Practical decoy-state method for twin-field quantum key distribution

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
5 February 2019

REVISED
3 June 2019

ACCEPTED FOR PUBLICATION
19 June 2019

PUBLISHED
1 July 2019

PAPER

Practical decoy-state method for twin-field quantum key distribution

Federico Grasselli[1] and **Marcos Curty**[2]

[1] Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany
[2] Escuela de Ingeniería de Telecomunicación, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain

E-mail: federico.grasselli@hhu.de

Keywords: twin-field quantum key distribution, decoy-state method, single-photon interference, measurement-device-independent quantum key distribution (MDI-QKD), analytical bounds

Abstract

Twin-field (TF) quantum key distribution (QKD) represents a novel QKD approach whose principal merit is to beat the point-to-point private capacity of a lossy quantum channel, thanks to performing single-photon interference in an untrusted node. Indeed, recent security proofs of various TF-QKD type protocols have confirmed that the secret key rate of these schemes scales essentially as the square root of the transmittance of the channel. Here, we focus on the TF-QKD protocol introduced by Curty *et al*, whose secret key rate is nearly an order of magnitude higher than previous solutions. Its security relies on the estimation of the detection probabilities associated to various photon-number states through the decoy-state method. We derive analytical bounds on these quantities assuming that each party uses either two, three or four decoy intensity settings, and we investigate the protocol's performance in this scenario. Our simulations show that two decoy intensity settings are enough to beat the point-to-point private capacity of the channel, and that the use of four decoys is already basically optimal, in the sense that it almost reproduces the ideal scenario of infinite decoys. We also observe that the protocol seems to be quite robust against intensity fluctuations of the optical pulses prepared by the parties.

The last few decades have witnessed major advancements in the field of quantum communication [1, 2], with quantum key distribution (QKD) [3–13] being its most developed application. Recent experiments over about 400 km of optical fibers [14, 15] and over about 1000 km of satellite-to-ground links [16, 17] demonstrated that QKD over long distances is possible. Despite such remarkable experimental achievements, the private capacity of point-to-point QKD is intrinsically limited by fundamental bounds [18, 19]. These bounds state that in the high-loss regime the key rate scales basically linearly with the transmittance of the channel connecting the end-users Alice and Bob, i.e. it decreases exponentially with the total channel length. This imposes strict practical constraints on the possibility of achieving point-to-point QKD over arbitrary long distances.

A way to overcome this limitation is to employ one or more intermediate nodes in the quantum channel connecting the parties. For instance, the use of quantum repeaters [20] yields a polynomial scaling of the communication efficiency with the distance [21]. Moreover, a quantum repeater scheme can be arbitrarily iterated along the quantum channel, thus increasing in principle the total communication distance between Alice and Bob as much as desired. Unfortunately, however, quantum repeaters are very challenging to build in practice with current technology: they either require quantum memories [20–22] or quantum error correction [23, 24]. Of course, technology is improving, and quantum repeaters may become viable in the future.

Other solutions, which attain a square-root improvement in the scaling of the key rate with respect to the transmittance of the channel, are obtained by placing a single untrusted relay between Alice and Bob. Such protocols include, for instance, measurement-device-independent-QKD [6] (MDI-QKD) with quantum memories [25, 26] and adaptive MDI-QKD featuring quantum non-demolition measurements [27]. The philosophy behind both types of protocols is that the central relay is able to adapt the pairings of photons received from Alice and Bob to the photon losses. In this way, for every signal sent by Alice and Bob to the central relay, just one of the two signals is required to arrive, leading to the mentioned square-root improvement in the key rate scaling. However, both protocols still require two-photon interference in the central node, as in the

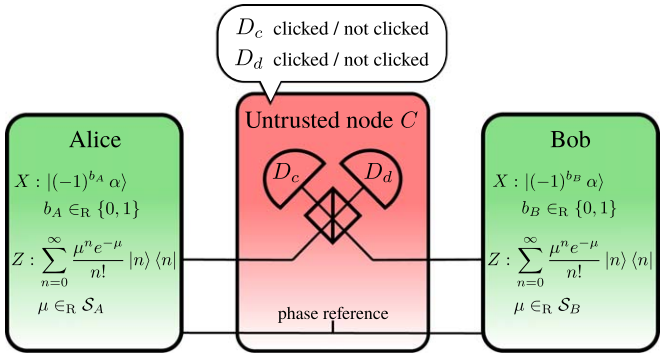

Figure 1. The twin-field QKD protocol introduced in [33].

original MDI-QKD scheme [6]. More recently, [28] proposed the twin-field (TF) QKD protocol, still characterized by an untrusted central node, and conjectured a square-root improvement in the key rate scaling. This scaling has been later on confirmed in [29, 30] for two variants of the original scheme. The advantage of TF-QKD lies in the fact that it is designed to generate key bits from single-photon interference in the central node, thus naturally retaining the scaling with the square-root of the transmittance without the need to adapt to photon losses via sophisticated devices.

Since the original proposal, there has been an intense research activity to develop different versions of TF-QKD protocols equipped with their security proofs [29–33] as well as to investigate their experimental feasibility [34–36]. Among these protocols, the one that seems to deliver the higher secret ket rate [37] is that introduced in [33]. Its security relies on the ability to estimate the detection statistics (usually called yields) of various Fock states sent by Alice and Bob through the decoy-state method [38–40]. The key-rate simulations provided in [33] indeed exhibit an improved scaling with the loss, but the estimation of the yields is only carried out by means of *numerical* tools based on linear programming and considering only the case of three decoy intensity settings.

In this paper, we derive *analytical* bounds on the yields which are required to evaluate the key rate formula of [33], assuming two, three and four decoy intensity settings. In so doing, we are able to show, for instance, that the use of two decoy intensity settings is already enough to beat the point-to-point private capacity bound reported in [19]. Also, we show that the use of four decoys is basically optimal in the sense that the resulting secret key rate is already very close to the ideal scenario which assumes infinite decoy intensity settings. Analytical bounds imply a fully-analytical expression for the protocol's secret key rate, which could be very convenient for performance optimization in scenarios where the number of parameters is high, like for instance in finite-key security analyses. In addition, we study how the performance of TF-QKD is affected under intensity fluctuations, which are inevitable in practice, and we demonstrate that the protocol in [33] seems to be actually quite robust against such fluctuations.

Like in [33], for simplicity, here we focus on the asymptotic-key rate scenario. However, we remark that by using the techniques reported in [41], it is cumbersome but straightforward to adapt our analytical methods also to the finite-key rate scenario, where, as mentioned above, it becomes particularly useful to have analytical bounds for the main quantities that enter the key rate formula.

The article is structured as follows. In section 1 we present the TF protocol from [33] and highlight the main yields that need to be bounded. In section 2 we provide the analytical bounds on the yields for the case of two decoys (the cases of three and four decoys are treated in appendices C and D, respectively). In section 3 we provide simulations of the secret key rate versus the loss for a typical channel model (briefly described in appendix A), and we also evaluate the effect of intensity fluctuations. We conclude the paper in section 4.

1. The TF-QKD protocol

As discussed above, we consider the TF-QKD protocol presented in [33] and sketched in figure 1. Alice and Bob establish a secret shared key by sending optical pulses to a central untrusted node, C. It is assumed that the node C shares a phase reference with Alice and Bob, which can be achieved by the transmission of strong optical pulses. The protocol is composed of the following five steps.

(i) Alice (Bob) chooses the X-basis with probability p_X and the Z-basis with probability $p_Z = 1 - p_X$. Upon choosing the X-basis, Alice (Bob) prepares an optical pulse in a coherent state $|\alpha\rangle$ or $|-\alpha\rangle$ at random, corresponding to the key bit $b_A = 0$ ($b_B = 0$) or $b_A = 1$ ($b_B = 1$), respectively. Upon choosing the Z-basis,

she (he) prepares an optical pulse in a phase-randomized coherent state:

$$\hat{\rho}_{\beta_A} = \frac{1}{2\pi}\int_0^{2\pi} \mathrm{d}\theta |\beta_A \mathrm{e}^{\mathrm{i}\theta}\rangle\langle\beta_A \mathrm{e}^{\mathrm{i}\theta}| = \sum_{n=0}^{\infty} \frac{(\beta_A^2)^n \mathrm{e}^{-\beta_A^2}}{n!} |n\rangle\langle n| \tag{1.1}$$

($\hat{\rho}_{\beta_B}$) whose intensity β_A^2 (β_B^2) is drawn randomly from a set $\mathcal{S}_A = \{\beta_i^2\}_i$ ($\mathcal{S}_B = \{\beta_j^2\}_j$) of real non-negative numbers.

(ii) Both parties send their optical pulses to the untrusted node C via optical channels in a synchronized manner.

(iii) The central node C applies a balanced beamsplitter to the incoming pulses and features two threshold detectors at its output ports. The detector placed at the output port associated to constructive (destructive) interference is denoted by D_c (D_d).

(iv) The node C announces the measurement outcome k_c (k_d) of detector D_c (D_d), with $k_c = 0$ and $k_c = 1$ ($k_d = 0$ and $k_d = 1$) corresponding to a no-click and a click event, respectively.

(v) Alice and Bob form their raw keys with the bits b_A and b_B collected when both parties chose the X-basis and node C reported a click in only one detector ($k_c + k_d = 1$). Bob flips his bits b_B for which the click occurred in D_d.

1.1. Secret key rate formula

The security analysis performed in [33] yields the following lower bound on the asymptotic key rate R:

$$R \geqslant \max\{R_{10}, 0\} + \max\{R_{01}, 0\}, \tag{1.2}$$

where the terms $R_{k_c k_d}$, for $(k_c, k_d) \in \{(1,0),(0,1)\}$, are defined as:

$$R_{k_c k_d} = p_X^2\, p(k_c, k_d)[1 - f\, h(e_{k_c k_d}) - h(e^{\mathrm{ph}}_{k_c k_d})], \tag{1.3}$$

with $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ being the binary entropy function, f the inefficiency function associated to error correction, and $p(k_c, k_d)$ the conditional probability that node C announces the outcome (k_c, k_d) when both parties selected the X-basis. The probability $p(k_c, k_d)$ can be expressed as:

$$p(k_c, k_d) = \sum_{b_A, b_B = 0}^{1} p(b_A, b_B)\, p(k_c, k_d | b_A, b_B), \tag{1.4}$$

where $p(b_A, b_B)$ is the joint probability of Alice and Bob preparing the coherent states $|(-1)^{b_A}\alpha\rangle$ and $|(-1)^{b_B}\alpha\rangle$, respectively. According to the protocol description above, we have: $p(b_A, b_B) = 1/4\ \forall\, b_A, b_B$. $p(k_c, k_d | b_A, b_B)$ instead denotes the conditional probability that node C announced (k_c, k_d) given that Alice and Bob sent the coherent states $|(-1)^{b_A}\alpha\rangle$ and $|(-1)^{b_B}\alpha\rangle$, respectively. Since we consider the asymptotic key-rate scenario, we assume that $p(k_c, k_d | b_A, b_B)$ coincides with the correspondent distribution observed by the parties.

Finally, the terms $e_{k_c k_d}$ and $e^{\mathrm{ph}}_{k_c k_d}$ in (1.3) represent the bit-error rate in the X-basis and an upper bound on the phase-error rate, respectively. The former is defined as:

$$e_{10} = \frac{\sum_{i,j=0|i\oplus j=1}^{1} p(b_A = i, b_B = j)\, p(k_c = 1, k_d = 0 | b_A = i, b_B = j)}{p(k_c = 1, k_d = 0)}, \tag{1.5}$$

$$e_{01} = \frac{\sum_{i=0}^{1} p(b_A = i, b_B = i)\, p(k_c = 0, k_d = 1 | b_A = i, b_B = i)}{p(k_c = 0, k_d = 1)}, \tag{1.6}$$

and the latter as:

$$e^{\mathrm{ph}}_{k_c k_d} = \frac{1}{p(k_c, k_d)}\left[\left(\sum_{n,m=0}^{\infty} c_{2n} c_{2m} \sqrt{Y^{k_c,k_d}_{2n\,2m}}\right)^2 + \left(\sum_{n,m=0}^{\infty} c_{2n+1} c_{2m+1} \sqrt{Y^{k_c,k_d}_{2n+1\,2m+1}}\right)^2\right], \tag{1.7}$$

where the coefficients c_n are defined as $c_n = \mathrm{e}^{\frac{-\alpha^2}{2}}\alpha^n/\sqrt{n!}$ and the yields Y^{k_c,k_d}_{nm} are the conditional probabilities that node C announces the outcome (k_c, k_d) given that Alice and Bob emitted an n-photon state and an m-photon state, respectively. Note that the only yields contributing to (1.7) are those Y^{k_c,k_d}_{nm} such that $n + m$ is an even number.

The yields Y^{k_c,k_d}_{nm} are quantities that are not directly observed by the parties, however they can be estimated either numerically or analytically with techniques based on the decoy-state method [38–40]. Here we consider the analytical approach. In particular, we assume that Alice and Bob have at their disposal either two, three or four decoy intensity settings when choosing the Z-basis. To each further decoy intensity correspond additional linear constraints on the yields, leading to tighter estimations of Y^{k_c,k_d}_{nm} and thus to a higher key rate. However, a

finite number of decoys only allows to derive non-trivial upper bounds[3] on a limited number of yields in (1.7), whereas the other yields are set to 1. Nevertheless, even bounding just four yields in a non-trivial way is enough for the secret key rate to beat the point-to-point private capacity bound (PLOB bound) [19] at high losses (see section 3). Also, as we show below, with four decoy intensity settings one can already obtain a secret key rate very close to that achievable with infinite decoy intensity settings.

We remark that standard decoy-state-based QKD protocols require to *lower* bound the value of a few yields (typically those associated to vacuum and single-photon pulses) [42], while the TF-QKD protocol considered here upper bounds the value of the phase-error rate (1.7) by *upper* bounding several yields. In particular, we upper bound the yields $Y_{nm}^{k_c,k_d}$ for $(n,\ m) \in \mathcal{I}$, where $\mathcal{I}$ is a certain subset of $\{(n,\ m)|\ n,\ m \in \mathbb{N}_0\}$ which depends on the number of decoys. Thanks to the derived upper bounds on the yields (which we shall denote by Y_{nm}^{U,k_c,k_d}) we are able to estimate the phase error rate (1.7) as follows:

$$e_{k_c k_d}^{\mathrm{ph}} \leqslant \frac{1}{p(k_c,\ k_d)}\left[\left(\sum_{(2n,2m)\in\mathcal{I}} c_{2n}c_{2m}\sqrt{Y_{2n\ 2m}^{U,k_c,k_d}} + \sum_{(2n,2m)\notin\mathcal{I}} c_{2n}c_{2m}\right)^2 + \left(\sum_{(2n+1,2m+1)\in\mathcal{I}} c_{2n+1}c_{2m+1}\sqrt{Y_{2n+1\ 2m+1}^{U,k_c,k_d}} + \sum_{(2n+1,2m+1)\notin\mathcal{I}} c_{2n+1}c_{2m+1}\right)^2\right]. \tag{1.8}$$

2. Yields estimation

When both Alice and Bob choose the Z-basis in the first step of the TF-QKD protocol, they prepare phase-randomized coherent states with intensities β_A^2 and β_B^2, respectively, and send them to C. From Eve's viewpoint, she cannot distinguish this scenario from the case in which the parties prepared number states $|n\rangle$ and $|m\rangle$ according to the Poissonian distributions $P_{\beta_A^2}(n)$ and $P_{\beta_B^2}(m)$ (see equation (1.1)), where $P_\mu(n) = \mathrm{e}^{-\mu}\mu^n/n!$. Therefore Eve's attack can only depend on the number states $|n\rangle$ and $|m\rangle$ but not on the signals' intensities β_A^2 and β_B^2. As a consequence, the probability that Eve announces outcomes (k_c, k_d) only depends on the number of photons (n, m) she received from Alice and Bob, i.e. the yields $Y_{nm}^{k_c,k_d}$ are independent of the decoy intensities chosen by the parties.

For this reason, one can derive a set of linear constraints on the yields $Y_{nm}^{k_c,k_d}$ by expressing the experimentally observed gains $Q_{k_c,k_d}^{\beta_A^2,\beta_B^2}$—which are defined as the conditional probabilities that node C announced the outcome (k_c, k_d) given that Alice and Bob sent phase-randomized coherent states of intensities β_A^2 and β_B^2, respectively—in terms of the yields:

$$Q_{k_c,k_d}^{\beta_A^2,\beta_B^2} = \sum_{n,m=0}^{\infty} \mathrm{e}^{-\beta_A^2-\beta_B^2}\frac{(\beta_A^2)^n(\beta_B^2)^m}{n!m!}Y_{nm}^{k_c,k_d}. \tag{2.1}$$

As it is clear from (2.1), to every distinct pair of decoy intensities $(\beta_A^2,\ \beta_B^2)$ corresponds a new constraint on the set of infinite yields $\{Y_{nm}^{k_c,k_d}\}_{n,m}$, which leads to tighter upper bounds and thus to a higher secret key rate. On the other hand, having a large number of decoy intensities is experimentally demanding, hence the need to derive the tightest possible bounds on the yields with a limited number of decoys.

In this section we present a simple analytical method to obtain tight bounds on the yields of largest contribution[4] in (1.7)—i.e. relative to the largest coefficients c_n—when the parties use two intensity settings in the Z-basis. It is basically a Gaussian elimination-type technique but involving infinite-size coefficient matrices. In particular, the guiding principle that we use is to combine the constraints (2.1) so that in the resulting expression the yield to be bounded is the one with the largest coefficient, while the yields which had larger coefficients in the initial constraints have been removed in the combination. However, in some cases it turns out that is not possible to remove all the yields with larger coefficients than the one to be bounded, due to a lack of decoy intensity settings (i.e. constraints). In other cases, we manage to remove from the resulting expression even some yields which had a smaller coefficient than the one to be bounded. Such a procedure can be readily extended to the case of three and four decoy intensity settings. The results for these last two cases are presented in appendices C and D, respectively.

From now on, we assume that both optical channels linking the parties to the central node C have the same transmittance $\sqrt{\eta}$. Therefore the set of optimal decoy intensities β_A^2 and β_B^2 is the same for both parties [43] and we define it as: $\{\mu_0, \mu_1\}$. In order to simplify the notation, we also omit the measurement outcome (k_c, k_d) from

[3] Every yield is a probability, thus it is trivially bounded by 1.

[4] The same method can-in principle-be applied to any yield, however the limited number of decoy settings prevents from obtaining a non-trivial bound on every yield.

the constraints given by (2.1). Hence the yields are subjected to the following four equality constraints:

$$\tilde{Q}^{k,l} \equiv e^{\mu_k+\mu_l} Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} {\mu_k}^n {\mu_l}^m \quad k, l \in \{0, 1\}, \tag{2.2}$$

and to the inequality constraints:

$$0 \leqslant Y_{nm} \leqslant 1 \quad \forall\, n, m. \tag{2.3}$$

Below we derive upper bounds on the yields: Y_{00}, Y_{11}, Y_{02} and Y_{20}.

2.1. Upper bound on Y_{11}

Consider the following combination of gains:

$$G_{11} = \tilde{Q}^{0,0} + \tilde{Q}^{1,1} - (\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m). \tag{2.4}$$

The subscript in G_{11} indicates the yield that is going to be bounded with this combination of gains. In (2.4) the coefficients of the yields Y_{0m} and Y_{n0}, for any n and m, are identically zero. Thus (2.4) can be rewritten as:

$$G_{11} = Y_{11}(\mu_0 - \mu_1)^2 + \sum_{\substack{n,m=1 \\ n+m>2}}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m). \tag{2.5}$$

We observe that the coefficients that multiply the yields Y_{nm} are always positive, being the product of two factors of equal sign. A valid upper bound for Y_{11} is obtained considering the worst-case scenario for the other yields, taking into account that (2.3) holds. Since all the yield's coefficients carry the same sign in (2.5)—regardless of the relation between μ_0 and μ_1—, 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 (2.5):

$$Y_{11}^U = \frac{G_{11}}{(\mu_0 - \mu_1)^2}, \tag{2.6}$$

where G_{11} is defined in (2.4).

We remark that by combining the gains as in (2.4), we manage to obtain a closed expression for Y_{11} in which the contribution of all the yields Y_{0m} and Y_{n0} is removed. Additionally, Y_{11} is now the yield with the 'highest weight' in (2.5) since it has the largest coefficient. All the yield's bounds presented in this work follow the same philosophy.

2.2. Upper bound on Y_{02}

Consider the following combination of gains:

$$G_{02} = \mu_1 \tilde{Q}^{0,0} + \mu_0 \tilde{Q}^{1,1} - \mu_1 \tilde{Q}^{0,1} - \mu_0 \tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_1 \mu_0^n - \mu_0 \mu_1^n)(\mu_0^m - \mu_1^m). \tag{2.7}$$

In (2.7) the coefficients of the yields Y_{n0} and Y_{1m} are identically zero. Thus (2.7) can be rewritten as:

$$\begin{aligned} G_{02} = &-Y_{01}(\mu_0 - \mu_1)^2 - \frac{Y_{02}}{2}(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2 - \sum_{m=3}^{\infty} \frac{Y_{0m}}{m!}(\mu_0 - \mu_1)(\mu_0^m - \mu_1^m) \\ &+ \sum_{\substack{n=2 \\ m=1}}^{\infty} \frac{Y_{nm}}{n!m!} \mu_0 \mu_1 (\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^m - \mu_1^m). \end{aligned} \tag{2.8}$$

Like in the derivation of Y_{11}'s bound given by (2.6), a valid upper bound for Y_{02} is obtained by considering the worst-case scenario for the remaining yields in (2.8). More specifically, Y_{02} is maximal when the yields whose coefficient has the same sign as Y_{02}'s coefficient are minimal, and the yields whose coefficient has opposite sign to Y_{02}'s are maximal. Recalling constraint (2.3), this means setting Y_{01} and Y_{0m} to zero and Y_{nm} with $n \geqslant 2$ and $m \geqslant 1$, to 1 in (2.8). In so doing, after rearranging the terms we obtain:

$$Y_{02}^U = \frac{2}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2} \left[-G_{02} + \left(\sum_{m=1}^{\infty} \frac{\mu_0^m}{m!} - \frac{\mu_1^m}{m!} \right) \left(\sum_{n=2}^{\infty} \mu_1 \frac{\mu_0^n}{n!} - \mu_0 \frac{\mu_1^n}{n!} \right) \right], \tag{2.9}$$

which leads to the following upper bound on Y_{02}:

$$Y_{02}^U = \frac{2(e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1}) - 2G_{02}}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2}. \tag{2.10}$$

2.3. Upper bound on Y_{20}

Consider the following combination of gains:

$$G_{20} = \mu_1 \tilde{Q}^{0,0} + \mu_0 \tilde{Q}^{1,1} - \mu_0 \tilde{Q}^{0,1} - \mu_1 \tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\mu_1 \mu_0^m - \mu_0 \mu_1^m). \tag{2.11}$$

In (2.11) the coefficients of the yields Y_{n1} and Y_{0m} are identically zero. Thus (2.11) can be rewritten as:

$$G_{20} = -Y_{10}(\mu_0 - \mu_1)^2 - \frac{Y_{20}}{2}(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2 - \sum_{n=3}^{\infty} \frac{Y_{n0}}{n!}(\mu_0 - \mu_1)(\mu_0^n - \mu_1^n) + \sum_{\substack{n=1 \\ m=2}}^{\infty} \frac{Y_{nm}}{n!m!}\mu_0 \mu_1 (\mu_0^n - \mu_1^n)(\mu_0^{m-1} - \mu_1^{m-1}). \tag{2.12}$$

A valid upper bound for Y_{20} is obtained by setting to zero the yields whose coefficient has the same sign as Y_{20}'s coefficient, and by setting to 1 the yields whose coefficient has opposite sign to Y_{20}'s. In the case of (2.12) this means setting Y_{10} and Y_{n0} to zero and Y_{nm} with $n \geqslant 1$ and $m \geqslant 2$, to 1. In this way we obtain:

$$Y_{20}^U = \frac{2}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2}\left[-G_{20} + \left(\sum_{n=1}^{\infty} \frac{\mu_0^n}{n!} - \frac{\mu_1^n}{n!}\right)\left(\sum_{m=2}^{\infty} \mu_1 \frac{\mu_0^m}{m!} - \mu_0 \frac{\mu_1^m}{m!}\right)\right], \tag{2.13}$$

which leads to the following upper bound on Y_{20}:

$$Y_{20}^U = \frac{2(e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1}) - 2G_{20}}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2}. \tag{2.14}$$

2.4. Upper bound on Y_{00}

Consider the following combination of gains:

$$G_{00} = \mu_1^2 \tilde{Q}^{0,0} + \mu_0^2 \tilde{Q}^{1,1} - \mu_0 \mu_1 (\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n \mu_1 - \mu_0 \mu_1^n)(\mu_0^m \mu_1 - \mu_0 \mu_1^m). \tag{2.15}$$

In (2.15) the coefficients of the yields Y_{1m} and Y_{n1}, for any n and m, are identically zero. Thus (2.15) can be rewritten as:

$$G_{00} = Y_{00}(\mu_0 - \mu_1)^2 - \mu_0 \mu_1 (\mu_0 - \mu_1)\left[\sum_{m=2}^{\infty} \frac{Y_{0m}}{m!}(\mu_0^{m-1} - \mu_1^{m-1}) + \sum_{n=2}^{\infty} \frac{Y_{n0}}{n!}(\mu_0^{n-1} - \mu_1^{n-1})\right] + \mu_0^2 \mu_1^2 \sum_{n,m=2}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^{m-1} - \mu_1^{m-1}). \tag{2.16}$$

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 Y_{00}'s coefficient (which correspond to the Y_{nm} with $n,\ m \geqslant 2$), and by setting to their maximum value the yields whose coefficient has opposite sign to Y_{00}'s coefficient (which correspond to Y_{0m} and Y_{n0}). We know that every yield is trivially bounded by (2.3). However, in order to derive a tighter bound on Y_{00}, we employ non-trivial bounds for all the yields Y_{nm} with $n + m \leqslant 4$ in (2.16). The upper bound on Y_{00} thus satisfies:

$$G_{00} = Y_{00}^U(\mu_0 - \mu_1)^2 - \mu_0 \mu_1 (\mu_0 - \mu_1)\left[\frac{(\mu_0 - \mu_1)}{2}(Y_{02}^U + Y_{20}^U) + \frac{(\mu_0^2 - \mu_1^2)}{6}(Y_{03}^U + Y_{30}^U) + \frac{(\mu_0^3 - \mu_1^3)}{24}(Y_{04}^U + Y_{40}^U) + 2\sum_{n=5}^{\infty} \frac{(\mu_0^{n-1} - \mu_1^{n-1})}{n!}\right] + \frac{\mu_0^2 \mu_1^2 (\mu_0 - \mu_1)^2}{4} Y_{22}^L. \tag{2.17}$$

In this equation Y_{ij}^U are upper bounds and Y_{ij}^L are lower bounds. From (2.17) we obtain the following upper bound on Y_{00}:

$$Y_{00}^U = \frac{G_{00}}{(\mu_0 - \mu_1)^2} + \frac{\mu_0 \mu_1}{\mu_0 - \mu_1}\left[\frac{(\mu_0 - \mu_1)}{2}(Y_{02}^U + Y_{20}^U) + \frac{(\mu_0^2 - \mu_1^2)}{6}(Y_{03}^U + Y_{30}^U) + \frac{(\mu_0^3 - \mu_1^3)}{24}(Y_{04}^U + Y_{40}^U)\right] + \frac{2}{\mu_0 - \mu_1}\left[\mu_1\left(e^{\mu_0} - 1 - \frac{\mu_0^2}{2} - \frac{\mu_0^3}{6} - \frac{\mu_0^4}{24}\right) - \mu_0\left(e^{\mu_1} - 1 - \frac{\mu_1^2}{2} - \frac{\mu_1^3}{6} - \frac{\mu_1^4}{24}\right)\right] - \frac{\mu_0^2 \mu_1^2}{4} Y_{22}^L, \tag{2.18}$$

where Y_{02}^U and Y_{20}^U are given in (2.10) and (2.14), respectively. The expressions for Y_{03}^U and Y_{04}^U in (2.18) can be found by starting from the same expression (2.8) that we used to derive Y_{02}^U, i.e.:

$$G_{02} = -\sum_{m=1}^{\infty} \frac{Y_{0m}}{m!}(\mu_0 - \mu_1)(\mu_0^m - \mu_1^m) + \sum_{\substack{n=2 \\ m=1}}^{\infty} \frac{Y_{nm}}{n!m!}\mu_0\mu_1(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^m - \mu_1^m). \tag{2.19}$$

From this expression we can extract an upper bound on any generic Y_{0m} as follows:

$$Y_{0m}^U = \min\left\{\frac{m!}{(\mu_0 - \mu_1)(\mu_0^m - \mu_1^m)}[-G_{02} + (e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1})],\ 1\right\}, \tag{2.20}$$

where we employ the constraint (2.3). Similarly, the expressions for Y_{30}^U and Y_{40}^U are obtained starting from (2.12) and deriving an upper bound on a generic Y_{n0} as follows:

$$Y_{n0}^U = \min\left\{\frac{n!}{(\mu_0 - \mu_1)(\mu_0^n - \mu_1^n)}[-G_{20} + (e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1})],\ 1\right\}. \tag{2.21}$$

At last, the expression for Y_{22}^L can be derived from the same combination of yields which led to Y_{11}^U. In particular, from (2.5) we have that:

$$G_{11} = \sum_{n,m=1}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m).$$

Then, by setting to 1 all the yields whose coefficient has equal sign to Y_{22}'s we obtain:

$$G_{11} = \sum_{n,m=1}^{\infty} \frac{\mu_0^n - \mu_1^n}{n!}\frac{\mu_0^m - \mu_1^m}{m!} - \frac{(\mu_0^2 - \mu_1^2)^2}{4} + \frac{(\mu_0^2 - \mu_1^2)^2}{4}Y_{22}^L, \tag{2.22}$$

which yields:

$$Y_{22}^L = \max\left\{\frac{4}{(\mu_0 - \mu_1)^2(\mu_0 + \mu_1)^2}[G_{11} - (e^{\mu_0} - e^{\mu_1})^2] + 1,\ 0\right\}. \tag{2.23}$$

Note that the upper bounds derived on Y_{04} and Y_{40} in this section could be used to improve the estimation of the phase error rate given by (1.8). However, the resulting improvement in the secret key rate would be extremely small in this case and we neglect it for simplicity.

3. Simulations

In this section we provide plots of the secret key rate given by (1.2) against the overall loss ($-10\log_{10}\eta$) measured in dB of the two optical channels linking Alice and Bob to node C. The channel model we use to simulate the quantities that would be observed experimentally—i.e. the gains $p(k_c, k_d|b_A, b_B)$ and $Q_{k_c,k_d}^{\beta_A^2,\beta_B^2}$—is given in appendix A [33]. It accounts for: the loss in the optical channels together with the non-unity detection efficiency of D_c and D_d (altogether described by the parameter η), the polarization and phase misalignments introduced by the channel and a dark count probability p_d in each detector. For concreteness, in all the plots below we assume fixed polarization and phase misalignments of 2%, independently of the channel loss. Note that, as pointed out in [33], the TF-QKD protocol analyzed in this work is quite robust against phase mismatch. This is so because phase misalignment only affects the quantum bit error rate but not the phase error rate.

For illustration purposes every plot is obtained for three different values of the dark count rate of the detectors, $p_d \in \{10^{-6}, 10^{-7}, 10^{-8}\}$. The plots are obtained by numerically optimizing[5] the secret key rate—for every value of the loss—over the signal intensity (α^2) and over one decoy intensity, while for simplicity the other decoy intensities are fixed to near-to-optimal values for all values of the overall loss. More specifically, we preliminarily performed an optimization of the key rate over the whole set of intensity settings and noticed that most of the decoy intensities are roughly constant with the loss and tend to be as low as possible. For instance, if we consider the case with two decoy intensity settings (μ_0 and μ_1, with $\mu_0 > \mu_1$), we observe that the optimal value for the weakest decoy μ_1 is basically the lowest possible for any value of the loss. In practice, however, it might be difficult to generate very weak signals due to the finite extinction ratio of a practical intensity modulator [44], so we fix μ_1 to a reasonable small value from an experimental point of view, say $\mu_1 = 10^{-5}$ [34, 36], while keeping the optimization over the remaining intensities. Similarly, if we consider the case with three decoy intensity settings (μ_0, μ_1 and μ_2, with $\mu_0 > \mu_1 > \mu_2$), we find that the optimal values for the weakest decoys μ_1 and μ_2 are also the lowest possible for any value of the loss. Moreover, in this last case, we show in appendix B that the system performance remains basically unchanged if one increases the value of the weakest intensity to say $\mu_2 = 10^{-3}$, which might be even easier to implement experimentally than 10^{-5}. Thus, we fix $\mu_2 = 10^{-3}$ and we differentiate it from μ_1 by, for example, one order of magnitude (i.e. we take $\mu_1 = 10^{-2}$). The same argument

[5] The optimization is carried out by using the built-in function 'NMaximize' of the software Wolfram Mathematica 10.0.

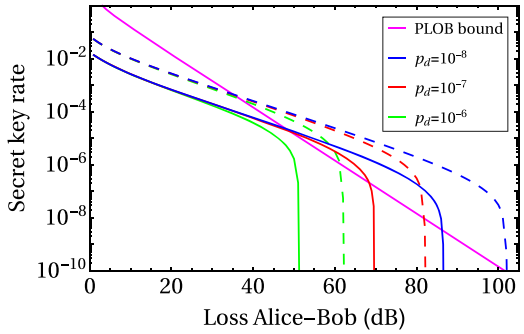

Figure 2. Secret key rate in logarithmic scale as a function of the overall loss in the channels Alice-C and Bob-C for three different dark count rates (10^{-6} green, 10^{-7} red, 10^{-8} blue). The solid lines correspond to the case where the yields Y_{00}, Y_{02}, Y_{20} and Y_{11} are estimated by means of two decoy intensity settings through the bounds presented in section 2 and the key rate is optimized over the signal intensity α^2 (see figure 3(a)) and the decoy intensity μ_0 (see figure 3(b)). The other decoy intensity, μ_1, is fixed to $\mu_1 = 10^{-5}$. The dashed lines assume that all the yields are known from the channel model and the secret key rate is optimized over α^2. That is, these lines show the maximum value of the secret key rate which could be achieved with an infinite number of decoy intensity settings and the security analysis reported in [33]. The solid magenta line illustrates the PLOB bound [19]. The plot shows that in the presence of a dark count rate of at most about $p_d = 10^{-7}$ the protocol can beat the PLOB bound even with just two decoy intensity settings.

holds in the case with four decoy intensity settings (see appendix B), where we fix $\mu_2 = 10^{-3}$, $\mu_1 = 10^{-2}$, and $\mu_0 = 10^{-1}$. We remark, however, that our method is general in the sense that the analytical upper bounds on the yields can be evaluated with any desired combination of intensity settings, while we select these particular decoy intensity values only for illustration purposes. Also, let us emphasize that the optimal decoy intensity values in the finite-key regime might be different from the values mentioned above. The analysis of the finite-key regime is, however, beyond the scope of this paper. Importantly, it turns out that the resulting asymptotic secret key rates in these scenarios are almost indistinguishable from those obtained by optimizing the value of all the intensity settings.

The optimal values of the signal and decoy intensities which are optimized as a function of the loss are also plotted in this section. In this regard, we also study how the key rate is affected when the intensities are subjected to fluctuations around their optimal values in section 3.4.

3.1. Two decoy intensity settings

In figure 2 we plot the secret key rate against the overall loss for the case where Alice and Bob use two decoy intensity settings each. The solid lines are obtained by bounding from above the yields Y_{00}, Y_{02}, Y_{20} and Y_{11} by means of the expressions derived in section 2 and by optimizing the rate over the signal intensity α^2 and the decoy intensity μ_0, while the other decoy intensity is fixed to $\mu_1 = 10^{-5}$ as explained above. The optimal values for α^2 and μ_0 are shown in figures 3(a) and (b), respectively. The dashed lines are instead obtained by employing the exact expression of the yields[6] which is given by (A.6) for the channel model considered. This represents the ideal scenario in which the parties have an infinite number of decoys through which they can estimate all the yields precisely. Note that in order to obtain the dashed lines in figure 2 we use the exact expression of the yields Y_{nm} only for $n,\ m \leqslant 12$ while we set the other yields to 1. This is enough to basically reproduce the behavior of the secret key rate when all the infinite number of yields are computed via the channel model's formula given by (A.6), as argued in [33]. The dashed lines are only optimized over the signal intensity, since the yields are directly given by the channel model. Finally, we also insert in figure 2 the PLOB bound on the secret key capacity [19], which reads as follows in terms of the transmittance η:

$$K(\eta) = -\log_2(1-\eta). \tag{3.1}$$

In figure 2 we observe that even by means of just two decoy intensity settings the key rate can beat the PLOB bound, provided that the dark count rate is $p_d \lesssim 10^{-7}$. This happens because with two decoys the parties can already non-trivially estimate the yields Y_{nm} with $n + m \leqslant 2$ as we showed in section 2, and these yields are the most relevant terms in the phase-error rate formula given by (1.7) [33]. Note that we did not estimate the yields Y_{01} and Y_{10} since only the yields Y_{nm} with $n + m$ an even number contribute to the phase-error rate (1.7).

However, figure 2 also shows that there is a sensible gap between the rates where the yields are estimated with two decoys (solid lines) and the best possible rates one could achieve (dashed lines) if all the yields were known. This clearly indicates that, although two decoys allow to estimate the yields of largest contribution in the phase-error rate, such estimations are not sufficiently tight and the ability to estimate a larger number of yields would increase the performance of the protocol.

[6] By 'exact expression' we mean that if the experimental apparatus were accurately described by the channel model in appendix A, then the yields associated to that experimental setup would be precisely predicted by (A.6).

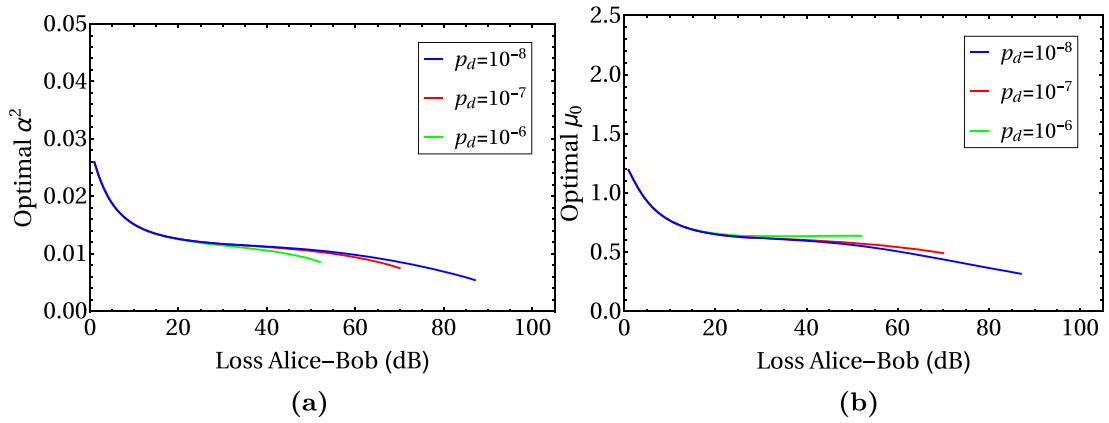

Figure 3. Optimal values of the signal and decoy intensities α^2 and μ_0 for the TF-QKD protocol [33] when the parties have at their disposal two decoy intensity settings to estimate the yields. (a) Optimal values of the signal intensity α^2 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 2. (b) Optimal values of the decoy intensity μ_0 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 2. The other decoy intensity is set to: $\mu_1 = 10^{-5}$.

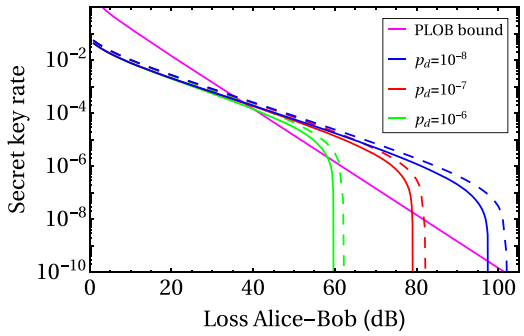

Figure 4. Secret key rate in logarithmic scale as a function of the overall loss in the channels Alice-C and Bob-C for three different dark count rates (10^{-6} green, 10^{-7} red, 10^{-8} blue). The solid lines correspond to the case where the yields Y_{00}, Y_{02}, Y_{20}, Y_{11}, Y_{13}, Y_{31}, Y_{04}, Y_{40} and Y_{22} are estimated by means of three decoy intensity settings through the bounds presented in appendix C and the key rate is optimized over the signal intensity α^2 (see figure 5(a)) and the decoy intensity μ_0 (see figure 5(b)). The other decoy intensities are fixed to $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. The dashed lines assume that all the yields are known from the channel model and the secret key rate is optimized over α^2. That is, these lines show the maximum value of the secret key rate which could be achieved with an infinite number of decoy intensity settings and the security analysis reported in [33]. The solid magenta line illustrates the PLOB bound [19]. The plot shows that already with three decoy intensity settings the key rate (solid lines) is sensibly close to the ideal one in which all the yields are known (dashed lines), meaning that the contribution of the other yields trivially bounded by 1 in the phase error rate is minimal.

By considering figure 3 and the fixed value of the decoy intensity μ_1, one notices that the optimal intensities are rather small and thus, in a real experimental implementation, intensity fluctuations might be an issue. In section 3.4 we address this problem by studying how the key rate is affected under intensity fluctuations and show that for fluctuations up to about 40% the change in the key rate performance is minimal.

Also, we notice that the optimal values of the signal intensity α^2 (see figure 3(a)) and the decoy intensity μ_0 (see figure 3(b)) are almost constant with the loss, for losses $\gtrsim$20 dB. This means that in a scenario where the loss in the quantum channels varies dynamically with time within a reasonable interval, one could still fix the signal intensity and both decoy intensities to constant values which happen to be close to the optimal ones. This argument also holds in the case of three (see section 3.2) and four decoy intensity settings (see section 3.3).

3.2. Three decoy intensity settings

In figure 4 we plot the secret key rate against the overall loss for the case where Alice and Bob use three decoy intensity settings each. The solid lines are obtained by bounding from above the relevant yields Y_{nm} such that $n + m \leqslant 4$ (i.e. we upper bound the yields Y_{00}, Y_{02}, Y_{20}, Y_{11}, Y_{13}, Y_{31}, Y_{04}, Y_{40} and Y_{22}). The exact expressions for the different upper bounds on the yields can be found in appendix C, and we omit them here for simplicity. The solid lines are optimized over the signal intensity α^2 and the decoy intensity μ_0, while the weakest decoy intensities are fixed for simplicity to $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. As explained above, the resulting secret key rate in this scenario is almost

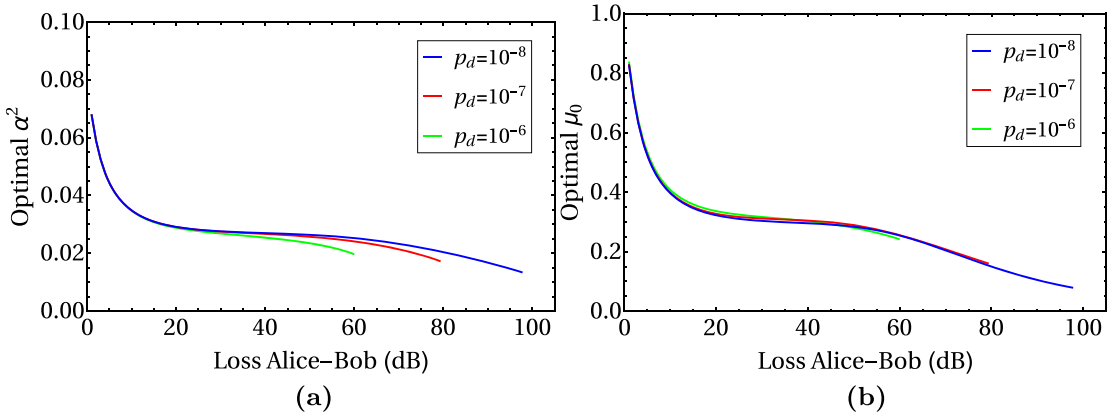

Figure 5. Optimal values of the signal and decoy intensities α^2 and μ_0 for the TF-QKD protocol [33] when the parties have at their disposal three decoy intensity settings to estimate the yields. (a) Optimal values of the signal intensity α^2 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 4. We observe that the optimal signal intensity is roughly doubled with respect to the two-decoys case (figure 3(a)). (b) Optimal values of the decoy intensity μ_0 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 4. The other decoy intensities are set to: $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$.

indistinguishable from that obtained by optimizing over all the intensity settings. The optimal values for α^2 and μ_0 are shown in figures 5(a) and (b), respectively. The dashed lines are again obtained by employing the exact expression of the yields given by the channel model (A.6) and coincide with those plotted in figure 2.

We observe in figure 4 that the use of three decoys yields a significant improvement in the protocol's performance with respect to the two-decoys case (see figure 2). As a matter of fact, in figure 4 the solid lines are almost overlapping the dashed lines for most values of the channel loss. This is due to the fact that with three decoys the parties constrain the yields with nine independent equations (instead of four equations as in the two-decoys case), which enable a tighter estimation of Y_{00}, Y_{02}, Y_{20} and Y_{11} and the non-trivial estimation of five additional yields.

Moreover, in the case of three decoys the optimal signal intensity α^2 (see figure 5(a)) is roughly double the value of the correspondent intensity when using two decoys (see figure 3(a)). The reason for this is connected to the role of α^2 in the protocol's key rate. In fact, the prefactor $p(k_c, k_d)$ with $k_c + k_d = 1$ of the key rate formula given by (1.3) increases for increasing α^2: the higher the mean number of photons sent by the parties (within certain limits) the higher the probability of having a click in one of the two detectors. On the other hand, increasing α^2 excessively also affects the phase-error rate. Note that by setting some yields to 1 in the phase error rate formula given by (1.7) we give rise to addends like $c_{2n}\, c_{2m}$ and $c_{2n+1}c_{2m+1}$ which increase for increasing α^2, leading to an overall increase of the phase-error rate and thus decrease of the key rate. The optimal value of α^2 is thus given by the trade-off between the effect of the prefactor $p(k_c, k_d)$ and that of the terms $c_{2n}\, c_{2m}$ and $c_{2n+1}c_{2m+1}$. Now, by noting that the contribution of the therms $c_{2n}\, c_{2m}$ and $c_{2n+1}c_{2m+1}$ decreases for increasing n, m, we understand that their negative effect on the key rate is diminished in the case of three decoys since we non-trivially estimate more yields, i.e. a lower number of yields is set to 1. This allows α^2 to acquire higher values with respect to the two-decoys case, as we observed in figure 5(a).

Finally we point out that such an argument does not apply to the discussion about the optimal value of the decoy intensity μ_0 in the case of two and three decoys. As a matter of fact, the key rate does not depend on the decoy intensities in the same way as on the signal intensity: the decoy intensities only appear in the yield's bounds inserted in the phase-error rate. Additionally, the analytical bounds on the yields when using two or three decoys cannot be compared in a straightforward way. Nonetheless we observe a similar behavior of the optimal μ_0 for two (see figure 3(b)) and three decoys (see figure 5(b)).

3.3. Four decoy intensity settings

In figure 6 we plot the secret key rate against the overall loss for the case where Alice and Bob use four decoy intensity settings each. Like in the three-decoys case, the solid lines are obtained by bounding from above the yields Y_{00}, Y_{02}, Y_{20}, Y_{11}, Y_{13}, Y_{31}, Y_{04}, Y_{40} and Y_{22} by means of four decoys. In particular, for the yields Y_{00}, Y_{02}, Y_{20}, Y_{11} and Y_{22} we use the exact same analytical bounds derived with three decoys since they are tight enough, and the use of a fourth decoy intensity would just make them more cumbersome without providing a significant improvement of the resulting secret key rate. For the remaining four yields we instead derived tighter bounds with the help of the fourth intensity μ_3 (see appendix D). The solid lines are obtained by optimizing the rate over the signal intensity α^2 and the fourth decoy intensity μ_3. It turns out that the optimal values for the other decoy intensities are basically the lowest possible

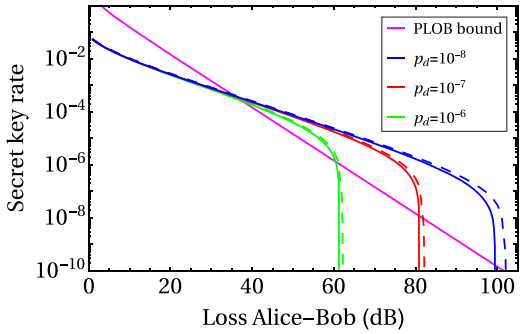

Figure 6. Secret key rate in logarithmic scale as a function of the overall loss in the channels Alice-C and Bob-C for three different dark count rates (10^{-6} green, 10^{-7} red, 10^{-8} blue). The solid lines correspond to the case where the yields Y_{00}, Y_{02}, Y_{20}, Y_{11} and Y_{22} are estimated by means of three decoys through the bounds presented in appendix C (i.e. for simplicity here we disregard the information provided by the additional fourth decoy intensity setting) and Y_{13}, Y_{31}, Y_{04} and Y_{40} are estimated with four decoys via the bounds in appendix D. The key rate is optimized over the signal intensity α^2 (see figure 7(a)) and the decoy intensity μ_3 (see figure 7(b)), while the other decoy intensities are fixed to $\mu_0 = 10^{-1}$, $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. The dashed lines are optimized over α^2 and assume that all the yields are known from the channel model. They correspond to the maximum value of the secret key rate which could be achieved with an infinite number of decoy intensity settings. The solid magenta line illustrates the PLOB bound [19]. The plot indicates that the tighter estimation of the yields Y_{13}, Y_{31}, Y_{04} and Y_{40} with respect to the case of three decoy intensity settings is enough to basically reproduce the ideal scenario in which all the yields are known (dashed lines).

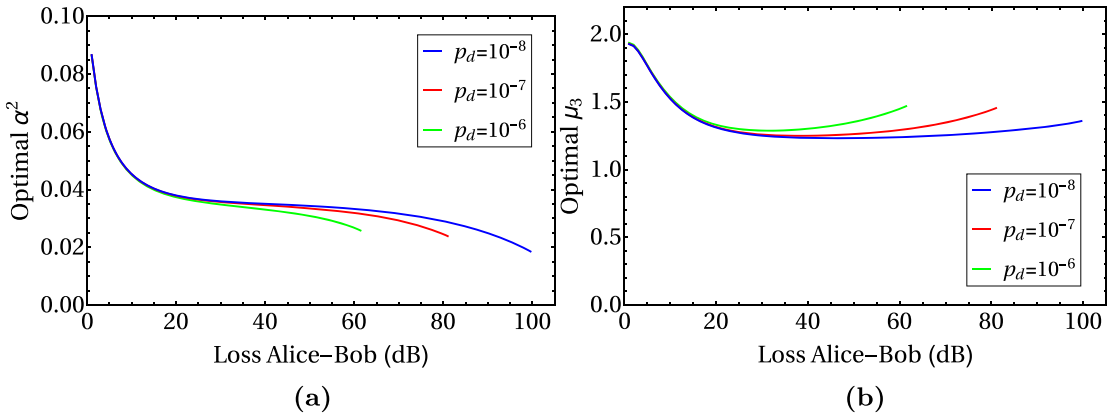

Figure 7. Optimal values of the signal and decoy intensities α^2 and μ_3 for the TF-QKD protocol [33] when the parties have at their disposal four decoy intensity settings to estimate the yields. (a) Optimal values of the signal intensity α^2 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 6. (b) Optimal values of the decoy intensity μ_3 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 6. The other decoy intensities are set to: $\mu_0 = 10^{-1}$, $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. The difference between this plot and the optimal μ_0 plots (see figures 3(b) and 5(b)) in the case of two and three decoys is due to the fact that, unlike μ_0, the intensity μ_3 does not appear in all the yield's bounds since we used the fourth decoy just for bounding Y_{13}, Y_{31}, Y_{04} and Y_{40}.

for any value of the loss, so, as explained above, for simplicity we fix the smallest one to an experimentally reasonable small value (say $\mu_2 = 10^{-3}$), and then we differentiate it from the other two decoys, μ_1 and μ_0, by one order of magnitude, i.e. we take $\mu_1 = 10^{-2}$ and $\mu_0 = 10^{-1}$. Importantly, this decision has a neglectable effect on the resulting secret key rate, when compared to that obtained by optimizing over all intensity settings. The optimal values for α^2 and μ_3 are shown in figures 7(a) and (b), respectively. The dashed lines are the same as in figures 2 and 4.

With four decoys (see figure 6) the key rates basically reproduces the ideal ones (dashed lines) in which all the yields are known, with the gap being at maximum of 1 dB at the very end of the plot lines (i.e. in the very high loss regime). This demonstrates that there is no need to bound further yields than the nine yields we bounded in the cases of three and four decoys. Of course, the tighter estimation of the yields Y_{13}, Y_{31}, Y_{04} and Y_{40} achieved with four decoys results in an improvement of the key rate with respect to the case of three decoys (see figure 4), especially in the region of high losses.

Concerning the optimal signal intensity (see figure 7(a)), we notice a slight increase with respect to the three-decoys case (see figure 5(a)) due to the tighter estimation of some yields in the phase-error rate formula, which allows their correspondent coefficients to acquire a slightly higher value under an increase of α^2.

Finally, the reason why the optimal μ_3 plot (see figure 7(b)) looks quite different (with values above 1) from the optimal μ_0 plots for the cases of two and three decoys (see figures 3(b) and 5(b)) is the following. In the TF-QKD protocol considered, the most important yields (i.e. those with a bigger impact on the resulting phase error

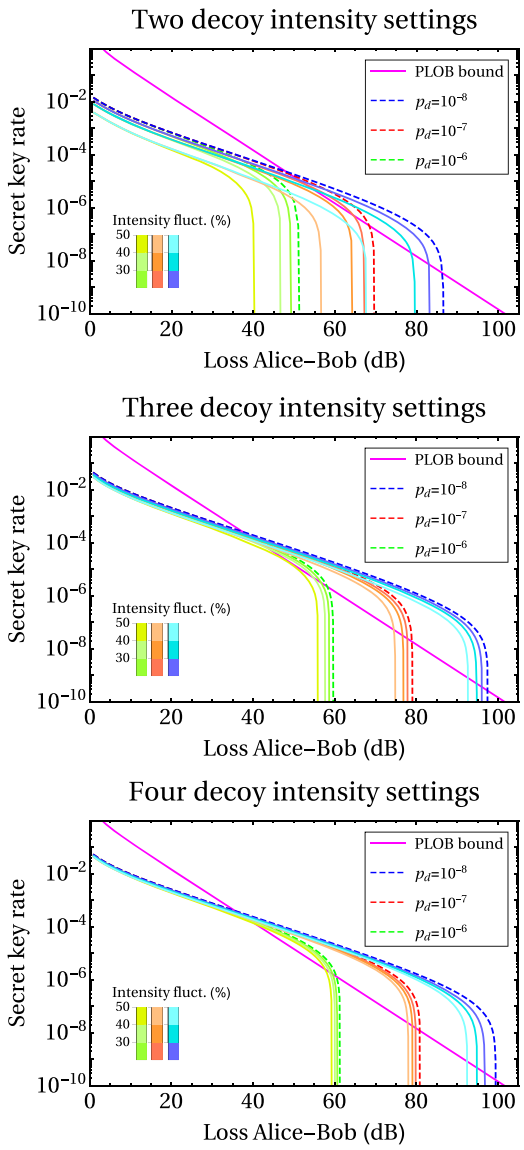

Figure 8. Comparison of the secret key rate with optimal signal and decoys intensities (dashed lines, computed in section 3) with the secret key rates affected by increasing intensity fluctuations (solid lines): 30%, 40% and 50% (brighter colors; right to left). We assume that the fluctuations affect each decoy intensity and the signal intensity as well. The plots show that the TF-QKD protocol is quite robust against intensity fluctuations, and that its robustness increases with the number of decoys.

rate) are those associated to pairs of pulses with zero or with a very low number of photons. It is therefore very important to be able to estimate these yields as tightly as possible. For this, we have that the optimal intensities μ_0 and μ_1 (μ_0, μ_1 and μ_2) for the case with two (three) decoys are well below 1, just like in standard decoy-state QKD protocols [39, 40]. However, as explained above, here we use the intensity μ_3 to improve the upper bounds for the yields Y_{13}, Y_{31}, Y_{04} and Y_{40}. That is, the intensity μ_3 is only used to estimate yields associated to pairs of pulses with a total number of photons equal to four. Thus, it is natural that the optimal value of μ_3 is not too low and greater than 1.

3.4. Intensity fluctuations

Here we investigate the robustness of the TF-QKD protocol against intensity fluctuations that may occur in the preparation of the pulses sent by Alice and Bob. This is motivated by the fact that the optimal signal and decoy intensities that the parties should adopt in order to maximize the key rate for a given loss are quite small, thus the effect of intensity fluctuations might be an issue in practice. On the other hand, we also note that the optimal value of a given decoy or signal intensity is either constant or varies very moderately with the loss.

Here we consider the simple scenario in which the intensity fluctuations are symmetric, i.e. we assume that the intensity of Alice's signal matches perfectly with the intensity of Bob's signal. Or, to put it in other words, we consider that Alice's and Bob's signals suffer from the same intensity fluctuations and thus their intensities are

equal. This means that such analysis is only valid to evaluate auto-compensating TF-QKD set-ups like, for instance, the one introduced in [36]. It cannot be used however to analyze set-ups where more than one laser source is used [34, 35]. Although we do not expect a dramatic change of our results when asymmetric intensity fluctuations are considered in the latter case, specially if they are not too large.

Also, we assume that the signal and all the decoy intensities suffer from a fluctuation of magnitude 30%, 40% or 50% around their optimal value. This means for example that, for a fluctuation say of 30%, the signal intensity α^2 and all the decoy intensities μ_k fluctuate in the intervals: $0.7\ \alpha^2_{\rm opt} \leqslant \alpha^2 \leqslant 1.3\ \alpha^2_{\rm opt}$ and $0.7\ \mu_k^{\rm opt} \leqslant \mu_k \leqslant 1.3\ \mu_k^{\rm opt}$, respectively, where $\alpha^2_{\rm opt}$ and $\mu_k^{\rm opt}$ represent the optimal values. We then account for the worst-case scenario by numerically minimizing the key rate over all the intensities constrained in their respective fluctuation interval. Only in this way we can still guarantee that the resulting key rate is associated to a secure protocol.

The results of this study are given in figure 8. Here we plot the original key rates—i.e. without fluctuations of the signal and decoy intensities—as dashed lines[7] and the key rates affected by intensity fluctuations as solid lines. The plots are given for the same dark count rates and misalignments used in section 3, in the case of two, three and four decoy intensity settings. The color of the solid lines becomes brighter for increasing fluctuation magnitude.

We observe that the performance of the protocol is considerably affected by intensity fluctuations in the case of two decoys, while the effect becomes almost negligible for three and four decoys. The reason for this lies in the fact that the tightness of the yield's bounds has a stronger dependence on the value of the decoy intensities when the number of decoys—and thus constraints on the yields—is low. In other words, if the parties have at their disposal a larger number of decoys, they can properly combine the numerous constraints on the yields and obtain inherently tight bounds, i.e. bounds that are tight regardless of the actual values of the intensities involved. If, instead, the parties have few decoys, say two, then the bounds they derive on the yields can be tight or loose depending on the values assigned to the decoy intensities, since the constraints on the yields are fewer.

In conclusion, in the case of two decoys the parties can tolerate intensity fluctuations up to 40%, which correspond to a decrease in the protocol's key rate especially in the high-loss region, quantified by a reduction of about 5–6 dB of the maximum tolerated loss[8]. Remarkably, with three decoys the decrease of the maximum tolerated loss would be under 5 dB for fluctuations up to 50%. Finally, for four decoys the protocol's performance remains almost the same for fluctuations up to about 50% around the optimal values (except when the dark count probability is the smallest considered: $p_d = 10^{-8}$). We deduce that the TF-QKD protocol introduced in [33] seems to be quite robust against intensity fluctuations.

4. Conclusions

In this paper we have investigated in detail the performance of the TF-QKD protocol presented in [33] in the realistic scenario of a finite number of decoy intensity settings at the parties' disposal. Indeed, the protocol requires that Alice and Bob use the decoy-state method [38–40] to estimate the phase-error rate by upper bounding certain yields. Unlike most QKD protocols which employ such method, in this case the protocol's key rate depends-in principle-on infinitely many yields and it is essential to upper bound (rather than lower bound) their values. Clearly, the more yields the parties tightly upper bound, the better the protocol's performance is. We have introduced an analytical method to perform such estimation when Alice and Bob use two, three or four decoy intensity settings each. The yield's analytical bounds provided in this work imply a fully-analytical expression for the protocol's secret key rate, which is very convenient for performance optimization (e.g. in the finite-key scenario). Also, we remark that the secret key rates obtained with our analytical bounds basically overlap those achievable with numerical tools like linear programming for most values of the overall loss, which confirms that the analytical approach is actually quite tight.

In so doing, we have shown that the TF-QKD protocol can beat the PLOB bound [19] even with just two decoys for reasonable values of the setup parameters, which include: the loss, the dark count rate, the polarization misalignment and the phase mismatch. Furthermore the plots assuming four decoys demonstrate that one can approximately achieve the best possible performance by tightly estimating only nine yields. The optimization of the key rate over the signal and decoy intensities indicates that their optimal values are all either constant or weakly-dependent on the loss of the channel. This means that the protocol is particularly suitable for contexts where the channel loss varies in time, for instance in the scalable MDI-QKD networks conceived in [43]. Finally we have investigated the scenario where the intensities of the optical states prepared by Alice and Bob are affected by fluctuations and observed that the protocol seems to be very robust against such phenomena.

[7] The dashed lines of the key rates without fluctuations correspond to the solid lines in figures 2, 4 and 6.

[8] By 'maximum tolerated loss' we mean the loss threshold above which the protocol's key rate becomes roughly zero.

A natural continuation of this work would take into account the finite-key effects due to the finite number of pulses sent by the parties to the central relay. This could be done by combining the results presented in this paper with the finite-keys estimation techniques used in [41].

Acknowledgments

We thank Dagmar Bruß and Hermann Kampermann for helpful discussions, and an anonymous referee for very useful comments. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 675662, and from the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2017-88243-R.

Appendix A. Channel model

The channel model that we employ to simulate the gains that would be observed experimentally in the X-basis (i.e. the probabilities $p(k_c, k_d|b_A, b_B)$) and Z-basis (i.e. the probabilities $Q^{k,l}_{k_c,k_d}$) is taken from [33]. In all the expressions of this section we assume $k_c + k_d = 1$.

In particular, a beam splitter of transmittance $\sqrt{\eta}$ accounts for the loss in the quantum channel linking Alice (Bob) to node C and for the non-unity detection efficiency of detectors D_c and D_d. The polarization misalignment introduced by the channel Alice-C (Bob-C) is modeled with a unitary operation mapping the polarization input modes $a^\dagger_{\rm in}$ ($b^\dagger_{\rm in}$) to the orthogonal polarization output modes $a^\dagger_{\rm out}$ and $a^\dagger_{{\rm out}\perp}$ ($b^\dagger_{\rm out}$ and $b^\dagger_{{\rm out}\perp}$) according to: $a^\dagger_{\rm in} \to \cos\theta_A a^\dagger_{\rm out} - \sin\theta_A a^\dagger_{{\rm out}\perp}$ ($b^\dagger_{\rm in} \to \cos\theta_B b^\dagger_{\rm out} - \sin\theta_B b^\dagger_{{\rm out}\perp}$), for an angle θ_A (θ_B). Moreover, the phase mismatch between Alice and Bob's signals arriving at node C is modeled by shifting the phase of Bob's signals by an angle $\phi = \delta\pi$, for a certain parameter δ. Finally the model considers that both detectors are affected by a dark count probability p_d, which is independent of the signals received and has the same value for both detectors.

With this setup, the gains in the X-basis can be written as:

$$p(k_c, k_d|b_A, b_B) = (1 - p_d)[p_d e^{-2\gamma} + q(k_c, k_d|b_A, b_B)], \tag{A.1}$$

where $\gamma = \sqrt{\eta}\alpha^2$ (with α being the amplitude of the signal states) and

$$q(k_c, k_d|b_A, b_B) = \begin{cases} e^{-\gamma(1-\cos\phi\cos\theta)} - e^{-2\gamma} & \text{if } k_c \oplus b_A \oplus b_B = 1 \\ e^{-\gamma(1+\cos\phi\cos\theta)} - e^{-2\gamma} & \text{if } k_c \oplus b_A \oplus b_B = 0 \end{cases} \tag{A.2}$$

with $\theta = \theta_A - \theta_B$. Starting from (A.1), one can readily compute the probability $p(k_c, k_d)$ and the bit-error rate e_{k_c,k_d} by means of equations (1.4) and (1.5), (1.6), respectively:

$$p(k_c, k_d) = \frac{1}{2}(1 - p_d)(e^{-\gamma\cos\phi\cos\theta} + e^{\gamma\cos\phi\cos\theta})e^{-\gamma} - (1 - p_d)^2 e^{-2\gamma}, \tag{A.3}$$

$$e_{k_c,k_d} = \frac{e^{-\gamma\cos\phi\cos\theta} - (1 - p_d)e^{-\gamma}}{e^{-\gamma\cos\phi\cos\theta} + e^{\gamma\cos\phi\cos\theta} - 2(1 - p_d)e^{-\gamma}}. \tag{A.4}$$

The gains in the Z-basis instead read:

$$Q^{k,l}_{k_c,k_d} = (1 - p_d)[(p_d - 1)e^{-\sqrt{\eta}(\mu_k+\mu_l)} + e^{-\sqrt{\eta}(\mu_k+\mu_l)/2} I_0(\sqrt{\eta\mu_k\mu_l}\cos\theta)], \tag{A.5}$$

where the function $I(z) = \frac{1}{2\pi i}\oint e^{(z/2)(t+1/t)}t^{-1}dt$ is the modified Bessel function of first kind.

In the simulations shown in section 3 we compare the key rate computed with our analytical bounds on the yields with the key rate evaluated with the exact expressions of the yields, i.e. the expressions obtained directly from the channel model. According to the above channel model, the yields read:

$$Y^{k_c,k_d}_{nm} = (1 - p_d)[(p_d - 1)(1 - \sqrt{\eta})^{n+m} + y^{k_c,k_d}_{nm}], \tag{A.6}$$

where

$$y^{k_c,k_d}_{nm} = \sum_{k=0}^{n}\binom{n}{k}\sum_{l=0}^{m}\binom{m}{l}\frac{\sqrt{\eta}^{k+l}(1 - \sqrt{\eta})^{n+m-k-l}}{2^{k+l}k!l!}\sum_{r=0}^{k}\binom{k}{r}\sum_{p=0}^{l}\binom{l}{p}\sum_{q=\max(0,r+p-l)}^{\min(k,r+p)}\binom{k}{q}$$
$$\binom{l}{r+p-q}(r + p)!(k + l - r - p)!\cos^{r+q}(\theta_A)\cos^{r+2p-q}(\theta_B)\sin^{2k-r-q}(\theta_A)\sin^{2l-r-2p+q}(\theta_B). \tag{A.7}$$

To conclude, we remark that all the quantities entering the key rate formula (1.2)—i.e. (A.3), (A.4) and the gains (A.5) indirectly through the yield's bounds—are symmetric under the swap $k_c \leftrightarrow k_d$ due to the symmetries of the channel model.

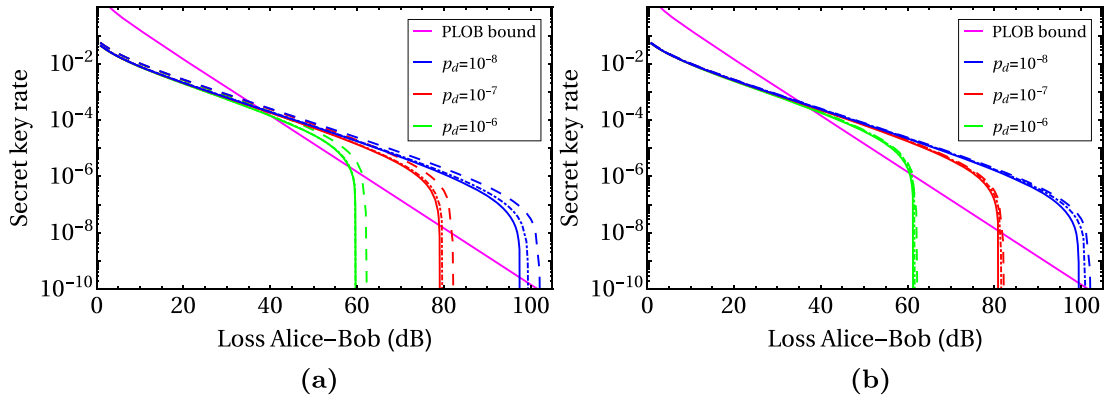

Figure B1. Comparison of the optimal key rates achievable with different fixed values of the weaker decoy intensities. The two cases analyzed (solid and dotted–dashed lines) are almost indistinguishable. (a) Optimal key rate as a function of the overall loss when the parties use three decoy intensity settings, for three different values of the dark count rate (p_d). The solid lines are obtained by fixing the weaker decoy intensities to $\mu_2 = 10^{-3}$ and $\mu_1 = 10^{-2}$, while the dotted–dashed lines are obtained by fixing the same intensities to $\mu_2 = 10^{-5}$ and $\mu_1 = 10^{-4}$. The dashed lines assume that all the yields are known from the channel model and the magenta line is the PLOB bound [19]. Note that the green dotted–dashed lines and green solid lines ($p_d = 10^{-6}$) are almost perfectly overlapping. (b) Optimal key rate as a function of the overall loss when the parties use four decoy intensity settings, for three different values of the dark count rate (p_d). The solid lines are obtained by fixing the weaker decoy intensities to $\mu_2 = 10^{-3}$, $\mu_1 = 10^{-2}$ and $\mu_0 = 10^{-1}$, while the dotted–dashed lines are obtained by fixing the same intensities to $\mu_2 = 10^{-5}$, $\mu_1 = 10^{-4}$ and $\mu_0 = 10^{-3}$. The dashed lines assume that all the yields are known from the channel model and the magenta line is the PLOB bound [19].

In all the simulations shown in section 3 we fix both polarization and phase misalignments to 2%, which means that: $\theta_A = -\theta_B = \arcsin\sqrt{0.02}$ and $\delta = 0.02$.

Appendix B. Stronger and weaker decoy intensities

As explained in section 3, the optimal key rates are basically not affected if their optimization is only performed over the signal intensity (α) and over one decoy intensity, while having the remaining weaker decoy intensities fixed to near-to-optimal values for all losses. In figure B1, we compare the optimal key rate that the parties can achieve when fixing their weaker decoy intensities to substantially different values, in the case of three (left) and four (right) decoy intensity settings. In particular, the solid lines are the same plotted in figures 4 and 6 for the three- and four-decoys case, respectively, i.e. they are obtained by fixing the weaker decoy intensities to $\mu_2 = 10^{-3}$ and $\mu_1 = 10^{-2}$ (three decoy intensity settings) and to $\mu_2 = 10^{-3}$, $\mu_1 = 10^{-2}$ and $\mu_0 = 10^{-1}$ (four decoy intensity settings). The dotted–dashed lines, instead, are obtained by fixing the weaker intensities to values which are two orders of magnitude lower, that is $\mu_2 = 10^{-5}$ and $\mu_1 = 10^{-4}$ in the case of three decoy intensity settings and $\mu_2 = 10^{-5}$, $\mu_1 = 10^{-4}$ and $\mu_0 = 10^{-3}$ in the case of four decoy intensity settings. Clearly, the optimal key rates are basically not affected by employing relatively stronger pulses (those with $\mu_2 = 10^{-3}$ as the weakest intensity) for the weaker decoy intensity settings. Such stronger pulses could be more easily implemented experimentally and, for this, have been chosen in our simulations.

Appendix C. Yield's bounds with three decoys

Here we derive analytical upper bounds on the yields appearing in (1.7), following the same lines of section 2. In this case we assume that Alice and Bob can prepare their phase-randomized coherent pulses with three different intensity settings: $\{\mu_0, \mu_1, \mu_2\}$, which are the same for both parties. This choice is optimal since we assumed that the two optical channels linking the parties to the central node C have equal transmittance $\sqrt{\eta}$ [43].

The whole set of infinite yields is subjected to the following nine equality constraints:

$$\tilde{Q}^{k,l} \equiv e^{\mu_k+\mu_l} Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} \mu_k{}^n \mu_l{}^m \quad k, l \in \{0, 1, 2\}, \tag{C.1}$$

and to the inequality constraints given by (2.3).

We derive bounds on the yields Y_{00}, Y_{11}, Y_{02}, Y_{20}, Y_{22}, Y_{13}, Y_{31}, Y_{04} and Y_{40}.

C.1. Upper bound on Y_{22}

Consider the following combinations of gains in which all the terms Y_{1m} and Y_{n1} are removed (i.e. their coefficients are equal to zero):

$$G_{22}^{0,1} = \mu_1^2\tilde{Q}^{0,0} + \mu_0^2\tilde{Q}^{1,1} - \mu_0\mu_1(\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m);$$

$$G_{22}^{0,2} = \mu_2^2\tilde{Q}^{0,0} + \mu_0^2\tilde{Q}^{2,2} - \mu_0\mu_2(\tilde{Q}^{0,2} + \tilde{Q}^{2,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m);$$

$$G_{22}^{1,2} = \mu_2^2\tilde{Q}^{1,1} + \mu_1^2\tilde{Q}^{2,2} - \mu_1\mu_2(\tilde{Q}^{1,2} + \tilde{Q}^{2,1}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m), \tag{C.2}$$

where the superscripts in $G_{22}^{k,l}$ indicate which intensities are involved, while the subscripts indicate the yield that is going to be bounded.

We now combine $G_{22}^{0,1}$, $G_{22}^{0,2}$ and $G_{22}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{0m} and Y_{n0} removed as well:

$$G_{22}^{0,1} + c_0\, G_{22}^{0,2} + c_1\, G_{22}^{1,2} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}[(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + c_0(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + c_1(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)]. \tag{C.3}$$

Note that the linear combination above is already the most general for our needs. As a matter of fact, for every linear combination of $G_{22}^{0,1}$, $G_{22}^{0,2}$ and $G_{22}^{1,2}$ one can always factor out the coefficient in front of $G_{22}^{0,1}$, as far as it is not zero. However, if the particular combination of gains which removes the terms Y_{0m} and Y_{n0} has a null coefficient in front of $G_{22}^{0,1}$, for symmetry reasons there would also exist another combination—that also removes the yields Y_{0m} and Y_{n0}—with a null coefficient in front of say $G_{22}^{0,2}$, and this one could be found in our case given by (C.3).

For Y_{0m} and Y_{n0} to be removed in (C.3) it suffices that:

$$(\mu_1 - \mu_0)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + c_0(\mu_2 - \mu_0)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + c_1(\mu_2 - \mu_1)(\mu_1^m\mu_2 - \mu_1\mu_2^m) = 0 \quad \forall\ m, \tag{C.4}$$

which implies:

$$\mu_0^m[\mu_1(\mu_1 - \mu_0) + c_0\mu_2(\mu_2 - \mu_0)] + \mu_1^m[-\mu_0(\mu_1 - \mu_0) + c_1\mu_2(\mu_2 - \mu_1)] + \mu_2^m[-c_0\mu_0(\mu_2 - \mu_0) - c_1\mu_1(\mu_2 - \mu_1)] = 0 \quad \forall\, m. \tag{C.5}$$

A sufficient condition for this is that every coefficient of μ_i^m is identically zero, which happens for:

$$c_0 = -\frac{\mu_1(\mu_0 - \mu_1)}{\mu_2(\mu_0 - \mu_2)}, \tag{C.6}$$

$$c_1 = \frac{\mu_0(\mu_0 - \mu_1)}{\mu_2(\mu_1 - \mu_2)}. \tag{C.7}$$

Substituting (C.6) and (C.7) back into (C.3) and multiplying both sides by μ_2, we get an expression where all the terms Y_{0m}, Y_{1m}, Y_{n0} and Y_{n1} are removed and where the term Y_{22} gives the largest contribution:

$$\mu_2 G_{22}^{0,1} - \mu_1\frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}\, G_{22}^{0,2} + \mu_0\frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}\, G_{22}^{1,2} = \sum_{n,m=2}^{\infty} \frac{Y_{nm}}{n!m!}\Big[\mu_2(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m) - \mu_1\frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + \mu_0\frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)\Big]. \tag{C.8}$$

In order to extract a bound for Y_{22} we need to recast the yield's coefficients in such a way that their sign becomes manifest. Each term of the sum in (C.8) may be recast as follows:

$$\frac{Y_{nm}}{n!m!}\mu_0\mu_1\mu_2\Big[(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^m\mu_1 - \mu_0\mu_1^m) - \frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^{n-1} - \mu_2^{n-1})(\mu_0^m\mu_2 - \mu_0\mu_2^m) + \frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^{n-1} - \mu_2^{n-1})(\mu_1^m\mu_2 - \mu_1\mu_2^m)\Big], \tag{C.9}$$

or equivalently as:

$$\frac{Y_{nm}}{n!m!}\frac{\mu_0\mu_1\mu_2}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)}\, A_{22}(\mu_0, \mu_1, \mu_2, m)\cdot A_{22}(\mu_0, \mu_1, \mu_2, n), \tag{C.10}$$

where

$$A_{22}(\mu_0, \mu_1, \mu_2, m) \equiv \mu_1^m(\mu_0 - \mu_2) + \mu_2^m(\mu_1 - \mu_0) + \mu_0^m(\mu_2 - \mu_1). \tag{C.11}$$

We can now rewrite factor A_{22} as:

$$\begin{aligned}
A_{22}(\mu_0,\mu_1,\mu_2,m) &= \mu_1[\mu_1^{m-1}(\mu_0-\mu_2)-(\mu_0^m-\mu_2^m)]+\mu_0\mu_2(\mu_0^{m-1}-\mu_2^{m-1})\\
&= \mu_1\left[\mu_1^{m-1}(\mu_0-\mu_2)-(\mu_0-\mu_2)\left(\sum_{k=0}^{m-1}\mu_0^{m-1-k}\mu_2^k\right)\right]+\mu_0\mu_2(\mu_0-\mu_2)\left(\sum_{j=0}^{m-2}\mu_0^{m-2-j}\mu_2^j\right)\\
&= (\mu_0-\mu_2)\left[\mu_1^m-\mu_1\sum_{k=0}^{m-1}\mu_0^{m-1-k}\mu_2^k+\mu_0\mu_2\sum_{j=0}^{m-2}\mu_0^{m-2-j}\mu_2^j\right]\\
&= (\mu_0-\mu_2)\left[\mu_1^m+\sum_{k=0}^{m-1}\mu_2^k(-\mu_1\mu_0^{m-1-k}+\mu_0\mu_2\mu_0^{m-2-k})-\mu_0\mu_2\frac{\mu_2^{m-1}}{\mu_0}\right]\\
&= (\mu_0-\mu_2)\left[-(\mu_2^m-\mu_1^m)+\sum_{k=0}^{m-1}\mu_2^k\mu_0^{m-1-k}(\mu_2-\mu_1)\right]\\
&= (\mu_0-\mu_2)(\mu_2-\mu_1)\left[\sum_{k=0}^{m-1}\mu_2^k\mu_0^{m-1-k}-\sum_{j=0}^{m-1}\mu_2^j\mu_1^{m-1-j}\right]\\
&= (\mu_0-\mu_2)(\mu_2-\mu_1)\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k}-\mu_1^{m-1-k}).
\end{aligned}\tag{C.12}$$

Of course we can employ this expression also for $A_{22}(\mu_0,\mu_1,\mu_2,n)$, under the substitution $m\rightarrow n$. We will apply this consideration from now on to similar scenarios. By substituting (C.12) into (C.10), we get the final expression for each term of the sum in (C.8):

$$\begin{aligned}
&\frac{Y_{nm}}{n!m!}\frac{\mu_0\mu_1\mu_2}{(\mu_0-\mu_2)(\mu_1-\mu_2)}(\mu_0-\mu_2)^2(\mu_2-\mu_1)^2\\
&\quad\times\left[\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k}-\mu_1^{m-1-k})\right]\left[\sum_{j=0}^{n-1}\mu_2^j(\mu_0^{n-1-j}-\mu_1^{n-1-j})\right].
\end{aligned}\tag{C.13}$$

That is, the sign of Y_{nm}'s coefficient is independent of n and m and it is the same for all terms in (C.8) (note that the product of the two sums in (C.13) is always positive). Thus a valid upper bound for Y_{22} is obtained by setting all the other yields to zero in (C.8), except for Y_{22}. We obtain:

$$\mu_2 G_{22}^{0,1}-\mu_1\frac{(\mu_0-\mu_1)}{(\mu_0-\mu_2)}G_{22}^{0,2}+\mu_0\frac{(\mu_0-\mu_1)}{(\mu_1-\mu_2)}G_{22}^{1,2}=\frac{Y_{22}^U\mu_0\mu_1\mu_2}{4}(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_0-\mu_1)^2,\tag{C.14}$$

which implies the following expression for the upper bound on Y_{22}:

$$Y_{22}^U=4\frac{\frac{G_{22}^{0,1}}{\mu_0\mu_1(\mu_0-\mu_1)}-\frac{G_{22}^{0,2}}{\mu_0\mu_2(\mu_0-\mu_2)}+\frac{G_{22}^{1,2}}{\mu_1\mu_2(\mu_1-\mu_2)}}{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)}.\tag{C.15}$$

We remark that the bound given by (C.15) is not valid when any of the intensities μ_0, μ_1 or μ_2 is equal to zero. As a matter of fact, in any of these cases the starting expression given by (C.8) becomes trivial. However, in most practical situations, due to the finite extinction ratio of amplitude modulators, none of the decoy intensities is actually equal to zero.

C.2. Upper bound on Y_{11}

Consider the following combinations of gains in which all the terms Y_{0m} and Y_{n0} are removed:

$$\begin{aligned}
G_{11}^{0,1}&=\tilde{Q}^{0,0}+\tilde{Q}^{1,1}-(\tilde{Q}^{0,1}+\tilde{Q}^{1,0})=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n-\mu_1^n)(\mu_0^m-\mu_1^m);\\
G_{11}^{0,2}&=\tilde{Q}^{0,0}+\tilde{Q}^{2,2}-(\tilde{Q}^{0,2}+\tilde{Q}^{2,0})=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n-\mu_2^n)(\mu_0^m-\mu_2^m);\\
G_{11}^{1,2}&=\tilde{Q}^{1,1}+\tilde{Q}^{2,2}-(\tilde{Q}^{1,2}+\tilde{Q}^{2,1})=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_1^n-\mu_2^n)(\mu_1^m-\mu_2^m).
\end{aligned}\tag{C.16}$$

We now combine $G_{11}^{0,1}$, $G_{11}^{0,2}$ and $G_{11}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{2m} and Y_{n2} also removed:

$$G_{11}^{0,1} + c_0\, G_{11}^{0,2} + c_1\, G_{11}^{1,2} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}[(\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m) + c_0(\mu_0^n - \mu_2^n)(\mu_0^m - \mu_2^m) + c_1(\mu_1^n - \mu_2^n)(\mu_1^m - \mu_2^m)]. \tag{C.17}$$

For Y_{2m} and Y_{n2} to be removed it suffices:

$$(\mu_0^n - \mu_1^n)(\mu_0^2 - \mu_1^2) + c_0(\mu_0^n - \mu_2^n)(\mu_0^2 - \mu_2^2) + c_1(\mu_1^n - \mu_2^n)(\mu_1^2 - \mu_2^2) = 0 \quad \forall n, \tag{C.18}$$

which is fulfilled by:

$$c_0 = -\frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)}, \tag{C.19}$$

$$c_1 = \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)}. \tag{C.20}$$

Substituting these terms back into (C.17) yields a combination of gains in which the terms Y_{0m}, Y_{n0}, Y_{2m} and Y_{n2} are removed:

$$\begin{aligned} G_{11}^{0,1} - \frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)} G_{11}^{0,2} + \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)} G_{11}^{1,2} &= Y_{11}(\mu_0 - \mu_1)\Bigg[(\mu_0 - \mu_1) - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}(\mu_0 - \mu_2) \\ &+ \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}(\mu_1 - \mu_2)\Bigg] \\ &+ \sum_{m=3}^{\infty} \frac{Y_{1m}}{m!}(\mu_0 - \mu_1)\Bigg[(\mu_0^m - \mu_1^m) - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}(\mu_0^m - \mu_2^m) + \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}(\mu_1^m - \mu_2^m)\Bigg] \\ &+ \sum_{n=3}^{\infty} \frac{Y_{n1}}{n!}(\mu_0 - \mu_1)\Bigg[(\mu_0^n - \mu_1^n) - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}(\mu_0^n - \mu_2^n) + \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}(\mu_1^n - \mu_2^n)\Bigg] \\ &+ \sum_{n,m=3}^{\infty} \frac{Y_{nm}}{n!m!}\Bigg[(\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m) - \frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)}(\mu_0^n - \mu_2^n)(\mu_0^m - \mu_2^m) \\ &+ \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)}(\mu_1^n - \mu_2^n)(\mu_1^m - \mu_2^m)\Bigg]. \end{aligned} \tag{C.21}$$

In order to get a valid upper bound for Y_{11} we need to determine the signs of the coefficients of the remaining yields. We start by recasting each term of the sum in (C.21) corresponding to the Y_{nm}, with $n,\ m \geqslant 3$, as follows:

$$\frac{Y_{nm}}{n!m!} \frac{1}{(\mu_0^2 - \mu_2^2)(\mu_1^2 - \mu_2^2)} A_{11}(\mu_0, \mu_1, \mu_2, m) \cdot A_{11}(\mu_0, \mu_1, \mu_2, n), \tag{C.22}$$

where

$$A_{11}(\mu_0, \mu_1, \mu_2, m) \equiv \mu_1^m(\mu_0^2 - \mu_2^2) + \mu_2^m(\mu_1^2 - \mu_0^2) + \mu_0^m(\mu_2^2 - \mu_1^2). \tag{C.23}$$

The factor A_{11} can be rewritten as:

$$\begin{aligned} A_{11}(\mu_0, \mu_1, \mu_2, m) &= \mu_1^2[\mu_1^{m-2}(\mu_0^2 - \mu_2^2) - (\mu_0^m - \mu_2^m)] + \mu_0^2\mu_2^2(\mu_0^{m-2} - \mu_2^{m-2}) \\ &= (\mu_0 - \mu_2)\Bigg[\mu_1^m(\mu_0 + \mu_2) - \mu_1^2 \sum_{k=0}^{m-1} \mu_0^{m-1-k}\mu_2^k + \mu_0^2\mu_2^2 \sum_{j=0}^{m-3} \mu_0^{m-3-j}\mu_2^j\Bigg] \\ &= (\mu_0 - \mu_2)\Bigg[\mu_1^m(\mu_0 + \mu_2) + \sum_{k=0}^{m-1} \mu_2^k(-\mu_1^2\mu_0^{m-1-k} + \mu_0^2\mu_2^2\mu_0^{m-3-k}) - \mu_0^2\mu_2^2\left(\frac{\mu_2^{m-2}}{\mu_0} + \frac{\mu_2^{m-1}}{\mu_0^2}\right)\Bigg] \\ &= (\mu_0 - \mu_2)\Bigg[(\mu_1^m - \mu_2^m)(\mu_0 + \mu_2) + \sum_{k=0}^{m-1} \mu_2^k\mu_0^{m-1-k}(\mu_2^2 - \mu_1^2)\Bigg] \\ &= (\mu_0 - \mu_2)\Bigg[(\mu_0 + \mu_2)(\mu_1 - \mu_2)\left(\sum_{j=0}^{m-1} \mu_1^{m-1-j}\mu_2^j\right) - (\mu_1 + \mu_2)(\mu_1 - \mu_2) \sum_{k=0}^{m-1} \mu_2^k\mu_0^{m-1-k}\Bigg] \\ &= (\mu_0 - \mu_2)(\mu_1 - \mu_2) \sum_{k=0}^{m-1} \mu_2^k[(\mu_0 + \mu_2)\mu_1^{m-1-k} - (\mu_1 + \mu_2)\mu_0^{m-1-k}] \\ &= (\mu_0 - \mu_2)(\mu_1 - \mu_2)\Bigg\{\sum_{k=0}^{m-3} \mu_2^k[\mu_2(\mu_1^{m-1-k} - \mu_0^{m-1-k}) + \mu_0\mu_1(\mu_1^{m-2-k} - \mu_0^{m-2-k})] \end{aligned}$$

$$
\begin{aligned}
&+ \mu_2^{m-1}(\mu_0-\mu_1) + \mu_2^{m-1}(\mu_1-\mu_0)\} \\
&= (\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_1-\mu_0)\sum_{k=0}^{m-3}\mu_2^k\left[\mu_2\sum_{j=0}^{m-2-k}\mu_1^{m-2-k-j}\mu_0^j + \mu_0\mu_1\sum_{j=0}^{m-3-k}\mu_1^{m-3-k-j}\mu_0^j\right] \\
&= (\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_1-\mu_0)\sum_{k=0}^{m-3}\mu_2^k\left[(\mu_2+\mu_0)\sum_{j=0}^{m-3-k}\mu_1^{m-2-k-j}\mu_0^j + \mu_2\mu_0^{m-2-k}\right] \\
&\equiv (\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_1-\mu_0)F(m),
\end{aligned}
\tag{C.24}
$$

where the factor $F(m) \geqslant 0,\ \forall\, m \geqslant 3$. Substituting (C.24) back into (C.22), we recast each term of the sum in (C.21) corresponding to the Y_{nm}, with $n,\ m \geqslant 3$, as:

$$
\frac{Y_{nm}}{n!m!}\frac{(\mu_0-\mu_2)^2(\mu_1-\mu_2)^2(\mu_1-\mu_0)^2}{(\mu_0^2-\mu_2^2)(\mu_1^2-\mu_2^2)}F(n)F(m),
\tag{C.25}
$$

so that its sign is manifestly dependent on the factor $(\mu_0-\mu_2)(\mu_1-\mu_2)$.

In a similar fashion, one can rewrite each term of the sum in (C.21) corresponding to the Y_{1m}, with $m \geqslant 3$, as:

$$
-\frac{Y_{1m}}{m!}\frac{(\mu_0-\mu_1)^2(\mu_1-\mu_2)(\mu_0-\mu_2)}{(\mu_0+\mu_2)(\mu_1+\mu_2)}F(m),
\tag{C.26}
$$

thus deducing that this expression has opposite sign with respect to that given by (C.25). Same holds for Y_{n1}, since it can be shown that its coefficient is exactly (C.26) with thesubstitution $m \to n$.

Finally, by showing that the term corresponding to Y_{11} in (C.21) can be factorized as:

$$
Y_{11}\frac{(\mu_0-\mu_1)^2(\mu_1-\mu_2)(\mu_0-\mu_2)}{(\mu_0+\mu_2)(\mu_1+\mu_2)},
\tag{C.27}
$$

one concludes that this expression has the same sign as that given by (C.25).

Putting together these considerations into (C.21), a valid upper bound on Y_{11} is obtained when the yields Y_{nm}, with $n,\ m \geqslant 3$, are set to zero and the yields Y_{1m} and Y_{n1} are set to their maximum allowed value. Since in appendices C.5 and C.6 we derive upper bounds on Y_{13} and Y_{31} (see (C.65)and (C.73)), we can employ them in (C.21) instead of trivially bounding these yields with 1. In this way we obtain:

$$
\begin{aligned}
&G_{11}^{0,1} - \frac{(\mu_0^2-\mu_1^2)}{(\mu_0^2-\mu_2^2)}G_{11}^{0,2} + \frac{(\mu_0^2-\mu_1^2)}{(\mu_1^2-\mu_2^2)}G_{11}^{1,2} = Y_{11}^U\frac{(\mu_0-\mu_1)^2(\mu_1-\mu_2)(\mu_0-\mu_2)}{(\mu_0+\mu_2)(\mu_1+\mu_2)} \\
&+ \frac{(\mu_0-\mu_1)}{6}(Y_{13}^U+Y_{31}^U)\left[\mu_0^3-\mu_1^3-\frac{(\mu_0+\mu_1)}{(\mu_0+\mu_2)}(\mu_0^3-\mu_2^3)+\frac{(\mu_0+\mu_1)}{(\mu_1+\mu_2)}(\mu_1^3-\mu_2^3)\right] \\
&+ 2(\mu_0-\mu_1)\sum_{n=4}^{\infty}\left[\frac{(\mu_0^n-\mu_1^n)}{n!}-\frac{(\mu_0+\mu_1)}{(\mu_0+\mu_2)}\frac{(\mu_0^n-\mu_2^n)}{n!}+\frac{(\mu_0+\mu_1)}{(\mu_1+\mu_2)}\frac{(\mu_1^n-\mu_2^n)}{n!}\right],
\end{aligned}
\tag{C.28}
$$

which leads to the following upper bound on Y_{11}:

$$
\begin{aligned}
Y_{11}^U \;=\; &\frac{(\mu_0+\mu_2)(\mu_1+\mu_2)}{(\mu_0-\mu_1)^2(\mu_1-\mu_2)(\mu_0-\mu_2)}\left[G_{11}^{0,1}-\frac{(\mu_0^2-\mu_1^2)}{(\mu_0^2-\mu_2^2)}G_{11}^{0,2}+\frac{(\mu_0^2-\mu_1^2)}{(\mu_1^2-\mu_2^2)}G_{11}^{1,2}-2(\mu_0-\mu_1)E_{11}\right] \\
&+\frac{(\mu_1\mu_2+\mu_0\mu_1+\mu_0\mu_2)}{6}(Y_{13}^U+Y_{31}^U),
\end{aligned}
\tag{C.29}
$$

where the term E_{11} is defined as:

$$
\begin{aligned}
E_{11} = {} & \mathrm{e}^{\mu_0}-\mathrm{e}^{\mu_1}-(\mu_0-\mu_1)\left(1+\frac{\mu_0}{2}+\frac{\mu_1}{2}+\frac{\mu_0^2}{6}+\frac{\mu_1^2}{6}+\frac{\mu_0\mu_1}{6}\right) \\
&+\frac{\mu_0+\mu_1}{\mu_1+\mu_2}\left[\mathrm{e}^{\mu_1}-\mathrm{e}^{\mu_2}-(\mu_1-\mu_2)\left(1+\frac{\mu_1}{2}+\frac{\mu_2}{2}+\frac{\mu_1^2}{6}+\frac{\mu_2^2}{6}+\frac{\mu_1\mu_2}{6}\right)\right] \\
&-\frac{\mu_0+\mu_1}{\mu_0+\mu_2}\left[\mathrm{e}^{\mu_0}-\mathrm{e}^{\mu_2}-(\mu_0-\mu_2)\left(1+\frac{\mu_0}{2}+\frac{\mu_2}{2}+\frac{\mu_0^2}{6}+\frac{\mu_2^2}{6}+\frac{\mu_0\mu_2}{6}\right)\right].
\end{aligned}
\tag{C.30}
$$

C.3. Upper bound on Y_{02} and Y_{04}

Consider the following combinations of gains in which all the terms Y_{1m} and , Y_{n0} are removed:

$$G_{02}^{0,1} = \mu_1\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{1,1} - \mu_1\tilde{Q}^{0,1} - \mu_0\tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m - \mu_1^m);$$
$$G_{02}^{0,2} = \mu_2\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{2,2} - \mu_2\tilde{Q}^{0,2} - \mu_0\tilde{Q}^{2,0} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m - \mu_2^m);$$
$$G_{02}^{1,2} = \mu_2\tilde{Q}^{1,1} + \mu_1\tilde{Q}^{2,2} - \mu_2\tilde{Q}^{1,2} - \mu_1\tilde{Q}^{2,1} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m - \mu_2^m). \tag{C.31}$$

We now combine $G_{02}^{0,1}$, $G_{02}^{0,2}$ and $G_{02}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{2m} and Y_{n1} also removed:

$$G_{02}^{0,1} + c_0\,G_{02}^{0,2} + c_1\,G_{02}^{1,2} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}[(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m - \mu_1^m) + c_0(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m - \mu_2^m) + c_1(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m - \mu_2^m)]. \tag{C.32}$$

For Y_{2m} and Y_{n1} to be removed the coefficients c_0 and c_1 must satisfy:

$$\begin{cases}(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0 - \mu_1) + c_0(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0 - \mu_2) + c_1(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1 - \mu_2) = 0\,\forall\ n\\ (\mu_0^2\mu_1 - \mu_0\mu_1^2)(\mu_0^m - \mu_1^m) + c_0(\mu_0^2\mu_2 - \mu_0\mu_2^2)(\mu_0^m - \mu_2^m) + c_1(\mu_1^2\mu_2 - \mu_1\mu_2^2)(\mu_1^m - \mu_2^m) = 0\,\forall\, m\end{cases} \tag{C.33}$$

or equivalently:

$$\begin{cases}\mu_0^n[\mu_1(\mu_0 - \mu_1) + c_0\mu_2(\mu_0 - \mu_2)] + \mu_1^n[-\mu_0(\mu_0 - \mu_1) + c_1\mu_2(\mu_1 - \mu_2)]\\ -\mu_2^n[\mu_0c_0(\mu_0 - \mu_2) + \mu_1c_1(\mu_1 - \mu_2)] = 0\,\forall\ n\\ \mu_0^m[\mu_1\mu_0^2 - \mu_0\mu_1^2 + c_0(\mu_2\mu_0^2 - \mu_0\mu_2^2)] + \mu_1^m[-(\mu_1\mu_0^2 - \mu_0\mu_1^2) + c_1(\mu_2\mu_1^2 - \mu_1\mu_2^2)]\\ -\mu_2^m[c_0(\mu_2\mu_0^2 - \mu_0\mu_2^2) + c_1(\mu_2\mu_1^2 - \mu_1\mu_2^2)] = 0\,\forall\, m.\end{cases} \tag{C.34}$$

A sufficient condition for this is that the coefficient of every μ_i^n and every μ_i^m is identically zero. This imposes six conditions on c_0 and c_1, however thanks to the inherent symmetries of the system a solution exists, and reads:

$$c_0 = -\frac{\mu_1(\mu_0 - \mu_1)}{\mu_2(\mu_0 - \mu_2)}, \tag{C.35}$$

$$c_1 = \frac{\mu_0(\mu_0 - \mu_1)}{\mu_2(\mu_1 - \mu_2)}. \tag{C.36}$$

Substituting these expressions back into (C.32) and multiplying both sides by μ_2, yields a combination of gains in which the terms Y_{n0}, Y_{n1}, Y_{1m} and Y_{2m} are removed. In particular, we obtain:

$$\begin{aligned}&\mu_2G_{02}^{0,1} - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}\,G_{02}^{0,2} + \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}\,G_{02}^{1,2}\\ &= \sum_{m=2}^{\infty}\frac{Y_{0m}}{m!}(\mu_0 - \mu_1)[-\mu_2(\mu_0^m - \mu_1^m) + \mu_1(\mu_0^m - \mu_2^m) - \mu_0(\mu_1^m - \mu_2^m)]\\ &+ \sum_{\substack{n=3\\ m=2}}^{\infty}\frac{Y_{nm}}{n!m!}\left[\mu_2(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m - \mu_1^m) - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m - \mu_2^m)\right.\\ &\left.+ \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m - \mu_2^m)\right].\end{aligned} \tag{C.37}$$

In order to get a valid upper bound for Y_{02} and Y_{04} we need to study the sign of the coefficients of the remaining yields. We start by recasting each term of the sum corresponding to the Y_{nm}, with $n \geqslant 3$ and $m \geqslant 2$, in (C.37) as follows:

$$\frac{Y_{nm}}{n!m!}\frac{1}{(\mu_0 - \mu_2)(\mu_2 - \mu_1)}A_{22}(\mu_0, \mu_1, \mu_2, m)\cdot B_{02}(\mu_0, \mu_1, \mu_2, n), \tag{C.38}$$

where

$$B_{02}(\mu_0, \mu_1, \mu_2, n) \equiv \mu_1\mu_2\mu_0^n(\mu_1 - \mu_2) + \mu_0^2(\mu_1\mu_2^n - \mu_2\mu_1^n) + \mu_0(\mu_2^2\mu_1^n - \mu_1^2\mu_2^n) \tag{C.39}$$

and A_{22} is the one found when bounding Y_{22}, thus we know from (C.12) it can be recast as:

$$A_{22}(\mu_0, \mu_1, \mu_2, m) = (\mu_0 - \mu_2)(\mu_2 - \mu_1) \sum_{k=0}^{m-1} \mu_2^k (\mu_0^{m-1-k} - \mu_1^{m-1-k}). \tag{C.40}$$

We can rewrite B_{02} as:

$$\begin{aligned} B_{02}(\mu_0, \mu_1, \mu_2, n) &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)\left[\mu_0^{n-1} - \mu_0 \sum_{k=0}^{n-2} \mu_1^{n-2-k}\mu_2^k + \mu_1\mu_2 \sum_{j=0}^{n-3} \mu_1^{n-3-j}\mu_2^j\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)\left[\mu_0^{n-1} + \sum_{k=0}^{n-2} \mu_1^{n-2-k}\mu_2^k(\mu_2 - \mu_0) - \mu_2^{n-1}\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)\left[\mu_0^{n-1} - \mu_2^{n-1} - \sum_{k=0}^{n-2} \mu_1^{n-2-k}\mu_2^k(\mu_0 - \mu_2)\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2)\left[\sum_{k=0}^{n-2} \mu_2^k\mu_0^{n-2-k} - \sum_{k=0}^{n-2} \mu_2^k\mu_1^{n-2-k}\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2) \sum_{k=0}^{n-2} \mu_2^k(\mu_0^{n-2-k} - \mu_1^{n-2-k}). \end{aligned} \tag{C.41}$$

Employing (C.40) and (C.41) into (C.38) we get:

$$\frac{Y_{nm}}{n!m!}\mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2)\left[\sum_{k=0}^{n-2} \mu_2^k(\mu_0^{n-2-k} - \mu_1^{n-2-k})\right]\left[\sum_{k=0}^{m-1} \mu_2^k(\mu_0^{m-1-k} - \mu_1^{m-1-k})\right], \tag{C.42}$$

which means that the sign of this expression is fully determined by the factor $(\mu_1 - \mu_2)(\mu_0 - \mu_2)$ (note that the product of the two sums in (C.42) is always positive).

Concerning the terms that appear in the sum in (C.37) corresponding to the Y_{0m}, with $m \geqslant 2$, we have:

$$\begin{aligned} &\frac{Y_{0m}}{m!}(\mu_1 - \mu_0)[\mu_2(\mu_0^m - \mu_1^m) - \mu_1(\mu_0^m - \mu_2^m) + \mu_0(\mu_1^m - \mu_2^m)] \\ &= \frac{Y_{0m}}{m!}(\mu_1 - \mu_0)A_{22}(\mu_0, \mu_1, \mu_2, m) \\ &= \frac{Y_{0m}}{m!}(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1) \sum_{k=0}^{m-1} \mu_2^k(\mu_0^{m-1-k} - \mu_1^{m-1-k}), \end{aligned} \tag{C.43}$$

where we used (C.11) in the first equality and (C.40) in the second equality. Expression (C.43) implies that its sign is always equal to the sign of the terms given by (C.42), since it is determined by the same factor $(\mu_1 - \mu_2)(\mu_0 - \mu_2)$ (note that the product of the last two factors in (C.43) is always positive).

A valid upper bound on Y_{02} is thus obtained by setting all the other yields to zero in (C.37). By doing so, we obtain:

$$Y_{02}^U = 2\frac{\frac{\mu_2 G_{02}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{02}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{02}^{1,2}}{\mu_1 - \mu_2}}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1)}. \tag{C.44}$$

One can do the same when bounding Y_{04}, i.e. setting all the other yields to zero except for Y_{04}, in (C.37). We find that:

$$Y_{04}^U = 4!\frac{\frac{\mu_2 G_{02}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{02}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{02}^{1,2}}{\mu_1 - \mu_2}}{\mu_1(\mu_0^4 - \mu_2^4) - \mu_0(\mu_1^4 - \mu_2^4) - \mu_2(\mu_0^4 - \mu_1^4)}. \tag{C.45}$$

C.4. Upper bound on Y_{20} and Y_{40}

Consider the following combinations of gains in which all the terms Y_{0m} and Y_{n1} are removed:

$$\begin{aligned} G_{20}^{0,1} &= \mu_1\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{1,1} - \mu_0\tilde{Q}^{0,1} - \mu_1\tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m); \\ G_{20}^{0,2} &= \mu_2\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{2,2} - \mu_0\tilde{Q}^{0,2} - \mu_2\tilde{Q}^{2,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m); \\ G_{20}^{1,2} &= \mu_2\tilde{Q}^{1,1} + \mu_1\tilde{Q}^{2,2} - \mu_1\tilde{Q}^{1,2} - \mu_2\tilde{Q}^{2,1} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_1^n - \mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m). \end{aligned} \tag{C.46}$$

We now combine $G_{20}^{0,1}$, $G_{20}^{0,2}$ and $G_{20}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{1m} and Y_{n2} also removed:

$$G_{20}^{0,1} + c_0\, G_{20}^{0,2} + c_1\, G_{20}^{1,2} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}[(\mu_0^n - \mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + c_0(\mu_0^n - \mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + c_1(\mu_1^n - \mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)]. \tag{C.47}$$

For Y_{1m} and Y_{n2} to be removed the coefficients c_0 and c_1 must satisfy:

$$\begin{cases}(\mu_0^m\mu_1 - \mu_0\mu_1^m)(\mu_0 - \mu_1) + c_0(\mu_0^m\mu_2 - \mu_0\mu_2^m)(\mu_0 - \mu_2) + c_1(\mu_1^m\mu_2 - \mu_1\mu_2^m)(\mu_1 - \mu_2) = 0\,\forall\ m \\ (\mu_0^2\mu_1 - \mu_0\mu_1^2)(\mu_0^n - \mu_1^n) + c_0(\mu_0^2\mu_2 - \mu_0\mu_2^2)(\mu_0^n - \mu_2^n) + c_1(\mu_1^2\mu_2 - \mu_1\mu_2^2)(\mu_1^n - \mu_2^n) = 0\,\forall\, n.\end{cases} \tag{C.48}$$

This system of linear equations coincides with the one given by (C.33) that we found when bounding Y_{02}, thus the solution is given by (C.35) for c_0 and by (C.36) for c_1. Substituting these expressions back into (C.47) and multiplying both sides by μ_2, yields a combination of gains in which the terms Y_{n1}, Y_{n2}, Y_{0m} and Y_{1m} are removed:

$$\begin{aligned}&\mu_2 G_{20}^{0,1} - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}\, G_{20}^{0,2} + \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}\, G_{20}^{1,2} \\ &= \sum_{n=2}^{\infty} \frac{Y_{n0}}{n!}(\mu_0 - \mu_1)[-\mu_2(\mu_0^n - \mu_1^n) + \mu_1(\mu_0^n - \mu_2^n) - \mu_0(\mu_1^n - \mu_2^n)] \\ &+ \sum_{\substack{n=2\\ m=3}}^{\infty} \frac{Y_{nm}}{n!m!}\Bigg[\mu_2(\mu_0^n - \mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m) - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^n - \mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m) \\ &+ \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^n - \mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)\Bigg].\end{aligned} \tag{C.49}$$

Since the coefficients of Y_{n0} and Y_{nm} coincide with those found when bounding Y_{02} if one exchanges $m \longleftrightarrow n$, we can directly use the results obtained in appendix C.3 to recast the terms that contain the Y_{nm} with $n \geqslant 2$ and $m \geqslant 3$. In particular, according to (C.42), we obtain:

$$\frac{Y_{nm}}{n!m!}\mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2)\left[\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k} - \mu_1^{m-2-k})\right]\left[\sum_{k=0}^{n-1}\mu_2^k(\mu_0^{n-1-k} - \mu_1^{n-1-k})\right], \tag{C.50}$$

and according to (C.43) the terms that contain the yields Y_{n0} can be written as:

$$\frac{Y_{n0}}{n!}(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1)\sum_{k=0}^{n-1}\mu_2^k(\mu_0^{n-1-k} - \mu_1^{n-1-k}). \tag{C.51}$$

Like in the case of Y_{02} (see appendix C.3), a valid upper bound on Y_{20} is thus obtained setting all the other yields to zero in (C.49). We obtain:

$$Y_{20}^U = 2\frac{\frac{\mu_2 G_{20}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{20}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{20}^{1,2}}{\mu_1 - \mu_2}}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1)}. \tag{C.52}$$

One can do the same to bound Y_{40}, i.e. to set all the other yields to zero, except for Y_{40}. In this case we obtain:

$$Y_{04}^U = 4!\frac{\frac{\mu_2 G_{20}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{20}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{20}^{1,2}}{\mu_1 - \mu_2}}{\mu_1(\mu_0^4 - \mu_2^4) - \mu_0(\mu_1^4 - \mu_2^4) - \mu_2(\mu_0^4 - \mu_1^4)}. \tag{C.53}$$

C.5. Upper bound on Y_{13}

We look for that combination of gains in which all the terms proportional to Y_{n0}, Y_{n1}, Y_{0m} and Y_{2m} are removed. In order to find it, we consider the most general combination of all gains:

$$G_{13} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n\mu_j^m\right], \tag{C.54}$$

and impose proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\text{ removed: }\sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right) = 0\,\forall\, n \quad\Leftarrow\quad c_{i,0} + c_{i,1} + c_{i,2} = 0 \quad \text{for } i = 0,\ 1,\ 2, \tag{C.55}$$

$$Y_{n1}\text{ removed: }\sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\mu_j c_{i,j}\right)=0\,\forall\, n \quad\Leftarrow\quad \mu_0 c_{i,0}+\mu_1 c_{i,1}+\mu_2 c_{i,2}=0 \quad \text{for } i=0,\,1,\,2, \tag{C.56}$$

$$Y_{0m}\text{ removed: }\sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}c_{i,j}\right)=0\,\forall\, m \quad\Leftarrow\quad c_{0,j}+c_{1,j}+c_{2,j}=0 \quad \text{for } j=0,\,1,\,2, \tag{C.57}$$

$$Y_{2m}\text{ removed: }\sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}\mu_i^2 c_{i,j}\right)=0\,\forall\, m \quad\Leftarrow\quad \mu_0^2 c_{0,j}+\mu_1^2 c_{1,j}+\mu_2^2 c_{2,j}=0 \quad \text{for } j=0,\,1,\,2. \tag{C.58}$$

The conditions given by equations (C.55)–(C.58) form an overdetermined system of equations for the nine variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0}=1$):

$$\begin{aligned}
&c_{0,0}=1,\\
&c_{0,1}=-\frac{(\mu_0-\mu_2)}{\mu_1-\mu_2},\\
&c_{0,2}=-1-c_{0,1}=\frac{\mu_0-\mu_1}{\mu_1-\mu_2},\\
&c_{1,0}=-\frac{(\mu_0^2-\mu_2^2)}{\mu_1^2-\mu_2^2},\\
&c_{1,1}=c_{1,0}c_{0,1}=\frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
&c_{1,2}=-c_{1,0}-c_{1,1}=c_{1,0}c_{0,2}=-\frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
&c_{2,0}=-1-c_{1,0}=\frac{\mu_0^2-\mu_1^2}{\mu_1^2-\mu_2^2},\\
&c_{2,1}=-c_{0,1}-c_{1,1}=c_{0,1}c_{2,0}=\frac{(\mu_1^2-\mu_0^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
&c_{2,2}=-c_{2,0}-c_{2,1}=(1+c_{1,0})(1+c_{0,1})=\frac{(\mu_0^2-\mu_1^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)}.
\end{aligned} \tag{C.59}$$

By substituting (C.59) back into (C.54) we get an expression in which the terms Y_{n0}, Y_{n1}, Y_{0m} and Y_{2m} are removed:

$$\begin{aligned}
G_{13}=&\sum_{m=2}^{\infty}\frac{Y_{1m}}{m!}\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_2)(\mu_1+\mu_2)}\cdot A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,m)\\
&+\sum_{\substack{m=2\\ n=3}}^{\infty}\frac{Y_{nm}}{n!m!}\frac{A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,m)\cdot A_{11}(\mu_0,\,\mu_1,\,\mu_2,\,n)}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)},
\end{aligned} \tag{C.60}$$

where A_{22} is the factor given by (C.11) also present in the bounds for Y_{02} and Y_{22}, whereas A_{11} is the factor given by (C.23) which appears in the bound on Y_{11}. Note that this is somehow expected: when bounding Y_{02} and Y_{22} we removed the terms Y_{n0} and Y_{n1} as we just did for Y_{13}, and in bounding Y_{11} we removed the terms Y_{0m} and Y_{2m} as we did here. Therefore, by exploiting the result given by (C.12) we can recast each term of the sum corresponding to the Y_{1m}, with $m\geqslant 2$, in (C.60) as:

$$-\frac{Y_{1m}}{m!}\frac{(\mu_0-\mu_2)^2}{(\mu_1+\mu_2)}(\mu_0-\mu_1)\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k}-\mu_1^{m-1-k}), \tag{C.61}$$

and realize that it is always negative, regardless of the value of the intensities.

By employing the results (C.12), (C.24) we can recast each term of the sum corresponding to the Y_{nm} with $n\geqslant 3$ and $m\geqslant 2$, in (C.60) as:

$$\frac{Y_{nm}}{n!m!}\frac{(\mu_0-\mu_2)^2(\mu_1-\mu_2)^2}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)}(\mu_0-\mu_1)\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k}-\mu_1^{m-1-k})F(n), \tag{C.62}$$

and realize that it is always positive[9], regardless of the intensities.

[9] $F(n)$ is defined in (C.24).

A valid upper bound on Y_{13} is then obtained by setting $Y_{1m} \to 0$ (except for Y_{13}) and $Y_{nm} \to 1$ for all $n \geqslant 3$ and $m \geqslant 2$ in (C.60). As a result we obtain:

$$G_{13} = -\frac{Y_{13}^U}{3!}\frac{(\mu_0-\mu_2)^2}{(\mu_1+\mu_2)}(\mu_0-\mu_1)[\mu_0^2-\mu_1^2+\mu_2(\mu_0-\mu_1)] + \sum_{\substack{m=2\\ n=3}}^{\infty} \frac{[\mu_1^m(\mu_0-\mu_2)+\mu_2^m(\mu_1-\mu_0)+\mu_0^m(\mu_2-\mu_1)]\cdot[\mu_1^n(\mu_0^2-\mu_2^2)+\mu_2^n(\mu_1^2-\mu_0^2)+\mu_0^n(\mu_2^2-\mu_1^2)]}{n!m!(\mu_1-\mu_2)^2(\mu_1+\mu_2)}, \tag{C.63}$$

which implies:

$$\begin{aligned}\frac{Y_{13}^U}{6}\frac{(\mu_0-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)}{\mu_1+\mu_2} &= -G_{13} \\ &+ \frac{(e^{\mu_1}-\mu_1-1)(\mu_0-\mu_2)+(e^{\mu_2}-\mu_2-1)(\mu_1-\mu_0)+(e^{\mu_0}-\mu_0-1)(\mu_2-\mu_1)}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)} \\ &\times\left[\left(e^{\mu_1}-\frac{\mu_1^2}{2}-\mu_1-1\right)(\mu_0^2-\mu_2^2)+\left(e^{\mu_2}-\frac{\mu_2^2}{2}-\mu_2-1\right)(\mu_1^2-\mu_0^2)\right. \\ &\left.+\left(e^{\mu_0}-\frac{\mu_0^2}{2}-\mu_0-1\right)(\mu_2^2-\mu_1^2)\right].\end{aligned} \tag{C.64}$$

We thus obtain the following upper bound on Y_{13}:

$$\begin{aligned}Y_{13}^U &= -\frac{6(\mu_1+\mu_2)G_{13}}{(\mu_0-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)} + \frac{6}{(\mu_0-\mu_2)^2(\mu_1-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)} \\ &\times[e^{\mu_2}(\mu_1-\mu_0)+e^{\mu_1}(\mu_0-\mu_2)+e^{\mu_0}(\mu_2-\mu_1)] \\ &\times[e^{\mu_2}(\mu_1^2-\mu_0^2)+e^{\mu_1}(\mu_0^2-\mu_2^2)+e^{\mu_0}(\mu_2^2-\mu_1^2)-(\mu_0-\mu_1)(\mu_1-\mu_2)(\mu_0-\mu_2)],\end{aligned} \tag{C.65}$$

where G_{13} is defined in (C.54) and the coefficients of the combination of gains in (C.59).

C.6. Upper bound on Y_{31}

We look for that combination of gains in which all the terms proportional to Y_{n0}, Y_{n2}, Y_{0m} and Y_{1m} are removed. In order to find it, we proceed like in the previous case. That is, we consider the most general combination of all gains:

$$G_{31} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n\mu_j^m\right], \tag{C.66}$$

and impose proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\text{removed: } \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right) = 0\,\forall\, n \quad \Leftarrow \quad c_{i,0}+c_{i,1}+c_{i,2}=0 \quad \text{for } i=0,\,1,\,2, \tag{C.67}$$

$$Y_{n2}\text{removed: } \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\mu_j^2 c_{i,j}\right) = 0\,\forall\, n \quad \Leftarrow \quad \mu_0^2c_{i,0}+\mu_1^2c_{i,1}+\mu_2^2c_{i,2}=0 \quad \text{for } i=0,\,1,\,2, \tag{C.68}$$

$$Y_{0m}\text{removed: } \sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}c_{i,j}\right) = 0\,\forall\, m \quad \Leftarrow \quad c_{0,j}+c_{1,j}+c_{2,j}=0 \quad \text{for } j=0,\,1,\,2, \tag{C.69}$$

$$Y_{1m}\text{removed: } \sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}\mu_i c_{i,j}\right) = 0\,\forall\, m \quad \Leftarrow \quad \mu_0c_{0,j}+\mu_1c_{1,j}+\mu_2c_{2,j}=0 \quad \text{for } j=0,\,1,\,2. \tag{C.70}$$

The conditions (C.67)–(C.70) form an overdetermined system of equations for the nine variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0}=1$):

$$
\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= -\frac{(\mu_0^2-\mu_2^2)}{\mu_1^2-\mu_2^2},\\
c_{0,2} &= -1-c_{0,1} = \frac{\mu_0^2-\mu_1^2}{\mu_1^2-\mu_2^2},\\
c_{1,0} &= -\frac{(\mu_0-\mu_2)}{\mu_1-\mu_2},\\
c_{1,1} &= c_{1,0}c_{0,1} = \frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{1,2} &= -c_{1,0}-c_{1,1} = c_{1,0}c_{0,2} = \frac{(\mu_1^2-\mu_0^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{2,0} &= -1-c_{1,0} = \frac{\mu_0-\mu_1}{\mu_1-\mu_2},\\
c_{2,1} &= -c_{0,1}-c_{1,1} = c_{0,1}c_{2,0} = -\frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{2,2} &= -c_{2,0}-c_{2,1} = (1+c_{1,0})(1+c_{0,1}) = \frac{(\mu_0^2-\mu_1^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)}.
\end{aligned}
\tag{C.71}
$$

By substituting (C.71) back into (C.66) we get an expression in which the terms Y_{n0}, Y_{n2}, Y_{0m} and Y_{1m} are removed:

$$
\begin{aligned}
G_{31} = &\sum_{n=2}^{\infty}\frac{Y_{n1}}{n!}\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_2)(\mu_1+\mu_2)}\cdot A_{22}(\mu_0,\mu_1,\mu_2,n)\\
&+\sum_{\substack{n=2\\m=3}}^{\infty}\frac{Y_{nm}}{n!m!}\frac{A_{22}(\mu_0,\mu_1,\mu_2,n)\cdot A_{11}(\mu_0,\mu_1,\mu_2,m)}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)},
\end{aligned}
\tag{C.72}
$$

where A_{22} and A_{11} are again the factors from Y_{22} and Y_{11} bounds given by equations (C.11), (C.23), similarly to what happens when bounding Y_{13} (see appendix C.5). Therefore the analysis of the coefficient's sign is the same as in appendix C.5. Hence a valid upper bound on Y_{31} is obtained by setting $Y_{n1}\to 0$ (except for Y_{31}) and $Y_{nm}\to 1$ in (C.72) for all $n\geqslant 2$ and $m\geqslant 3$ in (C.72). Analogous steps to those in appendix C.5 lead to the following upper bound:

$$
\begin{aligned}
Y_{31}^{U} \;=\; &-\frac{6(\mu_1+\mu_2)G_{31}}{(\mu_0-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)}+\frac{6}{(\mu_0-\mu_2)^2(\mu_1-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)}\\
&\times[\mathrm{e}^{\mu_2}(\mu_1-\mu_0)+\mathrm{e}^{\mu_1}(\mu_0-\mu_2)+\mathrm{e}^{\mu_0}(\mu_2-\mu_1)]\\
&\times[\mathrm{e}^{\mu_2}(\mu_1^2-\mu_0^2)+\mathrm{e}^{\mu_1}(\mu_0^2-\mu_2^2)+\mathrm{e}^{\mu_0}(\mu_2^2-\mu_1^2)-(\mu_0-\mu_1)(\mu_1-\mu_2)(\mu_0-\mu_2)],
\end{aligned}
\tag{C.73}
$$

where G_{31} is defined in (C.66) and the coefficients of the combination of gains in (C.71).

C.7. Upper bound on Y_{00}

Consider the following combinations of gains in which all the terms Y_{1m} and Y_{n1} are removed:

$$
\begin{aligned}
G_{00}^{0,1} &= \mu_1^2\tilde{Q}^{0,0}+\mu_0^2\tilde{Q}^{1,1}-\mu_0\mu_1(\tilde{Q}^{0,1}+\tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_1-\mu_0\mu_1^n)(\mu_0^m\mu_1-\mu_0\mu_1^m);\\
G_{00}^{0,2} &= \mu_2^2\tilde{Q}^{0,0}+\mu_0^2\tilde{Q}^{2,2}-\mu_0\mu_2(\tilde{Q}^{0,2}+\tilde{Q}^{2,0}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_2-\mu_0\mu_2^n)(\mu_0^m\mu_2-\mu_0\mu_2^m);\\
G_{00}^{1,2} &= \mu_2^2\tilde{Q}^{1,1}+\mu_1^2\tilde{Q}^{2,2}-\mu_1\mu_2(\tilde{Q}^{1,2}+\tilde{Q}^{2,1}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_1^n\mu_2-\mu_1\mu_2^n)(\mu_1^m\mu_2-\mu_1\mu_2^m).
\end{aligned}
\tag{C.74}
$$

We now combine $G_{00}^{0,1}$, $G_{00}^{0,2}$ and $G_{00}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the terms Y_{2m} and Y_{n2} are also removed in the resulting expression:

$$
\begin{aligned}
G_{00}^{0,1}+c_0\,G_{00}^{0,2}+c_1\,G_{00}^{1,2} = &\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}[(\mu_0^n\mu_1-\mu_0\mu_1^n)(\mu_0^m\mu_1-\mu_0\mu_1^m)\\
&+c_0(\mu_0^n\mu_2-\mu_0\mu_2^n)(\mu_0^m\mu_2-\mu_0\mu_2^m)+c_1(\mu_1^n\mu_2-\mu_1\mu_2^n)(\mu_1^m\mu_2-\mu_1\mu_2^m)].
\end{aligned}
\tag{C.75}
$$

For Y_{2m} and Y_{n2} to be removed it suffices that for every m it holds:

$$(\mu_0^2\mu_1 - \mu_0\mu_1^2)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + c_0(\mu_0^2\mu_2 - \mu_0\mu_2^2)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + c_1(\mu_1^2\mu_2 - \mu_1\mu_2^2)(\mu_1^m\mu_2 - \mu_1\mu_2^m) = 0, \tag{C.76}$$

which is fulfilled by:

$$c_0 = -\frac{\mu_1^2(\mu_0 - \mu_1)}{\mu_2^2(\mu_0 - \mu_2)}, \tag{C.77}$$

$$c_1 = \frac{\mu_0^2(\mu_0 - \mu_1)}{\mu_2^2(\mu_1 - \mu_2)}. \tag{C.78}$$

Substituting (C.77) and (C.78) back into (C.75) and multiplying both sides by μ_2^2, we get an expression where all the terms Y_{0m}, Y_{2m}, Y_{n0} and Y_{n2} are removed and where the term Y_{00} gives the largest contribution. More precisely, we find that:

$$\begin{aligned}
&\mu_2^2 G_{00}^{0,1} - \mu_1^2\frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}G_{00}^{0,2} + \mu_0^2\frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}G_{00}^{1,2} \\
&= Y_{00}[\mu_2^2(\mu_0 - \mu_1)^2 - \mu_1^2(\mu_0 - \mu_1)(\mu_0 - \mu_2) + \mu_0^2(\mu_0 - \mu_1)(\mu_1 - \mu_2)] \\
&+ \sum_{m=3}^{\infty}\frac{Y_{0m}}{m!}[\mu_2^2(\mu_1 - \mu_0)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + \mu_1^2(\mu_0 - \mu_1)(\mu_0^m\mu_2 - \mu_0\mu_2^m) - \mu_0^2(\mu_0 - \mu_1)(\mu_1^m\mu_2 - \mu_1\mu_2^m)] \\
&+ \sum_{n=3}^{\infty}\frac{Y_{n0}}{n!}[\mu_2^2(\mu_1 - \mu_0)(\mu_0^n\mu_1 - \mu_0\mu_1^n) + \mu_1^2(\mu_0 - \mu_1)(\mu_0^n\mu_2 - \mu_0\mu_2^n) - \mu_0^2(\mu_0 - \mu_1)(\mu_1^n\mu_2 - \mu_1\mu_2^n)] \\
&+ \sum_{n,m=3}^{\infty}\frac{Y_{nm}}{n!m!}\mu_0^2\mu_1^2\mu_2^2[(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^{m-1} - \mu_1^{m-1}) \\
&- \frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^{n-1} - \mu_2^{n-1})(\mu_0^{m-1} - \mu_2^{m-1}) + \frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^{n-1} - \mu_2^{n-1})(\mu_1^{m-1} - \mu_2^{m-1})\Big].
\end{aligned} \tag{C.79}$$

In order to extract an upper bound on Y_{00} we need to study the sign of the yield's coefficients. We start by recasting the term corresponding to Y_{00} as:

$$\begin{aligned}
&Y_{00}(\mu_0 - \mu_1)[\mu_2^2(\mu_0 - \mu_1) - \mu_1^2(\mu_0 - \mu_2) + \mu_0^2(\mu_1 - \mu_2)] \\
&= Y_{00}(\mu_0 - \mu_1)^2(\mu_1 - \mu_2)(\mu_0 - \mu_2).
\end{aligned} \tag{C.80}$$

We observe that the sign of this expression is determined by the factors $(\mu_1 - \mu_2)(\mu_0 - \mu_2)$.

We then proceed by recasting each term of the sum corresponding to the Y_{nm}, with $n,\ m \geqslant 3$ in (C.79) as:

$$\frac{Y_{nm}}{n!m!}\frac{A_{00}(\mu_0, \mu_1, \mu_2, m)\cdot A_{00}(\mu_0, \mu_1, \mu_2, n)}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)}, \tag{C.81}$$

where

$$A_{00}(\mu_0, \mu_1, \mu_2, m) \equiv \mu_1^m(\mu_2^2\mu_0 - \mu_2\mu_0^2) + \mu_2^m(\mu_0^2\mu_1 - \mu_0\mu_1^2) + \mu_0^m(\mu_1^2\mu_2 - \mu_1\mu_2^2). \tag{C.82}$$

This factor can be rewritten as:

$$\begin{aligned}
A_{00}(\mu_0, \mu_1, \mu_2, m) &= \mu_0\mu_1\mu_2[\mu_1^{m-1}(\mu_2 - \mu_0) + \mu_2^{m-1}(\mu_0 - \mu_1) + \mu_0^{m-1}(\mu_1 - \mu_2)] \\
&= -\mu_0\mu_1\mu_2\, A_{22}(\mu_0, \mu_1, \mu_2, m-1),
\end{aligned} \tag{C.83}$$

where A_{22} is defined as (C.11) in appendix C.1. Thus we can use the result (C.12) obtained in appendix C.1 to directly recast A_{00} as:

$$A_{00}(\mu_0, \mu_1, \mu_2, m) = \mu_0\mu_1\mu_2(\mu_0 - \mu_2)(\mu_1 - \mu_2)\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k} - \mu_1^{m-2-k}). \tag{C.84}$$

By substituting (C.84) back into (C.81), we get the final expression for each term of the sum corresponding to the Y_{nm}, with $n,\ m \geqslant 3$ in (C.79):

$$\frac{Y_{nm}}{n!m!}\mu_0^2\mu_1^2\mu_2^2(\mu_0 - \mu_2)(\mu_1 - \mu_2)\left[\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k} - \mu_1^{m-2-k})\right]\left[\sum_{k=0}^{n-2}\mu_2^k(\mu_0^{n-2-k} - \mu_1^{n-2-k})\right], \tag{C.85}$$

which has manifestly the same sign as the expression given by (C.80), for any value of the intensities (the product of the last two factors is always positive).

Finally, we recast the Y_{0m}'s terms (Y_{n0}'s terms are identical under the replacement $m \to n$) as:

$$\begin{aligned}&\frac{Y_{0m}}{m!}\mu_0\mu_1\mu_2(\mu_0-\mu_1)[\mu_2(\mu_1^{m-1}-\mu_0^{m-1})+\mu_1(\mu_0^{m-1}-\mu_2^{m-1})-\mu_0(\mu_1^{m-1}-\mu_2^{m-1})]\\&=\frac{Y_{0m}}{m!}(\mu_0-\mu_1)A_{00}(\mu_0,\mu_1,\mu_2,m)\\&=\frac{Y_{0m}}{m!}\mu_0\mu_1\mu_2(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k}-\mu_1^{m-2-k}),\end{aligned} \tag{C.86}$$

where we employed (C.83) in the first equality and (C.84) in the second one. We observe that the sign of the Y_{0m}'s terms is again determined by the factors $(\mu_0-\mu_2)(\mu_1-\mu_2)$.

We conclude that the coefficients of Y_{0m}, Y_{n0} and Y_{nm}, with $n,\ m\geqslant 3$, carry the same sign as Y_{00}'s, which implies that a valid upper bound on Y_{00} is obtained by setting all the other yields to zero in (C.79). In so doing, we find that:

$$Y_{00}^U=\frac{\frac{\mu_2^2G_{00}^{0,1}}{\mu_0-\mu_1}-\frac{\mu_1^2G_{00}^{0,2}}{\mu_0-\mu_2}+\frac{\mu_0^2G_{00}^{1,2}}{\mu_1-\mu_2}}{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)}. \tag{C.87}$$

Appendix D. Yield's bounds with four decoys

Here we derive analytical upper bounds on the yields appearing in (1.7), following the same lines of section 2. In this case we assume that Alice and Bob can prepare their phase-randomized coherent pulses with four different intensity settings: $\{\mu_0,\mu_1,\mu_2,\mu_3\}$, which are the same for both parties. This choice is optimal since we assumed that the two optical channels linking the parties to the central node C have equal transmittance $\sqrt{\eta}$ [43].

The whole set of infinite yields is subjected to the following sixteen equality constraints:

$$\tilde{Q}^{k,l}\equiv e^{\mu_k+\mu_l}Q^{k,l}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\mu_k{}^n\mu_l{}^m\quad k,\,l\in\{0,\,1,\,2,\,3\}, \tag{D.1}$$

and to the same inequality constraints given by (2.3).

In this appendix we only obtain bounds on the yields Y_{13}, Y_{31}, Y_{04} and Y_{40} since the bounds derived on the yields Y_{00}, Y_{11}, Y_{02}, Y_{20} and Y_{22} in appendix C 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.

D.1. Upper bound on Y_{04}

Consider the following combinations of gains in which all the terms Y_{1m} and Y_{n0} are removed:

$$G_{04}^{i,j}=\mu_j\tilde{Q}^{i,i}+\mu_i\tilde{Q}^{j,j}-\mu_j\tilde{Q}^{i,j}-\mu_i\tilde{Q}^{j,i}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i^m-\mu_j^m), \tag{D.2}$$

where $i,\,j\in\{0,\,1,\,2,\,3\}$. Since $G_{04}^{i,i}=0$ and $G_{04}^{i,j}=G_{04}^{j,i}$, we only have six distinct combinations that read (for $j>i$): $G_{04}^{0,1}$, $G_{04}^{0,2}$, $G_{04}^{0,3}$, $G_{04}^{1,2}$, $G_{04}^{1,3}$, $G_{04}^{2,3}$.

We now take the linear combination of the $G_{04}^{i,j}$ such that even the yields Y_{2m}, Y_{3m}, Y_{n1} and Y_{n2} are removed:

$$\sum_{j>i}c_{i,j}G_{04}^{i,j}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\sum_{j>i}c_{i,j}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i^m-\mu_j^m), \tag{D.3}$$

where we implicitly assume that both indexes i,j run over the set $\{0,1,2,3\}$. For Y_{2m}, Y_{3m}, Y_{n1} and Y_{n2} to be removed, the real coefficients $c_{i,j}$ must satisfy:

$$\begin{cases}\sum_{j>i}c_{i,j}(\mu_j\mu_i^2-\mu_i\mu_j^2)(\mu_i^m-\mu_j^m)=0\ \forall m\\ \sum_{j>i}c_{i,j}(\mu_j\mu_i^3-\mu_i\mu_j^3)(\mu_i^m-\mu_j^m)=0\ \forall m\\ \sum_{j>i}c_{i,j}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i-\mu_j)=0\ \forall n\\ \sum_{j>i}c_{i,j}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i^2-\mu_j^2)=0\ \forall n\end{cases}. \tag{D.4}$$

In order to solve system (D.4), we look for those coefficients $c_{i,j}$ such that the multiplicative factors of μ_i^m and μ_i^n (for $i=0,1,2,3$) are all set to zero. This corresponds to imposing sixteen conditions on the six coefficients $c_{i,j}$. These conditions are not all independent, and a solution can be found even when we require (for simplicity) that $c_{0,1}=1$:

$$
\begin{aligned}
c_{0,1} &= 1,\\
c_{0,2} &= -\frac{(\mu_0-\mu_1)\mu_1(\mu_1-\mu_3)}{(\mu_0-\mu_2)\mu_2(\mu_2-\mu_3)},\\
c_{0,3} &= \frac{(\mu_0-\mu_1)\mu_1(\mu_1-\mu_2)}{(\mu_0-\mu_3)\mu_3(\mu_2-\mu_3)},\\
c_{1,2} &= \frac{(\mu_0-\mu_1)\mu_0(\mu_0-\mu_3)}{(\mu_1-\mu_2)\mu_2(\mu_2-\mu_3)},\\
c_{1,3} &= -\frac{(\mu_0-\mu_1)\mu_0(\mu_0-\mu_2)}{(\mu_1-\mu_3)\mu_3(\mu_2-\mu_3)},\\
c_{2,3} &= \frac{\mu_0\mu_1(\mu_0-\mu_1)^2}{\mu_2\mu_3(\mu_2-\mu_3)^2}.
\end{aligned}
\tag{D.5}
$$

By substituting the solution for the coefficients given by (D.5) back into (D.3), one gets:

$$
\sum_{j>i} c_{i,j}G_{04}^{i,j} = \sum_{m=3}^{\infty}\frac{Y_{0m}}{m!}A_{04}(\mu_0,\mu_1,\mu_2,\mu_3,m) + \sum_{\substack{n=4\\m=3}}^{\infty}\frac{Y_{nm}}{n!m!}B_{04}(\mu_0,\mu_1,\mu_2,\mu_3,n,m),
\tag{D.6}
$$

where:

$$
\begin{aligned}
A_{04}(\mu_0,\mu_1,\mu_2,\mu_3,m) &= -\frac{(\mu_0-\mu_1)}{\mu_2\mu_3(\mu_2-\mu_3)}[\mu_0^m(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\\
&- \mu_1^m(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3) + \mu_2^m(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)\\
&- \mu_3^m(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)]\\
&= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_0-\mu_3)(\mu_1-\mu_3)}{\mu_2\mu_3}\left(\sum_{i_1\leqslant i_2\leqslant\ldots\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{m-3}}\right),
\end{aligned}
\tag{D.7}
$$

and

$$
\begin{aligned}
&B_{04}(\mu_0,\mu_1,\mu_2,\mu_3,n,m)\\
&= \frac{-\mu_0\mu_1}{(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_0-\mu_3)(\mu_2-\mu_3)^2}[\mu_0^m(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\\
&- \mu_1^m(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3) + \mu_2^m(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)\\
&- \mu_3^m(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)]\times[-\mu_0^{n-1}(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\\
&+ \mu_1^{n-1}(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3) - \mu_2^{n-1}(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)\\
&+ \mu_3^{n-1}(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)]\\
&= -\mu_0\mu_1\mu_2\mu_3\,A_{04}(\mu_0,\mu_1,\mu_2,\mu_3,m)\cdot\left(\sum_{i_1\leqslant i_2\leqslant\ldots\leqslant i_{n-4}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{n-4}}\right).
\end{aligned}
\tag{D.8}
$$

In (D.7), (D.8) we again assume that the indexes in the sums run over the set $\{0,1,2,3\}$ and we define $\sum_{i_1\leqslant i_2\leqslant\ldots\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{m-3}}|_{m=3}=1$. From (D.7) we deduce that the sign of Y_{0m}'s coefficient is independent of m, while from (D.8) we deduce that Y_{nm}'s coefficient has always opposite sign to that of Y_{0m}. Therefore a valid upper bound on Y_{04} is obtained by setting to zero all the other yields Y_{0m} and to 1 the yields Y_{nm} with $n\geqslant 4$ and $m\geqslant 3$ in (D.6). We thus obtain:

$$
\sum_{j>i} c_{i,j}G_{04}^{i,j} = \frac{Y_{04}^U}{4!}A_{04}(\mu_0,\mu_1,\mu_2,\mu_3,4) + \sum_{\substack{n=4\\m=3}}^{\infty}\frac{B_{04}(\mu_0,\mu_1,\mu_2,\mu_3,n,m)}{n!m!},
\tag{D.9}
$$

which implies the following upper bound on Y_{04}:

$$
Y_{04}^U = \frac{4!}{A_{04}(\mu_0,\mu_1,\mu_2,\mu_3,4)}\left[\sum_{j>i} c_{i,j}G_{04}^{i,j} - \sum_{\substack{n=4\\m=3}}^{\infty}\frac{B_{04}(\mu_0,\mu_1,\mu_2,\mu_3,n,m)}{n!m!}\right],
\tag{D.10}
$$

where $c_{i,j}$ are given in (D.5), $G_{04}^{i,j}$ is defined in (D.2), the coefficient A_{04} reads:

$$
A_{04}(\mu_0,\mu_1,\mu_2,\mu_3,4) = -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_0-\mu_3)(\mu_1-\mu_3)(\mu_0+\mu_1+\mu_2+\mu_3)}{\mu_2\mu_3},
\tag{D.11}
$$

and the sum over the coefficient B_{04} reads:

$$\sum_{\substack{n=4\\m=3}}^{\infty}\frac{B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n,\,m)}{n!m!}=\frac{\mu_0\mu_1}{(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_0-\mu_3)(\mu_2-\mu_3)^2}$$
$$\times\left[\left(e^{\mu_0}-1-\mu_0-\frac{\mu_0^2}{2}\right)(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\right.$$
$$-\left(e^{\mu_1}-1-\mu_1-\frac{\mu_1^2}{2}\right)(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3)$$
$$+\left(e^{\mu_2}-1-\mu_2-\frac{\mu_2^2}{2}\right)(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)$$
$$\left.-\left(e^{\mu_3}-1-\mu_3-\frac{\mu_3^2}{2}\right)(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)\right]^2. \tag{D.12}$$

D.2. Upper bound on Y_{40}

Consider the following combinations of gains in which all the terms Y_{0m} and Y_{n1} are removed:

$$G_{40}^{i,j}=\mu_j\tilde{Q}^{i,i}+\mu_i\tilde{Q}^{j,j}-\mu_i\tilde{Q}^{i,j}-\mu_j\tilde{Q}^{j,i}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^m-\mu_i\mu_j^m), \tag{D.13}$$

where $i,\,j\in\{0,\,1,\,2,\,3\}$. Since $G_{40}^{i,i}=0$ and $G_{40}^{i,j}=G_{40}^{j,i}$, we only have six distinct combinations that read (for $j>i$): $G_{40}^{0,1}$, $G_{40}^{0,2}$, $G_{40}^{0,3}$, $G_{40}^{1,2}$, $G_{40}^{1,3}$, $G_{40}^{2,3}$.

We now take the linear combination of the $G_{40}^{i,j}$ such that even the yields Y_{1m}, Y_{2m}, Y_{n2} and Y_{n3} are removed:

$$\sum_{j>i}c_{i,j}G_{40}^{i,j}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\sum_{j>i}c_{i,j}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^m-\mu_i\mu_j^m), \tag{D.14}$$

where we implicitly assume that both indexes i,j run over the set $\{0,1,2,3\}$. For Y_{1m}, Y_{2m}, Y_{n2} and Y_{n3} to be removed, the real coefficients $c_{i,j}$ must satisfy:

$$\begin{cases}\sum_{j>i}c_{i,j}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^2-\mu_i\mu_j^2)=0\ \forall\, n\\ \sum_{j>i}c_{i,j}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^3-\mu_i\mu_j^3)=0\ \forall\, n\\ \sum_{j>i}c_{i,j}(\mu_i-\mu_j)(\mu_j\mu_i^m-\mu_i\mu_j^m)=0\ \forall\, m\\ \sum_{j>i}c_{i,j}(\mu_i^2-\mu_j^2)(\mu_j\mu_i^m-\mu_i\mu_j^m)=0\ \forall\, m.\end{cases} \tag{D.15}$$

We now notice that the system (D.15) is exactly the same system solved in appendix D.2 while bounding Y_{04}, thus the solution for the coefficients $c_{i,j}$ is given in (D.5). By substituting the solution (D.5) back into (D.14), one gets:

$$\sum_{j>i}c_{i,j}G_{40}^{i,j}=\sum_{n=3}^{\infty}\frac{Y_{n0}}{n!}A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n)+\sum_{\substack{n=3\\m=4}}^{\infty}\frac{Y_{nm}}{n!m!}B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m,\,n), \tag{D.16}$$

where A_{04} and B_{04} are the coefficients defined in (D.7), (D.8) while bounding Y_{04}. Hence we can adopt the observations made on the sign of A_{04} and B_{04} from appendix D.1 and conclude that a valid upper bound on Y_{40} is obtained by setting to zero all the other yields Y_{n0} and to 1 the yields Y_{nm} with $n\geqslant 3$ and $m\geqslant 4$ in (D.16). The upper bound on Y_{40} then reads:

$$Y_{40}^U=\frac{4!}{A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,4)}\left[\sum_{j>i}c_{i,j}G_{40}^{i,j}-\sum_{\substack{n=3\\m=4}}^{\infty}\frac{B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m,\,n)}{n!m!}\right], \tag{D.17}$$

where $c_{i,j}$, $G_{40}^{i,j}$, $A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,4)$ and the sum over B_{04} are given in (D.5), (D.13), (D.11) and (D.12), respectively.

D.3. Upper bound on Y_{13}

We consider the most general combination of all sixteen gains:

$$\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{3} c_{i,j}\mu_i^n \mu_j^m\right], \tag{D.18}$$

and require that the terms Y_{n0}, Y_{n1}, Y_{n2}, Y_{0m}, Y_{2m} and Y_{3m} are removed, by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0} \text{ removed:} \quad \sum_{i,j=0}^{3} c_{i,j}\mu_i^n = 0 \ \ \forall n \quad \Leftarrow \quad \sum_{j=0}^{3} c_{i,j} = 0 \ \ \text{for} \ \ i = 0,\, 1,\, 2,\, 3, \tag{D.19}$$

$$Y_{n1} \text{ removed:} \quad \sum_{i,j=0}^{3} c_{i,j}\mu_i^n \mu_j = 0 \ \ \forall n \quad \Leftarrow \quad \sum_{j=0}^{3} c_{i,j}\mu_j = 0 \ \ \text{for} \ \ i = 0,\, 1,\, 2,\, 3, \tag{D.20}$$

$$Y_{n2} \text{ removed:} \quad \sum_{i,j=0}^{3} c_{i,j}\mu_i^n \mu_j^2 = 0 \ \ \forall n \quad \Leftarrow \quad \sum_{j=0}^{3} c_{i,j}\mu_j^2 = 0 \ \ \text{for} \ \ i = 0,\, 1,\, 2,\, 3, \tag{D.21}$$

$$Y_{0m} \text{ removed:} \quad \sum_{i,j=0}^{3} c_{i,j}\mu_j^m = 0 \ \ \forall m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j} = 0 \ \ \text{for} \ \ j = 0,\, 1,\, 2,\, 3, \tag{D.22}$$

$$Y_{2m} \text{ removed:} \quad \sum_{i,j=0}^{3} c_{i,j}\mu_i^2 \mu_j^m = 0 \ \ \forall m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j}\mu_i^2 = 0 \ \ \text{for} \ \ j = 0,\, 1,\, 2,\, 3, \tag{D.23}$$

$$Y_{3m} \text{ removed:} \quad \sum_{i,j=0}^{3} c_{i,j}\mu_i^3 \mu_j^m = 0 \ \ \forall m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j}\mu_i^3 = 0 \ \ \text{for} \ \ j = 0,\, 1,\, 2,\, 3. \tag{D.24}$$

The twenty-four conditions given by (D.19)–(D.24) form an over-determined system of equations for the sixteen variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0} = 1$):

$$\begin{aligned}
c_{0,0} &= 1, \\
c_{0,1} &= \frac{(\mu_0-\mu_2)(\mu_0-\mu_3)}{(\mu_2-\mu_1)(\mu_1-\mu_3)}, \\
c_{0,2} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)}{(\mu_1-\mu_2)(\mu_2-\mu_3)}, \\
c_{0,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_3)(\mu_3-\mu_2)}, \\
c_{1,0} &= -\frac{(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}, \\
c_{1,1} &= \frac{(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}, \\
c_{1,2} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}, \\
c_{1,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}, \\
c_{2,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}, \\
c_{2,1} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},
\end{aligned}$$

$$
\begin{aligned}
c_{2,2} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,3} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)(\mu_3-\mu_2)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,1} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,2} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,3} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}.
\end{aligned}
\tag{D.25}
$$

By substituting these expressions back into (D.18) and by making some simplifications, one gets:

$$
\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j} = \sum_{m=3}^{\infty}\frac{Y_{1m}}{m!}A_{13}(\mu_0,\mu_1,\mu_2,\mu_3,m) + \sum_{\substack{n=4\\m=3}}^{\infty}\frac{Y_{nm}}{n!m!}A_{13}(\mu_0,\mu_1,\mu_2,\mu_3,m)\cdot C_n,
\tag{D.26}
$$

where:

$$
A_{13}(\mu_0,\mu_1,\mu_2,\mu_3,m) = \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2}{\mu_2\mu_3+\mu_1\mu_2+\mu_1\mu_3}\left(\sum_{i_1\leqslant i_2\leqslant\ldots\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{m-3}}\right),
\tag{D.27}
$$

and C_n ($n\geqslant 5$) is defined recursively as:

$$
\begin{cases}
C_n &= \left[\sum_{j=1}^{n-4}(\mu_0^j+\mu_1^j+\mu_2^j+\mu_3^j)C_{n-j} - \mu_0\mu_1\mu_2\mu_3\left(\sum_{i_1\leqslant i_2\leqslant\ldots\leqslant i_{n-5}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{n-5}}\right)\right]/(n-4)\\
C_4 &= \mu_0\mu_1\mu_2+\mu_0\mu_1\mu_3+\mu_0\mu_2\mu_3+\mu_1\mu_2\mu_3.
\end{cases}
\tag{D.28}
$$

In (D.27), (D.28) we assume that the indexes i_j in the sums run over the set $\{0,1,2,3\}$ and we define $\sum_{i_1\leqslant i_2\leqslant\ldots\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{m-3}}|_{m=3}=1$. From (D.27) we deduce that the sign of Y_{1m}'s coefficient is always positive, while from (D.28) we deduce that Y_{nm}'s coefficient has always equal sign to that of Y_{1m}, since C_n is always a positive quantity. Therefore a valid upper bound on Y_{13} is obtained by setting to zero all the other yields in (D.26). The upper bound on Y_{13} then reads:

$$
Y_{13}^U = \frac{6}{A_{13}(\mu_0,\mu_1,\mu_2,\mu_3,3)}\left(\sum_{i,j=0}^{3}c_{i,j}\tilde{Q}^{i,j}\right),
\tag{D.29}
$$

where $c_{i,j}$ are defined in (D.25) and $A_{13}(\mu_0,\mu_1,\mu_2,\mu_3,3)$ reads:

$$
A_{13}(\mu_0,\mu_1,\mu_2,\mu_3,3) = \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2}{\mu_2\mu_3+\mu_1\mu_2+\mu_1\mu_3}.
\tag{D.30}
$$

D.4. Upper bound on Y_{31}

We consider the most general combination of all sixteen gains:

$$
\sum_{i,j=0}^{3}c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{3}c_{i,j}\mu_i^n\mu_j^m\right],
\tag{D.31}
$$

and require that the terms Y_{n0}, Y_{n2}, Y_{n3}, Y_{0m}, Y_{1m} and Y_{2m} are removed, by imposing proper conditions on the real coefficients $c_{i,j}$:

$$
Y_{n0}\text{ removed:}\quad \sum_{i,j=0}^{3}c_{i,j}\mu_i^n = 0\ \ \forall\, n \quad\Leftarrow\quad \sum_{j=0}^{3}c_{i,j}=0\ \text{ for }\ i=0,1,2,3,
\tag{D.32}
$$

$$
Y_{n2}\text{ removed:}\quad \sum_{i,j=0}^{3}c_{i,j}\mu_i^n\mu_j^2 = 0\ \ \forall\, n \quad\Leftarrow\quad \sum_{j=0}^{3}c_{i,j}\mu_j^2=0\ \text{ for }\ i=0,1,2,3,
\tag{D.33}
$$

$$
Y_{n3}\text{ removed:}\quad \sum_{i,j=0}^{3}c_{i,j}\mu_i^n\mu_j^3 = 0\ \ \forall\, n \quad\Leftarrow\quad \sum_{j=0}^{3}c_{i,j}\mu_j^3=0\ \text{ for }\ i=0,1,2,3,
\tag{D.34}
$$

$$Y_{0m} \text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_j^m = 0 \ \forall m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j} = 0 \ \text{ for } \ j = 0,\ 1,\ 2,\ 3, \tag{D.35}$$

$$Y_{1m} \text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_i\mu_j^m = 0 \ \forall m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j}\mu_i = 0 \ \text{ for } \ j = 0,\ 1,\ 2,\ 3, \tag{D.36}$$

$$Y_{2m} \text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_i^2\mu_j^m = 0 \forall m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j}\mu_i^2 = 0 \ \text{ for } \ j = 0,\ 1,\ 2,\ 3. \tag{D.37}$$

The twenty-four conditions (D.32)–(D.37) form an over-determined system of equations for the sixteen variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0} = 1$):

$$\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= -\frac{(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{0,2} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{0,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)(\mu_3-\mu_2)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,0} &= \frac{(\mu_0-\mu_2)(\mu_0-\mu_3)}{(\mu_2-\mu_1)(\mu_1-\mu_3)},\\
c_{1,1} &= \frac{(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,2} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)}{(\mu_1-\mu_2)(\mu_2-\mu_3)},\\
c_{2,1} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,2} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,3} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_3)(\mu_3-\mu_2)},\\
c_{3,1} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,2} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,3} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}.
\end{aligned} \tag{D.38}$$

By substituting these expressions back into (D.31) and by making some simplifications, one gets:

$$\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j} = \sum_{n=3}^{\infty} \frac{Y_{n1}}{n!} A_{13}(\mu_0,\ \mu_1,\ \mu_2,\ \mu_3,\ n) + \sum_{\substack{n=3\\m=4}}^{\infty} \frac{Y_{nm}}{n!m!} A_{13}(\mu_0,\ \mu_1,\ \mu_2,\ \mu_3,\ n)\cdot C_m, \tag{D.39}$$

where A_{13} and C_m also appear in appendix D.3 when bounding Y_{13} and are defined as (D.27) and (D.28), respectively. Thus, following the same lines of appendix D.3, we conclude that all yields in (D.39) are multiplied by a positive factor. A valid upper bound on Y_{31} is then obtained by setting to zero all the other yields in (D.39). We obtain:

$$Y_{31}^{U} = \frac{6}{A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,3)}\left(\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j}\right), \tag{D.40}$$

where $c_{i,j}$ and $A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,3)$ are defined in (D.38) and (D.30), respectively.

ORCID iDs

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

References

[1] Gisin N and Thew R 2007 *Nat. Photon.* **1** 165–71
[2] Kimble H J 2008 *Nature* **453** 1023
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* pp 175–9
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Scarani V, Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[6] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[7] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[8] Lo H-K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595–604
[9] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 *NPJ Quantum Inf.* **2** 16025
[10] Epping M, Kampermann H, Macchiavello C and Bruß D 2017 *New J. Phys.* **19** 093012
[11] Friedman R A, Dupuis F, Fawzi O, Renner R and Vidick T 2018 *Nat. Commun.* **9** 459
[12] Ribeiro J, Murta G and Wehner S 2018 *Phys. Rev.* A **97** 022307
[13] Grasselli F, Kampermann H and Bruß D 2018 *New J. Phys.* **20** 113014
[14] Yin H-L *et al* 2016 *Phys. Rev. Lett.* **117** 190501
[15] Boaron A *et al* 2018 *Phys. Rev. Lett.* **121** 190502
[16] Liao S-K *et al* 2017 *Nature* **549** 43
[17] Takenaka H *et al* 2017 *Nat. Photon.* **11** 502
[18] Takeoka M, Guha S and Wilde M M 2014 *Nat. Commun.* **5** 5235
[19] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[20] Sangouard N, Simon C, de Riedmatten N and Gisin N 2011 *Rev. Mod. Phys.* **83** 33–80
[21] Duan L-M, Lukin M D, Cirac J I and Zoller P 2001 *Nature* **414** 413–8
[22] Grudka A *et al* 2014 *Phys. Rev.* A **90** 062311
[23] Munro W J, Stephens A M, Devitt S J, Harrison K A and Nemoto K 2012 *Nat. Photon.* **6** 777–81
[24] Azuma K, Tamaki K and Lo H-K 2015 *Nat. Commun.* **6** 6787
[25] Abruzzo S, Kampermann H and Bruß D 2014 *Phys. Rev.* A **89** 012301
[26] Panayi C, Razavi M, Ma X and Lütkenhaus N 2014 *New J. Phys.* **16** 043005
[27] Azuma K, Tamaki K and Munro W J 2015 *Nat. Commun.* **6** 10171
[28] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[29] Tamaki K, Lo H-K, Wang W and Lucamarini M 2018 arXiv:1805.05511
[30] Ma X, Zeng P and Zhou H 2018 *Phys. Rev.* X **8** 031043
[31] Cui C *et al* 2019 *Phys. Rev. Appl.* **11** 034053
[32] Lin J and Lütkenhaus N 2018 *Phys. Rev.* A **98** 042332
[33] Curty M, Azuma K and Lo H-K 2018 arXiv:1807.07667
[34] Minder M, Pittaluga M, Roberts G L, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2019 *Nat. Photon.* **13** 334–8
[35] Liu Y *et al* 2019 arXiv:1902.06268
[36] Zhong X, Hu J, Curty M, Qian L and Lo H-K 2019 arXiv:1902.10209
[37] Lucamarini M 2018 *8th Int. Conf. on Quantum Cryptography (QCrypt'2018) (Shanghai, China)* http://2018.qcrypt.net
[38] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[39] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[40] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[41] Curty M, Xu F, Cui W, Lim C, Tamaki K and Lo H-K 2014 *Nat. Commun.* **5** 3732
[42] Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326
[43] Wang W, Xu F and Lo H-K 2018 arXiv:1807.03466
[44] Rosenberg D *et al* 2009 *New J. Phys.* **11** 045009