$d_{0,1,2} = 1$$

$$d_{0,1,3} = \frac{(\mu_0 - \mu_2)(\nu_0 - \nu_2)[\mu_0(\nu_1 - \nu_3) + \mu_1(\nu_3 - \nu_0) + \mu_2(\nu_0 - \nu_1)]}{(\mu_0 - \mu_1)(\nu_0 - \nu_3)[\mu_0(\nu_2 - \nu_1) + \mu_1(\nu_1 - \nu_2) + \mu_2(\nu_2 - \nu_3)]}$$

$$d_{0,2,3} = \frac{(\mu_0 - \mu_1)(\nu_1 - \nu_2)[\mu_0(\nu_2 - \nu_3) + \mu_1(\nu_3 - \nu_0) + \mu_2(\nu_0 - \nu_1)]}{(\mu_0 - \mu_1)(\nu_1 - \nu_2)[\mu_0(\nu_2 - \nu_1) + \mu_1(\nu_1 - \nu_2) + \mu_2(\nu_2 - \nu_3)]}$$

$$d_{1,2,3} = \frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_2)(\nu_0 - \nu_3)[\mu_1(\nu_3 - \nu_2) + \mu_2(\nu_2 - \nu_3) + \mu_3(\nu_2 - \nu_1)]}{\mu_1(\nu_1 - \nu_2)(\mu_1 - \mu_3)(\nu_1 - \nu_3)(\nu_1 - \nu_2)[\mu_1(\nu_2 - \nu_1) + \mu_2(\nu_1 - \nu_2) + \mu_2(\nu_2 - \nu_3) + \mu_2(\nu_3 - \nu_1)]}$$

(H.8)

By substituting the solution (H.8) back into (H.6) and by rearranging the rhs, one gets a combination of gains where all the terms $Y_{00}, Y_{01}, Y_{1m}, Y_{2m},$ and $Y_{3m}$ are removed:

$$H_{04} = \sum_{m=3}^{\infty} \frac{Y_{nm}}{m!} A_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, m) + \sum_{m=3}^{\infty} \frac{Y_{nm}}{n!m!} B_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, n, m),$$

(H.9)

where:

$$A_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, m) = \frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_2)(\nu_0 - \nu_3) \nu_0(\mu_0 - \mu_2) + \mu_2(\nu_0 - \mu_2) + \mu_0(\nu_0 - \mu_1)}{\mu_1(\mu_1 - \mu_2)(\nu_1 - \nu_2)(\nu_1 - \nu_3)[\mu_1(\nu_2 - \nu_1) + \mu_2(\nu_1 - \nu_2) + \mu_2(\nu_2 - \nu_3) + \mu_2(\nu_3 - \nu_1)]} \times \left( \sum_{\nu_i \leq \nu_j \leq \cdots \leq \nu_{m-3}} \nu_i \nu_j \nu_k \cdots \nu_{l_{m-3}} \right).$$

(H.10)

4 Note that we identify such a combination as $H_{04}$ since it appears in bounding $Y_{04}$. However the elements in the combination, namely $G_{1,2}^{0,4}$, have a different subscript since they are borrowed from the bounds on $Y_{02}$ and $Y_{04}$ with three decoy intensity settings.
We remark that in deriving the bound and the series of where

\[ H \]

We assume that the indexes in the sums run over the set \( \{0, 1, 2, 3\} \) and we implicitly assumed that at least one of the following equalities does not hold: \( \nu_0 = \mu_0, \nu_1 = \mu_1 \) and \( \nu_2 = \mu_2 \). Indeed, when all three equalities hold (i.e. when Alice and Bob are using the same intensities settings for three out of four decoy pulses) one gets a \( \nu = 0 \) form in the bound expression (H.13). In order to overcome this issue (which is not likely to happen in practice due to intensity fluctuations), we derive an additional upper bound on \( Y_{d4} \) which is valid in the particular case of: \( \nu_0 = \mu_0, \nu_1 = \mu_1 \) and \( \nu_2 = \mu_2 \).

\[ B_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, n, m) = -\mu_0 \mu_1 \mu_2 A_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, n, m) \]

\[ \times \left( \sum_{i \leq i_1 \leq \ldots \leq i_{n-1} \leq \nu_{i-1}} \mu_{i_1} \mu_{i_2} \ldots \mu_{i_{n-1}} \right) \]

\[ \text{We assume that the indexes in the sums run over the set } \{0, 1, 2, 3\} \text{ and we deduce that the coefficients of } Y_{d0m} \text{ and } Y_{d0m} \text{ have always opposite sign, hence the upper bound on } Y_{d04} \text{ is obtained from (H.9) by setting all the yields } Y_{d0m} \text{ (with } m \geq 4, m \geq 3 \text{) to zero. After rearranging the terms, we get the following expression for the upper bound on } Y_{d04}: \]

\[ Y_{d04}^{U} = \frac{24}{A_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, \nu_2, \nu_3, 4)} \left( H_{d4} - \sum_{m=4}^{\infty} B_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, \nu_2, \nu_3, n, m) \right) \]

\[ \text{where } H_{d4} \text{ is given in the first line of (H.6), the function } A_{d4} \text{ evaluated for } m = 4 \text{ reads:} \]

\[ A_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, \nu_2, \nu_3, 4) = -\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 + \nu_1 + \nu_2 + \nu_3) P_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, \nu_2, \nu_3, 4)}{\mu_1 \mu_2 \nu_0(\nu_0 - \nu_1) + \nu_1(\nu_0 - \mu_2) + \nu_2(\mu_0 - \mu_1)} \]

\[ \text{and the series of } B_{d4} \text{ sums to:} \]

\[ \sum_{m=4}^{\infty} \frac{B_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, \nu_2, \nu_3, n, m)}{n!m!} \]

\[ = \mu_0 P_{d4}(\mu_0, \mu_1, \mu_2, \nu_0, \nu_1, \nu_2, \nu_3) [\nu_2(\mu_0 - \mu_1) - \nu_1(\mu_0 - \mu_2) + \nu_0(\mu_1 - \mu_2)] + \frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 + \nu_1 + \nu_2 + \nu_3)}{\nu_0(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_0 - \nu_3)(\nu_1 - \nu_2)(\nu_1 - \nu_3)(\nu_2 - \nu_3)} \]

\[ \times \left( e^{\nu_0} - \frac{\nu_0^2}{2} - \nu_0 - 1 \right) \left( \mu_1 - \mu_2 \right) (\mu_1 - \mu_3)(\mu_2 - \mu_3) \]

\[ - \left( e^{\nu_1} - \frac{\nu_1^2}{2} - \nu_1 - 1 \right) (\mu_0 - \mu_2)(\mu_0 - \mu_3)(\mu_2 - \mu_3) \]

\[ + \left( e^{\nu_2} - \frac{\nu_2^2}{2} - \nu_2 - 1 \right) (\mu_0 - \mu_1)(\mu_0 - \mu_3)(\mu_1 - \mu_3) \]

\[ - \left( e^{\nu_3} - \frac{\nu_3^2}{2} - \nu_3 - 1 \right) (\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2) \]

\[ \times \left( e^{\nu_0} - \frac{\nu_0^2}{2} - \nu_0 - 1 \right) (\nu_1 - \nu_2)(\nu_1 - \nu_3)(\nu_2 - \nu_3) \]

\[ - \left( e^{\nu_1} - \frac{\nu_1^2}{2} - \nu_1 - 1 \right) (\nu_0 - \nu_2)(\nu_0 - \nu_3)(\nu_2 - \nu_3) \]

\[ + \left( e^{\nu_2} - \frac{\nu_2^2}{2} - \nu_2 - 1 \right) (\nu_0 - \nu_1)(\nu_0 - \nu_3)(\nu_1 - \nu_3) \]

\[ - \left( e^{\nu_3} - \frac{\nu_3^2}{2} - \nu_3 - 1 \right) (\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_1 - \nu_2) \]
The procedure resembles that used in deriving \( (H.13) \). We start by considering the four combinations of gains \((H.2), (H.3), (H.4)\) and \((H.5)\) and we impose the conditions: \( \nu_0 = \mu_0, \nu_1 = \mu_1 \) and \( \nu_2 = \mu_2 \). Let us indicate the resulting gains combinations as follows:

\[
\tilde{C}_{0,2}^{0,1,2} = \sum_{n,m} \frac{Y_{nm}}{n!m!} \tilde{C}_{0,2}^{0,1,2} (n, m), \tag{H.16}
\]

\[
\tilde{C}_{0,2}^{0,1,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} \tilde{C}_{0,2}^{0,1,3} (n, m), \tag{H.17}
\]

\[
\tilde{C}_{0,2}^{0,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} \tilde{C}_{0,2}^{0,2,3} (n, m), \tag{H.18}
\]

\[
\tilde{C}_{0,2}^{1,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} \tilde{C}_{0,2}^{1,2,3} (n, m). \tag{H.19}
\]

The tilde symbol above the gains combinations \( C_{0,2} \) and the corresponding yields coefficients \( C_{0,2} \) indicates that we operated the substitutions \( \nu_0 \rightarrow \mu_0, \nu_1 \rightarrow \mu_1 \) and \( \nu_2 \rightarrow \mu_2 \) in their original expressions.

We further combine the expressions \((H.16), (H.17), (H.18)\) and \((H.19)\) with arbitrary real coefficients \( \tilde{d}_{i,j,k} \):

\[
\tilde{H}_{04} \equiv \tilde{d}_{0,1,2} \tilde{C}_{0,2}^{0,1,2} + \tilde{d}_{0,1,3} \tilde{C}_{0,2}^{0,1,3} + \tilde{d}_{0,2,3} \tilde{C}_{0,2}^{0,2,3} + \tilde{d}_{1,2,3} \tilde{C}_{0,2}^{1,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} \big[ \tilde{d}_{0,1,2} \tilde{C}_{0,2}^{0,1,2} (n, m) + \tilde{d}_{0,1,3} \tilde{C}_{0,2}^{0,1,3} (n, m) + \tilde{d}_{0,2,3} \tilde{C}_{0,2}^{0,2,3} (n, m) + \tilde{d}_{1,2,3} \tilde{C}_{0,2}^{1,2,3} (n, m) \big], \tag{H.20}
\]

and impose that even the terms \( Y_{n0} \) and \( Y_{m0} \) are removed. The solution for the coefficients \( \tilde{d}_{i,j,k} \) reads:

\[
\begin{align*}
\tilde{d}_{0,1,2} &= 0, \\
\tilde{d}_{0,1,3} &= \mu_3, \\
\tilde{d}_{0,2,3} &= -\frac{(\mu_0 - \mu_1)\mu_2}{\mu_0 - \mu_2}, \\
\tilde{d}_{1,2,3} &= -\frac{\mu_0\mu_3(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_0 - \nu_3)}{\mu_1(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_1 - \nu_3)}. \tag{H.21}
\end{align*}
\]

By substituting the solution \((H.8)\) back into \((H.6)\) and by rearranging the rhs, one gets a combination of gains where all the terms \( Y_{n0}, Y_{m1}, Y_{n,2}, Y_{n,m}, Y_{m,0} \) and \( Y_{m,0} \) are removed:

\[
\tilde{H}_{04} = \sum_{m=3}^\infty \frac{Y_{nm}}{m!} \tilde{A}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, m) + \sum_{m=3}^\infty \frac{Y_{nm}}{n!m!} \tilde{B}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, n, m), \tag{H.22}
\]

where:

\[
\tilde{A}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, m) = \frac{(\mu_0 - \mu_1)^2(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_3)(\mu_0 - \nu_3)}{\mu_1\mu_2} \times \left( \sum_{i_4 \leq i_5 \leq \ldots \leq i_{m-3}} \mu_{i_4}\mu_{i_5} \cdots \mu_{i_{m-3}} \right)_{\nu_3 \rightarrow \nu_3} \tag{H.23}
\]

and

\[
\tilde{B}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, n, m) = -\mu_0\mu_1\mu_2\mu_3 \tilde{A}_{04}(\mu_0, \mu_0, \mu_2, \mu_3, \nu_3, m) \times \left( \sum_{i_4 \leq i_5 \leq \ldots \leq i_{m-4}} \mu_{i_4}\mu_{i_5} \cdots \mu_{i_{m-4}} \right)_{\nu_3 \rightarrow \nu_3} \tag{H.24}
\]

We assume that the indexes in the sums run over the set \( \{0, 1, 2, 3\} \), we define \( \sum_{i_4 \leq i_5 \leq \ldots \leq i_{m-3}} \nu_3 = 1 \) and with \( \mu_3 \rightarrow \nu_3 \) in \((H.23)\) we intend that every \( \mu_3 \) contained in the sum must be replaced with a \( \nu_3 \).

From \((H.23)\) and \((H.24)\) we deduce that the coefficients of \( Y_{0,m} \) and \( Y_{m,0} \) have always opposite sign, hence the upper bound of \( Y_{0,4} \) is obtained from \((H.22)\) by setting all the yields \( Y_{nm} \) (with \( m > 4 \)) to zero and the yields \( Y_{nm} \) (with \( n > 4, m > 3 \)) to one. After rearranging the terms, we get the following expression for the upper bound on \( Y_{0,4} \) under the conditions \( \nu_0 = \mu_0, \nu_1 = \mu_1 \) and \( \nu_2 = \mu_2 \):
\[
\begin{align*}
Y_{40}^{U} = & \frac{24}{A_{04}(\mu_0, \mu_2, \mu_3, \nu_4)} \left[ \bar{H}_{04} - \sum_{n=4}^{\infty} \frac{\hat{B}_{04}(\mu_0, \mu_2, \mu_3, \nu_4, n, m)}{n!m!} \right], \\
\text{(H.25)}
\end{align*}
\]

where \( \bar{H}_{04} \) is given in the first line of \((H.20)\), the function \( A_{04} \) evaluated for \( m = 4 \) reads:

\[
A_{04}(\mu_0, \mu_2, \mu_3, \nu_4) = -\frac{(\mu_0 - \mu_2)(\mu_0 - \mu_3)(\mu_0 - \nu_4)}{\mu_1 \mu_2} (\mu_0 + \mu_1 + \mu_2 + \nu_4),
\]

and the series of \( \hat{B}_{04} \) sums to:

\[
\sum_{n=4}^{\infty} \frac{\hat{B}_{04}(\mu_0, \mu_2, \mu_3, \nu_4, n, m)}{n!m!} = \frac{\mu_0 \mu_3}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3)(\mu_1 - \nu_4)(\mu_2 - \nu_4)} \times \\
\left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3) \\
- \left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_0 - \mu_2)(\mu_0 - \mu_3)(\mu_2 - \mu_3) \\
+ \left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_0 - \mu_1)(\mu_0 - \mu_3)(\mu_1 - \mu_3) \\
- \left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)
\]

\[
\times \\
\left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_1 - \mu_2)(\mu_1 - \nu_4)(\mu_2 - \nu_4) \\
- \left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_0 - \mu_2)(\mu_0 - \nu_4)(\mu_2 - \nu_4) \\
+ \left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_0 - \mu_1)(\mu_0 - \nu_4)(\mu_1 - \nu_4) \\
- \left( e^{\nu_4} - \frac{\mu_0^2}{2} - \mu_0 - 1 \right) (\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2),
\]

\[
\text{(H.27)}
\]

**H.2. Upper bound on \( Y_{40} \)**

Similarly to the bound on \( Y_{04} \), we consider the combination of gains \((G.37)\) that leads to the bound on \( Y_{40} \) in the case of three decoy intensity settings:

\[
C_{20}^{0,1,2} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{20}^{0,1,2}(n, m),
\]

\[
\text{(H.28)}
\]

where the function \( C_{20}^{0,1,2}(n, m) \) is defined by the rhs of \((G.37)\), while \( C_{20}^{0,1,2} \) is the combination of gains given by \((G.31)\), with the coefficients \( c_{ij} \) of the combination given in \((G.36)\). From \( G.4 \) we know that the terms \( Y_{nt_1}, Y_{nt_2}, Y_{om} \) and \( Y_{1m} \) are removed in \((H.28)\). Following the same procedure described in \((H.1)\), we derive three additional combinations of gains in which the terms \( Y_{nt_1}, Y_{nt_2}, Y_{om} \) and \( Y_{1m} \) are removed:

\[
C_{20}^{0,1,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{20}^{0,1,3}(n, m),
\]

\[
\text{(H.29)}
\]

\[
C_{20}^{0,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{20}^{0,2,3}(n, m),
\]

\[
\text{(H.30)}
\]

\[
C_{20}^{1,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{20}^{1,2,3}(n, m).
\]

\[
\text{(H.31)}
\]
Now we further combine these expressions with arbitrary real coefficients \(d_{i,j,k}\):

\[
H_{40} \equiv d_{0,1,2}G_{20}^{0,1,2} + d_{0,1,3}G_{20}^{0,1,3} + d_{0,2,3}G_{20}^{0,2,3} + d_{1,2,3}G_{20}^{1,2,3}
\]

\[
= \sum_{n,m} Y_{nm} \sum_{n,m} \frac{d_{0,1,2}}{n!} (n,m) + \frac{d_{0,1,3}}{n!} (n,m) + \frac{d_{0,2,3}}{n!} (n,m) + \frac{d_{1,2,3}}{n!} (n,m),
\]

(H.32)

and impose that even the terms \(Y_{n0}\) and \(Y_{2m}\) are removed from the rhs of (H.32). This yields a linear system of equations in the variables \(d_{i,j,k}\), whose unique solution (up to a global rescaling) reads as follows:

\[
d_{0,1,2} = 1
\]

\[
d_{0,1,3} = \left( \frac{\nu_0 - \nu_2}{\nu_0 - \nu_1} \right) \left( \frac{\nu_0 - \nu_3}{\nu_0 - \nu_1} \right) \left( \nu_0 - \nu_3 \right)
\]

\[
d_{0,2,3} = \left( \frac{\nu_0 - \nu_1}{\nu_0 - \nu_2} \right) \left( \nu_0 - \nu_3 \right)
\]

\[
d_{1,2,3} = \frac{\nu_0}{\nu_1 - \nu_2} \frac{\nu_0}{\nu_1 - \nu_3} \frac{\nu_0}{\nu_2 - \nu_3} \frac{\nu_0}{\nu_2 - \nu_1} \frac{\nu_0}{\nu_3 - \nu_1} \frac{\nu_0}{\nu_3 - \nu_2} \frac{\nu_0}{\nu_3 - \nu_2} \frac{\nu_0}{\nu_3 - \nu_1}
\]

(H.33)

By substituting the solution (H.33) back into (H.32) and by rearranging the rhs, one gets a combination of gains where all the terms \(Y_{n1}\), \(Y_{2m}\), \(Y_{0m}\) and \(Y_{2m}\) are removed:

\[
H_{40} = \sum_{n=3}^{\infty} \frac{Y_{n0}}{A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, n)} + \sum_{m=4}^{\infty} \frac{Y_{nm}}{A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, m, n)}
\]

(H.34)

where the functions \(A_{04}\) and \(B_{04}\) are the same found in bounding \(Y_{04}\) with four decoys and are given by (H.10) and (H.12), respectively. Note that in this case the roles of the intensities \(\mu_i\) and \(\nu_i\) are exchanged with respect to the bound on \(Y_{04}\) (see (H.9)), as well as the roles of \(n\) and \(m\). Following the same reasoning of (H.1), we can conclude that the coefficients of \(Y_{04}\) and \(Y_{nm}\) have always opposite sign. Hence the upper bound on \(Y_{40}\) is obtained from (H.34) by setting all the yields \(Y_{n0}\) (with \(n \neq 4\)) to zero and the yields \(Y_{nm}\) (with \(n \geq 3, m \geq 4\)) to one. After rearranging the terms, we get the following expression for the upper bound on \(Y_{40}\):

\[
Y_{40}^U = \frac{24}{A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, 4)} \left[ H_{40} - \sum_{n=3}^{\infty} \frac{A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, m, n)}{n!m!} \right]
\]

(H.35)

where \(H_{40}\) is given in the first line of (H.32), while \(A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, 4)\) and the sum of the series are given in (H.14) and (H.15), respectively, under the replacement \(\mu_i \leftrightarrow \nu_i\) for \(i = 0, 1, 2, 3, 4\).

We remark that in deriving the bound (H.35) we implicitly assumed—as in the \(Y_{04}\) case—that at least one of the following equalities does not hold: \(\nu_0 = \mu_0\), \(\nu_1 = \mu_2\) and \(\nu_2 = \mu_2\). Indeed, when all three equalities hold (i.e., when Alice and Bob are using the same intensities settings for three out of four decoy pulses) one gets a \(0_0^0\) form in the bound expression (H.35). In order to overcome this issue, one can follow an analogous procedure to that performed for the same issue affecting the bound on \(Y_{04}\) (see last paragraph in (H.1)), and obtain an additional upper bound on \(Y_{40}\) which is valid in the particular case of: \(\nu_0 = \mu_0\), \(\nu_1 = \mu_1\) and \(\nu_2 = \mu_2\). The new bound on \(Y_{40}\) reads:

\[
Y_{40}^U = \frac{24}{A_{04}(\mu_0, \mu_1, \mu_2, \nu_3, \mu_3, 4)} \left[ H_{40} - \sum_{n=3}^{\infty} \frac{B_{04}(\mu_0, \mu_3, \mu_2, \nu_3, \mu_3, n, m)}{n!m!} \right]
\]

(H.36)

where \(H_{40}\) is given by:

\[
H_{40} = \tilde{d}_{0,1,2}G_{20}^{0,1,2} + \tilde{d}_{0,1,3}G_{20}^{0,1,3} + \tilde{d}_{0,2,3}G_{20}^{0,2,3} + \tilde{d}_{1,2,3}G_{20}^{1,2,3}
\]

(H.37)

where:

\[
\tilde{d}_{0,1,2} = 0
\]

\[
\tilde{d}_{0,1,3} = \nu_3
\]

\[
\tilde{d}_{0,2,3} = \frac{(\mu_0 - \nu_1)\nu_2}{\nu_1 - \nu_2}
\]

\[
\tilde{d}_{1,2,3} = \frac{\mu_0\nu_3(\mu_0 - \nu_1)(\mu_0 - \nu_2)(\mu_0 - \nu_3)}{\nu_1(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\nu_1 - \nu_3)}
\]

(H.38)
and \( \tilde{C}_{10} \) are the same gains combinations (H.28), (H.29), (H.30) and (H.31) derived at the beginning of this Subsection, under the replacements: \( \nu_0 \rightarrow \mu_0 \), \( \nu_1 \rightarrow \mu_1 \) and \( \nu_2 \rightarrow \mu_2 \). The quantity \( \tilde{A}_{04} \) and the sum of the series are instead given in (H.26) and (H.27), respectively, under the replacement \( \tilde{\nu}_3 \rightarrow \nu_3 \).

H.3. Upper bound on \( Y_{13} \)

We follow the same procedure used in bounding the other yields in the case of four decoy intensity settings. We start by considering the four combination of gains in which the terms \( Y_{10}, Y_{11}, Y_{0m} \) and \( Y_{2m} \) are removed:

\[
\begin{align*}
G_{13}^{0,1,2} &= \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{13}^{0,1,2}(n, m), \\
G_{13}^{0,1,3} &= \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{13}^{0,1,3}(n, m), \\
G_{13}^{0,2,3} &= \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{13}^{0,2,3}(n, m), \\
G_{13}^{1,2,3} &= \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{13}^{1,2,3}(n, m),
\end{align*}
\]

(H.39)

where the last three combinations are derived from the first one as described in (H.1), while the first combination is given by (G.44). Now we further combine these expressions with arbitrary real coefficients \( d_{i,j,k} \):

\[
H_{i3} \equiv d_{0,1,2} G_{13}^{0,1,2} + d_{0,1,3} G_{13}^{0,1,3} + d_{0,2,3} G_{13}^{0,2,3} + d_{1,2,3} G_{13}^{1,2,3} \\
= \sum_{n,m} \frac{Y_{nm}}{n!m!} \left[ d_{0,1,2} C_{13}^{0,1,2}(n, m) + d_{0,1,3} C_{13}^{0,1,3}(n, m) + d_{0,2,3} C_{13}^{0,2,3}(n, m) + d_{1,2,3} C_{13}^{1,2,3}(n, m) \right],
\]

(H.43)

and impose that even the terms \( Y_{12} \) and \( Y_{3m} \) are removed from the rhs of (H.43). This yields a linear system of equations in the variables \( d_{i,j,k} \), whose unique solution (up to a global rescaling) reads as follows:

\[
\begin{align*}
d_{0,1,2} &= 1 \\
d_{0,1,3} &= \frac{\left( \mu_0 - \mu_1 \right) \left( \mu_1 + \mu_2 \right) \left( \nu_0 - \nu_2 \right)}{\left( \mu_0 - \mu_2 \right) \left( \nu_0 - \nu_3 \right)} \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \\
&\quad \times \left\{ \frac{\nu_0^2 \left( \mu_1 - \mu_2 \right) \left( \nu_1 - \nu_3 \right) \left( \nu_3 - \nu_0 \right)}{\left( \mu_1 \nu_1 + \nu_3 \nu_0 - \mu_2 \nu_2 \right)} + \mu_1 \mu_2 \nu_0 \nu_3 \right\} \}.
\]

(H.44)

By substituting the solution (H.44) back into (H.43) and by rearranging the rhs, one gets a combination of gains where all the terms \( Y_{10}, Y_{11}, Y_{0m}, Y_{2m}, \) and \( Y_{3m} \) are removed:

\[
H_{i3} = \sum_{m=3}^{\infty} \frac{Y_{nm}}{m!} A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, m) \\
+ \sum_{m=3}^{\infty} \frac{Y_{nm}}{m!} A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, m) D_{04}(\mu_0, \mu_1, \mu_2, \mu_3),
\]

(H.45)

where:

\[
A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, m) = \left( \frac{\nu_0 - \nu_1}{\nu_0 - \nu_2} \right) \left( \frac{\nu_0 - \nu_1}{\nu_0 - \nu_2} \right) \left( \frac{\nu_0 - \nu_1}{\nu_0 - \nu_2} \right) \left( \frac{\nu_0 - \nu_1}{\nu_0 - \nu_2} \right) \left( \frac{\nu_0 - \nu_1}{\nu_0 - \nu_2} \right) \left( \frac{\nu_0 - \nu_1}{\nu_0 - \nu_2} \right) \\
\times \sum_{i_1, i_2, ..., i_{m-3} \in I_{\text{set}}} \nu_{i_1} \nu_{i_2} \cdots \nu_{i_{m-3}}.
\]

(H.46)
\( p_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3) = \mu_1^2 [\mu_2^2 (\nu_0 - \nu_3)(\nu_1 - \nu_2) - \mu_3^2 (\nu_0 - \nu_2)(\nu_1 - \nu_3)] \\
+ \mu_2^2 [\mu_1^2 (\nu_0 - \nu_2)(\nu_1 - \nu_3) - \mu_3^2 (\nu_0 - \nu_1)(\nu_2 - \nu_3)] \\
+ \mu_3^2 [\mu_1^2 (\nu_0 - \nu_1)(\nu_2 - \nu_3); \\
(\text{H.47})] \\
q_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3) = \mu_0^2 \mu_1 (\mu_1 + \mu_3) (\nu_1 - \nu_2) - \mu_1^2 (\mu_2 + \mu_3)(\nu_0 - \nu_2) \\
+ \mu_2^2 (\mu_0 + \mu_3)(\nu_0 - \nu_1), \\
(\text{H.48})

and \( D_n \) is defined recursively as [28]:

\[
D_n(\mu_0, \mu_1, \mu_2, \mu_3) = \sum_{i=1}^{n-4} \left( \mu_0^i + \mu_1^i + \mu_2^i + \mu_3^i \right) D_{n-i}(\mu_0, \mu_1, \mu_2, \mu_3) \mu_0 \mu_1 \mu_2 \mu_3 \left( \sum_{j=1}^{k} \mu_j \mu_{j+1} \cdots \mu_{k-1} \right)
\]

\( D_n(\mu_0, \mu_1, \mu_2, \mu_3) = \mu_0 \mu_1 \mu_2 + \mu_0 \mu_1 \mu_3 + \mu_0 \mu_2 \mu_3 + \mu_1 \mu_2 \mu_3 \).

\( (\text{H.49}) \)

We assume that the indexes in the sums run over the set \( \{0, 1, 2, 3\} \) and we define \( \sum_{i=0}^{n} \mu_i \nu_i \cdots \nu_{n-1} \nu_n = 1 \). Since \( D_n \geq 0 \) for every \( n \geq 4 \), we deduce that the coefficients of \( Y_{1m} \) and \( Y_{im} \) in (H.45) have always equal sign.

Hence the upper bound on \( Y_{13} \) is obtained from (H.45) by setting all the other yields to zero. After rearranging the terms, we get the following expression for the upper bound on \( Y_{13} \):

\[
Y_{13}^U = \frac{6 H_{13}}{A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3)},
\]

\( (\text{H.50}) \)

where \( H_{13} \) is given in the first line of (H.43), while \( A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3) \) is given by:

\[
A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3) = \frac{(\mu_0 - \mu_1)(\mu_2 - \mu_3)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)}.
\]

\( (\text{H.51}) \)

**H.4. Upper bound on \( Y_{13} \)**

We follow the same procedure used in bounding the other yields in the case of four decoy intensity settings. We start by considering the four combination of gains in which the terms \( Y_{00}, Y_{12}, Y_{01} \) and \( Y_{1m} \) are removed:

\[
C_{13}^{0,1,2} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{31}^{0,1,2}(n, m),
\]

\( (\text{H.52}) \)

\[
C_{13}^{0,1,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{31}^{0,1,3}(n, m),
\]

\( (\text{H.53}) \)

\[
C_{13}^{0,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{31}^{0,2,3}(n, m),
\]

\( (\text{H.54}) \)

\[
C_{13}^{1,2,3} = \sum_{n,m} \frac{Y_{nm}}{n!m!} C_{31}^{1,2,3}(n, m),
\]

\( (\text{H.55}) \)

where the last three combinations are derived from the first one as described in (H.1), while the first combination is given by (G.48). Now we further combine these expressions with arbitrary real coefficients \( d_{i,j,k} \):

\[
H_{13} = d_{0,1,2} C_{13}^{0,1,2} + d_{0,1,3} C_{13}^{0,1,3} + d_{0,2,3} C_{13}^{0,2,3} + d_{1,2,3} C_{13}^{1,2,3}
\]

\[
= \sum_{n,m} \frac{Y_{nm}}{n!m!} \left[ d_{0,1,2} C_{31}^{0,1,2}(n, m) + d_{0,1,3} C_{31}^{0,1,3}(n, m) + d_{0,2,3} C_{31}^{0,2,3}(n, m) + d_{1,2,3} C_{31}^{1,2,3}(n, m) \right],
\]

\( (\text{H.56}) \)

and impose that even the terms \( Y_{13} \) and \( Y_{2m} \) are removed from the rhs of (H.56). This yields a linear system of equations in the variables \( d_{i,j,k} \), whose unique solution (up to a global rescaling) is given in (H.44), under the replacement: \( \mu_i \leftrightarrow \nu_i \) for \( i = 0, 1, 2, 3 \). By substituting the solution back into (H.56) and by rearranging the rhs, one gets a combination of gains where all the terms \( Y_{00}, Y_{12}, Y_{01}, Y_{0m}, Y_{1m} \) and \( Y_{2m} \) are removed:

\[
H_{13} = \sum_{n=3}^{\infty} \frac{Y_{nm}}{n!} A_{13}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, n)
\]

\[
+ \sum_{n=4}^{\infty} \frac{Y_{nm}}{n!} A_{13}(\nu_0, \nu_2, \nu_3, \nu_0, \nu_1, \mu_0, \mu_1, \mu_2, \mu_3, n) D_n(\nu_0, \nu_1, \nu_2, \nu_3),
\]

\( (\text{H.57}) \)
where the functions $A_{13}$ and $D_m$ are defined in (H.46) and (H.49), respectively. Since $D_m \geq 0$ for every $m \geq 4$, we deduce that the coefficients of $Y_{13}$ and $Y_{mn}$ in (H.57) have always equal sign. Hence the upper bound on $Y_{31}$ is obtained from (H.57) by setting all the other yields to zero. After rearranging the terms, we get the following expression for the upper bound on $Y_{31}$:

$$Y_{31}^U = \frac{6H_{13}}{A_{13}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, 3)},$$

where $H_{13}$ is given in the first line of (H.56), while $A_{13}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, 3)$ is given by (H.51) under the substitution: $\mu_i \leftrightarrow \nu_i$ for $i = 0, 1, 2, 3$.

**ORCID iDs**

Federico Grasselli  🌐 https://orcid.org/0000-0003-2966-7813

**References**

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India) (Piscataway, NJ: IEEE) pp 175–9

[2] Ekert A K 1991 Phys. Rev. Lett. 67 661–3

[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301

[4] Lo H K, Curty M and Tamaki K 2014 Nat. Photon. 8 595–604

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

[6] Tamaki K, Lo H K, Wang W and Lucamarini M 2018 arXiv:1805.05511

[7] Liao S K et al 2017 Nature 549 43

[8] Takenaka H, Carrasco-Casadó A, Fujiwara M, Kitamura M, Sasaki M and Toyoshima M 2017 Nat. Photon. 11 502

[9] Takeoka M, Guha S and Wilde M M 2014 Nat. Commun. 5 5235

[10] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Nature 557 400

[11] Wang X B, Yu Z W and Hu X L 2018 Phys. Rev. A 98 062323

[12] Curty M, Azuma K and Lo H K 2019 NPJ Quantum Inf. 5 64

[13] Ma X, Zeng P and Zhou H 2018 Phys. Rev. X 8 031043

[14] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 Phys. Rev. Appl. 11 034053

[15] Tamaki K, Lo H K, Wang W and Lucamarini M 2018 arXiv:1805.05511

[16] Lin J and Lütkenhaus N 2018 Phys. Rev. A 98 022332

[17] Zhong X, Hu J, Curty M, Qian L and Lo H K 2019 Phys. Rev. Lett. 123 100506

[18] Minder M, Pittaluga M, Roberts G, Lucamarini M, Dynes J and Shields A 2019 Nat. Photon. 13 334–8

[19] Wang X B, Yu Z W and Hu X L 2018 Phys. Rev. A 98 062323

[20] Curty M, Azuma K and Lo H K 2019 New J. Phys. 21 037001

[21] Wang W, Xu F and Lo H K 2018 Phys. Rev. X 8 031043

[22] Zhou X Y, Zhang C H, Zhang C M and Wang Q 2019 Phys. Rev. A 99 062316

[23] Wang X B, Peng C Z and Pan J W 2007 Appl. Phys. Lett. 90 031110

[24] Wang X B 2007 Phys. Rev. A 75 052301

[25] Chi H H, Yu Z W and Wang X B 2012 Phys. Rev. A 86 042307

[26] Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2016 Phys. Rev. A 94 032335

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

[28] X. Ho L K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504

[29] Wang X B 2005 Phys. Rev. Lett. 94 230503

[30] Xu F, Curty M, Qi B and Lo H K 2013 New J. Phys. 15 113007

[31] Xu F, Sajeev S, Kaiser S, Tang Z, Qian L, Makarov V and Lo H K 2015 Phys. Rev. A 92 032305

[32] Liu H et al 2019 Phys. Rev. Lett. 122 160501

[33] Xu F, Xu H and Lo H K 2014 Phys. Rev. A 89 052333

[34] Boyd S and Vandenberghe L 2004 Convex Optimization (Cambridge: Cambridge University Press)

[35] WolfCam Research, Inc. 2016 Mathematica, Version 11.0, Champaign, IL

[36] Wang W and Lo H K 2019 arXiv:1907.05291