<table>
<thead>
<tr>
<th>Title</th>
<th>Quantum interference of multi-photon at beam splitter with application in measurement-device-independent quantum key distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Pradana, Andri; Chew, Lock Yue</td>
</tr>
<tr>
<td>Date</td>
<td>2019</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/49714">http://hdl.handle.net/10220/49714</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2019 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft. Original content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.</td>
</tr>
</tbody>
</table>
Quantum interference of multi-photon at beam splitter with application in measurement-device-independent quantum key distribution

Andri Pradana\textsuperscript{1} and Lock Yue Chew\textsuperscript{1,2,3}\textsuperscript{ DOI}

\textsuperscript{1} Division of Physics and Applied Physics, School of Physical and Mathematical Sciences, 21 Nanyang Link, Nanyang Technological University, 637371, Singapore
\textsuperscript{2} Data Science and Artificial Intelligence Research Centre, Block N4 #02a-32, Nanyang Avenue, Nanyang Technological University, 639798, Singapore
\textsuperscript{3} Complexity Institute, 61 Nanyang Drive, Nanyang Technological University, 637335, Singapore

E-mail: lockyue@ntu.edu.sg

Keywords: quantum interference, multi-photon interference, Hong–Ou–Mandel effect, squeezed coherent state, quantum cryptography, measurement-device-independent quantum key distribution, quantum bit error rate

Abstract

Despite the relative simplicity of the traditional Hong–Ou–Mandel (HOM) interferometer setup, it is of fundamental interest in various quantum optics applications and quantum information technologies. In this article, multi-photon interference using the original HOM interferometer setup is analyzed. More specifically, for any photon number state with Gaussian spectral distribution entering the beam splitter, the general analytical solution is calculated. The result is then used to study the coincident probability for coherent sources (laser) and squeezed coherent state. We also look into the potential benefits of implementing the squeezed coherent state in discrete-variable Measurement-Device-Independent Quantum Key Distribution and find that by optimizing the squeezing parameter, the error rate can be significantly reduced. This in turn also enhances the secret key rate performance over the coherent state.

When two identical single photons enter a 50:50 beam splitter, quantum interference of the photons causes both photons to exit at the same (but random) side of the beam splitter. This is known as the Hong–Ou–Mandel (HOM) effect. Experimentally, this is characterized by a dip in the coincidence rate [1], also referred to as the HOM dip. Coincidence here refers to mutual detection of photons at both sides or output modes of the beam splitter.

The original purpose of HOM experiment is to characterize the temporal distinguishability of single photons, by accurate measurement of time interval and bandwidth of the photons, allowed by the HOM interferometer setup. An account of HOM effect for single photons with various choices of spectra, and also taking into account photon distinguishability, can be seen in [2]. To accomplish the same task of characterizing the temporal distinguishability for multi photons, however, the experimental setup is generally modified to include multiple beam splitters and photon detectors [3]. A number of multi-photon interference experiments with various setups can be found, for example, in [4–11]. A summary for some of these experiments with discussion of temporal distinguishability is given in [12]. The general results for multi-photon quantum interference using traditional HOM interferometer, specifically, for any photon number state with Gaussian spectral distribution, have not been discussed in the literature.

Despite that, however, and despite the relative simplicity of the original HOM interferometer setup, it has proven to be useful and important in various applications, for example, in quantum interference of successive single photons from the same emitter [13–16], to determine the purity of photons emitted by quantum dot [13], in quantum interference between single photons emitted by independent atoms [17], to measure biphoton temporal wavefunction [18], in quantum interference of single photons with different colors via frequency-domain beam splitter [19], and in quantum interference of topological states of light [20]. The concept has also...
been applied to achieve entanglement between atoms [21] and distant spins [22], and realized as interference between microwave quantum memories [23].

Of particular interest here is its application in quantum cryptography protocol called the Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) [24–26]. MDI-QKD relies on quantum interference of photons for the distribution of secret keys between two parties. Ideally, single-photon source should be used. In practice however, weak coherent source (attenuated laser) is often used instead, due to limitations of single photon source for QKD applications. Indeed, recently a record maximum distance of 421 km for fiber-based QKD with state-of-the-art device performance employing laser source has been reported [27]. Therefore, the analysis of multi-photon interference is important in a MDI-QKD setup for calibration purpose, and for predicting coincidence probability using other states, such as the squeezed coherent state.

Furthermore, we also look into the application of squeezed coherent state in MDI-QKD. The implementation of squeezed state for continuous-variable MDI-QKD has been studied, for example, in [28, 29]. Here we focus on its application to discrete-variable version of MDI-QKD. In the coherent state, there is nonzero probability of multi-photon detection. This introduces two main disadvantages: increased error rate and the possibility of an eavesdropper implementing the photon-number-splitting (PNS) attack [30] to gain information about the secret bit without being detected. Sub-Poissonian photon state, such as the amplitude-squeezed coherent state, can have reduced multi-photon probability. For this reason, the potential improvement of the squeezed coherent state over the coherent state in this class of MDI-QKD is twofold: reducing the error rate and reducing the impact of PNS attack. In turn, this will improve the key rate and transmission distance. Here we discuss the potential error rate improvement in the context of time-bin coding MDI-QKD [26], but the arguments presented here also work for polarization coding one.

The structure of this paper is as follows: first, the description of multi-photon state is discussed. Second, the general expression for coincidence probability for multi photons in a Gaussian waveform is given for 50:50 lossless beam splitter. Additionally, the results are also extended for general asymmetric beam splitter. With the results, the total coincidence probability for the coherent state (from coherent source or laser) can be calculated. The coincidence probability for amplitude-squeezed coherent state (with sub-Poissonian distribution) is calculated as well and compared against the coherent state. Finally, we discuss the application of the squeezed coherent state to discrete-variable MDI-QKD and compare its error rates and secret key rates against the coherent state.

1. Description of $N$-photon state

The description of $N$-photon state is discussed in [3]. A general description of $N$-photon state is given by

$$|\Psi_N\rangle = \mathcal{N} \int d\omega_1 d\omega_2 \cdots d\omega_N \Phi(\omega_1, \ldots, \omega_N) \hat{a}^\dagger(\omega_1) \cdots \hat{a}^\dagger(\omega_N) |0\rangle,$$

where $\mathcal{N}$ is the normalization constant, $\Phi(\omega_1, \ldots, \omega_N)$ is a spectral weight function. The normalization constant can be determined by

$$\langle \Psi_N | \Psi_N \rangle = 1,$$

$$\mathcal{N}^2 \int d\omega_1 d\omega_2 \cdots d\omega_N \Phi(\omega_1, \ldots, \omega_N) \sum_{\mathcal{P}} \Phi(\omega_{\mathcal{P}(1)}, \ldots, \omega_{\mathcal{P}(N)}) = 1,$$

where $\mathcal{P}$ is permutation acting on the indices $\{1, 2, \ldots, N\}$, so $\mathcal{P}(j)$ denotes the integer that $j$ is permuted into, and the sum is taken over all permutations.

For indistinguishable photons in a single wave packet, all photons have identical spectral function $\phi(\omega)$. Furthermore, let $\Phi(\omega)$ be normalized in the sense that $\int d\omega |\phi(\omega)|^2 = 1$. Physically, $|\phi(\omega)|^2$ represents the spectral probability distribution of the photons. In this special case, $\Phi(\omega_1, \ldots, \omega_N) = \phi(\omega_1) \cdots \phi(\omega_N)$ and $\Phi(\omega_{\mathcal{P}(1)}, \ldots, \omega_{\mathcal{P}(N)}) = \Phi(\omega_1, \ldots, \omega_N)$. Then, proceeding from (2),

$$\mathcal{N}^2 N! \left[ \int d\omega |\phi(\omega)|^2 \right]^N = 1,$$

$$\mathcal{N} = \frac{1}{\sqrt{N!}},$$

where in the last line $\int d\omega |\phi(\omega)|^2 = 1$ has been used and $\mathcal{N}$ has been assumed to be real and positive for simplicity. With this, the $N$-photon state can be written as

$$|\Psi_N\rangle = |N\rangle_\phi = \frac{1}{\sqrt{N!}} \hat{A}(\phi)^N |0\rangle,$$
with
\[ \hat{A}(\phi^\dagger) = \int d\omega \phi(\omega) \hat{a}^\dagger(\omega). \] (5)

\( \hat{A}(\phi^\dagger) \) represents the creation operator for a mode characterized by \( \phi(\omega) \). As in [1], the spectral function \( \phi(\omega) \) is assumed to follow the form
\[ \phi(\omega) = (\sqrt{2\pi} \Delta)^{-\frac{1}{2}} \exp \left[ -\frac{(\omega - \omega_0)^2}{4\Delta^2} \right]. \] (6)

The spectral distribution \( |\phi(\omega)|^2 \) following this description is a Gaussian distribution, where \( \Delta \) is the standard deviation and \( \omega_0 \) is the mean. One can check that this satisfies \( \int d\omega |\phi(\omega)|^2 = 1 \).

In the HOM experiment, some arbitrary delay time \( \tau \) can be applied to the wave packet. To account for this, the phase factor \( e^{i\omega \tau} \) may be included in the spectral function
\[ \phi_\tau(\omega) = \phi(\omega) e^{i\omega \tau} = (\sqrt{2\pi} \Delta)^{-\frac{1}{2}} \exp \left[ -\frac{(\omega - \omega_0)^2}{4\Delta^2} \right] \exp(i\omega \tau). \] (7)

When the delay is zero, \( \tau = 0 \) and \( \phi_\tau(\omega) = \phi(\omega) \) as described in (6). Different delay times \( \tau_A \) and \( \tau_B \) can also be applied to photons traveling in the different paths of the interferometer. Experimentally, this is equivalent to setting different interferometer path lengths and/or different source emission times. The separation time between the wave packets is signified by \( \tau_A - \tau_B \).

Note that the photons from the two sources are required to have the same polarization, otherwise they will not interfere perfectly even if they overlap perfectly in time.

2. Coincidence probability for multi photons

A beam splitter has two input channels, denoted by \( A \) and \( B \), and two output channels (each directed to a detector), denoted by \( C \) and \( D \) (see figure 1). Coincident detection refers to mutual detection of photons at both output modes/channels of the beam splitter. Let \( P_{m,n}^{\text{co}} \) be the probability of coincidence detection when \( m \) photons enter input channel \( A \) and \( n \) photons enter input channel \( B \) of the beam splitter. Also, let \( P_{m,n}^{\text{det}}(k, l) \) be the probability \( k \) and \( l \) photons are detected exiting channel \( C \) and \( D \), respectively, given \( m \) photons enter \( A \) and \( n \) photons enter \( B \). Obviously, coincident detection cannot occur if all the photons exit the beam splitter in the same output channel, otherwise coincident detection will occur. A special case is when \( m = n = 0 \), in which there is no coincident detection. Therefore,
\[ P_{m,n}^{\text{co}} = \begin{cases} 0 & \text{for } m = n = 0, \\ 1 - P_{m,n}^{\text{det}}(m + n, 0) - P_{m,n}^{\text{det}}(0, m + n) & \text{for } (m + n) \geq 1. \end{cases} \] (8)

Furthermore, since 50:50 lossless beam splitter is used, the detection probability follows
\[ P_{m,n}^{\text{det}}(p, q) = P_{m,n}^{\text{det}}(q, p) = P_{n,m}^{\text{det}}(p, q) = P_{n,m}^{\text{det}}(q, p). \] (9)

Here, the final results for coincidence probability involving zero, one, and two photons in input channel \( A \), together with the general photon number case, are given. The setup is such that the delay times at \( A \) and \( B \) are \( \tau_A \) and \( \tau_B \), and the detectors are placed immediately after the beam splitter output channels \( C \) and \( D \). Readers interested in the technical details are encouraged to take a look at the full derivation, which can be found in appendix A.
2.1. Zero photons in input channel $A$

In this scenario, zero photons are in $A$ and $n$ photons are in $B$. This scenario is trivial: all $n$ photons go to only one detector with probability $\frac{1}{2^n}$. Then,

$$P_n = P_{n,0} = 0, \quad P_n = 1, \quad n = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.$$  

So, from (8),

$$P_{0,n} = \begin{cases} 
0 & \text{for } n = 0, \\
1 - \frac{1}{2^n} & \text{for } n \geq 1. 
\end{cases}$$

2.2. One photon in input channel $A$

The general expression for the probabilities from interference of one photon in input channel $A$ and $n$ in $B$ are

$$P_{1,n} = P_{1,n} = \frac{1}{2^{n+1}} \left[ 1 + ne^{-\Delta(t_A - t_B)^2} \right],$$

and

$$P_{1,n} = \frac{1}{2^n} \left[ 2^n - 1 - ne^{-\Delta(t_A - t_B)^2} \right].$$

The results of coincidence probability against the scaled separation time $\Delta(t_A - t_B)$ for $m = 1$ photon in input $A$ and $n$ photons in $B$ are plotted in figure 2(a). In general, as more photons interfere, the coincidence probability increases and the dip also becomes less pronounced.

The notion of relative dip can be made more precise by a useful quantity: the interference visibility

$$\mathcal{V} = \frac{P_{Co}(\tau_A - \tau_B = \pm \infty) - P_{Co}(\tau_A - \tau_B = 0)}{P_{Co}(\tau_A - \tau_B = \pm \infty)},$$

which quantifies the amount of dip of coincidence probability at maximum interference, relative to the coincidence probability when there is no interference. Since the dip is caused by photon interference, the measure of the dip is also a measure of degree of interference. So, more precisely, visibility here is the quantification of the degree of interference of the state of perfect temporal overlap (i.e. when $\tau_A = \tau_B = 0$) relative to the state of perfect non-overlap (i.e. when $\tau_A = \tau_B = \pm \infty$). Higher visibility indicates a higher degree of quantum interference. In fact, the interference visibility has been shown to be an important tool to characterize photon interference in MDI-QKD using multi-photon source like the coherent source [31, 32].

Table 1 shows the interference visibility for $n = 1$ to $n = 10$ photons at input $B$. For a fixed $m = 1$, it shows that visibility gets smaller as $n$ is larger, indicating a decrease in the degree of interference.
The probabilities are:

\[ P_{\text{det}}(n, 2 + n) = \frac{1}{2^{n+2}} \left\{ 1 + 2ne^{-\Delta(\tau_A - \tau_B)s} + \frac{n(n - 1)}{2} e^{-2\Delta(\tau_A - \tau_B)s}^2 \right\}, \]

and

\[ P_{\text{co}}(n, 2 + n) = \frac{1}{2^{n+1}} \left\{ 2^{n+1} - 1 - 2ne^{-\Delta(\tau_A - \tau_B)s} - \frac{n(n - 1)}{2} e^{-2\Delta(\tau_A - \tau_B)s}^2 \right\}. \]

The results of coincidence probability against the scaled separation time \( \Delta(\tau_A - \tau_B) \) for \( m = 2 \) photons in input \( A \) and \( n \) photons at \( B \) are plotted in figure 2(b). As more photons interfere, the coincidence probability increases. The dip also becomes less pronounced with higher photon number. Compared to \( m = 1 \), the coincidence probability is generally greater for \( m = 2 \). Interestingly, the lowest point of the dip for \( n = 1 \) coincide with that for \( n = 2 \), although the coincidence probability is generally greater for \( n = 2 \) at other points.

From the results of visibility in table 1, for a fixed \( m = 2 \), highest visibility occurs when \( n = m = 2 \). As \( n \) is increased from 2, visibility gets smaller. As compared to \( m = 1 \) for the same value of \( n \), the visibility for \( m = 2 \) is greater for \( n \geq 2 \).

In general for \( n < m \), visibility increases as \( n \) is increased, up to \( n = m \) where the visibility is maximum. Then visibility decreases again as \( n \) is increased for \( n > m \) see table 1. To summarize, for a fixed photon number \( m \), highest visibility is obtained when \( n = m \), which suggest that a higher degree of interference is attained with interference of the same photon number states.

Apart from that, there is also a general tendency that visibility and, by extension, degree of interference becomes lower with more photon numbers. This is consistent with the discussion of multi-photon interference in [12]. More multi-photons cause degradation in interference due to partial or incomplete multi-photon destructive interference, increasing coincidence probability. This is in contrast to interference of single photons with complete destructive interference, hence zero coincidence probability.

### 2.4. The general case

Here, \( m \) photons enter beam splitter input \( A \) and \( n \) photons enter \( B \). The detection probability is

\[ p_{\text{det}}(m + n, 0) = \frac{1}{2^{m + n}} \sum_{j=0}^{\min(m, n)} \binom{m}{j} \binom{n}{j} e^{-j\Delta(\tau_A - \tau_B)s} \]

where \( \binom{m}{j} \) and \( \binom{n}{j} \) are binomial coefficients. Therefore, with (8) and (9),

\[ p_{\text{co}}(m, n) = \left\{ \begin{array}{ll} 0 & \text{for } m = n = 0, \\ \frac{1}{2^{m + n}} \sum_{j=0}^{\min(m, n)} \binom{m}{j} \binom{n}{j} e^{-j\Delta(\tau_A - \tau_B)s} & \text{for } (m + n) \geq 1. \end{array} \right. \]
The results of coincidence probability for interference of the same photon number \( m = n \) at 50:50 beam splitter are shown in figure 3. With higher photon number, the coincidence probability generally displays an overall increase, the dip becomes less pronounced, and the width of the dip gets narrower.

Note that the narrowing of the dip width does not imply broadening of the incoming photons’ spectral width. There is no broadening of the spectral width as we have set the photon number states to all have identical spectral distribution in section 1. To see this further, consider a simple example of \( m = 1 \) photon at \( A \) and \( n = 2 \) photons at \( B \), at the same time arriving and interfering at 50:50 beam splitter. If the photons perfectly overlap in all degrees of freedom (the difference being only the photon number), then the output state can be easily obtained as follows,

\[
|1_A, 2_B\rangle = \frac{1}{\sqrt{2}} d^2b^2|0_A, 0_B\rangle \rightarrow \frac{(c^2 + d^2)(c^2 - d^2)^2}{4} |0_C, 0_D\rangle
= \sqrt{\frac{3}{8}} (|3_C, 0_D\rangle + |0_C, 3_D\rangle) = \sqrt{\frac{1}{8}} (|2_C, 1_D\rangle + |1_C, 2_D\rangle).
\]

With coincidence detection coming from \( |2_C, 1_D\rangle \) and \( |1_C, 2_D\rangle \), the coincidence probability from the above output state is 1/4. Now, for the photon states described in section 1, the result of the coincidence probability according to equation (13) or (18) is also precisely \( P_{\phi\phi}^{\Delta m} (\tau_A - \tau_B = 0) = 1/4 \). That the result is the same shows that our photon states are indeed perfectly overlapping, meaning that they have the same spectral distribution or spectral width \( \Delta \). If the spectral width was different, the overlap would not be perfect, and the result for coincidence probability would be different. In fact, this same method would continue to show that the result is the same for any \( m \) and \( n \).

The narrowing of the dip width is the effect of quantum interference. For a given temporal difference \( |\tau_A - \tau_B| > 0 \) of the wavefunctions, higher photon number state exhibits a lesser degree of interference, making the coincidence probability relatively higher and closer to the baseline \( (\tau_A - \tau_B = \pm \infty) \). In the study of multi-photon interference in [12], there are three physical conditions that can affect interference: spectral wave function/distribution, temporal non-overlap, and partial (incomplete) multi-photon destructive interference. Temporal non-overlap causes temporal distinguishability that diminishes the interference effect, the degree of which depends on the spectral wave function/distribution of the interfering photons. Furthermore, more multi-photon also cause degradation in interference due to partial multi-photon destructive interference, increasing coincidence probability. This is in contrast to interference of single photons with complete destructive interference, hence zero coincidence probability.

Let us discuss the notion of narrowing of the dip in equation (18). Notice that each term in the summation has a factor \( e^{-\Delta m (\tau_A - \tau_B)^2} \). This has the shape of a Gaussian function with a width of \( 1/2\Delta^2 \). So, with larger \( j \), the width is smaller and the Gaussian shape is narrower. All these terms essentially contribute in the summation, but the contribution also depends on the binomial coefficients in the term. Due to this, the leading terms are somewhere in the middle of \( j = 0 \) and \( j = n \). For example, in the case of \( m = n \), the largest term occurs at \( j = (n + 2)/2 \) when \( n \) is even; and at \( j = (n + 1)/2 \) or \( j = (n + 3)/2 \) when \( n \) is odd. As \( n \) gets larger, the shape/width of these leading terms becomes better representation of the overall width of the dip. Also, as \( n \) gets larger, the width of these leading terms decreases as the value of \( j \) that specify them becomes larger, which defines the feature of narrowing of the dip.

---

**Figure 3.** Coincidence probability against scaled separation time for interference of \( n \) photons at both \( A \) and \( B \). From bottom to top: \( n = 1, 2, 3, 5, 10, 20, \) and 50.
Thus, the narrowing of the dip is affected by spectral width $\Delta$ (which depends on the spectral function/distribution) and the temporal non-overlap $|\tau_A - \tau_B| > 0$, degrading the quality of interference through larger distinguishability, which becomes more severe with more photons. Mathematically, these effects manifest in the term $e^{-i\Delta(\tau_A - \tau_B)^2}$ in the series in equations (17) and (18), with a greater $j$ indicating more photons.

### 2.4.1. Asymmetric beam splitter

With an asymmetric beam splitter with reflection coefficient $R$ and transmission coefficient $T$, the probabilities are

$$P_{mn}^{\text{det}}(m + n, 0) = R^m T^n \sum_{j=0}^{\min(m,n)} \frac{m! n!}{(m-j)! (n-j)! (j)!^2} e^{-i\Delta(\tau_A - \tau_B)^2},$$

(19)

$$P_{mn}^{\text{det}}(0, m + n) = R^n T^m \sum_{j=0}^{\min(m,n)} \frac{m! n!}{(m-j)! (n-j)! (j)!^2} e^{-i\Delta(\tau_A - \tau_B)^2},$$

(20)

### 3. Application to the coherent state

When a coherent source is used, the state of the pulse is described by the coherent state

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle,$$

(21)

with $\alpha = |\alpha| e^{i\theta}$, where $|\alpha|$ and $\theta$ are the amplitude and phase of the coherent state. Also,

$$\langle n|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}}.$$

(22)

The photon number in a coherent state follows the Poisson distribution

$$D(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!},$$

(23)

with mean photon number of the coherent state $\langle n\rangle = |\alpha|^2$.

For security reasons in QKD applications, the pulse from the photon source is often required to be phase-randomized [33–35]. A phase-randomized coherent state is described by

$$\rho = \frac{1}{2\pi} \int_{0}^{2\pi} |\alpha| e^{i\theta} (|\alpha| e^{i\theta})^* d\theta = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{|\alpha|^n}{n!} |n\rangle \langle n| = \sum_{n=0}^{\infty} D(n) |n\rangle \langle n|,$$

(24)

which is a statistical mixture of number states. Physically, it means that the source can be effectively treated as emitting photon number state $|n\rangle$ with probability $D(n)$. Note that the phase randomization does not change the distribution statistics of the photon number.

Under this condition, consider a coherent source emitting photons to input channel $A$, and another coherent source to $B$. Let $D_A(m)$ be the probability to find $m$ photons at $A$ as given in (23). Similarly, let $D_B(n)$ be the probability to find $n$ photons at $B$. The coincidence probability is then $D_A(m) D_B(n) P_{mn}^{\text{Co}}$. The total coincidence probability is the sum of the probabilities over the photon number,

$$P_{\text{Co}} = \sum_{m,n} D_A(m) D_B(n) P_{mn}^{\text{Co}},$$

(25)

The results of coincidence probability for the coherent source against the scaled separation time $\Delta(\tau_A - \tau_B)$ are plotted in figure 4(a). For simplicity, the mean photon number at $A$ and $B$ are assumed to be equal. The analytical derivation of the total coincidence probability is given in appendix B. It is

$$P_{\text{Co}} = 1 + e^{-\langle n\rangle} - 2e^{-\langle n\rangle} I_0(\langle n\rangle e^{-\Delta(\tau_A - \tau_B)^2}),$$

(26)

where $I_0$ is the modified Bessel function of the first kind with order 0.

Similar to results observed in the previous section, generally the coincidence probability increases as the mean photon number is higher. The dip also exists and it gets less pronounced with higher mean photon number $\langle n\rangle$. The width of the dip gets narrower with higher mean photon number $\langle n\rangle$. Since coherent state is superposition of many multi-photon states, the narrowing of the dip width, discussed in previous section, is also observed in the interference of coherent states.
The interference visibility can be calculated from equations (14) and (26) and it is

\[ V(n) = \frac{2e^{-\langle n \rangle}}{1 + e^{-2\langle n \rangle} - 2e^{-\langle n \rangle}} = \frac{I_0(\langle n \rangle) - 1}{2 \sinh^2 \left( \frac{1}{2} \langle n \rangle \right)}. \]  

(27)

The results are plotted in figure 4(b). The maximum limit of visibility is \( V \to 50\% \) as \( \langle n \rangle \to 0 \). The visibility is a monotonically decreasing function of mean photon number, and \( V \to 0 \) as \( \langle n \rangle \to \infty \). However, the dip is still noticeably present for a relatively high mean photon number of \( \langle n \rangle = 50.0 \), with a visibility of 11.3%.

For comparison, the results of visibility for interference of \( n \) photons at both A and B are also shown in the figure. In general, the visibility of the coherent states interference shows an overall decrease, compared to the \( m = n \) photons interference. As shown in table 1 discussed previously, for a given \( n \), visibility is highest when \( m = n \). Since the coherent state is a superposition of many number states, there are \( m \neq n \) contributions, lowering the overall visibility.

Since the behavior of the coherent state closely resembles that of the classical coherent light, let us for a moment consider interference of classical coherent light at beam splitter. For a particular value of relative phase between interfering classical coherent light, it is possible to have constructive interference at one beam splitter output and destructive interference at the other. So only in this particular case there is no coincidence detection. However, for all the other cases, interference is not totally constructive or destructive, and therefore, coincidence detection occurs. Since we consider phase randomization, the phase-averaged coincidence detection probability will converge to unity. So the dip shown here is a purely quantum effect. With higher and higher mean photon number \( \langle n \rangle \), coincidence probability for coherent state interference is expected to approach that of the classical coherent light, which is unity.

### 4. Application to the squeezed coherent state

The squeezed coherent state can be generated from the vacuum by the application of displacement and squeeze operators. First, the displacement operator is defined as

\[ \hat{D}(\alpha) = \exp(\alpha \hat{A}^\dagger - \alpha^\ast \hat{A}). \]  

(28)

When applied to the vacuum, it generates the coherent state, |\( \alpha \rangle = \hat{D}(\alpha) |0 \rangle \). As in the previous section, \( \alpha = |\alpha| e^{i\phi} \). Next, the squeeze operator is defined as

\[ \hat{S}(\zeta) = \exp \left\{ \frac{1}{2} (\zeta \hat{A}^\dagger \hat{A} - \zeta^\dagger \hat{A}^\dagger \hat{A}) \right\}, \quad \text{with} \quad \zeta = r e^{i\phi}, \]  

(29)

where \( r \) is the squeezing parameter. The squeezed coherent state can be generated from the vacuum by

\[ |\alpha, \zeta \rangle = \hat{D}(\alpha) \hat{S}(\zeta) |0 \rangle, \]  

(30)

with [36,37]

\[ |n|\alpha, \zeta \rangle = \frac{1}{\sqrt{n! \cosh r}} \left[ \frac{1}{2} e^{i\phi} \tanh r \right]^n \exp \left\{ - \frac{1}{2} |\alpha|^2 + \alpha^* e^{i\phi} \tanh r \right\} H_n \left( \frac{\alpha + \alpha^* e^{i\phi} \tanh r}{\sqrt{2 e^{i\phi} \tanh r}} \right), \]  

(31)

where \( H_n \) is the Hermite polynomial with degree \( n \).
Nevertheless, the total coincidence probability for any value of \(n\) with mean photon number \(\langle n \rangle = 1.00\) at both beam splitters. For the squeezed coherent states, \(A\) and \(B\) have the same squeezing parameter \(r\). The solid curve shows interference of coherent states, while the dashed curves show interference of squeezed coherent states for \(r = 0.30\) and \(r = 0.75\).

Figure 5. Coincidence probability of coherent states interference and amplitude-squeezed coherent states interference at 50:50 beam splitter. For all the cases, the mean photon number is \(\langle n \rangle = 1.00\) at \(A\) and at \(B\). For the squeezed coherent states, \(A\) and \(B\) have the same squeezing parameter \(r\). The solid curve shows interference of coherent states, while the dashed curves show interference of squeezed coherent states for \(r = 0.30\) and \(r = 0.75\).

We are interested in the amplitude-squeezed states with sub-Poissonian distribution. This can be achieved by setting \(\phi = 2\theta\) [37]. In this specific case,

\[
\langle n|\alpha, r \rangle = \frac{e^{i\phi}}{\sqrt{n!\cosh r}} (\tanh r \, \frac{\alpha}{2})^{n} \exp \left[ -\frac{|\alpha|^{2}}{2} (1 + \tanh r) \right] H_{n} \left( |\alpha| \frac{1 + \tanh r}{\sqrt{2 \tanh r}} \right).
\]

(32)

The photon number distribution is then

\[
D(n) = |\langle n|\alpha, r \rangle |^{2} = \frac{1}{n!\cosh r} (\tanh r \, \frac{\alpha}{2})^{n} \exp \left[ -\frac{|\alpha|^{2}}{2} (1 + \tanh r) \right] H_{n} \left( |\alpha| \frac{1 + \tanh r}{\sqrt{2 \tanh r}} \right)^{2},
\]

(33)

with mean photon number \(\langle n \rangle = |\alpha|^{2} + \sinh^{2} r\).

Similar to the previous section, here we consider phase-randomized squeezed coherent state. In this case phase randomization also yields the mixed state

\[\rho = \sum_{n=0}^{\infty} D(n)|n\rangle \langle n|\]

with photon number distribution \(D(n)\) given in (33).

Unlike the coincidence probability for coherent state, the general analytical expression of coincidence probability for the amplitude-squeezed coherent state can only be obtained for \(|\tau_A - \tau_B| = \infty\) (see appendix B for derivation). It is

\[
P_{\text{total}}^{\text{Co}}(\tau_A - \tau_B = \pm \infty) = 1 + \frac{\exp \left[ -2 |\alpha|^{2} (1 + \tanh r) \right]}{\cosh^{2} r} \frac{8 \exp \left[ -2 |\alpha|^{2} \frac{1 + \tanh r}{2 + \tanh r} \right]}{1 + 3 \cosh^{2} r}.
\]

(34)

Nevertheless, the total coincidence probability for any value of \(\tau_A - \tau_B\) can be numerically calculated using (25) very straightforwardly. In the computation, the summation is taken up to a certain photon number so that it covers \(1 - 10^{6}\) of the whole distribution. When checked against the analytical solution in (34), the numerical calculation gives a very accurate result for \(|\tau_A - \tau_B| = \infty\).

Figure 5 shows the coincidence probabilities of coherent states with mean photon number \(\langle n \rangle = 1.00\) and the amplitude-squeezed coherent states of the same mean photon number \(\langle n \rangle = 1.00\), with two choices of squeezing parameter, \(r = 0.30\) and \(r = 0.75\). For simplicity, the mean photon number and squeezing parameters at \(A\) and \(B\) are set to be equal. Visibility is also calculated for each of the instances. For interference of coherent states, \(V_{\text{Coherent}} = 49.0\%\). As for the squeezed coherent states, a choice of squeezing parameter \(r = 0.30\) yields a higher visibility of \(V_{r=0.30} = 60.1\%\), while a choice of \(r = 0.75\) yields a lower visibility of \(V_{r=0.75} = 38.4\%\).

Indeed, the results of visibility exhibited in figure 6(a) shows that as squeezing parameter is increased, visibility also increases to some point only, but then decreases afterwards. The photon number distribution for \(\langle n \rangle = 1.00\) for the coherent state, squeezed coherent states with maximum visibility and with maximum squeezing are plotted in figure 6(b). For fixed \(\langle n \rangle\), as squeezing parameter is increased, initially the distribution becomes sub-Poissonian, as can be seen from the decrease in standard deviation \(\sigma\) in figure 6(a). This means the distribution becomes narrower or less spread out (see figure 6(b)), which reduces the \(m \approx n\) in the distribution.
As discussed in the previous section, for superposition of number states, the $m = n$ photons interference contributions lower the overall visibility. Therefore, qualitatively speaking, if the distribution now is less spread out, the contributions from $m \neq n$ photons interference decrease, and this causes the visibility to increase. But at some point, increasing the squeezing parameter further causes the distribution to become more spread out again, decreasing visibility. At maximum squeezing, $|\alpha| = 0$ and $r = \sinh^{-1}((n)^{1/2})$ (also known as squeezed vacuum), the distribution has actually become super-Poissonian.

The value of visibility itself is not perfectly correlated with the standard deviation, as seen in figure 6(a). This is because the exact contributions from $m = n$ and $m \neq n$ photons interference to the visibility depend on the individual probability of the photon number itself and the weight of each of the $m = n$ and $m \neq n$ components towards visibility, which are factors that are not included in the standard deviation as a measure of the spread.

5. Application of the squeezed coherent state to MDI-QKD

In MDI-QKD employing BB84 protocol [38], Alice and Bob—two parties who wish to share secret keys—prepare photons randomly in the $Z$-basis states $|0\rangle$ and $|1\rangle$ or in the $X$-basis states $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. In polarization coding, $|0\rangle$ and $|1\rangle$ represent polarization states of the photons (horizontal and vertical) [24]. In the time-bin coding, $|0\rangle$ and $|1\rangle$ represent the early and late temporal modes or time-bins [26]. The following discussion will be in the context of time-bin coding MDI-QKD, but it can be similarly applied to the polarization coding as well.

After the state preparation, Alice and Bob send their photons to a third party, Charlie. Charlie then performs quantum interference of the photons by means of a 50:50 beam splitter as depicted in figure 1, where input channel $A$ represents Alice’s channel and input channel $B$ represents Bob’s. An accepted detection event is one in which the two detectors at $C$ and $D$ click and detect photons at different time-bins (see appendix D.1 for the reason why this detection event is applied). Charlie announces such detection events to Alice and Bob. They then publicly announce their respective basis and only keep the bits for which they choose the same basis. Ideally, in the end Alice and Bob possess anti-correlated keys. Finally either Alice or Bob flips their bits in order for them to share the same key. In this scheme, the accepted detection event only indicates that Alice’s and Bob’s states are anti-correlated, and it does not reveal what the individual states are.

If single photon sources are used, when Alice and Bob send identical photon states, the photons will only exit at the same beam splitter output due to HOM effect. This indicates no accepted detection event, since both detectors have to click to be accepted. An error is caused when Alice and Bob prepare identical states, yet Charlie’s measurement indicates an accepted detection event. This may be caused by multi-photon detection. However, multi-photon detection does not cause error in the $Z$-basis, because even if both detectors may click, they will only click in the same time-bin. However, in the $X$-basis, multi-photon detection may cause error.

The calculation of error rate follows the one presented in [26]. Here, we focus on error rate caused by multi-photon detection in the $X$-basis assuming ideal devices. The detailed calculation of the error rate is given in

\[4\] For polarization coding, a polarization beam splitter is required at each output to project the photons to horizontal or vertical polarization.
appendix C. It includes only up to three photons from Alice and Bob combined, since for small mean photon number $n \lesssim 0.5$, probabilities of higher photon number do not contribute significantly. In this approximation, the probability of erroneous detection (when Alice and Bob prepare identical states)

$$P_{\text{error}} = \frac{1}{4} \left[ D_A(0) D_B(2) + D_A(2) D_B(0) \right] + \frac{3}{16} \left[ D_A(0) D_B(3) + D_A(3) D_B(0) \right]$$

$$+ \frac{1}{16} \left[ D_A(1) D_B(2) + D_A(2) D_B(1) \right].$$

(35)

The probability of correct detection (when Alice and Bob prepare states that are orthogonal to each other) is

$$P_{\text{correct}} = \frac{1}{4} \left[ D_A(0) D_B(2) + D_A(2) D_B(0) \right] + \frac{1}{2} D_A(1) D_B(1)$$

$$+ \frac{3}{16} \left[ D_A(0) D_B(3) + D_A(3) D_B(0) \right] + \frac{9}{16} \left[ D_A(1) D_B(2) + D_A(2) D_B(1) \right].$$

(36)

The error rate is then given by

$$Q = \frac{P_{\text{error}}}{P_{\text{correct}} + P_{\text{error}}}.$$  

(37)

For the amplitude-squeezed coherent state, the squeezing parameter $r$ is optimized for each mean photon number to obtain optimal error rate. In other words, we find the squeezing parameter that minimizes the error rate. So in the following, optimized squeezing parameter refers to the squeezing parameter that gives the lowest error rate. For comparison, error rates for coherent state and optimal error rates for amplitude-squeezed coherent state in the $X$-basis for mean photon number $\langle n \rangle = 0.05$ to $\langle n \rangle = 0.50$ are illustrated in figure 7. For simplicity, the mean photon number and squeezing parameter of Alice and Bob are assumed to be equal. The optimized squeezing parameters are given in table 2.

For the values of mean photon number used ($\langle n \rangle \lesssim 0.5$), the amplitude-squeezed coherent state has optimized error rates of around or less than 0.1, while for the coherent state the error rates are $Q > 0.2$. Therefore, we see significant reduction in the error rates in the $X$-basis. Additionally, as expected, the multi-photon (and vacuum) probabilities are reduced, while the single photon probability is increased (see figure 8, right). Since multi-photon in the pulse can be exploited by an eavesdropper via PNS attack, reduced multi-photon probability means opportunity for PNS attack is decreased. Both of these facts—reduced error rate and reduced impact of PNS attack—contribute towards improvement of key generation rates and transmission distances.

Figure 8 shows the coincidence probabilities (left) and photon number distribution (right) of the amplitude-squeezed coherent states with error-optimized squeezing parameter for mean photon number $\langle n \rangle = 0.10$, 0.25, and 0.50. For comparison, the results for the coherent state with the same mean photon number $\langle n \rangle$ and coherent state with the same coincidence probability at $|\tau_A - \tau_B| = \infty$ are shown as well. As previously mentioned for the squeezed coherent states, the multi-photon and vacuum probabilities are reduced while the single photon probability is increased, as compared to the coherent states. Additionally, the visibility for the squeezed coherent states is higher compared to the coherent states, implying that error rate is reduced with a higher degree of quantum interference.
5.1. Secret key rate

To illustrate the improvement of the amplitude-squeezed coherent state over the coherent state, we simulate the secret key rate of a time-bin BB84 MDI-QKD system based on the realistic model presented in [26], employing the three intensity decoy states protocol [25]. The model includes experimental imperfections, such as detector’s

![Figure 8](image-url)

**Figure 8.** (Left) Coincidence probabilities and (Right) photon number distribution of the amplitude-squeezed coherent states with error-optimized squeezing parameter for mean photon number \(n = 0.10, 0.25, \text{ and } 0.50\), compared to coherent state with the same mean photon number \(|n|\), and coherent state with the same coincidence probability at \(\tau_a - \tau_b = \infty\).

<table>
<thead>
<tr>
<th>(n)</th>
<th>Q coherent (%)</th>
<th>Q squeezed (%)</th>
<th>Optimized (r)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.05</td>
<td>24.7</td>
<td>2.2</td>
<td>0.0488</td>
</tr>
<tr>
<td>0.10</td>
<td>24.4</td>
<td>4.0</td>
<td>0.0953</td>
</tr>
<tr>
<td>0.15</td>
<td>24.2</td>
<td>5.5</td>
<td>0.1398</td>
</tr>
<tr>
<td>0.20</td>
<td>23.9</td>
<td>6.7</td>
<td>0.1826</td>
</tr>
<tr>
<td>0.25</td>
<td>23.7</td>
<td>7.6</td>
<td>0.2240</td>
</tr>
<tr>
<td>0.30</td>
<td>23.5</td>
<td>8.4</td>
<td>0.2640</td>
</tr>
<tr>
<td>0.35</td>
<td>23.3</td>
<td>9.0</td>
<td>0.3027</td>
</tr>
<tr>
<td>0.40</td>
<td>23.1</td>
<td>9.5</td>
<td>0.3402</td>
</tr>
<tr>
<td>0.45</td>
<td>22.9</td>
<td>9.9</td>
<td>0.3763</td>
</tr>
<tr>
<td>0.50</td>
<td>22.7</td>
<td>10.3</td>
<td>0.4111</td>
</tr>
</tbody>
</table>

5.1. Secret key rate

Table 2. Calculated error rates in the X-basis and optimized squeezing parameters for various mean photon number.

Optimized squeezing parameter refers to squeezing parameter that gives the lowest error rate.
and $m \mathbb{Z}$ here represent the early and late temporal modes. The superscript indicates whether the

$\eta = \frac{P_d}{P_{th}}$, dark counts (with probability $P_d$ per time-bin), and imperfect state preparation. For
the state preparation, Alice and Bob prepare their qubit states in the form of

$$|\psi\rangle = \frac{1}{\sqrt{1 + 2b^{X,Z}}}(\sqrt{m^{X,Z} + b^{X,Z}}|0\rangle + e^{i\phi^{X,Z}}\sqrt{1 - m^{X,Z} + b^{X,Z}}|1\rangle).$$

(38)

As before, $|0\rangle$ and $|1\rangle$ here represent the early and late temporal modes. The superscript indicates whether
the state is in the $X$-basis or $Z$-basis. The parameter $b^{X,Z}$ is included to account for the transmission of light by
an imperfect intensity modulator. As example, in perfect $Z$-basis, $m^{Z} = 0$, and the relative phase $\phi^{Z}$ is
irrelevant since it will not affect the measurement. In perfect $X$-basis, $m^{X} = 1/2$, $\phi^{X} \in [0, \pi]$, and $b^{X} = 0$.

Table 3 lists the aforementioned parameters, which mostly follow the experimental characterization in [26].

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\eta$</td>
<td>40%</td>
</tr>
<tr>
<td>$P_d$</td>
<td>$5 \times 10^{-6}$</td>
</tr>
</tbody>
</table>

Table 3. List of parameters relating to state preparation and detector properties.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Alice’s value</th>
<th>Bob’s value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b^{X=0} = b^{X=1}$</td>
<td>$7.12 \times 10^{-3}$</td>
<td>$1.14 \times 10^{-3}$</td>
</tr>
<tr>
<td>$b^{X=0} = b^{X=1}$</td>
<td>$5.45 \times 10^{-3}$</td>
<td>$1.14 \times 10^{-3}$</td>
</tr>
<tr>
<td>$m^{Z} = 0$</td>
<td>$0.9944$</td>
<td>$0.9967$</td>
</tr>
<tr>
<td>$m^{Z} = 1$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$m^{X=0} = m^{X=1}$</td>
<td>$0.4972$</td>
<td>$0.5018$</td>
</tr>
<tr>
<td>$\phi^{X=0} = \phi^{X=1} = \phi^{X=1}$ (rad)</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$\phi^{X=0}$ (rad)</td>
<td>$\pi + 0.075$</td>
<td>$\pi - 0.075$</td>
</tr>
</tbody>
</table>

limited efficiency ($\eta$), dark counts (with probability $P_d$ per time-bin), and imperfect state preparation. For
the state preparation, Alice and Bob prepare their qubit states in the form of

$$|\psi\rangle = \frac{1}{\sqrt{1 + 2b^{X,Z}}}(\sqrt{m^{X,Z} + b^{X,Z}}|0\rangle + e^{i\phi^{X,Z}}\sqrt{1 - m^{X,Z} + b^{X,Z}}|1\rangle).$$

(38)

As before, $|0\rangle$ and $|1\rangle$ here represent the early and late temporal modes. The superscript indicates whether
the state is in the $X$-basis or $Z$-basis. The parameter $b^{X,Z}$ is included to account for the transmission of light by
an imperfect intensity modulator. As example, in perfect $Z$-basis, $m^{Z} = 0$, and the relative phase $\phi^{Z}$ is
irrelevant since it will not affect the measurement. In perfect $X$-basis, $m^{X} = 1/2$, $\phi^{X} \in [0, \pi]$, and $b^{X} = 0$.

Table 3 lists the aforementioned parameters, which mostly follow the experimental characterization in [26].

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\eta$</td>
<td>40%</td>
</tr>
<tr>
<td>$P_d$</td>
<td>$5 \times 10^{-6}$</td>
</tr>
</tbody>
</table>

Table 3. List of parameters relating to state preparation and detector properties.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Alice’s value</th>
<th>Bob’s value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b^{X=0}$</td>
<td>$7.12 \times 10^{-3}$</td>
<td>$1.14 \times 10^{-3}$</td>
</tr>
<tr>
<td>$b^{X=0}$</td>
<td>$5.45 \times 10^{-3}$</td>
<td>$1.14 \times 10^{-3}$</td>
</tr>
<tr>
<td>$m^{Z} = 0$</td>
<td>$0.9944$</td>
<td>$0.9967$</td>
</tr>
<tr>
<td>$m^{Z} = 1$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$m^{X=0}$</td>
<td>$0.4972$</td>
<td>$0.5018$</td>
</tr>
<tr>
<td>$\phi^{X=0} = \phi^{X=1} = \phi^{X=1}$ (rad)</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$\phi^{X=0}$ (rad)</td>
<td>$\pi + 0.075$</td>
<td>$\pi - 0.075$</td>
</tr>
</tbody>
</table>

The model also takes into account the fact that in practice, Alice’s and Bob’s pulses may not perfectly overlap
in all degrees of freedom, which results in imperfect interference at the beam splitter, and in turn reduced
visibility. In [26], it is experimentally characterized and approximately described by a visibility factor of 0.94. So
for example, experimental visibility of single photons interference is 94% instead of the theoretical 100%,
and the maximum experimental visibility of the weak coherent states interference is 47% instead of the theoretical
maximum limit of 50%. In addition, the optical channel loss is assumed to be 0.2 dB km$^{-1}$.

Under the three intensity decoy states protocol, three different intensities of light are used: signal, decoy,
and vacuum states. In the simulation, the mean photon number of the signal and decoy states are taken to be
$(n)_s = 0.5$ and $(n)_d = 0.1$, respectively. For the vacuum state, no light pulse is sent, so mean photon number
is zero. For the squeezed coherent state, the squeezing parameters for the signal and decoy states are taken to be
$\eta_s = 0.4111$ (from table 2) and $\eta_d = 0.0684$ (see appendix D.2 for why this value is chosen). We assume Alice
and Bob use the same parameters for their sources. The secret key rate for BB84 MDI-QKD protocol [24, 25] is
given by

$$K = G_{11}^{Z} (1 - h(Q_{11}^{Z})) = G_{11}^{Z} f_{EC} h(Q_{11}^{Z}),$$

(39)

where $h(Q)$ is the binary entropy of $Q_{11}^{Z}$, $f_{EC}$ is the error correction efficiency which is realistically taken to be 1.14
[39], $Q_{11}^{Z}$ is the error rate in the $Z$-basis when Alice and Bob send single photons in the signal states, while $Q_{11}^{Z}$ is
the overall error rate in the $Z$-basis when Alice and Bob send signal states, and $G_{11}^{Z}$ is the gain in the $Z$-basis when
Alice and Bob send single photons in the signal states, while $G_{11}^{Z}$ is the overall gain when Alice and Bob send signal
states. Gain refers to the number of exchanged bits (from the accepted detection events) between Alice and Bob
per pulse sent in each time step. $G_{11}^{Z}$ and $Q_{11}^{Z}$ can be directly measured in experiment, while $G_{11}^{Z}$ and $Q_{11}^{Z}$
cannot be directly measured and have to be estimated. The decay states protocol provides the lower bound of $G_{11}^{Z}$
and upper bound of $Q_{11}^{Z}$.

The results are presented in figure 9, assuming Alice’s and Bob’s transmission distances to Charlie are the same,
for simplicity. Secret key rates are also calculated with the perfect/infinite decoy states, in which $G_{11}^{Z}$ and $Q_{11}^{Z}$
can be determined exactly. The results show that, with the three intensity decoy states, the amplitude-squeezed coherent
state is capable of achieving almost twice the total distance of the coherent state. Furthermore, the performance of
squeezed coherent states with three intensity decoy states is comparable to that of the coherent states with infinite
decoy states.
6. Conclusion

We conclude this article by first pointing out the novelty of our results. We comment that multi-photon at the same time arriving and interfering at a single beam splitter, assuming perfect overlap is, in fact, quite straightforward to analyze, even by hand. This, for example, is shown in chapter 5.7 of the textbook *Quantum Optics* by Agarwal [40]. With this assumption, the spectral distribution of the photons is ignored. Our work (in section 2), however, takes into account the Gaussian spectral distribution of the photons. With this consideration, the two photon waves need not arrive at beam splitter at exactly the same time. So, in this sense, our work is more general; the temporal overlap of the interfering photons can be adjusted and the coincidence probability for any temporal difference/separation time can be obtained. The perfect overlap mentioned previously is just a special case of zero temporal difference. Therefore, coincidence probability as a function of temporal difference can be determined exactly, without the need to resort to curve fitting, which can be useful in experiments. Moreover, our analysis takes into account any photon number $m$ at one input and $n$ at the other, instead of the same number of photons $N$ at both inputs of the beam splitter [40].

Existing works in literature by Wang et al [31] and Moschandreou et al [32] study experimental measurement of visibility of HOM interference using phase-randomized coherent state, with real device imperfections. Our work, however, is focused more on the coincidence probability of photons states with Gaussian spectral distribution, taking into account the temporal separation of the interfering photon states. The visibility only comes later as a quantifier of the relative dip at maximum interference/maximum temporal overlap. Furthermore, the application is not just limited to the coherent state, but also the phase-randomized amplitude-squeezed coherent state and the multi-photon states. Another difference is that we also include the application to MDI-QKD, specifically the optimization of the error rates and secret key rates using the amplitude-squeezed coherent state. Although we do not include device imperfections in the study of coincidence probability, they are taken into account in the time-bin MDI-QKD model [26] employed here.

In summary, we have applied the quantum theory of optical coherence to obtain the coincidence probability for general multi-photon interference for the original HOM interferometer setup. Subsequently, the results are directly applied to interference of phase-randomized coherent states and amplitude-squeezed coherent states with sub-Poissonian distribution. It is shown that the interference visibility for the squeezed coherent state could be increased by increasing the squeezing parameter, but only up to a certain point, after which, visibility decreases with increasing squeezing parameter. We expect that the results can also be applied for other states of light, not just limited to the coherent states and the squeezed coherent states.

We have also shown that the implementation of amplitude-squeezed coherent state in BB84 MDI-QKD results in significantly reduced error rate in the $X$-basis as compared to the coherent state. We have obtained the optimized squeezing parameter for the respective mean photon number that optimally reduced the error rate in the $X$-basis. Even if there is no error rate improvements in the $Z$-basis, application of the squeezed coherent state still has the advantage of reducing the multi-photon probabilities, making it more secure against PNS attack. We also note that, although the results are calculated in the absence of device imperfections, the calculations of error rate for the $X$-basis for the weak coherent state are close to ones obtained experimentally in [26] with real device imperfections. With currently available state-of-the-art device performance (see [27]), the results would be even

![Secret key rates against total transmission distance between Alice and Bob. For simplicity, Alice's and Bob's transmission distances to Charlie are assumed to be the same. Mean photon number of the signal state is $\langle n \rangle = 0.5$ and the decoy state is $\langle n \rangle = 0.1$.](image-url)
more representative of the actual error rates. Therefore, we expect that the results for the amplitude-squeezed coherent state obtained here represent a potential improvement over the weak coherent state.

Finally, we have employed a realistic time-bin MDI-QKD model with the three intensity decoy state protocol, available in literature, to simulate the secret key rate. It is found that the amplitude-squeezed coherent state is capable of achieving almost twice the distance of the coherent state.

Appendix A. Derivation of coincidence probability for multi-photons

The theories of photon detection and beam splitter form the basis on which coincidence probability is calculated. So, they are discussed first. Afterwards, some derivations for one photon in one input channel are presented for illustration purpose. This is to ease the reader into the calculation, and also to introduce subtleties in the derivations. Finally, the derivation for the general photon number case will be given. The setup is such that the delay times at A and B are \( \tau_A \) and \( \tau_B \), and the detectors are placed immediately after the beam splitter output channels C and D.

A.1. Theory of photon detection

Photon detection is described in Glauber’s quantum theory of coherence [41]. In the interferometer, the photons propagate in a straight line (one dimension) towards the beam splitter. The one-dimensional electric field operators are defined as

\[
\hat{E}^+(t) = i \int d\omega \sqrt{\frac{\hbar \omega}{4\pi c\epsilon_0}} \exp(-i\omega t) \hat{a}(\omega) = i \int d\omega \mathcal{E}_\omega \exp(-i\omega t) \hat{a}(\omega),
\]

where \( x = 0 \) has been set at the beam splitter for convenience. Next, the probability of \( N \)-photon joint measurement is proportional to the correlation function

\[
G_{\phi} = \langle \hat{E}^{-\dagger}(t_1) \cdots \hat{E}^{-\dagger}(t_n) \hat{E}^{+(t_1)} \cdots \hat{E}^{+(t_n)} \rangle.
\]

For illustration purpose, consider the case of \( N \)-photon state \( |N\rangle_\phi \) in (4) going straight to a detector (without beam splitter). Let

\[
|\varphi\rangle = \hat{E}^{-\dagger}(t_N) \cdots \hat{E}^{-\dagger}(t_1) |N\rangle_\phi = \hat{E}^{-\dagger}(t_N) \cdots \hat{E}^{-\dagger}(t_1) \frac{1}{\sqrt{N!}} \hat{A}(\phi)^N |0\rangle = \frac{1}{\sqrt{N!}} \int d\omega_1 d\omega_2 \cdots d\omega_N \left( \prod_{j=1}^{N} \mathcal{E}_{\omega_j}(\phi(\omega_j)) \right) \sum_P \left( -i \sum_{j=1}^{N} \omega_{p(j)} t_{p(j)} \right) |0\rangle.
\]

Under the assumption that the standard deviation \( \Delta \) in (6) is very narrow [1, 36], the quantity \( \mathcal{E}_{\omega} \) varies only slightly over \( \Delta \). Therefore it is treated as approximately a constant \( \mathcal{E}_{\omega} \approx \mathcal{E}_{\omega_0} \) and can be brought out of the integration. So,

\[
|\varphi\rangle = \frac{\mathcal{E}_{\omega_0}^N}{\sqrt{N!}} \int d\omega_1 d\omega_2 \cdots d\omega_N \left( \prod_{j=1}^{N} \phi(\omega_j) \right) N! \exp(-i \sum_{j=1}^{N} \omega_j t_j) \left| 0 \right\rangle = \mathcal{E}_{\omega_0}^N (2\sqrt{2\pi} \Delta)^N \sqrt{N!} \exp\left( -\frac{1}{2} \sum_{j=1}^{N} (\omega_0 t_j + \Delta^2 t_j^2) \right) |0\rangle.
\]

Therefore,

\[
\Gamma(t_1, t_2, \ldots, t_N) = \langle N| \hat{E}^{-\dagger}(t_1) \cdots \hat{E}^{-\dagger}(t_N) \hat{E}^{+(t_1)} \cdots \hat{E}^{+(t_n)} |N\rangle_\phi = \langle \varphi |\varphi\rangle = \mathcal{E}_{\omega_0}^{2N} (2\sqrt{2\pi} \Delta)^N N! \exp\left(-2\Delta^2 \sum_{j=1}^{N} t_j^2 \right).
\]
The probability of detection $P^\text{det}_N$ will then be proportional to the integration of $\Gamma(t_1, t_2, \ldots, t_N)$ over $t_1, \ldots, t_N$. Therefore,

$$P^\text{det}_N \propto \int \cdots \int \Gamma(t_1, t_2, \ldots, t_N)$$

$$\propto \mathcal{E}_{\omega_0}^{2N}(2\sqrt{2\pi}\Delta)^N N! \int \cdots \int \exp \left( -2\Delta^2 \sum_{j=1}^{N} t_j^2 \right)$$

$$\propto (2\pi \mathcal{E}_{\omega_0}^2)^N N!.$$  \hspace{1cm} (46)

Obviously, the probability of detection should be equal to unity, since the $N$-photon state just goes straight to the detector. Therefore, by applying the appropriate normalization factor, the expression for the probability is given by

$$P^\text{det}_N = \frac{1}{(2\pi \mathcal{E}_{\omega_0}^2)^N N!} \int \cdots \int \Gamma(t_1, t_2, \ldots, t_N), \quad \text{where} \quad \mathcal{E}_{\omega_0} = \sqrt{\frac{\hbar \omega_0}{4\pi \epsilon_0 c}}.$$  \hspace{1cm} (47)

### A.2. Beam splitter description

A beam splitter has two input channels, denoted by $A$ and $B$, and two output channels (each directed to a detector), denoted by $C$ and $D$ (see figure 1). The channels are populated by the creation operators $\hat{a}^\dagger$, $\hat{b}^\dagger$, $\hat{c}^\dagger$, and $\hat{d}^\dagger$ corresponding to the channels, and they obey the following linear transformation:

$$\begin{pmatrix} \hat{a}^\dagger \\ \hat{b}^\dagger \end{pmatrix} \rightarrow \begin{pmatrix} \sqrt{R} e^{i\theta} \\ \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{c}^\dagger \\ \hat{d}^\dagger \end{pmatrix},$$  \hspace{1cm} (48)

where $R$ and $T$ are the reflection and transmission coefficients of the beam splitter, and $\theta \in [0, 2\pi]$ is the phase shift associated with beam splitter reflection. The phase $\theta$ does not have direct physical significance to the observed probabilities. Therefore, $\theta = 0$ will be chosen for convenience. Furthermore, here a 50:50 lossless beam splitter will be considered, so $R = T = 50\%$.

Following the operators relation in (48) for 50:50 lossless beam splitter and $\theta = 0$, using the definition in (40) and (41) the electric field operators at the beam splitter follow the relations

$$\hat{E}_C^{(+)}(t) = \frac{1}{\sqrt{2}} [\hat{E}_A^{(+)}(t) + \hat{E}_B^{(+)}(t)],$$

$$\hat{E}_D^{(+)}(t) = \frac{1}{\sqrt{2}} [\hat{E}_A^{(+)}(t) - \hat{E}_B^{(+)}(t)].$$  \hspace{1cm} (49) \hspace{1cm} (50)

### A.3. One photon in input channel $A$

Here, the derivation details are provided for illustration purpose.

#### A.3.1. One photon in input channel $B$. This is the original HOM interference discussed in [1]. Consider photon detection at output channel $C$; similar to (43) as the starting point,

$$|\varphi\rangle = \hat{E}_C^{(+)}(t_2)\hat{E}_C^{(+)}(t_1)|1_A, 0_B\rangle$$

$$= \frac{1}{2} [\hat{E}_A^{(+)}(t_2) + \hat{E}_B^{(+)}(t_2)]|1_A, 0_B\rangle\hat{A}(\phi_{t_1})\hat{B}(\phi_{t_2})|0\rangle$$

$$= \frac{1}{2} [\hat{E}_A^{(+)}(t_2)\hat{E}_B^{(+)}(t_1) + \hat{E}_A^{(+)}(t_2)\hat{E}_B^{(+)}(t_1)]\hat{A}(\phi_{t_1})\hat{B}(\phi_{t_2})|0\rangle$$

$$= \frac{\mathcal{E}_{\omega_0}^2}{2} \int d\omega_1 d\omega_2 \phi(\omega_1)\phi(\omega_2) \left[ e^{i\omega_1(t_2-t_1)} e^{i\omega_2(t_2-t_1)} + e^{i\omega_2(t_2-t_1)} e^{i\omega_1(t_2-t_1)} \right]|0\rangle$$

$$= \sqrt{2\pi} \Delta_{\omega}^{\pm} e^{i\omega_1(t_2-t_1)} \left[ e^{-\Delta^2[(t_1-t_2)^2 + (t_2-t_1)^2]} + e^{-\Delta^2[(t_1-t_2)^2 + (t_2-t_1)^2]} \right]|0\rangle.$$  \hspace{1cm} (51)

Then,

$$\Gamma_C(t_1, t_2) = \langle \varphi | \varphi \rangle$$

$$= 2\pi \Delta_{\omega}^{\pm} \left[ e^{-\Delta^2[(t_1-t_2)^2 + (t_2-t_1)^2]} + e^{-\Delta^2[(t_1-t_2)^2 + (t_2-t_1)^2]} \right]$$

$$+ 2e^{-\Delta^2[(t_1-t_2)^2 + (t_2-t_1)^2] + (t_1-t_2)^2 + (t_2-t_1)^2}.$$  \hspace{1cm} (52)
Continuing with (47),
\[
P_{\text{det}}^{1,1}(2, 0) = \frac{1}{(2\pi \Delta^2)^{3/2}} \int \mathrm{d}t_1 \mathrm{d}t_2 \Gamma(t_1, t_2)
\]
\[
= \frac{\Delta^2}{4\pi} \left\{ \frac{\pi}{\Delta^2} + 2 \int \mathrm{d}t_1 \mathrm{d}t_2 e^{-\Delta^2[(\gamma_a - h)^2 + (\gamma_b - h)^2 + (\gamma_a - \gamma_b)^2]} \right\}
\]
\[
= \frac{\Delta^2}{4\pi} \left\{ \frac{\pi}{\Delta^2} + 2 \int \mathrm{d}t_1 \mathrm{d}t_2 e^{-\Delta^2\left[\frac{1}{2}((\gamma_a - h)^2 + \frac{(\gamma_a - \gamma_b)^2}{1})\right]} \right\}
\]
\[
= \frac{\Delta^2}{4\pi} \left\{ \frac{\pi}{\Delta^2} + \frac{\pi}{\Delta^2} e^{-\Delta^2(\gamma - \gamma_a)^2} \right\} = \frac{1}{4} \{1 + e^{-\Delta^2(\gamma - \gamma_a)^2}\}. \tag{53}
\]

Combining this with (8) and (9) gives
\[
P_{1,1}^\text{Co} = \frac{1}{2} \{1 - e^{-\Delta^2(\gamma - \gamma_a)^2}\}, \tag{54}
\]
which is precisely the HOM dip equation given in [1].

### A.3.2. Two photons in input channel B

Next, \(P_{1,2}^\text{Co}\) (which is equal to \(P_{2,1}^\text{Co}\)) will be calculated. The steps are similar to the above. Starting with \(|\varphi\rangle = \hat{E}_C^{(+)}(t_1)\hat{E}_C^{(+)}(t_2)\hat{E}_C^{(+)}(h)\rangle 1, 2\alpha\)
\[
= \frac{1}{4}\left\{ \hat{E}_A^{(+)}(t_1) + \hat{E}_B^{(+)}(t_2)\right\}\left\{ \hat{E}_A^{(+)}(t_2) + \hat{E}_B^{(+)}(t_2)\right\}\hat{A}(\phi_{\alpha}\hat{y}\hat{B}(\phi_{\alpha})^2\rangle 0
\]
\[
+ \hat{E}_A^{(+)}(t_1)\hat{E}_B^{(+)}(t_2)\hat{E}_A^{(+)}(t_2)\hat{E}_B^{(+)}(t_2)\rangle 0 \hat{A}(\phi_{\alpha}\hat{y}\hat{B}(\phi_{\alpha})^2\rangle 0
\]
\[
= \frac{\Delta^3}{4} \int \mathrm{d}\omega_1 \omega_2 \omega_3 \phi(\omega_1)\phi(\omega_2)\phi(\omega_3) 2!\{e^{i\omega_1(\gamma_a - h)}e^{i\omega_2(\gamma_b - h)}e^{i\omega_3(\gamma - (\gamma_a - \gamma_b))\rangle 0
\]
\[
+ e^{i\omega_1(\gamma_a - h)}e^{i\omega_2(\gamma_b - h)}e^{i\omega_3(\gamma_a - \gamma_b)}\rangle 0\}
\]
\[
+ e^{-\Delta^2(\gamma_a - h)^2 + (\gamma - \gamma_a)^2 + (\gamma_b - h)^2}) + e^{-\Delta^2(\gamma_a - h)^2 + (\gamma - \gamma_a)^2 + (\gamma_b - h)^2}) \rangle 0. \tag{55}
\]

Then,
\[
\Gamma_C(t_1, t_2, t_3) = \langle \varphi | \varphi \rangle
\]
\[
= 2\sqrt{\Delta^3} \Delta^3 \hat{E}_A^{(+)}\{e^{-2\Delta^2((\gamma_a - h)^2 + (\gamma_b - h)^2 + (\gamma_a - \gamma_b)^2)} + e^{-2\Delta^2((\gamma_a - h)^2 + (\gamma_b - h)^2 + (\gamma_a - \gamma_b)^2)}
\]
\[
+ e^{-2\Delta^2((\gamma_a - h)^2 + (\gamma_b - h)^2 + (\gamma_a - \gamma_b)^2)} + 2e^{-\Delta^2((\gamma_a - h)^2 + (\gamma_b - h)^2 + (\gamma_a - \gamma_b)^2) + 2(\gamma - h)^2})
\]
\[
+ 2e^{-\Delta^2((\gamma_a - h)^2 + (\gamma_b - h)^2 + (\gamma_a - \gamma_b)^2) + 2(\gamma - h)^2)}
\]
\[
+ 2e^{-\Delta^2((\gamma_a - h)^2 + (\gamma_b - h)^2 + (\gamma_a - \gamma_b)^2) + 2(\gamma - h)^2)} \rangle 0. \tag{56}
\]

Next, with (47),
\[
P_{\text{det}}^{1,2}(3, 0) = \frac{1}{(2\pi \Delta^2)^{3/2}} \int \mathrm{d}t_1 \mathrm{d}t_2 \mathrm{d}t_3 \Gamma(t_1, t_2, t_3)
\]
\[
= \frac{(\sqrt{2})\Delta^3}{24(\sqrt{\pi})\Delta^3} \left\{ \frac{3}{(\sqrt{2})\Delta^3} + 6\frac{1}{(\sqrt{2})\Delta^3} e^{-\Delta^2(\gamma_a - h)^2} \right\}
\]
\[
= \frac{1}{8} \{1 + 2e^{-\Delta^2(\gamma_a - h)^2}\}. \tag{57}
\]

The coincidence probability is then
\[
P_{1,2}^\text{Co} = \frac{1}{4} \{3 - 2e^{-\Delta^2(\gamma_a - h)^2}\}. \tag{58}
\]

### A.3.3. n photons in input channel B

Using the same method, it can also be shown that
\[
P_{1,3}^\text{Co} = \frac{1}{8} \{7 - 3e^{-\Delta^2(\gamma_a - h)^2}\}. \tag{59}
\]
In fact, a general expression can be calculated using the same method for the probabilities from interference of one photon in input channel \(A\) and \(n\) in \(B\). The probabilities are given by equations (12) and (13) in the main text.

**A4. The general case**

Here, \(m\) photons enter beam splitter input \(A\) and \(n\) photons enter \(B\). Starting with \(|\varphi\rangle\),

\[
|\varphi\rangle = \mathcal{E}_{\Lambda}^{(+)}(t_{m+n}) \cdots \mathcal{E}_{\Lambda}^{(+)}(t_{2}) |m_{A}, n_{B}\rangle
\]

\[
= \frac{1}{\sqrt{m! \cdot n! \cdot (m+n)!}} \left[ \mathcal{E}_{\Lambda}^{(+)}(t_{m+n}) + \mathcal{E}_{\Lambda}^{(+)}(t_{m+n}) \right] \cdots \left[ \mathcal{E}_{\Lambda}^{(+)}(t_{2}) + \mathcal{E}_{\Lambda}^{(+)}(t_{2}) \right] \hat{A}^{\dagger}(\phi_{\alpha}) \hat{B}^{\dagger}(\phi_{\beta}) |0\rangle
\]

\[
= \mathcal{E}_{\Lambda}^{m+n} \sqrt{m! \cdot n! \cdot (m+n)!} \int d\omega_1 \cdots d\omega_{m+n} \left[ \prod_{j=1}^{m+n} \phi(\omega_{j}) \right] m! \cdot n!
\]

\[
\times \sum_{c} \exp \left[ i \sum_{k \in u_{m}} \omega_{k}(\tau_{A} - t_{k}) + i \sum_{l \in u_{n}} \omega_{l}(\tau_{B} - t_{l}) \right] |0\rangle
\]

\[
= \mathcal{E}_{\Lambda}^{m+n} \sqrt{m! \cdot n! \cdot (m+n)!} \exp \left[ i \sum_{k \in u_{m}} m_{A} \cdot n_{B} = \sum_{j=1}^{m+n} t_{j} \right]
\]

\[
\times \sum_{c} \exp \left\{ -\Delta^{2} \left[ \sum_{k \in u_{m}} (\tau_{A} - t_{k})^{2} + \sum_{l \in u_{n}} (\tau_{B} - t_{l})^{2} \right] \right\} |0\rangle .
\]

(60)

Let the complete set of *labels* or *indices* be \( \mathbf{U} = \{1, 2, \ldots, m + n\} \). In the above, \( u_{m} \) is a set containing \( m \) indices that is a subset of the complete set of indices, i.e. \( u_{m} \subseteq \mathbf{U} \). \( u_{m} \) is only one possible combination of a set that contains \( m \) labels. \( u_{m} \) is defined the same way such that with \( u_{m} \), they form the complete set of indices, i.e. \( u_{m} \cup u_{n} = \mathbf{U} \). The sum \( \sum_{c} \) is taken over all possible combinations of \( u_{m} \) and \( u_{n} \). The total number of combinations is \((m + n)!/m! \cdot n! \).

Similarly, let \( u_{m-j}, u_{n-j}, u_{j}, \) and \( u_{j'} \) be subsets of \( \mathbf{U} \) with number of elements \( m - j, n - j, j, \) and \( j' \), respectively, such that \( u_{m-j} \cup u_{n-j} \cup u_{j} \cup u_{j'} = \mathbf{U} \). The subscript \( j' \) in \( u_{j'} \) signifies that it is a different set from \( u_{j} \), although they have the same number of elements \( j \). In this context, the sum \( \sum_{c} \) will be taken over all possible combinations of \( u_{m-j}, u_{n-j}, u_{j}, \) and \( u_{j'} \). The total number of combinations is \((m + n)!/(m - j)!/(n - j)!/(j')!/(j)!^{2} \). Continuing from before,

\[
\Gamma_{c}(t_{0}, \ldots, t_{m+n}) = \langle \varphi | \varphi \rangle
\]

\[
= \mathcal{E}_{\Lambda}^{2(m+n)} \sum_{j=0}^{\min(m,n)} \sum_{c} \exp \left\{ -\Delta^{2} \left[ \sum_{k \in u_{m-j}} (\tau_{A} - t_{k})^{2} \right.ight.
\]

\[
+ \sum_{l \in u_{n-j}} (\tau_{B} - t_{l})^{2} + \sum_{p \in u_{j}} (\tau_{A} - t_{p})^{2} + (\tau_{B} - t_{p})^{2} \left. \right] \right\}.
\]

(61)

Next, with (47),

\[
P_{m,n}^{\mathrm{det}}(m + n, 0) = \frac{1}{(2\pi\mathcal{E}_{\omega}^{2})^{m+n}(m + n)!} \int dt_{1} \cdots dt_{m+n} \Gamma(t_{1}, \ldots, t_{m+n})
\]

\[
= \frac{m! \cdot n! \cdot (m+n)!^{\sum_{j=0}^{\min(m,n)} (m + n)!}}{(m - j)!/(n - j)!/(j')!/(j)!^{2} \left(2\pi\mathcal{E}_{\omega}^{2}\right)^{m+n} e^{-2\Delta^{2}(\tau_{A} - \tau_{B})^{2}}
\]

\[
= \frac{1}{2^{m+n} \sum_{j=0}^{\min(m,n)} (m - j)!/(n - j)!/(j')!/(j)!^{2} e^{-2\Delta^{2}(\tau_{A} - \tau_{B})^{2}},
\]

which is equation (17) in the main text. Therefore, with (8) and (9), \( P_{m+n}^{\mathrm{CO}} \) in equation (18) in the main text is obtained.

The results can also be extended to a general beam splitter described in (8). It is fairly straightforward to include the coefficients \( R \) and \( T \) from the beginning of the derivation, and it leads to equations (19) and (20) in the main text.
Appendix B. Total coincidence probabilities for coherent state and squeezed coherent state

B.1. Coherent state

We derive the total coincidence probability for the interference between coherent states first. Let the mean photon number of coherent source at \( A \) be \( \mu_A = \langle n \rangle_A \) and at \( B \) be \( \mu_B = \langle n \rangle_B \). With asymmetric beam splitter, equations (19) and (20) can be used. Starting from (25),

\[
P_{\text{total}}^{\text{Co}} = \sum_{m+n \geq 1} e^{-\mu_A} e^{-\mu_B} \frac{\mu_A^m \mu_B^n}{m! n!} \left[ 1 - (R^m T^n + T^m R^n)^{\min(m,n)} \sum_{j=0}^{\min(m,n)} \frac{m! n!}{(m-j)!(n-j)!} \frac{e^{-j\Delta(\gamma_A - \gamma_B)^2}}{(j!)^2} \right]
\]

\[
= \sum_{m+n \geq 0} e^{-\mu_A} e^{-\mu_B} \frac{\mu_A^m \mu_B^n}{m! n!} \left[ 1 - (R^m T^n + T^m R^n)^{\min(m,n)} \sum_{j=0}^{\min(m,n)} \frac{m! n!}{(m-j)!(n-j)!} \frac{e^{-j\Delta(\gamma_A - \gamma_B)^2}}{(j!)^2} \right]
\]

\[
e^{-\mu_A - \mu_B} + \sum_{m,n} e^{-\mu_A} e^{-\mu_B} \frac{\mu_A^m \mu_B^n}{m! n!} \left[ 1 - (R^m T^n + T^m R^n)^{\min(m,n)} \sum_{j=0}^{\min(m,n)} \frac{m! n!}{(m-j)!(n-j)!} \frac{e^{-j\Delta(\gamma_A - \gamma_B)^2}}{(j!)^2} \right]
\]

\[
= 1 + e^{-\mu_A - \mu_B} - e^{-\mu_A - \mu_B} \sum_{m,n} \sum_{j=0}^{\infty} \sum_{u=0}^{\infty} \frac{(\mu_A R)^m (\mu_B T)^n}{(j!)^2} \frac{(\mu_B T)^n}{(k-j)!} \frac{(\mu_B R)^j}{(l-j)!} \frac{e^{-j\Delta(\gamma_A - \gamma_B)^2}}{(j!)^2}
\]

\[
= 1 + e^{-\mu_A - \mu_B} - e^{-\mu_A - \mu_B} \sum_{m,n} \sum_{j=0}^{\infty} \frac{(\mu_A R)^m (\mu_B T)^n}{(j!)^2} \frac{(\mu_B T)^n}{(k-j)!} \frac{(\mu_B R)^j}{(l-j)!} \frac{e^{-j\Delta(\gamma_A - \gamma_B)^2}}{(j!)^2}
\]

\[
= 1 + e^{-\mu_A - \mu_B} - e^{-\mu_A - \mu_B} (e^{\mu_A R + \mu_B T} + e^{\mu_B T + \mu_A R}) \sum_{j=0}^{\infty} \frac{(\mu_A R)^m (\mu_B T)^n}{(j!)^2} \frac{(\mu_B T)^n}{(k-j)!} \frac{(\mu_B R)^j}{(l-j)!} \frac{e^{-j\Delta(\gamma_A - \gamma_B)^2}}{(j!)^2}
\]

\[
= 1 + e^{-\mu_A - \mu_B} - e^{-\mu_A - \mu_B} (e^{\mu_A R + \mu_B T} + e^{\mu_B T + \mu_A R}) \sum_{j=0}^{\infty} \frac{\sqrt{\mu_A R T e^{-j\Delta(\gamma_A - \gamma_B)^2}}}{(j!)^2}
\]

\[
= 1 + e^{-\mu_A - \mu_B} - e^{-\mu_A - \mu_B} (e^{\mu_A R + \mu_B T} + e^{\mu_B T + \mu_A R}) I_0(2\sqrt{\mu_A R T e^{-j\Delta(\gamma_A - \gamma_B)^2}}),
\]

where \( I_0 \) is the modified Bessel function of the first kind with order 0. With this, assuming 50:50 beam splitter \( (R = T = 50\%) \) and under the condition that \( \mu_A = \mu_B = \langle n \rangle \), the total coincidence probability is given by equation (26) in the main text.

B.2. Squeezed coherent state

On the other hand, the general expression for the squeezed coherent state is intractable due to the appearance of the Hermite polynomial in the infinite sums. However, it is possible to calculate for the special case of \( |\gamma_A - \gamma_B| = \infty \). First, we note that the sum of the photon number distribution in (33) should be equal to unity, i.e.,

\[
\exp \left[ -|\alpha|^2 (1 + \tanh r) \right] \sum_n \frac{1}{n!} \left( \frac{\tanh r}{2} \right)^n \left[ H_n \left( |\alpha| \frac{1 + \tanh r}{\sqrt{2} \tanh r} \right) \right]^2 = 1
\]

\[
\sum_n \frac{1}{n!} \left( \frac{\tanh r}{2} \right)^n \left[ H_n \left( |\alpha| \frac{1 + \tanh r}{\sqrt{2} \tanh r} \right) \right]^2 = \exp \left[ |\alpha|^2 (1 + \tanh r) \right] \cosh r.
\]

To assist with the derivation later, by using equation (63) it is useful to calculate the sum

\[
\sum_n \frac{K^n}{n!} \left( \frac{\tanh s}{2} \right)^n \left[ H_n \left( |\alpha'| \frac{1 + \tanh s}{\sqrt{2} \tanh s} \right) \right]^2 = \sum_n \frac{1}{n!} \left( \frac{\tanh s}{2} \right)^n \left[ H_n \left( |\alpha'| \frac{1 + \tanh s}{\sqrt{2} \tanh s} \right) \right]^2
\]

\[
= \exp \left[ |\alpha'|^2 (1 + \tanh s) \right] \cosh s,
\]

where \( K \) is a constant, \( \tanh s = K \tanh r \), and \( |\alpha'| = |\alpha| \sqrt{K^2 \frac{1 + \tanh s}{1 + K \tanh r}} \). Furthermore, since \( \cosh s = (1 - \tanh^2 s)^{-1/2} \),
\[
\cosh s = \frac{1}{\sqrt{1 - K^2 \tanh^2 r}} = \frac{1}{\sqrt{(1 - K^2) + K^2 (1 - \tanh^2 r)}} = \frac{\cosh r}{\sqrt{K^2 + (1 - K^2) \cosh^2 r}}.
\]

Therefore,
\[
\sum_n K^n n! \left( \frac{\tanh r}{2} \right)^n \left[ H_n \left( |\alpha| \frac{1 + \tanh r}{\sqrt{2} \tanh r} \right) \right]^2 = \exp[|\alpha|^2 (1 + \tanh s)] \cosh s
\]
\[
= \exp \left[ |\alpha|^2 \frac{K(1 + \tanh r)^2}{1 + \tanh r} \right] \cosh r
\]
\[
= \frac{\cosh r}{\sqrt{K^2 + (1 - K^2) \cosh^2 r}}.
\]

(64)

Let the parameters of the source at A be \( \alpha \) and \( r_A \) and at B be \( \beta \) and \( r_B \). With asymmetric beam splitter and for \( |r_A - r_B| = \infty \), the total coincidence probability (25):
\[
p_{\text{total}} = \frac{\exp[-|\alpha|^2 (1 + \tanh r_A) - |\beta|^2 (1 + \tanh r_B)]}{\cosh r_A \cosh r_B} \left\{ \sum_{m+n \geq 1} \frac{1}{m! n!} \left( \frac{\tanh r_A}{2} \right)^m \left( \frac{\tanh r_B}{2} \right)^n \right\}
\times \left[ H_n \left( |\alpha| \frac{1 + \tanh r_A}{\sqrt{2} \tanh r_A} \right) H_n \left( |\beta| \frac{1 + \tanh r_B}{\sqrt{2} \tanh r_B} \right) \right]^2 \left[ 1 - (R^m T^n + T^m R^n) \right]
\]
\[
= \frac{\exp[-|\alpha|^2 (1 + \tanh r_A) - |\beta|^2 (1 + \tanh r_B)]}{\cosh r_A \cosh r_B} \left\{ 1 + \cosh r_A \cosh r_B \right\}
\times \left[ \frac{\tanh r_A}{2} \right]^m \left( \frac{\tanh r_B}{2} \right)^n \left[ H_n \left( |\alpha| \frac{1 + \tanh r_A}{\sqrt{2} \tanh r_A} \right) H_n \left( |\beta| \frac{1 + \tanh r_B}{\sqrt{2} \tanh r_B} \right) \right]^2 \left[ 1 - (R^m T^n + T^m R^n) \right]
\]
\[
= 1 + \exp[-|\alpha|^2 (1 + \tanh r_A) - |\beta|^2 (1 + \tanh r_B)]
\]
\[
\times \left\{ 1 - \frac{\exp[|\alpha|^2 R(1 + \tanh r_A)^2 + |\beta|^2 T(1 + \tanh r_B)^2]}{\sqrt{R^2 + (1 - R^2) \cosh^2 r_A} \sqrt{T^2 + (1 - T^2) \cosh^2 r_B}} \cosh r_A \cosh r_B \right\}
\times \left[ \frac{\tanh r_A}{2} \right]^m \left( \frac{\tanh r_B}{2} \right)^n \left[ \frac{\tanh r_A}{\sqrt{2} \tanh r_A} \right]^m \left[ \frac{\tanh r_B}{\sqrt{2} \tanh r_B} \right]^n \left[ H_n \left( |\alpha| \frac{1 + \tanh r_A}{\sqrt{2} \tanh r_A} \right) H_n \left( |\beta| \frac{1 + \tanh r_B}{\sqrt{2} \tanh r_B} \right) \right]^2 \left[ 1 - (R^m T^n + T^m R^n) \right]
\]
\[
= 1 + \exp[-|\alpha|^2 (1 + \tanh r_A) - |\beta|^2 (1 + \tanh r_B)]
\]
\[
\times \left\{ \frac{\cosh r_A \cosh r_B}{\sqrt{R^2 + (1 - R^2) \cosh^2 r_A} \sqrt{T^2 + (1 - T^2) \cosh^2 r_B}} \right\}.
\]

(65)

where equations (63) and (64) have been used in the last lines of the equation. Assuming 50:50 beam splitter \((R = T = 50\%)\) and under the condition that \( |\beta| = |\alpha| \) and \( r_A = r_B = r \), equation (65) yields equation (34) in the main text.

**Appendix C. Calculation of error rate in the X-basis**

The calculation of error rate follows the one presented in [26]. Here, we focus on error rate caused by multiphoton detection in the X-basis assuming ideal devices. The calculation includes only up to three photons from Alice and Bob combined, since for small mean photon number \( \langle n \rangle \leq 0.5 \), probabilities of higher photon number do not contribute significantly.

In the X-basis, with single photon source, Alice and Bob prepare photons randomly in \( |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \) states, where \( |0\rangle \) and \( |1\rangle \) represent the early and late temporal modes or time-bins. With sources involving multi-photon state, however, this becomes more complicated. To account for this, a change in notation is introduced. Let \( |n\rangle \) now be the photon number state (instead of the temporal modes). For the state preparation, let Alice’s creation operator be \( \hat{A}_n = \frac{1}{\sqrt{2}}(\hat{a}_n + e^{i\phi_n} \hat{a}_n^\dagger) \), where \( \hat{a}_n^\dagger \) and \( \hat{a}_n^\dagger \) denote the creation operators in the early and late
time-bins, respectively, and \(\phi_A \in \{0, \pi\}\) is the relative phase that Alice chooses randomly. For example, if Alice prepares \(n\) photons, the state is

\[
\frac{1}{\sqrt{n!}} \hat{A}^n |0\rangle.
\]

Similarly, Bob’s creation operator is \(\hat{B}^\dagger = \frac{1}{\sqrt{2}} (\hat{a}^\dagger_0 + \text{e}^{i\phi_B} \hat{a}^\dagger_1)\), where \(\phi_B \in \{0, \pi\}\) is relative phase that Bob chooses randomly. The creation operators obey the beam splitter transformation relation in (8). The phase \(\theta\) associated with beam splitter reflection does not have direct physical consequence, so \(\theta = 0\) is chosen for convenience. For 50:50 lossless beam splitter,

\[
\begin{pmatrix}
\hat{a}_0 \\
\hat{a}_1 \\
\end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix}
\hat{c}_0 \\
\hat{c}_1 \\
\end{pmatrix}, \quad \begin{pmatrix}
\hat{b}_0 \\
\hat{b}_1 \\
\end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix}
\hat{d}_0 \\
\hat{d}_1 \\
\end{pmatrix}
\]

Also, let the output photon state be denoted by \(|n\rangle_{n,C}\) at output \(C\) and \(|n\rangle_{n,D}\) at output \(D\), where \(n\) is the photon number and \(t \in \{0, 1\}\) is the temporal mode (0 for early and 1 for late).

An accepted detection event occurs when the two detectors click and detect photons at different time-bins. An erroneous detection event happens when Alice and Bob prepare identical states, yet measurement by detectors indicates an accepted detection event. Since error rate is the erroneous detection probability over the total probability of detection (eq. (37) in the main text), the probabilities of correct and erroneous detection need to be calculated. To do this, full analysis of photon interference taking into account the temporal and input-output modes has to be performed.

When the total number of photons entering beam splitter is zero or one, no detection event can occur. Therefore, the analysis is split into the two photons case and three photons case. The total erroneous and correct detection probabilities are just the sum of individual probabilities in each scenario.

**C.1. Two photons entering beam splitter**

There are two possible input configurations: two photons at one input and zero photons at the other, and one photon at each input. The probabilities of correct and erroneous detection are calculated for each of the input configurations.

For the first configuration (two photons at one input and zero photons at the other), the state becomes

\[
\frac{1}{\sqrt{2}} \hat{A}^{12} |0\rangle = \frac{1}{\sqrt{2}} \left[ \frac{1}{\sqrt{2}} (\hat{a}_0^\dagger + \text{e}^{i\phi_A} \hat{a}_1^\dagger) \right]^2 |0\rangle
\]

\[
= \frac{1}{2 \sqrt{2}} (\hat{a}_0^\dagger + 2\text{e}^{i\phi_A} \hat{a}_0^\dagger \hat{a}_1^\dagger + \text{e}^{2i\phi_A} \hat{a}_1^{2\dagger}) |0\rangle
\]

\[
= \frac{1}{4} \left[ (\hat{c}_0^\dagger + \hat{d}_1^\dagger)^2 + 2\text{e}^{i\phi_A} (\hat{c}_1^\dagger + \hat{d}_0^\dagger) (\hat{c}_0^\dagger + \hat{d}_1^\dagger) + \text{e}^{2i\phi_A} (\hat{c}_1^\dagger + \hat{d}_1^\dagger)^2 \right] |0\rangle
\]

\[
= \frac{1}{4} [2 |0,C\rangle \langle 0,C| + |2,C\rangle \langle 2,C|]
\]

\[
+ \frac{1}{2 \sqrt{2}} (|1,C\rangle \langle 0,D| + \text{e}^{2i\phi_A} |1,D\rangle \langle 1,C|)
\]

\[
+ \frac{\text{e}^{i\phi_A}}{2 \sqrt{2}} (|1,C\rangle \langle 1,D| + |1,D\rangle \langle 1,C| + |1,C\rangle \langle 0,D| + |1,D\rangle \langle 0,C|).
\]

An accepted detection event occurs when the photon state collapses to \(|1,C\rangle \langle 1,D|\) or \(|1,C\rangle \langle 0,D|\) during measurement. From (66), the combined probability for these states is

\[
2 \times \left| \frac{\text{e}^{i\phi_A}}{2 \sqrt{2}} \right|^2 = \frac{1}{4}.
\]

In this configuration, the choice of \(\phi_A\) and \(\phi_B\) does not affect the probability of accepted detection. This means the probabilities of erroneous and correct detection are the same regardless of Alice’s and Bob’s choice of states. Therefore, the probabilities in this configuration are

\[
P_{\text{error}} = P_{\text{correct}} = \frac{1}{4} \times [\mathcal{D}_A(0) \mathcal{D}_B(2) + \mathcal{D}_A(2) \mathcal{D}_B(0)].
\]
For the second configuration (one photon at each input), the state becomes
\[
\hat{A}^+ \hat{B}^+ |0\rangle = \frac{1}{2} (\hat{a}_0^+ + e^{i\phi_a} \hat{a}_1^+)(\hat{b}_0^+ + e^{i\phi_b} \hat{b}_1^+)|0\rangle
\]
\[
= \frac{1}{2} (\hat{a}_0^+ \hat{b}_0^+ + e^{i\phi_a} \hat{a}_1^+ \hat{b}_1^+ + e^{i\phi_b} \hat{a}_0^+ \hat{b}_0^+ + e^{i\phi_b} e^{i\phi_a} \hat{a}_1^+ \hat{b}_1^+)|0\rangle
\]
\[
- \frac{1}{4} (\hat{c}_0^+ + \hat{d}_0^+)(\hat{c}_1^+ + \hat{d}_1^+) + (e^{i\phi_a} - e^{i\phi_b})(\hat{c}_0^+ \hat{d}_1^+ + \hat{c}_1^+ \hat{d}_0^+)|0\rangle
\]
\[
= \frac{1}{2\sqrt{2}} ([2]_{0,C} - [2]_{0,D} + e^{i\phi_a + i\phi_b}([2]_{1,C} - [2]_{1,D})]
\]
\[
+ \frac{1}{4} (e^{i\phi_a} + e^{i\phi_b})([1]_{0,C}[1]_{1,C} - [1]_{0,D}[1]_{1,D})
\]
\[
+ \frac{1}{4} (e^{i\phi_a} - e^{i\phi_b})([1]_{0,C}[1]_{1,D} - [1]_{1,C}[1]_{0,D}).
\]  
(67)

An accepted detection event occurs when the photon state collapses to $[1]_{0,C}[1]_{1,D}$ or $[1]_{1,C}[1]_{0,D}$ during measurement. From (67), the combined probability for these states is
\[
2 \times \left| \frac{1}{4} (e^{i\phi_a} - e^{i\phi_b}) \right|^2 = \frac{1}{4} [1 - \cos(\phi_a - \phi_b)].
\]

The probability of erroneous detection (when Alice and Bob prepare identical states, $\phi_A = \phi_B$) in this case is
\[
P_{\text{error}} = \frac{1}{4} [1 - \cos(0)] \times D_A(1)D_B(1) = 0.
\]

The probability of correct detection (when Alice and Bob prepare states that are orthogonal to each other, $|\phi_A - \phi_B| = \pi$) in this case is
\[
P_{\text{correct}} = \frac{1}{4} [1 - \cos(\pi)] \times D_A(1)D_B(1) = \frac{1}{2} \times D_A(1)D_B(1).
\]

C.2. Three photons entering beam splitter

There are two possible input configurations: three photons at one input and zero photons at the other, and two photons at one input and one photon at the other. Similar to the two photons case, the probabilities of correct and erroneous detection are calculated for each input configuration.

For the first configuration (three photons at one input and zero photons at the other), the state becomes
\[
\frac{1}{\sqrt{6}} \hat{A}^{13} |0\rangle = \frac{1}{\sqrt{6}} \left[ \frac{1}{\sqrt{2}} (\hat{a}_0^+ + e^{i\phi_a} \hat{a}_1^+) \right] |0\rangle
\]
\[
= \frac{1}{4\sqrt{6}} ([3]_{0,C} + 3 [3]_{0,D} + e^{i\phi_a}([2]_{1,C} + [2]_{1,D} + [1]_{1,C}[1]_{1,D} + [1]_{1,D}[1]_{1,C})]
\]
\[
+ \frac{\sqrt{3}}{8} (e^{i\phi_a}([2]_{0,C}[1]_{0,D} + [1]_{0,C}[2]_{0,D} + e^{i\phi_b}([2]_{1,C}[1]_{1,D} + [1]_{1,C}[2]_{1,D}])
\]
\[
+ \frac{\sqrt{3}}{8} e^{i\phi_a}([2]_{0,C}[1]_{0,D} + [2]_{1,C}[1]_{1,D} + [1]_{0,C}[2]_{0,D} + [1]_{0,D}[2]_{1,D})
\]
\[
+ \frac{\sqrt{3}}{4\sqrt{2}} e^{i\phi_b}([1]_{0,C}[1]_{0,D} + [1]_{0,C}[1]_{0,D} + [1]_{1,C}[1]_{0,D} + [1]_{1,D}[1]_{0,D}).
\]  
(68)

An accepted detection event occurs when the photon state collapses to $[2]_{0,C}[1]_{1,D}$, $[1]_{0,C}[2]_{1,D}$, $[2]_{1,C}[1]_{0,D}$, or $[1]_{1,C}[2]_{0,D}$ during measurement. From (68), the combined probability for these states is
\[2 \times \left| \frac{\sqrt{3}}{8} e^{i\phi_A} \right|^2 + 2 \times \left| \frac{\sqrt{3}}{8} e^{2i\phi_A} \right|^2 = \frac{3}{16}.\]

In this configuration, the choice of \(\phi_A\) and \(\phi_B\) does not affect the probability of accepted detection. This means the probabilities of erroneous and correct detection are the same regardless of Alice’s and Bob’s choice of states. Therefore, the probabilities in this configuration are

\[P_{\text{error}} = P_{\text{correct}} = \frac{3}{16} \times [D_A(0) D_B(3) + D_A(3) D_B(0)].\]

For the second configuration (two photons at one input and one photon at the other), the state becomes

\[\frac{1}{\sqrt{2}} \left( \bar{\hat{A}}^{\dagger} \bar{\hat{B}} \right) |0\rangle = \frac{1}{2} \left[ \frac{1}{\sqrt{2}} \left( \hat{d}_0^+ + e^{i\phi_A} \hat{d}_1^+ \right) \right]^2 \left( \hat{b}_0^+ + e^{i\phi_B} \hat{b}_1^+ \right) |0\rangle \]

\[= \frac{1}{4} (\hat{d}_0^{(2)} + 2e^{i\phi_B} \hat{d}_0^+ \hat{d}_1^+ + e^{2i\phi_B} \hat{d}_1^2) \left( \hat{b}_0^+ + e^{i\phi_B} \hat{b}_1^+ \right) |0\rangle \]

\[\rightarrow \frac{1}{8\sqrt{2}} [ (\hat{c}_0^+ + \hat{d}_1^+)^2 + 2e^{i\phi_B} (\hat{c}_0^+ + \hat{d}_1^+) (\hat{c}_1^+ + \hat{d}_1^+) + e^{2i\phi_B} (\hat{c}_1^+ + \hat{d}_1^+)^2] \cdot [ (\hat{c}_0^+ - \hat{d}_1^+) + e^{i\phi_B} (\hat{c}_1^+ - \hat{d}_1^+)] |0\rangle \]

\[= \frac{\sqrt{3}}{8} \left[ |3\rangle_{0,C} - |3\rangle_{0,D} + e^{-2i\phi_B + \phi_A}(|3\rangle_{1,C} - |3\rangle_{1,D}) \right] \]

\[+ \frac{1}{4} (|2\rangle_{0,C} |1\rangle_{0,D} - |1\rangle_{0,C} |2\rangle_{0,D} + e^{2i\phi_B + \phi_A}(|2\rangle_{1,C} |1\rangle_{0,D} - |1\rangle_{1,C} |2\rangle_{0,D}) \]

\[+ \frac{1}{8} (2e^{i\phi_B} + e^{i\phi_A}) (|2\rangle_{0,C} |1\rangle_{0,D} - |2\rangle_{0,D} |1\rangle_{0,C}) \]

\[+ \frac{1}{8} (2e^{i\phi_B + \phi_A} + e^{2i\phi_B}) (|1\rangle_{0,C} |2\rangle_{1,D} - |1\rangle_{0,D} |2\rangle_{1,C}) \]

\[+ \frac{1}{8} (2e^{i\phi_A} - e^{i\phi_B}) (|2\rangle_{0,C} |1\rangle_{1,D} - |1\rangle_{1,C} |2\rangle_{0,D}) \]

\[+ \frac{1}{8} (2e^{i\phi_B + \phi_A} - e^{2i\phi_B}) (|1\rangle_{0,C} |2\rangle_{1,D} - |1\rangle_{0,D} |2\rangle_{1,C}) \]

\[+ \frac{1}{4\sqrt{2}} e^{i\phi_B} (|1\rangle_{0,C} |1\rangle_{1,D} - |1\rangle_{1,C} |1\rangle_{0,D}) . \tag{69} \]

An accepted detection event occurs when the photon state collapses to \(|2\rangle_{0,C} |1\rangle_{1,D}, |1\rangle_{0,C} |2\rangle_{1,D}, |1\rangle_{0,D} |2\rangle_{1,C},\) or \(|1\rangle_{1,C} |2\rangle_{0,D}\) during measurement. From (69), the combined probability for these states is

\[2 \times \frac{1}{8} (2e^{i\phi_A} \cdot e^{i\phi_B}) + 2 \times \frac{1}{8} (2e^{2i\phi_B} \cdot e^{2i\phi_B}) = \frac{1}{16} [5 - 4 \cos(\phi_A - \phi_B)]. \]

The probability of erroneous detection (when Alice and Bob prepare identical states, \(\phi_A = \phi_B\)) in this case is

\[P_{\text{error}} = \frac{1}{16} [5 - 4 \cos(0)] \times [D_A(1) D_B(2) + D_A(2) D_B(1)] = \frac{1}{16} \times [D_A(1) D_B(2) + D_A(2) D_B(1)]. \]

The probability of correct detection (when Alice and Bob prepare states that are orthogonal to each other, \(\phi_A = \phi_B = \pi\)) in this case is

\[P_{\text{correct}} = \frac{1}{16} [5 - 4 \cos(\pi)] \times [D_A(1) D_B(2) + D_A(2) D_B(1)] = \frac{9}{16} \times [D_A(1) D_B(2) + D_A(2) D_B(1)]. \]

**Appendix D. Some details on time-bin MDI-QKD**

**D.1. Charlie’s detection event**

In an ideal situation, if single photon sources are used, when Alice and Bob send identical photon states, the photons will only exit at the same beam splitter output due to HOM effect. When they send states that are orthogonal to each other, the photons may exit at the same beam splitter output or they may also exit at different outputs. The case where the photons exit at different outputs is conclusive: Alice and Bob send orthogonal states. Therefore, with this conclusive/accepted detection, Alice and Bob have anti-correlated pair of bits. In the time-bin basis (both X and Z-bases), when the photons exit at different outputs, they also exit in different time-bins.
So, Charlie’s accepted detection reflects this situation: the two detectors at \( C \) and \( D \) click and detect photons at different time-bins.

Now, when multi-photon sources are used, simply taking the event in which the two detectors at \( C \) and \( D \) click, without accounting for the different time-bins, will increase the error rates. To illustrate this using an example, consider Alice and Bob sending multi-photons in the same time-bin in \( Z \)-basis. Although the photons interfere, there is possibility that coincidence detection occurs (i.e. both detectors at \( C \) and \( D \) click, at the same time-bin). If this detection event is accepted, then Alice and Bob will end up with the same bits (because they choose the same time-bin), instead of anti-correlated bits that they want, contributing to error.

### D.2. Squeezing parameter for the decoy state

The condition laid out in [25] for the three intensity decoy states protocol is that the photon number probability distribution of the signal and decoy states should obey the relation

\[
\frac{D_s(n)}{D_d(n)} \geq \frac{D_s(2)}{D_d(2)} \geq \frac{D_s(1)}{D_d(1)}
\]

for \( n \geq 2 \), where the subscripts \( s \) and \( d \) denote the signal state and decoy state, respectively.

For the amplitude-squeezed coherent state with photon number distribution given in (33), one way to satisfy this condition is to set the argument of the Hermite polynomial of the signal and decoy states to be equal, i.e.

\[
|\alpha_d|^2 \leq |\alpha|^2 + \sinh^2(r_d)
\]

Together with the constraint \( \langle n \rangle_d = |\alpha|^2 + \sinh^2(r_d) \) this will ensure that the condition is satisfied when \( \langle n \rangle_d \leq \langle n \rangle \).

For \( \langle n \rangle = 0.5 \), \( \langle n \rangle = 0.1 \), and \( r_d = 0.4111 \), a numerical calculation is carried out to get \( r_d = 6.84 \times 10^{-2} \).

### ORCID iDs

Andri Pradana @ https://orcid.org/0000-0002-9749-8882
Lock Yue Chew @ https://orcid.org/0000-0003-1366-8205

### References


