

Spoofing resilience for simple-detection quantum illumination LIDAR

Richard J. Murchie

*Advanced Concepts Team, European Space Agency,
Keplerlaan 1, 2201 AZ, Noordwijk, The Netherlands.*

John Jeffers

*Department of Physics and SUPA, University of Strathclyde,
John Anderson Building, 107 Rottenrow, Glasgow G4 0NG, United Kingdom*

(Dated: October 29, 2025)

Object detection and range finding using a weak light source is vulnerable to jamming and spoofing attacks by an intruder. Quantum illumination with nonsimultaneous, phase-insensitive coincidence measurements can provide jamming resilience compared to identical measurements for classical illumination. We extend an experimentally-feasible object detection and range finding quantum illumination-based protocol to include spoofing resilience. This approach allows the system to be characterised by its experimental parameters and quantum states, rather than just its detector data. Therefore we can scope the parameter-space which provides some spoofing resilience without relying upon the prohibitive method of acquiring detector data for all combinations of the experimental parameters. We demonstrate that in certain regimes the intruder has an optimal relative detection basis angle to minimise the induced error. We also show that there are spoofing-vulnerable regimes where excessive background noise prevents any induced error, while it is still possible to perform object detection, i.e. our detectors have not been fully blinded. The sensing protocol which we describe can allow for the recognition of intrusion and the possible detection of our trustworthy return signal. Our results reinforce that quantum illumination is advantageous for spoofing resilience compared to a classical illumination-based protocol.

I. INTRODUCTION

Passive remote-sensing is fundamentally insecure as it relies upon uncontrolled incident light scattered from an object to form the image. An adversary can deploy countermeasures to attempt to hide this object by jamming (denial of sensing by excessive noise injection) or spoofing (attempting to fool the sensor operator into believing false information). An active remote sensing system, such as LIDAR, is more secure than passive remote sensing as control of the light beam provides more knowledge about the expected return signal imprinted by the presence and distance of the possible target object. Nevertheless, an active remote sensing system can still suffer from jamming and spoofing attempts that it would be useful to mitigate against. Active remote sensing is not used in some situations because the extra light directed to the target object can be seen, again allowing countermeasures to the sensing to be deployed. One possible solution to this is to extract the most information from the minimum amount of active sensing light, which implies exploiting its quantum properties.

Much theoretical and experimental work has been done on object detection and range finding protocols which use twin beam quantum illumination (QI) to improve performance in comparison to a suitable classical benchmark [1–17]. It has been shown that simple-detection QI (that uses Geiger-mode click/no-click photodetectors) can provide jamming resilience from stationary or dynamic background noise when undertaking object detection and range finding [18]. The strong non-classical inter-beam photon number correlations of the light allow

simple-detection QI to facilitate effective noise-filtering.

Various quantum-secure imaging (QSI) protocols with spoofing resilience capabilities have been proposed and implemented [19–28]. Moreover, in Ref [29] they consider the security of a quantum range finding protocol where the target object has an active role in verifying their position. The security of these protocols is enhanced by the laws of quantum mechanics and they are in effect modified quantum cryptography schemes [30]. Initial work used a modified BB84-inspired prepare-and-measure scheme for imaging, whereby the transmitter (conventionally Alice) randomly chooses a basis for which there are two quantum states to randomly choose from to use as the signal [19]. The receiver (conventionally Bob) measures this light in the same basis chosen by Alice. As Alice and Bob are co-located, we refer to them both as Alice henceforth. This co-location means an insecure public channel is not required and it is easy to ensure that the measurement is in the correct basis. The intruder (conventionally known as Eve) attempts spoofing via an intercept-resend strategy: she (partially or fully) intercepts the signal, measures it and then resends it according to how she wishes to spoof Alice [31]. For example, Eve can attempt to spoof target object spatial or range information by sending light towards Alice in a different spatial mode or time-bin, respectively. The security of this system is derived from the information advantage (the choice of basis) that Alice enjoys. This information advantage ensures that Eve introduces errors on average, as she is unable to know perfectly the quantum state being sent from just a measurement; therefore, her resent quantum state may differ [32]. QSI dif-

fers from quantum cryptography, as Eve's strategy is to deceive Alice rather than to obtain a supposed secret key. Here we extend the simple-detection QI-based object detection and range finding protocol from Ref. [17] to include spoofing resilience. We also build on work pertaining to non-classical correlation based quantum-secured imaging (QSI) [23, 26]. Furthermore, we choose non-classical correlation based-QSI instead of prepare-and-measure (BB84-inspired) QSI with a weak coherent-state pulse due to its noise-resilience (for improved SNR) and intrinsic timing-correlation for range finding.

The paper is organized as follows. In Section II A we describe an overview of the system. This includes details about the states of light involved and how we model the system measurements. Section II B gives the details about the security of this system. Section II C gives an analysis of the errors involved in this system. In Sect. II D we explain how Alice can recognise a spoofing attack by Eve. In Sect. II E we demonstrate how Alice can remove untrustworthy detector data due to the intrusion of Eve. Performance analysis of the different systems we consider is given in Sect. II F. In Sect. II G we give thresholds for erroneous conclusions about the detector data when restricted to limited number of samples. We present simulation results of a spoofing attack in a range finding problem in Sect. III. We conclude this paper with a discussion of the contents of this paper, the results and the outlook for future research in Sect. IV.

II. SPOOFING RESILIENCE

A. System overview

We want to be able to detect the presence of an intruder [33, 34], to determine the whereabouts of any trustworthy real signal (which may contain information about a target object) and to subtract any false information from detection statistics [20, 23, 26, 27]. This section gives a theoretical analysis and overview of a system that does this. The system is based on a simple-detection object detection and range finding protocol with non-classically correlated quantum states. The quantum states have two sets of non-classically correlated modes: the idler modes and the signal modes. The idler light field is measured locally at the idler detectors and does not interact with a possible target object, whereas the signal light field is sent towards the possible target object (assuming the signal light field is in a path untampered by Eve). Reflection of this light field from the target object is recorded by Alice's signal detectors. Measurement of the idler modes conditions the signal modes due to the signal-idler correlations. These correlations can be used to enhance the sensitivity of the signal mode measurement. As the system uses simple detection the detectors can only register a click or no-click. Therefore, from our theoretical model of the system, we calculate detector click probabilities. It is these click probabilities that al-

low us both to recognise the presence of an intruder and to detect the presence or absence of a target object.

We assume that our source produces polarisation-correlated pairs of photons and we use this degree of freedom in our protocol. We could equally-well choose another type of encoding, one which is fully preserved on scattering from an object, but the theory described here is independent of this choice. The state of light used is written in the Fock basis as

$$\hat{\rho} = c_0 |0, 0, 0, 0\rangle \langle 0, 0, 0, 0| + c_1 (|0, 1, 0, 1\rangle \langle 1, 0, 1, 0| + |1, 0, 1, 0\rangle \langle 0, 1, 0, 1|), \quad (1)$$

where the mode labelling is in the order (idler: horizontal, ..., signal: antidiagonal) : I:H, I:V, S:V, S:H or I:D, I:A, S:D, S:A, for a rectilinear or diagonal basis choice respectively and Alice randomly chooses whether the state is in the rectilinear or diagonal basis. We refer to the system that uses the state described in Eq. 1 as the QI system and this could be produced from Type-II SPDC, for example. Also, we omit the off-diagonal parts of the density operator as the detectors are only sensitive to its diagonal elements. The coefficients are $c_0 = \frac{1}{(\bar{n}+1)^2 \mathcal{N}_0}$ and $c_1 = \frac{\bar{n}}{(\bar{n}+1)^3 \mathcal{N}_0}$, where $\mathcal{N}_0 = \frac{1}{(\bar{n}+1)^2} + \frac{2\bar{n}}{(\bar{n}+1)^3}$ is a normalisation factor necessitated by the truncation of multiphoton contributions. From the mode labelling of Alice's state of light, we can see that the correlated polarisations for the idler and signal modes are as follows

$$\begin{aligned} \text{I : H} &\rightarrow \text{S : V}, \\ \text{I : V} &\rightarrow \text{S : H}, \\ \text{I : D} &\rightarrow \text{S : D}, \\ \text{I : A} &\rightarrow \text{S : A}. \end{aligned}$$

These mode label mappings inform what we describe as correct and wrong coincidence clicks.

In order to consider the impact of a spoofing attempt we imagine that there are two channels at Alice's signal detector which we dub the real channel $\mathfrak{R}$ and the false channel $\mathfrak{F}$. These channels can be separated spatially and/or temporally, for example, if Eve wishes to spoof the spatial and/or temporal information. The real channel possibly includes Alice's light, some of Eve's light and background light, whereas the false channel possibly includes some of Eve's light and background light. These channels are what Alice measures. Appendix A 1 describes the parameters for the system and Appendix A 2 onwards derives the click probabilities for the system.

We characterise the strength of intrusion by its proportion p , the probability that Eve intercepts Alice's light, with $p = 1$ meaning that all of Alice's light is intercepted and $p = 0$ meaning that there is no interception. The proportion of intrusion p can be partitioned into the intruded light resent towards the real channel $p_{\mathfrak{R}}$ and false channel $p_{\mathfrak{F}}$, where $p = p_{\mathfrak{R}} + p_{\mathfrak{F}}$. For our system we consider that Alice has a choice of two measurement bases. Following from this, Eve has a choice of which basis (out of the two options) she measures with. The fact that Eve

must make a choice of basis implies that she does not know which basis Alice used, i.e. this is the information disadvantage that Eve has. Furthermore, Eve's choice of which basis could be biased or random and we signify this biasing with the parameter r . For example, $r = \frac{1}{2}$ signifies random basis selection, $r = 0$ signifies that she only measures in one basis and $r = 1$ signifies that she only measures in the other basis. There could be a set of system parameters such that a particular proportion of basis choice r for Eve would minimise the induced error. Eve could optimise this scenario by biasing a proportion of basis choice if she knows the geometry of the problem and Alice's experimental conditions. Otherwise, she would just randomly guess the basis angle choice and set $r = \frac{1}{2}$. However, Alice could detect Eve's basis biasing by inspecting the detection statistics of the conjugate basis to Eve's biased basis, as this would have an elevated error in comparison to the reduced error detection statistics which has the closest match to her biased basis. Her basis-biasing strategy would instruct Alice to adjust her proportion of basis choice accordingly, thereby undoing any advantage Eve gained from biasing. An example scenario is that Alice has highly attenuated H/V detection statistics compared to D/A, if Eve was to only choose the D/A basis the total induced error would be reduced, as it is rare that Eve induces errors by measuring Alice's H/V photons in the wrong basis. However, for Alice's H/V statistics the error is increased beyond what is expected from random basis selection by Eve. As there is a viable counter-attack to Eve's basis biasing this ensures that Eve is best to randomly select a basis instead ($r = \frac{1}{2}$).

For each click probability, the particular polarisations involved signify which parameters we use, as detailed in Appendix A1 and Appendix A2. The idler detector click probability (which corresponds to polarisation $\mathcal{X}$) is $\Pr_{I:\mathcal{X}}$. Where $\mathcal{X} \in \{\mathcal{X}_+, \mathcal{X}_-\}$, with $\mathcal{X}_+ \in \{H, V\}$ and $\mathcal{X}_- \in \{D, A\}$. For light untampered by Eve, Alice's signal detector click probability (which corresponds to polarisation $\mathcal{Z}$) conditioned by an idler click (for polarisation $\mathcal{X}$) is $\Pr_{S:\mathcal{Z}|I:\mathcal{X}}$. Where $\mathcal{Z} \in \{\mathcal{Z}_+, \mathcal{Z}_-\}$, with $\mathcal{Z}_+ \in \{H, V\}$ and $\mathcal{Z}_- \in \{D, A\}$. Whether this click probability corresponds to a correct or wrong coincidence click is determined by which $\mathcal{X}$ and $\mathcal{Z}$ is measured. A polarisation state for Eve $\mathcal{Y}$ is part of the set $\mathcal{Y} \in \{\mathcal{Y}_+, \mathcal{Y}_-\}$, with $\mathcal{Y}_+ \in \{\hat{h}, \hat{v}\}$ and $\mathcal{Y}_- \in \{\hat{d}, \hat{a}\}$. Section IIB provides more details about the polarisation basis elements for Eve, where we define θ_T which relates Eve's basis elements to Alice's basis elements. Eve's signal detector click probability (which corresponds to polarisation $\mathcal{Y}$) conditioned by an idler click (for polarisation $\mathcal{X}$) is $\Pr_{S:\mathcal{Y}|I:\mathcal{X}}(\theta_T)$. Eve does not have knowledge of the idler measurement, but the state she receives is still influenced by it. Alice's signal detector click probability when Eve's resent light is incident is $\Pr_{S:\mathcal{Z}|E:\mathcal{Y}}(\theta_T)$, this is where Alice records a click at her signal detector corresponding to polarisation $\mathcal{Z}$ and Eve had sent out a single-photon with polarisation $\mathcal{Y}$. Whether Alice registers the light that Eve resent as a correct or wrong

coincidence click is determined by which idler click ($\mathcal{X}$) and signal click ($\mathcal{Z}$) is measured.

Figure 1 is a beamsplitter diagram that shows how Alice's light (when the H/V basis is chosen) is spatially separated according to polarisation and measured at the idler detectors. It also shows that Alice's signal mode light is intercepted by Eve, where she decides upon her measurement basis (whether it is the $\hat{h}/\hat{v}$ basis as expanded upon in the figure, or the $\hat{d}/\hat{a}$ basis). Eve then spatially separates the light field corresponding to the basis eigenstates. For the polarisation degree of freedom this spatial separation can be done with a polarising beamsplitter (PBS). Figure 1 does not visualise the full real/false channel system, which is what Alice actually measures. As specified by Eq. 2 and Eq. 3 the real/false channel click probabilities can comprise of contributions from Alice, Eve and background noise. Therefore, Fig. 1 visualises a component of Eve's contribution. In particular, Fig. 1 visualises the beamsplitter model for the click probabilities for the idler detectors $\Pr_{I:\mathcal{X}_+}$ and the click probabilities for Eve's detectors $\Pr_{S:\mathcal{Y}_+|I:\mathcal{X}_+}(\theta_T)$. The system structure shown in Fig. 1 is equivalent to the scenario where the signal mode light is not intercepted by Eve if her detectors are replaced by Alice's signal H/V detectors and the correct basis decision is always made. In that situation Fig. 1 instead visualises the beamsplitter model for the click probabilities for the idler detectors $\Pr_{I:\mathcal{X}_+}$ and the click probabilities for Alice's signal detectors when her untampered light is incident $\Pr_{S:\mathcal{Z}_+|I:\mathcal{X}_+}$. Moreover, Fig. 1 shows that background noise is modelled by mixing Alice's light state and the background noise state at a beamsplitter and where the signal loss is encoded by the transmission parameter of the beamsplitters.

Figure 2 is a beamsplitter diagram which shows Alice's signal detectors when Eve's light is incident. Here, Alice's basis choice is predetermined from her idler measurement. Figure 2 is similar to Fig. 1 in that it visualises a sub-system of Eve's contribution to the real/false channel click probabilities. In particular, Fig. 2 visualises the beamsplitter model which we use to calculate the click probabilities for Alice's signal detectors which has Eve's light incident $\Pr_{S:\mathcal{Z}_+|E:\mathcal{Y}}(\theta_T)$. Appendix A1 details and groups the parameters relevant to the system, as visualised in both Fig. 1 and Fig. 2.

The attenuation of Alice's untampered light from the interaction with a target object is encoded by the signal attenuation factor ξ , with $\xi = 1$ signifying no attenuation. This is because the (possible) target object is situated in the direct pathway between Alice's light source and Alice's signal detectors: a route untampered by Eve. Whereas, the signal attenuation factor ξ_e is set by Eve and does not involve the target object. This is because, for our system, the target object is not situated in-between Alice light source and Eve or in-between Eve and Alice's signal detectors. The geometry of this object

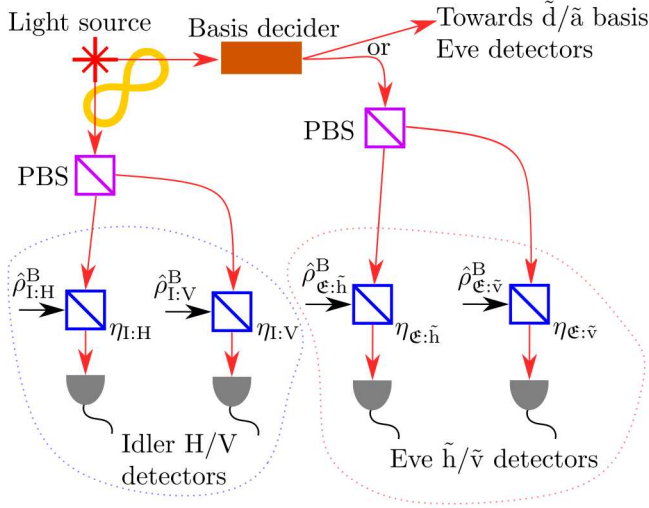


FIG. 1. Beamsplitter diagram of the intrusion of Eve upon Alice's signal mode light, if Alice measures in the H/V basis and Eve measures in her $\tilde{h}/\tilde{v}$ basis. This figure visualises the beamsplitter model which we use to calculate the click probabilities for the idler detectors $\Pr_{I:\mathcal{X}_+}$ and the click probabilities for Eve's detectors $\Pr_{S:\mathcal{Y}_+|I:\mathcal{X}_+}(\theta_T)$. The beamsplitter transmission parameter relevant to Alice's idler detectors or Eve's signal detectors is set by the corresponding detector quantum efficiency $\eta_{I/\mathcal{E}}$.

detection and range finding system is depicted in Fig. 8. Moreover, as shown in Appendix A1, there could be a different signal attenuation factor $\xi_{\mathcal{E}}$ for the light Eve resends towards the real and/or false channel from the signal attenuation factor of Alice's untampered light ξ .

For simplicity, we assume that the idler and Eve's detectors have minimal background noise incident. Therefore, we can disregard double coincidence clicks at each idler or each of Eve's detector. This assumption is justified if the idler detector system is shielded from the environment and if Eve's detector system is not subject to a jamming-attack which Alice's signal detectors may suffer from. Moreover, the inclusion of substantial background noise at Eve's detectors does not qualitatively affect how this protocol functions as Eve's policy of resending any light she measures means it will simply increase the background noise Alice experiences. We refer to a double (coincidence) click as an event in which both detectors corresponding to the eigenstates of the basis register a click. However, unlike for the idler and Eve's detectors, we cannot disregard the influence of double clicks for Alice's signal detectors: which can have substantial background noise incident. The double clicks include both correct and wrong coincidence clicks. The signal detector double click probability conditioned by an idler click (for polarisation $\mathcal{X}$) is $\Pr_{S:\mathcal{Z}_1, \mathcal{Z}_2|I:\mathcal{X}}$ and the signal detector double click probability resulting from the light sent

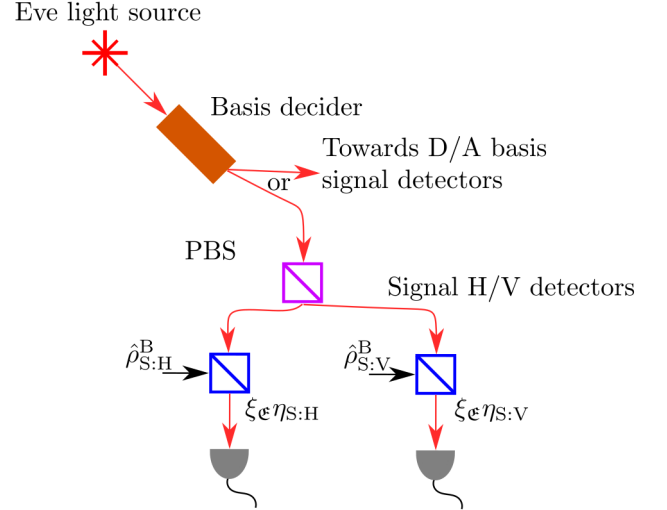


FIG. 2. Beamsplitter diagram of Alice's H/V signal detectors when Eve's light is incident. This choice of basis is predetermined from Alice's idler detector system not pictured. In this figure, the click probabilities for Alice's signal detectors relates to $\Pr_{S:\mathcal{Z}_+|E:\mathcal{Y}}(\theta_T)$. Here, the beamsplitter transmission parameter relevant to Alice's signal detectors is the product of the detector quantum efficiency η and signal attenuation (set by Eve) $\xi_{\mathcal{E}}$.

by Eve (for polarisation $\mathcal{Y}$) is $\Pr_{S:\mathcal{Z}_1, \mathcal{Z}_2|E:\mathcal{Y}}(\theta_T)$. Where $\mathcal{Z}_1, \mathcal{Z}_2 \in \{\mathcal{Z}_+\}$ or $\{\mathcal{Z}_-\}$.

We now denote the Eve and Alice contribution click probabilities as follows. The Alice/Eve ($\mathfrak{A}/\mathfrak{E}$) correct/wrong/double coincidence click probability is $\Pr_{c/w/wc}^{\mathfrak{A}/\mathfrak{E}}(\theta)$, where θ is the relative basis angle as detailed in Sect. II B. The background noise correct/wrong/double coincidence click probability is $\Pr_{c/w/wc}^B$. These are fully defined in Appendix A2. The background noise click probabilities for the real and false channels in principle could be different; however, we shall assume that they are equal for each channel.

However, it is the real or false channel that Alice measures, as the exact contribution of Alice and Eve are in practice unknown. Hence, we define the real/false channel $\mathfrak{R}/\mathfrak{F}$ correct/wrong/double coincidence click probability as $\Pr_{c/w/wc}^{\mathfrak{R}/\mathfrak{F}}(\theta)$. We are able to state the detection channel click probabilities in terms of the Alice and Eve contributions (and vice-versa). It is these click probabilities that we use to analyse the system henceforth. The correct/wrong/double click probabilities for the real and false channels, in terms of Alice, Eve and noise contributions are respectively

$$\Pr_{c/w/wc}^{\mathfrak{R}}(\theta) = (1 - p)\Pr_{c/w/wc}^{\mathfrak{A}} + p_{\mathfrak{R}}\Pr_{c/w/wc}^{\mathfrak{E}}(\theta) + p_{\mathfrak{F}}\Pr_{c/w/wc}^B, \quad (2)$$

$$\Pr_{c/w/wc}^{\mathfrak{F}}(\theta) = p_{\mathfrak{F}}\Pr_{c/w/wc}^{\mathfrak{E}}(\theta) + (1 - p_{\mathfrak{F}})\Pr_{c/w/wc}^B. \quad (3)$$

From the above equations, it is apparent that we have assumed that Eve's set of system parameters do not differ whether she sends light towards the real or false channel. It would be straightforward to adjust our definitions of the real and false channel click probabilities if the background noise and Eve system parameters differed between channels; however, this would complicate the following error analysis. Appendix A 1 details that each polarisation mode has its own set of parameters, such as background noise and detector quantum efficiency. Hence, unless stated otherwise, for the remainder of this paper we assume that all of Alice's polarisation modes share the same set of parameters. Similarly, all of Eve's polarisation modes share a different set of parameters. Due to this assumption, the relative basis angle θ is redundant as there is no difference in the detection statistics with varying the relative basis angle.

B. System security

In this section we describe how security is provided in our spoofing-resilient QI-based object detection and range finding protocol. As stated in the introduction, the security of our detection protocol is provided by the information advantage over Eve. The basis choice information advantage that Alice has is derived from the property of a basis set being mutually unbiased. For example, if Alice encodes a single-photon in an eigenstate in one basis of the set of mutually unbiased bases (MUB), then the measurement result in another basis within the set of MUB is randomly (and equally) distributed between the eigenstates of the measurement basis. Therefore, the information disadvantage that Eve has is due to her lack of knowledge of the selected basis. Eve's intercept-resend strategy can (on average) introduce errors to Alice's correlation measurements due to her wrong basis selection for the intercepted light. The consequent induced error in Alice's correlation measurements is the signature of the presence of Eve. It is in Eve's interest to minimise these wrong correlations. It is also implicit that Alice has to randomly change her basis, otherwise her security is based upon obscurity: which is highly vulnerable to becoming compromised if Eve was to discover that constant basis choice. We also assume that Eve is not technologically limited, that is they are able to produce a single-photon on demand in the degree of freedom of choice and that her measure and resend system can be effectively immediate.

Weaknesses in the security of our protocol can arise from the presence of multi-photons in Alice's source light. Eve can exploit this weakness with attacks such as described by Curty et. al [35]. However, as it is well-known that the benefit of QI-based protocols is more pronounced in the weak source mean photon number regime $\bar{n} \ll 1$. Hence, we assume that Alice's light is weak enough such that multi-photon contributions are negligible. Consequently, Alice's signal light only contains vacuum and

single-photon contributions and is immune from multi-photon-based attacks from Eve.

We will focus on the polarisation degree of freedom to realise the photonic encoding. In this paper, for Alice's MUB she uses the rectilinear basis and the diagonal basis. In terms of the bosonic creation operator $\hat{a}^\dagger$ the elements of Alice's rectilinear basis consists of the horizontal $\hat{a}_H^\dagger$ and vertical $\hat{a}_V^\dagger$ polarisations and the elements of Alice's diagonal basis consists of the diagonal $\hat{a}_D^\dagger = \frac{1}{\sqrt{2}}(\hat{a}_H^\dagger + \hat{a}_V^\dagger)$ and anti-diagonal $\hat{a}_A^\dagger = \frac{1}{\sqrt{2}}(-\hat{a}_H^\dagger + \hat{a}_V^\dagger)$ polarisations. We focus on polarisation as a degree of freedom as it is easy for Alice to produce a light source which has equal weighting between the elements of each basis for polarisation. However, in practice, polarisation could be unsuitable for object detection and range finding as the reflection coefficient of the target object for different polarisations may be different, depolarisation during transmission through an intermediate medium could occur or more significantly polarisation may not be preserved on reflection, even for normal incidence. However, if the target is a cooperative one then this may not be such an issue. Otherwise we could move to alternative degrees of freedom such as frequency or time-bin encoding.

Eve has her own MUB, the rectilinear ($\tilde{h}$ and $\tilde{v}$) basis and diagonal ($\tilde{d}$ and $\tilde{a}$) basis. However, her bases can differ from Alice's by a relative angle θ . For example, the relation of her MUB to Alice's is

$$\begin{aligned}\hat{a}_h^\dagger &= \cos(\theta)\hat{a}_H^\dagger + \sin(\theta)\hat{a}_V^\dagger, \\ &= \cos\left(\frac{\pi}{4} - \theta\right)\hat{a}_D^\dagger - \sin\left(\frac{\pi}{4} - \theta\right)\hat{a}_A^\dagger,\end{aligned}\quad (4)$$

$$\begin{aligned}\hat{a}_v^\dagger &= -\sin(\theta)\hat{a}_H^\dagger + \cos(\theta)\hat{a}_V^\dagger, \\ &= \sin\left(\frac{\pi}{4} - \theta\right)\hat{a}_D^\dagger + \cos\left(\frac{\pi}{4} - \theta\right)\hat{a}_A^\dagger,\end{aligned}\quad (5)$$

$$\begin{aligned}\hat{a}_d^\dagger &= \cos(\theta)\hat{a}_D^\dagger + \sin(\theta)\hat{a}_A^\dagger, \\ &= \cos\left(\frac{\pi}{4} - \theta\right)\hat{a}_V^\dagger + \sin\left(\frac{\pi}{4} - \theta\right)\hat{a}_H^\dagger,\end{aligned}\quad (6)$$

$$\begin{aligned}\hat{a}_{\tilde{a}}^\dagger &= -\sin(\theta)\hat{a}_D^\dagger + \cos(\theta)\hat{a}_A^\dagger, \\ &= \sin\left(\frac{\pi}{4} - \theta\right)\hat{a}_V^\dagger - \cos\left(\frac{\pi}{4} - \theta\right)\hat{a}_H^\dagger.\end{aligned}\quad (7)$$

We refer to the argument of the trigonometric functions as the total angle θ_T . This allows for both a possible $\frac{\pi}{4}$ shift and the relative basis angle θ to be considered when mapping from one basis to another. For example, if the relative basis angle $\theta = 0$, then the total angle $\theta_T = \frac{\pi}{4}$ is used to relate Eve's basis element $\tilde{a}$ to Alice's basis elements H and V. Conversely, the total angle $\theta_T = 0$ is used to relate Eve's basis element $\tilde{a}$ to Alice's basis elements D and A. The relations of her MUB to Alice's is also visualised in Fig. 3.

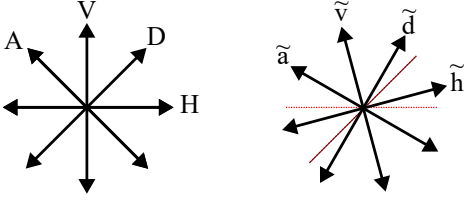


FIG. 3. Visual comparison of Alice's MUB to the MUB of Eve, for a relative basis angle $0 < \theta < \frac{\pi}{4}$.

C. Error analysis

The intrusion of Eve can introduce errors on average in Alice's detection statistics. If Eve only partially attacks ($p < 1$) then this reduces Alice's ability to recognise Eve's intrusion and hence counter her spoofing attempt. This section quantifies the error that Eve induces. In essence, for successful spoofing, Eve should make Alice believe that the false channel represents the true scene, instead of the real channel. In doing so she must ensure that the number of correct coincidence counts for the false channel is equal to or surpasses that for the real channel. However, in regimes without much double click influence, an increase of correct coincidence counts also increases the signature of her intrusion: wrong coincidence counts. A wise strategy for Eve is to resend some light towards the real channel to artificially raise the wrong coincidences; doing such will complicate Alice's attempts to exclude the false channel as it is no longer the sole channel containing the signature of Eve's intrusion.

We find a factor k which relates the correct coincidence click probability induced by Eve to the wrong coincidence probability. We also show that double click contributions can modify this relation. Moreover, we assume that the background noise is sufficiently static such that there can be accurate knowledge of it. We define k as

$$k = \frac{\Pr_c^E - \Pr_c^B}{\Pr_w^E - \Pr_w^B}. \quad (8)$$

For the following analysis, we assume that $k \geq 1$ and $\Pr_w^E - \Pr_w^B > 0$. As mentioned earlier, in general Alice does not know the Eve contribution click probabilities, but she can do a validity check that $\Pr_w^E(\xi) - \Pr_w^B > 0$ is true for any $0 < \xi \leq 1$. Instead, if $\Pr_w^E(\xi) - \Pr_w^B \leq 0$ for any $0 < \xi \leq 1$, Alice is particularly vulnerable to spoofing as double clicks contributions have caused the signature

of Eve's intrusion to be obscured by reducing the wrong coincidence click probability below what is expected from noise only.

Once the k -factor is calculated, the error (pertaining to Eve's noise-reduced contributions only) is

$$e_E = \frac{1}{k+1}. \quad (9)$$

The minimum of Eve's contribution error in previous literature is $e_E = 0.25$ [31]. Our analysis demonstrates this result for negligible double click regimes. However, we demonstrate that the influence of double clicks means that it is possible for $e_E < 0.25$. J. Heo et. al provide a threshold error rate e_T which instructs the minimal error to recognise spoofing in a partial attack [23, 26]. If Eve's interception is complete ($p = 1$) then $e_T = e_E$, otherwise for a partial spoofing attack ($p < 1$) the threshold error is lower $e_T < e_E$. We define the (noise-reduced) threshold error as

$$e_T = e_E \frac{p(\Pr^E - \Pr^B)}{p(\Pr^E - \Pr^B) + (1-p)(\Pr^A - \Pr^B)}, \quad (10)$$

where $\Pr^E = \Pr_w^E + \Pr_c^E$, $\Pr^A = \Pr_w^A + \Pr_c^A$ and $\Pr^B = \Pr_w^B + \Pr_c^B$. As Alice does not know the click probabilities, she instead must estimate the threshold error e_T from her detection statistics of the channels that she investigates.

For unknown click probabilities and proportions of intrusion, estimation of the threshold error is not straightforward as Alice cannot isolate the contributions from Eve and herself from the total detection statistics of the real and false channels. Due to this, there is an off-set between what Alice can measure and the threshold error; hence, we define the offset threshold error $e_{T,\text{off}}$ as

$$e_{T,\text{off}} = e_T + \text{offset}, \quad (11)$$

where

$$\text{offset} = \frac{(1-p)(\Pr_w^A - \Pr_w^B)}{p(\Pr^E - \Pr^B) + (1-p)(\Pr^A - \Pr^B)}. \quad (12)$$

If the idler detector background noise mean photon number $\bar{n}_{B,I} \approx 0$, then this ensures that Alice's noise-reduced wrong coincidence probability is $\Pr_w^A - \Pr_w^B \gtrless 0$, where less than zero is due to the influence of double clicks. Alice estimates the off-set threshold error from her detection statistics as

$$\hat{e}_{T,\text{off}} = \frac{(\hat{\Pr}_w^{\tilde{F}} - \Pr_w^B) + (\hat{\Pr}_w^{\mathfrak{A}} - \Pr_w^B)}{(\hat{\Pr}_w^{\tilde{F}} - \Pr_w^B) + (\hat{\Pr}_w^{\mathfrak{A}} - \Pr_w^B) + (\hat{\Pr}_c^{\tilde{F}} - \Pr_c^B) + (\hat{\Pr}_c^{\mathfrak{A}} - \Pr_c^B)}, \quad (13)$$

where $\hat{\Pr}_w^{\mathfrak{A}/\tilde{F}}$ is the measured real/false channel

wrong/correct coincidence click probability. Estimation

of k is straight-forward if there is a channel which has none of Alice's light, i.e. the false channel. However, Alice does not know a priori which (or if a) channel only contains light from Eve, therefore for both channels Alice estimates the respective k -factors, if possible. When $p_{\mathfrak{F}} > 0$ Alice estimates k as

$$\hat{k}_{\mathfrak{F}} = \frac{\hat{\text{Pr}}_{\text{c}}^{\mathfrak{F}} - \text{Pr}_{\text{c}}^{\text{B}}}{\hat{\text{Pr}}_{\text{w}}^{\mathfrak{F}} - \text{Pr}_{\text{w}}^{\text{B}}}. \quad (14)$$

Granted accurate estimation, from our definition of the false channel it is clear that $\hat{k}_{\mathfrak{F}} = k$, hence its suitability. If $p_{\mathfrak{R}} > 1$ Alice estimates the real channel k -factor as

$$\hat{k}_{\mathfrak{R}} = \frac{\hat{\text{Pr}}_{\text{c}}^{\mathfrak{R}} - \text{Pr}_{\text{c}}^{\text{B}}}{\hat{\text{Pr}}_{\text{w}}^{\mathfrak{R}} - \text{Pr}_{\text{w}}^{\text{B}}}, \quad (15)$$

where we assume $\hat{k}_{\mathfrak{R}} \geq 1$ and $\hat{\text{Pr}}_{\text{w}}^{\mathfrak{R}} - \text{Pr}_{\text{w}}^{\text{B}} > 0$. Later, we shall show how Alice can decide which channel (if any) contains light only from Eve and which channel (if any) contains her own light, which is possibly mixed with Eve's light.

However, if $p_{\mathfrak{F}} = 0$ accurate estimation of k must follow from an alternative method. Alice can estimate k by calculating

$$k(0 < \xi_{\mathfrak{E}} \leq 1) = \frac{\text{Pr}_{\text{c}}^{\mathfrak{E}}(0 < \xi_{\mathfrak{E}} \leq 1) - \text{Pr}_{\text{c}}^{\text{B}}}{\text{Pr}_{\text{w}}^{\mathfrak{E}}(0 < \xi_{\mathfrak{E}} \leq 1) - \text{Pr}_{\text{w}}^{\text{B}}}, \quad (16)$$

for range of values found by $0 < \xi \leq 1$. If there is a small relative error between $k(\xi_{\mathfrak{E}} \approx 0)$ and $k(\xi_{\mathfrak{E}} = 1)$, then Alice is able to estimate Eve's contribution error $e_{\mathfrak{E}}$. Although this method depends upon Alice knowing the system parameters (except for $\xi_{\mathfrak{E}}$) for Eve's detection system.

D. Recognition of Eve

In general, Alice does not know the signal detector click probabilities due to a lack of knowledge of the target object properties and/or the parameters used by Eve, therefore Alice depends upon what she measures for recognition of Eve's intrusion. By convention, we continue to refer to the channels as real and false, even if Alice does not know which is which a priori, or even if the real channel contains any of Alice's untampered light. This is because we define them from Eq. 2 and Eq. 3, where the real channel has the possibility of Alice's untampered light whereas the false channel does not. Prior to any decision-making about the presence of Eve and/or Alice's light, Alice checks if a channel $\mathfrak{G}$ has both noise-reduced wrong and correct coincidence click expectation values $\hat{\text{Pr}}_{\text{w/c}}^{\mathfrak{G}} - \text{Pr}_{\text{w/c}}^{\text{B}} = 0$. If this is true, then this absence of (additional) light infers that there is no target present there and/or Eve's light is entirely sent towards another channel.

Estimation of error values can help Alice recognise the presence of Eve. Alice initiates her attempt to recognise Eve's intrusion by checking if Eq. 13 (the measured offset threshold error) is greater than zero. If this is satisfied Alice has recognised the presence of Eve, but she has not said which channel(s) contains light from Eve. If the offset threshold error is $e_{\text{T,off}} \leq 0$ it is not as easy to recognise Eve's intrusion; Alice must instead look for discrepancies in the measured statistics. This approach is weaker for successful decision-making as it relies upon two layers of estimation. The discrepancy check method goes as follows. First, Alice checks if any channel has a positive noise-reduced wrong coincidence click expectation value: this infers the intrusion of Eve in that channel. If it is ruled out that any channel has a positive noise-reduced wrong coincidence click expectation value Alice uses the discrepancy method to check a channel which has a negative or approximately zero noise-reduced wrong coincidence click expectation value. For a channel $\mathfrak{G}$ which has a negative or approximately zero noise-reduced wrong coincidence click expectation value $\hat{\text{Pr}}_{\text{w}}^{\mathfrak{G}} - \text{Pr}_{\text{w}}^{\text{B}} \lesssim 0$ we assume that the correct coincidence click probability only contains Alice and noise contributions

$$\hat{\text{Pr}}_{\text{c}}^{\mathfrak{G}} = (1 - p^{\mathfrak{G}})\text{Pr}_{\text{c}}^{\mathfrak{A}}(\xi^{\mathfrak{G}}) + p^{\mathfrak{G}}\text{Pr}_{\text{c}}^{\text{B}}, \quad (17)$$

Alice now calculates the set of solutions with probability of channel $\mathfrak{G}$ intrusion $p^{\mathfrak{G}}$ and signal attenuation factor $\xi^{\mathfrak{G}}$ which satisfies Eq. 17. If there was no intrusion from Eve then the set of solutions $(p^{\mathfrak{G}}, \xi^{\mathfrak{G}})$ will also satisfy $(1 - p^{\mathfrak{G}})\text{Pr}_{\text{w}}^{\mathfrak{A}}(\xi^{\mathfrak{G}}) + p^{\mathfrak{G}}\text{Pr}_{\text{w}}^{\text{B}} = \hat{\text{Pr}}_{\text{w}}^{\mathfrak{G}}$ and if there was intrusion from Eve then $(1 - p^{\mathfrak{G}})\text{Pr}_{\text{w}}^{\mathfrak{A}}(\xi^{\mathfrak{G}}) + p^{\mathfrak{G}}\text{Pr}_{\text{w}}^{\text{B}} \neq \hat{\text{Pr}}_{\text{w}}^{\mathfrak{G}}$. This discrepancy check method requires that $\text{Pr}_{\text{w}}^{\mathfrak{E}} - \text{Pr}_{\text{w}}^{\text{B}} > 0$.

Once Alice has confirmed the intrusion or lack of intrusion from Eve on a channel she proceeds to determine whether or not there is a channel which contains her light (or not). It is this decision-making process which gives Alice a more potent form of spoofing resilience, the knowledge of which channel her trustworthy signal dwells in.

We begin with situations where the intrusion is complete $p = 1$, therefore $\hat{e}_{\text{off,T}} = e_{\mathfrak{E}}$ and Alice can conclude no channel contains her light. If $0 < p_{\mathfrak{R}} < 1$ and $0 < p_{\mathfrak{F}} < 1$, then the real and false channel k -factors are equal $\hat{k}_{\mathfrak{R}} = \hat{k}_{\mathfrak{F}}$ and both only include Eve's light. Alice can conclude that no channel contains her own light. If $p = p_{\mathfrak{F}} = 1$, then the real channel contains no additional light and the false channel only contains Eve's light, which leads Alice to the conclusion that no channel contains her light as $\hat{e}_{\text{off,T}} = e_{\mathfrak{E}}$. The same situation follows if $p = p_{\mathfrak{R}} = 1$, but instead the real channel contains Eve's light only. If an object is absent and there is complete intrusion $p = 1$ or incomplete intrusion $p < 1$, the same conclusions apply as the previous three examples, correspondingly. In other words, Alice is unable to distinguish between complete intrusion with an object

present and complete/incomplete intrusion when an object is absent. Alice can recognise the presence of Eve, but is unable to access any trustworthy signal. The remainder of our discussion about what conclusions Alice can make for different scenarios is only for when a target object is present.

Alice has the chance to decide which or if a channel contains her own light when the intrusion by Eve is incomplete $p < 1$ and hence the offset threshold error is $\hat{e}_{\text{off},T} < e_{\epsilon}$. When $p_{\mathfrak{F}} \neq p, 0$ and $p_{\mathfrak{R}} \neq p, 0$ then both the real channel and false channel contains light from Eve. If $\hat{\text{Pr}}_{\text{w}}^{\mathfrak{R}/\mathfrak{F}} - \text{Pr}_{\text{w}}^{\text{B}} > 0$ is true for both real and false channels then Alice decides that her light dwells in the channel with the larger k -factor, as $k_{\mathfrak{R}} > k_{\mathfrak{F}}$, as proven in Appendix B. Otherwise, if one channel has $\hat{\text{Pr}}_{\text{w}}^{\mathfrak{R}} - \text{Pr}_{\text{w}}^{\text{B}} < 0$, then Alice knows automatically that this channel contains her own light, due to the $\hat{\text{Pr}}_{\text{w}}^{\mathfrak{F}} - \text{Pr}_{\text{w}}^{\text{B}} > 0$ condition (implicitly) made earlier. If the intrusion is focused entirely on the false channel $p_{\mathfrak{F}} = p$ it is easy to conclude that the real channel has Alice's light as it is undisturbed, i.e. there is no discrepancy when Alice tests that channel for its wrong coincidence click probability. If the intrusion is focused entirely on the real channel $p_{\mathfrak{R}} = p$ Alice can see that the false channel has no additional light and she can exclude it. If there is a negative noise-reduced wrong coincidence click expectation value Alice knows that the real channel contains her own light. If there is a positive noise-reduced wrong coincidence click expectation value and Alice knows Eve's contribution error e_{ϵ} , Alice concludes that the real channel contains her own light as $\hat{e}_{\text{off},T} < e_{\epsilon}$.

The above analysis depends upon the requirement that $\text{Pr}_{\text{w}}^{\epsilon}(0 < \xi_{\epsilon} \leq 1) - \text{Pr}_{\text{w}}^{\text{B}} > 0$, otherwise Alice is vulnerable to spoofing. We now describe a scenario where this requirement is not satisfied (due to excessive background noise). The background noise in this scenario is not strong enough to constitute jamming as in theory Alice could detect the object if she knew which channel was real. Less background noise is required to ensure successful spoofing than successful jamming as the wrong coincidence count is smaller (and hence more vulnerable to being siphoned off by double clicks) than the correct coincidence clicks which enable object detection (the complete siphoning of correct coincidence clicks to double clicks would mean Eve has jammed us). For the parameter regimes such that $\text{Pr}_{\text{w}}^{\mathfrak{F}} - \text{Pr}_{\text{w}}^{\text{B}} < \text{Pr}_{\text{w}}^{\mathfrak{R}} - \text{Pr}_{\text{w}}^{\text{B}}$ and $\text{Pr}_{\text{c}}^{\mathfrak{F}} - \text{Pr}_{\text{c}}^{\text{B}} > \text{Pr}_{\text{c}}^{\mathfrak{R}} - \text{Pr}_{\text{c}}^{\text{B}}$ this would mean that Alice would be more inclined to believe that the false channel contains her own light rather than the real channel. In other words, Alice has been spoofed.

E. Removal of false information

Alice can remove false information if she knows which channel is false and that there is corresponding positive k -factor. For example, the noise-reduced trustworthy false

channel $\mathfrak{F}'$ correct coincidence click expectation value is

$$\text{Pr}^{\mathfrak{F}'|k_{\mathfrak{F}}} = (\text{Pr}_{\text{c}}^{\mathfrak{F}} - \text{Pr}_{\text{c}}^{\text{B}}) - k_{\mathfrak{F}}(\text{Pr}_{\text{w}}^{\mathfrak{F}} - \text{Pr}_{\text{w}}^{\text{B}}), \quad (18)$$

where from the above definitions it is clear that $\text{Pr}^{\mathfrak{F}'|k_{\mathfrak{F}}} = 0$, i.e. all of Eve's contribution has been removed and the background noise accounted for. If the real channel wrong noise-reduced coincidence click expectation value is $\text{Pr}_{\text{w}}^{\mathfrak{R}} - \text{Pr}_{\text{w}}^{\text{B}} > 0$ (because $p_{\mathfrak{R}} > 0$) Alice can attempt to remove untrustworthy information from this channel too. The noise-reduced trustworthy real channel $\mathfrak{R}'$ correct coincidence click expectation value is

$$\begin{aligned} \text{Pr}^{\mathfrak{R}'|k_{\mathfrak{F}}} &= (\text{Pr}_{\text{c}}^{\mathfrak{R}} - \text{Pr}_{\text{c}}^{\text{B}}) - k_{\mathfrak{F}}(\text{Pr}_{\text{w}}^{\mathfrak{R}} - \text{Pr}_{\text{w}}^{\text{B}}), \\ &= (1 - p)(\text{Pr}_{\text{c}}^{\mathfrak{R}} - \text{Pr}_{\text{c}}^{\text{B}}) - e(\text{Pr}^{\mathfrak{R}'|k_{\mathfrak{F}}}), \end{aligned} \quad (19)$$

where there is an erroneous term

$$e(\text{Pr}^{\mathfrak{R}'|k_{\mathfrak{F}}}) = k_{\mathfrak{F}}(1 - p)(\text{Pr}_{\text{w}}^{\mathfrak{R}} - \text{Pr}_{\text{w}}^{\text{B}}). \quad (20)$$

Information removal using the false channel k -factor $k_{\mathfrak{F}}$ results in Eq. 18 and Eq. 19 for the false and real channel, respectively. This results in the correct coincidence click expectation value of the (noise-reduced) false channel correctly being zero, it also results in the removal of Eve's contribution from the (noise-reduced) real channel correct coincidence click expectation value, albeit perturbed by $e(\text{Pr}^{\mathfrak{R}'|k_{\mathfrak{F}}})$. Here, we have assumed that there is a target object present and $p < 1$.

F. Performance analysis

For a set of parameters described in Appendix A 1 we show in Fig. 4 that there is an optimal choice of relative basis angle for Eve, whereby the optimal choice is the one which minimises the error rate of Eve's contributions $e_{\epsilon}(\theta)$. For this example, the optimal relative basis angle is $\theta = 0$. Eve could enact this optimisation granted she knows the entire set of parameters relevant to this system and its geometry. However, in general she does not have this information and shall randomly choose a relative basis angle.

We now compare Alice's QI light source with a weak-coherent state scenario. The weak-coherent state scenario uses a BB84-inspired prepare-and-measure scheme as described by Malik et. al. [19]. Appendix A 8 details the click probabilities used for the analysis with a weak-coherent state as Alice's source light. We define signal to noise (SNR) for the real/false channel as

$$\text{SNR}^{\mathfrak{R}/\mathfrak{F}} = \frac{\text{Pr}_{\text{c}}^{\mathfrak{R}/\mathfrak{F}} - \text{Pr}_{\text{c}}^{\text{B}} + \text{Pr}_{\text{w}}^{\mathfrak{R}/\mathfrak{F}} - \text{Pr}_{\text{w}}^{\text{B}}}{\text{Pr}_{\text{c}}^{\text{B}} + \text{Pr}_{\text{w}}^{\text{B}}}. \quad (21)$$

Figure 5 shows the QI and BB84 SNR for the real and false channels as a function of probability of interception

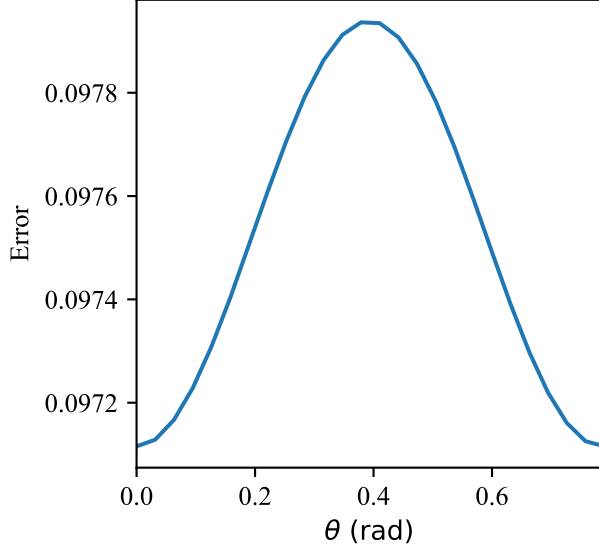


FIG. 4. The error rate of Eve's (isolated) contribution to Alice's detection statistics as a function of relative basis angle θ . For the parameter regime detailed in Appendix A 1 there is a minimal error for a particular relative basis angle θ . The quantum efficiencies of Eve's and Alice's signal detectors are all different, which causes the variation of the error rate shown.

p , where $p = p_{\mathcal{F}}$. When $p \approx 0.684$ the QI real and false channels have the same probability of correct coincidence click, this choice of p is wise for Eve as she does not unnecessarily induce extra wrong coincidence clicks. It is also apparent that the BB84-inspired system is inferior due to the low SNR compared to the QI system. Figure 6 shows the offset threshold error $e_{\text{off},T}$ for QI and BB84. The QI system is marginally better at the recognition of Eve's intrusion via her induced error. However, the noise-reduced technique is less realistic for BB84, as due to its high level of noise it would take far longer to sample an accurate estimate of the noise than it would for QI. Due to the advantage of the QI system over the BB84 one, we continue to focus on the QI one for the remainder of this paper.

G. Spoofing error thresholding

The above analysis depends upon accurate estimation of the underlying click probabilities from the detection statistics. However, Alice may be in a situation where such an accurate estimation is unavailable due to constrained integration times. In this section we describe the underlying distributions that Alice samples from. At the limit of many samples, our earlier approach for making

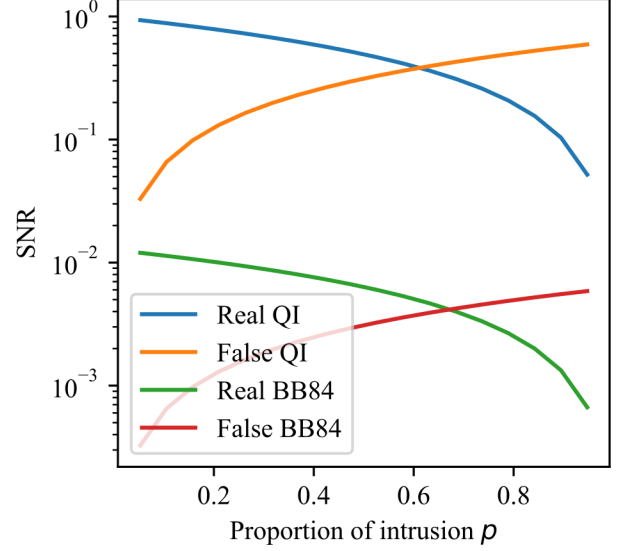


FIG. 5. SNR for the real and false channels as a function of probability of interception p . The parameter regime is detailed in Appendix A 1.

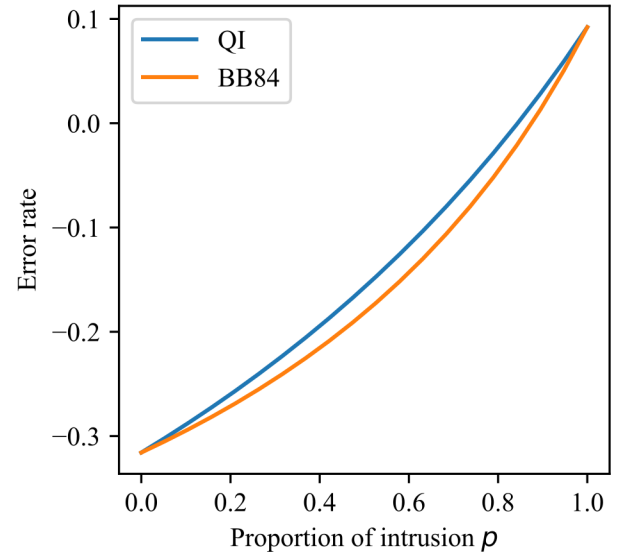


FIG. 6. Noise-reduced wrong coincidence click expectation value distributions for the real and false channels, for the parameter regime detailed in Appendix A 1.

conclusions about Eve's intrusion and for which channel Alice's signal data lies applies. Whereas from just one sample we show that such conclusions could be invalid due to the variances of the underlying distributions. In particular, the discrepancy check method is infeasible as it requires two accurate estimations.

For non-zero coincidence counts in both channels and when the requirement $\Pr_w^{\mathcal{E}} - \Pr_w^{\mathcal{B}} > 0$ is satisfied, an ex-

ample case of spoofing-vulnerability from limited sampling is that when the estimated false channel noise-reduced wrong coincidence expectancy is negative while the real channel is positive, Alice would be spoofed. From analysis of these distributions Alice can set thresholds on how much the possibility of spoofing is tolerable. If certain parameter regimes are within these spoofing thresholds for any value of the unknown signal attenuation factor, Alice can then ascertain that this parameter regime is spoofing-resilient even from a limited sample size of just one.

The object present distribution for the real and false channel is Poissonian, as is the background noise. The difference of these Poisson distributions is known as the Skellam distribution [36, 37]. There is a covariance for the two distributions (as the object present number of clicks is dependent upon the random variable for the number of background noise clicks). This covariance C is not trivial to find and we shall use our Monte-Carlo (M.C.) simulation for its calculation: the details of our simulation are in Appendix C. Hence, the noise-reduced real channel wrong coincidence click expectation value distribution is defined as

$$P(x, \mu_1, \mu_2) = e^{-\mu_1 - \mu_2} \left(\frac{\mu_1}{\mu_2} \right)^{\frac{x}{2}} I_{|x|}(2\sqrt{\mu_1 \mu_2}), \quad (22)$$

where x is the expected number of wrong coincidence clicks, $\mu_1 = N \Pr_w^{\mathfrak{R}} - C$ and $\mu_2 = N \Pr_w^{\mathfrak{B}} - C$, with N as the number of shots. Also $I_{|x|}$ is the modified Bessel function of the first kind. Figure 7 shows the real and false channel noise-reduced wrong coincidence click expectation value distributions when Eve only intrudes upon the false channel. Even when we have made the assumption that $\Pr_w^{\mathfrak{R}} - \Pr_w^{\mathfrak{B}} < 0$ we can see that there is the possibility of positive values for the real channel noise-reduced wrong coincidence click expectation value, which is at odds with the probability analysis section prior.

We can calculate the probability that some conclusions Alice makes about Eve's intrusion and the whereabouts of her own light are erroneous when sampling from a distribution rather than from the accurate expectation values as described in Sect. II D. An example conclusion Alice can threshold for is the probability that the noise-reduced false channel wrong coincidence expectation value is negative when the noise-reduced real channel wrong coincidence expectation value is positive $\Pr(\Pr_w^{\mathfrak{F}} - \Pr_w^{\mathfrak{B}} < 0 \mid \Pr_w^{\mathfrak{R}} - \Pr_w^{\mathfrak{B}} > 0)$. Another example of an erroneous conclusion is when both $\Pr_w^{\mathfrak{F}/\mathfrak{R}} - \Pr_w^{\mathfrak{B}} > 0$ Alice measures that $k_{\mathfrak{F}} > k_{\mathfrak{R}}$. The probability of this is stated as $\Pr(k_{\mathfrak{F}} > k_{\mathfrak{R}} > 0)$. Therefore, in both of these scenarios Alice erroneously concludes that the false channel contains her own light instead of the real channel. As explained earlier the discrepancy check is not feasible in this limited sampling situation, therefore Alice is unable to make decisions about the presence of Eve or

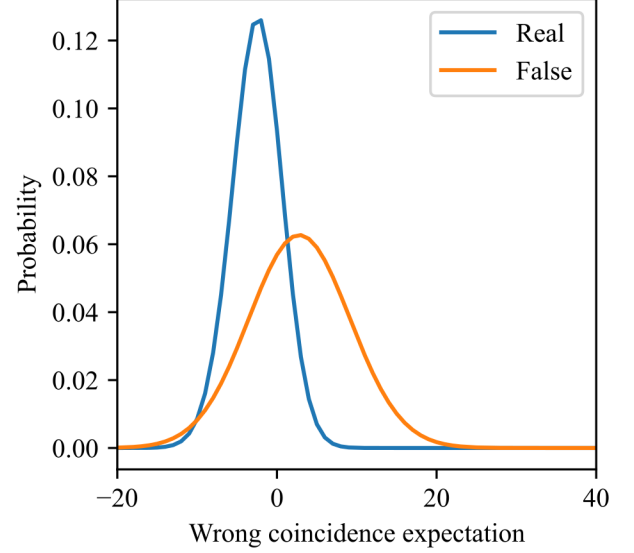


FIG. 7. Noise-reduced wrong coincidence click expectation value distributions for the real and false channels, for the parameter regime detailed in Appendix A 1. The noise-reduced wrong coincidence click expectation value is on the x-axis and the probability according to the expectation value is on the y-axis.

the whereabouts of her own light when she measures the off-set threshold error as $\hat{e}_{\text{off},T} \leq 0$.

When Alice measures that $\hat{e}_{T,\text{off}} \leq 0$ she does not recognise any intrusion by Eve. Erroneous conclusions can be made here with two possibilities. There is the probability that $\Pr(\Pr_w^{\mathfrak{R}} - \Pr_w^{\mathfrak{B}} > 0 \text{ and } \Pr_w^{\mathfrak{F}} - \Pr_w^{\mathfrak{B}} < 0 \mid \hat{e}_{T,\text{off}} \leq 0)$. There is also the probability that $\Pr(\Pr_w^{\mathfrak{F}} - \Pr_w^{\mathfrak{B}} \leq \Pr_w^{\mathfrak{R}} - \Pr_w^{\mathfrak{B}} < 0 \mid \hat{e}_{T,\text{off}} \leq 0)$.

III. RANGE FINDING CASE EXAMPLE

We simulate a situation where Eve attempts to temporally spoof Alice, i.e. spoof Alice's range finding decision-making. For simplicity, we assume that the real channel only includes Alice's untampered light and the signal detector background noise and the false channel only includes the tampered light and signal detector background noise. In other words we set $p_{\mathfrak{R}} = 0$ and $p_{\mathfrak{F}} = p$. We also assume that Alice effectively sends out the vacuum state to Eve for when Alice registers an idler no-click event. This is valid if the idler detector background noise $\bar{n}_{B,I} \approx 0$ and the idler detector quantum efficiency $\eta_I \approx 1$.

Figure 8 shows how Alice's light is redirected and delayed when Eve attempts temporal spoofing. The assumption that Eve is not technologically limited implies that the quantum efficiency of Eve's detectors are $\eta_{\mathfrak{E}} \approx 1$. The delay in time is δ , where we have discretised time in

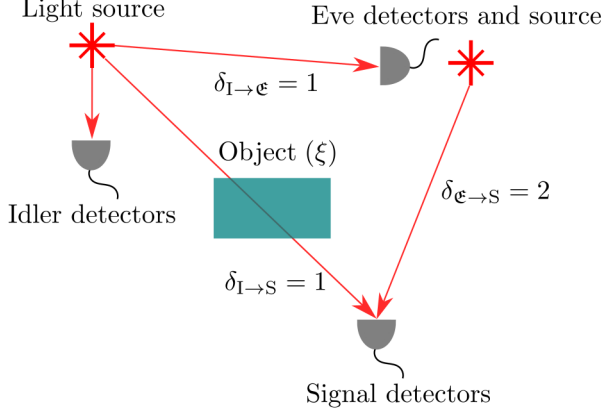


FIG. 8. Diagram of the pathways (and resulting delays) Alice's light can take when in the presence of Eve undertaking a temporal spoofing attempt. The delay in time is δ time-bins. The temporal spoofing by Eve delays the light incident upon Alice's signal detector by one time-bin. The influence of a possible target object lies in the direct pathway of Alice's light source and the signal detectors.

terms of time-bins which have the duration of a shot of the system. We can define the duration of a shot either artificially by the coincidence window size of Alice's coincidence counting hardware, or the repetition rate of a pulsed source, for example. Figure 8 shows that Eve is attempting to temporally spoof Alice by delaying the return light for the signal detectors by one time-bin ($\delta = 1$). Figure 8 also shows that the possible target object lies in the direct pathway of Alice's light source and the signal detectors. In our simulation we discard situations where a subsequent idler click initiates a real channel at time-bin z which already has a false channel initiated by a previous idler click. We refer to such events as polluted time-bins: these events are limited granted that $\bar{n} \ll 1$.

Figure 9 shows the noise-reduced wrong/correct coincidence click expectations for real and false channels. These distributions have been generated from 5000 runs of the M.C. simulation described in Appendix C. Inspecting the simulation data we can calculate the probabilities of erroneous conclusions with respect to the number of simulation runs. Alice does not recognise Eve's intrusion with the probability $\Pr(\hat{e}_{T,\text{off}} \leq 0) = 0.5104$. If Alice does not recognise spoofing she could proceed without realising the risk of being spoofed. Our simulation results for the probability of erroneous conclusions, given that spoofing is not recognised, is $\Pr(\Pr_w^{\mathfrak{R}} - \Pr_w^{\text{B}} > 0 \text{ and } \Pr_w^{\mathfrak{F}} - \Pr_w^{\text{B}} < 0 | \hat{e}_{T,\text{off}} \leq 0) = 0.0346$ and $\Pr(\Pr_w^{\mathfrak{F}} - \Pr_w^{\text{B}} \leq \Pr_w^{\mathfrak{R}} - \Pr_w^{\text{B}} < 0 | \hat{e}_{T,\text{off}} \leq 0) =$

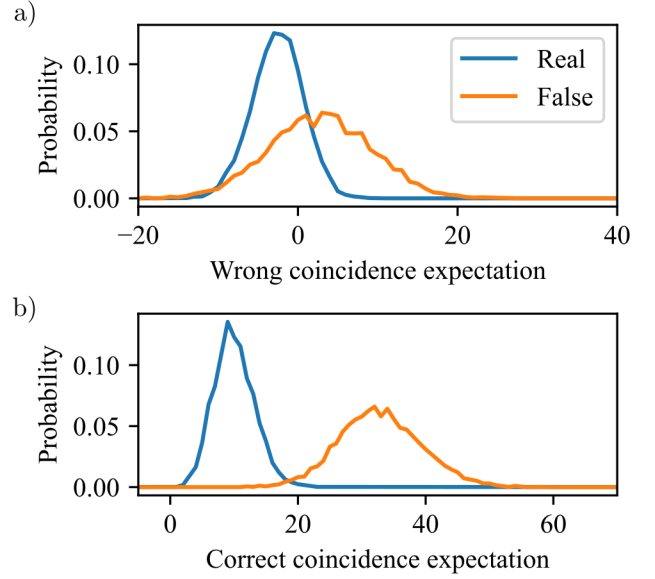


FIG. 9. a) Shows the noise-reduced wrong coincidence clicks expectation distributions for the real and false channels. The noise-reduced wrong coincidence click expectation value is on the x-axis and probability of that expectation value is on the y-axis. b) Shows the noise-reduced correct coincidence click expectation distributions for real and false. The noise-reduced correct coincidence click expectation value is on the x-axis and probability of that expectation value is on the y-axis. The parameter regime for this figure is detailed in Appendix A 1.

0.1668.

Even if Alice recognises Eve's intrusion there is probability that she is spoofed via $\Pr(\Pr_w^{\mathfrak{F}} - \Pr_w^{\text{B}} < 0 | \Pr_w^{\mathfrak{R}} - \Pr_w^{\text{B}} > 0) = 0.0222$. Lastly, the probability that Alice is spoofed via k -factor analysis is $\Pr(k_{\mathfrak{F}} > k_{\mathfrak{R}} > 0) = 0.07$.

IV. DISCUSSION

In this paper a theory for recognising and accounting for an intercept-resend spoofing attack by an intruder within the context of a simple-detection QI-based LIDAR protocol has been provided. Our model is written in terms of the Fock state formalism for the states of light and detectors involved and we include realistic features such as background noise and signal loss. We also benchmark our system performance with a classical illumination based protocol. This model extends the capabilities of our pre-existing jamming-resilient simple-detection QI-based LIDAR protocol [17].

Security when performing object detection and range finding can be provided when an imager sends their signal light in a degree of freedom which has the property of being an eigenstate of a basis in a set of mutually unbiased

bases. There is an information disadvantage that an intruder has as they do not know which basis was chosen by the imager. On average, the intruder will introduce errors in the light they resend (for certain parameter regimes) if they measure the imager's light that they intercept in the wrong basis. As we consider twin beam light - which is highly temporally-correlated - for our object detection and range finding system, the imager inspect the coincidence clicks of their locally sent light (idler) and the light sent towards the possible target object (signal). The imager can recognise that an intruder has attempted a spoofing attack by inspecting their detection statistics for wrong coincidence clicks. Where we define a wrong coincidence click as when the imager measures signal light in an eigenstate which was not correlated with their concurrent (to their chosen delay) idler light. We show that there are sets of system parameters which cause there to be an optimal relative basis angle an intruder can select for a minimised induced error. From the click probabilities that we calculate, we define error rates and signal-to-noise ratios. Analysis with these click probabilities can allow for the recognition of the spoofing attack. This analysis can also allow for finding the whereabouts of the imager's untampered light (if any) and the intruder light (if any). It can also allow for the removal of untrustworthy detector data. Furthermore, we compare the system performance of the QI- and classical illumination- based systems: the results of which reinforce the advantage of QI-based systems in the low signal strength and high background noise parameter regimes that we focus on.

Certain regimes can allow for a successful spoofing attack without also causing jamming to our object detection protocol. Such spoofing attacks will not be recognised by the conventional error analysis. However, this protocol provides an alternative method for recognising an attack by investigating if there is a discrepancy in the measured click probabilities against our expected click probabilities under the assumption there is no intruder present. In practice, accurate estimation of the system parameters is often impractical and hence the imager is constrained to limited sampling to make conclusions about the object detection and range finding situation. This analysis involves the difference of our object present and the noise-only click-count distributions, which invokes the use of the Skellam distribution. From analysing these distributions we provide thresholds for erroneous conclusions when constrained to limited sampling. This analysis allows for certain parameter regimes to be declared spoofing-resilient, as even from a limited sample the imager is able to ensure that the detector data conclusions are trustworthy.

As QI-based protocols are most advantageous in constrained signal strength regimes we need not worry about protocol weaknesses that arise from multi-photon contributions: assuming that we are in the weak signal strength limit. However, S. Johnson et. al. describe a potential attack where the imager's idler beam is compromised and an intruder can intercept it [27]. This attack would alter

the arrival time of the imager's idler photon while leaving its polarisation state unmeasured: therefore avoiding inducing any errors. This could lead to temporal spoofing which would be unrecognisable via the error or discrepancy methods. Although, current technology means that the success of this attack is low and would cause a drastic reduction of the imager's coincidence counting.

Further work could involve maximising the number of bases used for photonic encoding. For example, three is the maximum number of MUB for our 2-dimensional system [38]. For the polarisation degree-of-freedom the additional basis that we have not considered comprises of the left/right circular polarisation states. Beyond this, we could extend the dimensionality of our protocol's photonic encoding, which in turn would increase the maximum number of MUB. An increase of the number of MUB could reduce the likelihood that an intruder would successfully spoof the imager, as they would have a relatively larger information disadvantage. Furthermore, this protocol could be modified to have a non-adversarial application in the resilience to self-interference when performing object detection and range finding in complicated scenarios involving multiple targets (with correspondingly multiple signal echos). This could improve range finding as it would be harder for the imager's own return signals from previous time-bins to accidentally overlay with the imager's return signal at a desired delay, as their previous pulse in another basis has reflected from a more distant scatterer, for example. Lastly, in particular, single-photon underwater object detection and range finding could benefit from this resilience to self-interference due to the high level of backscattering by the medium [39].

ACKNOWLEDGEMENTS

The data presented in this work are available at [?]. The authors thank Jonathan D. Pritchard for useful discussions. The authors would also like to thank the UK Engineering and Physical Sciences Research Council for the partial funding of this work via the UK National Quantum Technology Programme and the Quantum Imaging Hub (Grant No. EP/T00097X/1).

Appendix A: Spoofing click probability

1. Parameters

This subsection groups and describes the many parameters in this system. It also states how the parameters are set for each non-schematic figure. As there is a detector for each basis element (polarisation), we can write the idler detector quantum efficiency as a vector $\eta_I = \{\eta_{I:H}, \eta_{I:V}, \eta_{I:D}, \eta_{I:A}\}$ and if all four polarisation channels have the same detector quantum efficiency then we can signify this as $\eta_I = \mathbf{0.001}$, for example. This

style of formatting will follow for the other applicable parameters.

There is also the Eve detector quantum efficiency $\eta_{\epsilon} = \{\eta_{\epsilon:\bar{h}}, \eta_{\epsilon:\bar{v}}, \eta_{\epsilon:\bar{d}}, \eta_{\epsilon:\bar{a}}\}$ and Alice's signal detector quantum efficiency $\eta_S = \{\eta_{S:H}, \eta_{S:V}, \eta_{S:D}, \eta_{S:A}\}$. The signal attenuation factor for Alice's untampered light is ξ and the signal attenuation factor which Eve sets for the resent light towards Alice is ξ_{ϵ} . The signal strength of the BB84 system is the mean photon number $\bar{n}_{\alpha}$. The mean photon number of the QI system is $\bar{n}$. To keep the comparison between the BB84 and QI system fair, the BB84 mean photon number relates to the QI mean photon number, under the condition of equal idler detector quantum efficiency over all polarisation channels, is $\bar{n} = \frac{\bar{n}_{\alpha}}{2 - \eta_I[0]\bar{n}_{\alpha} + 2\eta_I[0]\bar{n}_{\alpha}}$, where $\eta_I[0]$ is the first element from the idler detector quantum efficiency vector.

As per our beamsplitter model for incorporating noise and loss, we must rescale the background noise mean photon number by the reflection parameter of the beam-splitter in question. We define the idler detector background noise mean photon number vector as $\bar{n}_{B,I} = \{\frac{\bar{n}_{B,I:H}}{1 - \eta_{I:H}}, \frac{\bar{n}_{B,I:V}}{1 - \eta_{I:V}}, \frac{\bar{n}_{B,I:D}}{1 - \eta_{I:D}}, \frac{\bar{n}_{B,I:A}}{1 - \eta_{I:A}}\}$. The background noise mean photon number vector for Eve's detectors is $\bar{n}_{B,\epsilon} = \{\frac{\bar{n}_{B,\epsilon:\bar{h}}}{1 - \eta_{\epsilon:\bar{h}}}, \frac{\bar{n}_{B,\epsilon:\bar{v}}}{1 - \eta_{\epsilon:\bar{v}}}, \frac{\bar{n}_{B,\epsilon:\bar{d}}}{1 - \eta_{\epsilon:\bar{d}}}, \frac{\bar{n}_{B,\epsilon:\bar{a}}}{1 - \eta_{\epsilon:\bar{a}}}\}$. The background noise mean photon number vector for Alice's signal detectors when her untampered light is incident is $\bar{n}_{B,S} = \{\frac{\bar{n}_{B,S:H}}{1 - \eta_{S:H}\xi}, \frac{\bar{n}_{B,S:V}}{1 - \eta_{S:V}\xi}, \frac{\bar{n}_{B,S:D}}{1 - \eta_{S:D}\xi}, \frac{\bar{n}_{B,S:A}}{1 - \eta_{S:A}\xi}\}$. Lastly, the background noise mean photon number vector for Alice's signal detectors when Eve's resent light is incident is $\bar{n}_{B,S(\epsilon)} = \{\frac{\bar{n}_{B,S:H}}{1 - \eta_{S:H}\xi_{\epsilon}}, \frac{\bar{n}_{B,S:V}}{1 - \eta_{S:V}\xi_{\epsilon}}, \frac{\bar{n}_{B,S:D}}{1 - \eta_{S:D}\xi_{\epsilon}}, \frac{\bar{n}_{B,S:A}}{1 - \eta_{S:A}\xi_{\epsilon}}\}$.

There are also the parameters which specify the delays (in time-bins) for the temporal spoofing scenario we consider, as detailed in Sect. III. There is the delay from idler detectors to Alice's signal detectors $\delta_{I \rightarrow S}$, the delay from idler detectors to Eve's detectors $\delta_{I \rightarrow \epsilon}$ and the delay from Eve's detectors to Alice's signal detectors $\delta_{\epsilon \rightarrow S}$. However, as Alice does not know the specific delays which underlie the system we must define the delays they use for the two channels which they monitor. The real channel delay, from an idler click, is $\delta_{\Re}$ and the false channel delay, from an idler click is $\delta_{\Im}$. For the system considered here this relates to the aforementioned delay parameters as such $\delta_{\Re} = \delta_{I \rightarrow S}$ and $\delta_{\Im} = \delta_{I \rightarrow \epsilon} + \delta_{\epsilon \rightarrow S}$.

We can reduce the complexity of the event tree in our system by making some reasonable parameter assumptions. The possible combination of measurements from, for example, idler to Eve to Alice is a branch of the event tree. We assume that the idler background noise is $\bar{n}_{B,I} \ll 1$, as the idler arm can easily be shielded. This assumption means that the branch of the system event tree where Alice measures a double idler click (both detectors for a basis registering a click) is negligible and so this branch can be neglected. We place a stronger assumption on the idler detector background noise in Sect. II C, as this avoids the possibility of registering a wrong coincidence click due to a false measurement at the idler arm. Another assumption is that Alice's signal mean photon

number is $\bar{n} \ll 1$ due to the desire to avoid multi-photon contributions. This assumption means the rate of idler clicks is low and hence reduces the likelihood of polluted time-bins which complicate Alice's detection statistics. We define a polluted time-bin as when Eve resends light from a prior pulse of Alice's light or noise that they measure onto a channel which is populated by a subsequent pulse of Alice's light. For example, if Alice's first pulse defines a (first) real and false channel. Where Eve sends light to the first false channel. Then, Alice's second pulse defines a (second) real and false channel. If the second real channel overlaps with the first false channel we would refer to this as a polluted time-bin. The assumption that there is a limited number of polluted time-bins reduces the event tree complexity, as it means the statistics for Alice's two signal channels (real and false) are not dependent upon previous pulses of Alice's light or noise (that Eve measured) from earlier. We also assume that the background noise mean photon numbers for Eve's signal detectors are $\bar{n}_{B,\epsilon} \ll 1$, to ensure that double clicks are negligible for Eve's detectors. The number of polluted time-bins is also limited thanks to this assumption.

The parameters used in Fig. 4 are as follows $\eta_I = \mathbf{0.99999}$, $\eta_{\epsilon} = \{0.799, 0.099, 0.009, 0.989\}$, $\eta_S = \{0.201, 0.56, 0.07, 0.28\}$, $\bar{n} = 4.975 \times 10^{-3}$, $\xi_{\epsilon} = 0.1$, $\xi = 0.05$, $p_{\Re} = 0$, $p_{\Im} = p$, $\bar{n}_{B,I} = \mathbf{0.001}$, $\bar{n}_{B,\epsilon} = \mathbf{0.001}$, $\bar{n}_{B,S} = \{0.025, 0.0257, 0.0251, 0.0253\}$ and $\bar{n}_{B,S(\epsilon)} = \{0.0255, 0.0265, 0.0252, 0.0257\}$.

The parameters used in Fig. 5 and Fig. 6 are as follows $\eta_I = \mathbf{0.99999}$, $\eta_{\epsilon} = \mathbf{0.99999}$, $\eta_S = \mathbf{0.9}$, $\bar{n} = 4.975 \times 10^{-3}$, $\bar{n}_{\alpha} = 0.01$, $\xi_{\epsilon} = 0.4$, $\xi = 0.7$, $p_{\Re} = 0$, $p_{\Im} = p$, $\bar{n}_{B,I} = \mathbf{0.0001}$, $\bar{n}_{B,\epsilon} = \mathbf{0.0001}$, $\bar{n}_{B,S} = \mathbf{0.375}$ and $\bar{n}_{B,S(\epsilon)} = \mathbf{0.648}$.

The parameters used in Fig. 7 and Fig. 9 are as follows. $\eta_I = \mathbf{0.99999}$, $\eta_{\epsilon} = \mathbf{0.99999}$, $\eta_S = \mathbf{0.7}$, $\bar{n} = 4.975 \times 10^{-3}$, $\bar{n}_{\alpha} = 0.01$, $\xi_{\epsilon} = 0.4$, $\xi = 0.05$, $p_{\Re} = 0$, $p_{\Im} = p$, $\bar{n}_{B,I} = \mathbf{0.0001}$, $\bar{n}_{B,\epsilon} = \mathbf{0.0001}$, $\bar{n}_{B,S} = \mathbf{0.259}$, $\bar{n}_{B,S(\epsilon)} = \mathbf{0.347}$, $\delta_{I \rightarrow S} = 2$, $\delta_{I \rightarrow \epsilon} = 1$, and $\delta_{\epsilon \rightarrow S} = 2$.

2. Components

This subsection defines some components of the click probabilities for the QI system. The single-mode thermal state (which we use to model the background noise) is

$$\begin{aligned} \hat{\rho}_{\mathcal{Q}}^B(\bar{n}_B) &= \sum_{n=0}^{\infty} P(n, \bar{n}_B) |n\rangle \langle n|_{\mathcal{Q}}, \\ &= \sum_{n=0}^{\infty} \frac{\bar{n}_B^n}{(\bar{n}_B + 1)^{n+1}} |n\rangle \langle n|_{\mathcal{Q}}, \end{aligned} \quad (\text{A1})$$

where n is the photon number, $\mathcal{Q}$ is the mode and $\bar{n}_B$ is the corresponding mean photon number.

The following components are stated in general terms, such that they can have the relevant parameters substituted in for the click probability derivations. For example, we know which parameters to substitute in based off

the mode labelling and the particular click probability we are calculating. The beamsplitter transmission pa-

rameter is related to the reflectivity parameter as such $|t|^2 = 1 - |r|^2$. The first component is

$$\begin{aligned} \hat{\phi}(\bar{n}_{B:Q}, |t_Q|^2, \bar{n}_{B:W}, |t_W|^2) &= \sum_{q=0}^{\infty} P(q, \bar{n}_{B:Q}) \sum_{z=0}^q \binom{q}{z} |r_Q|^{2z} |t_Q|^{2(q-z)} \times \\ &\times \left(|t_Q|^2 (z+1) |z+1\rangle \langle z+1|_Q + |r_Q|^2 (q-z+1) |z\rangle \langle z|_Q \right) \otimes \hat{\rho}_W^B(|r_W|^2 \bar{n}_{B:W}), \end{aligned} \quad (A2)$$

where Q and W are mode labellings for the two elements in the chosen basis. This component (Eq. A2) describes the mixing of a single-photon with a thermal state in a tensor product with a thermal state in another mode. Throughout these appendices, the order of the mode labelling in the argument signifies which contains signal light mixed with background noise and which only contains background noise. In Eq. A2 we can see that mode Q contains signal light mixed with background noise and mode W only contains background noise.

We define the normalisation factor required due to the inclusion of loss and noise on the idler beam (derived from Eq. 1) as

$$\mathcal{N}_I = \text{Tr} \left(c_0 \hat{\rho}_Q^B(|r_Q|^2 \bar{n}_{B:Q}) \otimes \hat{\rho}_W^B(|r_W|^2 \bar{n}_{B:W}) + c_1 (\hat{\phi}(\bar{n}_{B:Q}, \eta_Q, \bar{n}_{B:W}, \eta_W) + \hat{\phi}(\bar{n}_{B:W}, \eta_W, \bar{n}_{B:Q}, \eta_Q)) \right). \quad (A3)$$

As Q and W signifies the idler beam basis elements here, then $\mathcal{J}$ and $\mathcal{K}$ signifies the signal mode basis elements. By convention $\mathcal{J}$ is the correlated mode to Q when $\theta_T = 0$. In general, however, the correlation of idler mode to signal mode is a function of θ_T according to Eq. 7. Hence, we can write Alice's state of light after the inclusion of noise and loss on the idler beam as

$$\begin{aligned} \hat{\rho}_{\text{NORM}} &= \frac{1}{\mathcal{N}_I} \left(c_0 \hat{\rho}_Q^B(|r_Q|^2 \bar{n}_{B:Q}) \otimes \hat{\rho}_W^B(|r_W|^2 \bar{n}_{B:W}) \otimes |0\rangle \langle 0|_{\mathcal{J}} \otimes |0\rangle \langle 0|_{\mathcal{K}} + \right. \\ &+ c_1 (\hat{\phi}(\bar{n}_{B:Q}, \eta_Q, \bar{n}_{B:W}, \eta_W) \otimes (\cos^2(\theta_T) |1\rangle \langle 1|_{\mathcal{J}} \otimes |0\rangle \langle 0|_{\mathcal{K}} + \sin^2(\theta_T) |0\rangle \langle 0|_{\mathcal{J}} \otimes |1\rangle \langle 1|_{\mathcal{K}}) + \\ &\left. + \hat{\phi}(\bar{n}_{B:W}, \eta_W, \bar{n}_{B:Q}, \eta_Q) \otimes (\sin^2(\theta_T) |1\rangle \langle 1|_{\mathcal{J}} \otimes |0\rangle \langle 0|_{\mathcal{K}} + \cos^2(\theta_T) |0\rangle \langle 0|_{\mathcal{J}} \otimes |1\rangle \langle 1|_{\mathcal{K}}) \right). \end{aligned} \quad (A4)$$

If there is a click for the Q mode and no-click for the W mode the vacuum contribution component (the sub-state associated with coefficient c_0) is

$$\text{vac}(Q) = \left(1 - \frac{1}{1 + |r_Q|^2 \bar{n}_{B:Q}} \right) \left(\frac{1}{1 + |r_W|^2 \bar{n}_{B:W}} \right). \quad (A5)$$

If there is a click for the Q mode and no-click for the W mode the single-photon contribution components (associated with coefficient c_1) are

$$\begin{aligned} a_{Q|1} &= \text{Tr} \left(\hat{\phi}(\bar{n}_{B:Q}, |t_Q|^2, \bar{n}_{B:W}, |t_W|^2) (\hat{1}_Q - |0\rangle \langle 0|_Q) \otimes |0\rangle \langle 0|_W \right), \\ &= \sum_{q=0}^{\infty} P(q, \bar{n}_{B:Q}) \left[\sum_{z=0}^q \binom{q}{z} |r_Q|^{2z} |t_Q|^{2(q-z)} \left(|t_Q|^2 (z+1) + |r_Q|^2 (q-z+1) \right) - |t_Q|^{2q} |r_Q|^2 (q+1) \right] \times \\ &\times \left(\frac{1}{1 + |r_W|^2 \bar{n}_{B:W}} \right), \end{aligned} \quad (A6)$$

and

$$\begin{aligned} a_{W|0} &= \text{Tr} \left(\hat{\phi}(\bar{n}_{B:W}, |t_W|^2, \bar{n}_{B:Q}, |t_Q|^2) (\hat{1}_Q - |0\rangle \langle 0|_Q) \otimes |0\rangle \langle 0|_W \right), \\ &= \sum_{q=0}^{\infty} P(q, \bar{n}_{B:W}) \left[|t_W|^{2q} |r_W|^2 (q+1) \right] \times \left(1 - \frac{1}{1 + |r_Q|^2 \bar{n}_{B:Q}} \right). \end{aligned} \quad (A7)$$

If there is a click for both Q and W the vacuum contribution is

$$\text{vac}(Q, W) = \left(1 - \frac{1}{1 + |r_Q|^2 \bar{n}_{B:Q}} \right) \left(1 - \frac{1}{1 + |r_W|^2 \bar{n}_{B:W}} \right), \quad (A8)$$

If there is a click for both $\mathcal{Q}$ and $\mathcal{W}$ the single-photon contribution component is

$$\begin{aligned} a_{\mathcal{Q},\mathcal{W}|1} &= \text{Tr} \left(\hat{\phi}(\bar{n}_{\mathcal{B}:\mathcal{Q}}, |t_{\mathcal{Q}}|^2, \bar{n}_{\mathcal{B}:\mathcal{W}}, |t_{\mathcal{W}}|^2) (\hat{1}_{\mathcal{Q}} - |0\rangle\langle 0|_{\mathcal{Q}}) \otimes (\hat{1}_{\mathcal{W}} - |0\rangle\langle 0|_{\mathcal{W}}) \right), \\ &= \sum_{q=0}^{\infty} P(q, \bar{n}_{\mathcal{B}:\mathcal{Q}}) \left[\sum_{z=0}^q \binom{q}{z} |r_{\mathcal{Q}}|^{2z} |t_{\mathcal{Q}}|^{2(q-z)} \left(|t_{\mathcal{Q}}|^2(z+1) + |r_{\mathcal{Q}}|^2(q-z+1) \right) - |t_{\mathcal{Q}}|^{2q} |r_{\mathcal{Q}}|^2(q+1) \right] \times \\ &\quad \times \left(1 - \frac{1}{1 + |r_{\mathcal{W}}|^2 \bar{n}_{\mathcal{B}:\mathcal{W}}} \right). \end{aligned} \quad (\text{A9})$$

We can see that these components are in terms of the two elements of a certain basis. These component definitions are useful for the sake of brevity in our derivations. The no-click component (when both mode $\mathcal{Q}$ and $\mathcal{W}$ does not register a click) for the noise-only contribution is

$$\text{vac}_0(\mathcal{Q}, \mathcal{W}) = \left(\frac{1}{1 + |r_{\mathcal{Q}}|^2 \bar{n}_{\mathcal{B},\mathcal{Q}}} \right) \left(\frac{1}{1 + |r_{\mathcal{W}}|^2 \bar{n}_{\mathcal{B},\mathcal{W}}} \right). \quad (\text{A10})$$

The no-click component for the single-photon contribution, where mode $\mathcal{Q}$ contains Alice's single photon and noise and mode $\mathcal{W}$ contains only noise is

$$a_{\mathcal{Q},\mathcal{W}|0} = \frac{1}{1 + |r_{\mathcal{W}}|^2 \bar{n}_{\mathcal{B},\mathcal{W}}} \sum_{m=0}^{\infty} \frac{\bar{n}_{\mathcal{B},\mathcal{Q}}^m}{(\bar{n}_{\mathcal{B},\mathcal{Q}} + 1)^{m+1}} |t_{\mathcal{Q}}|^{2m} |r_{\mathcal{Q}}|^2(m+1). \quad (\text{A11})$$

3. Idler

In the regime where the signal mean photon number $\bar{n} \ll 1$ and the idler detector background noise mean photon number $\bar{n}_{\mathcal{B},\mathcal{I}} \ll 1$ double coincidence idler clicks are negligible and so we focus only on events where there is a click for one mode and no-click for another.

If there is a click for $\mathcal{Q}$ and no-click for $\mathcal{W}$ the idler detector sub-system click probability is

$$\begin{aligned} \text{Pr}_{\mathcal{I}:\mathcal{Q}} &= \text{Tr} (\hat{\rho}_{\text{NORM}} (\hat{1}_{\mathcal{Q}} - |0\rangle\langle 0|_{\mathcal{Q}}) \otimes |0\rangle\langle 0|_{\mathcal{W}}), \\ &= \frac{c_0}{\mathcal{N}_{\mathcal{I}}} (\text{vac}(\mathcal{Q})) + \frac{c_1}{\mathcal{N}_{\mathcal{I}}} (a_{\mathcal{Q}|1} + a_{\mathcal{W}|0}). \end{aligned} \quad (\text{A12})$$

Measurement of the idler modes conditions the state which will be sent towards Eve or Alice. Of course, Eve does not have access to the idler mode measurement, but she could still receive this idler conditioned state. The idler click (click for $\mathcal{Q}$ and no-click for $\mathcal{W}$) conditioned state is

$$\begin{aligned} \hat{\rho}_{\mathcal{I}:\mathcal{Q}|1} &= \frac{\text{Tr}_{\mathcal{I}} (\hat{\rho}_{\text{NORM}} (\hat{1}_{\mathcal{Q}} - |0\rangle\langle 0|_{\mathcal{Q}}) \otimes |0\rangle\langle 0|_{\mathcal{W}})}{\text{Pr}_{\mathcal{I}:\mathcal{Q}}}, \\ &= \frac{1}{\text{Pr}_{\mathcal{I}:\mathcal{Q}}} \left(\frac{c_0}{\mathcal{N}_{\mathcal{I}}} (\text{vac}(\mathcal{Q}) |0\rangle\langle 0|_{\mathcal{J}} \otimes |0\rangle\langle 0|_{\mathcal{K}}) + \frac{c_1}{\mathcal{N}_{\mathcal{I}}} (q_2(\theta_{\text{T}}) |1\rangle\langle 1|_{\mathcal{J}} \otimes |0\rangle\langle 0|_{\mathcal{K}} + q_1(\theta_{\text{T}}) |0\rangle\langle 0|_{\mathcal{J}} \otimes |1\rangle\langle 1|_{\mathcal{K}}) \right), \end{aligned} \quad (\text{A13})$$

where we define

$$q_1(\theta_{\text{T}}) = a_{\mathcal{Q}|1} \sin^2(\theta_{\text{T}}) + a_{\mathcal{W}|0} \cos^2(\theta_{\text{T}}), \quad (\text{A14})$$

$$q_2(\theta_{\text{T}}) = a_{\mathcal{Q}|1} \cos^2(\theta_{\text{T}}) + a_{\mathcal{W}|0} \sin^2(\theta_{\text{T}}). \quad (\text{A15})$$

4. Signal

When the idler conditioned state (Eq. A13) is at the signal detector sub-system it has its basis elements sep-

arated and noise for each basis element mode included, we denote this state as $\hat{\rho}_{\mathcal{S}|\mathcal{I}:\mathcal{Q}}^{\text{UNNORM}}$. We normalise this state with normalisation factor $\mathcal{N}_{\mathcal{S}|\mathcal{I}:\mathcal{Q}} = \text{Tr} (\hat{\rho}_{\mathcal{S}|\mathcal{I}:\mathcal{Q}}^{\text{UNNORM}})$. Where this normalisation factor is

$$\mathcal{N}_{S|I:Q} = \frac{1}{\text{Pr}_{I:Q}\mathcal{N}_I} \left(c_0 \text{vac}(\mathcal{Q}) \hat{\rho}_{\mathcal{J}}^B(|r_{\mathcal{J}}|^2 \bar{n}_{B:\mathcal{J}}) \otimes \hat{\rho}_{\mathcal{K}}^B(|r_{\mathcal{K}}|^2 \bar{n}_{B:\mathcal{K}}) + c_1 (q_2(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2, \bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2) + q_1(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2, \bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2)) \right). \quad (\text{A16})$$

The normalised state incident upon the signal detector sub-system is

$$\begin{aligned} \hat{\rho}_{S|I:Q} &= \frac{\hat{\rho}_{S|I:Q}^{\text{UNNORM}}}{\mathcal{N}_{S|I:Q}}, \\ &= \frac{1}{\mathcal{N}_I \text{Pr}_{I:Q} \mathcal{N}_{S|I:Q}} \left(c_0 \text{vac}(\mathcal{Q}) \hat{\rho}_{\mathcal{J}}^B(|r_{\mathcal{J}}|^2 \bar{n}_{B:\mathcal{J}}) \otimes \hat{\rho}_{\mathcal{K}}^B(|r_{\mathcal{K}}|^2 \bar{n}_{B:\mathcal{K}}) + c_1 (q_2(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2, \bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2) + q_1(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2, \bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2)) \right). \end{aligned} \quad (\text{A17})$$

The following click probabilities can apply to Eve's signal detector or Alice's signal detector (if it is her untampered light incident). Hence, the click probability when signal detector for mode $\mathcal{J}$ clicks and $\mathcal{K}$ does not, when conditioned by an idler detector for mode $\mathcal{Q}$ click is

$$\begin{aligned} \text{Pr}_{S:\mathcal{J}|I:Q}(\theta_T) &= \text{Tr}(\hat{\rho}_{S|I:Q}(\hat{1}_{\mathcal{J}} - |0\rangle\langle 0|_{\mathcal{J}}) \otimes |0\rangle\langle 0|_{\mathcal{K}}), \\ &= \frac{1}{\mathcal{N}_I \text{Pr}_{I:Q} \mathcal{N}_{S|I:Q}} \left(c_0 \text{vac}(\mathcal{Q}) \text{vac}(\mathcal{J}) + c_1 (q_2(\theta_T) a_{\mathcal{J}|1} + q_1(\theta_T) a_{\mathcal{K}|0}) \right). \end{aligned} \quad (\text{A18})$$

The click probability when signal detector for mode $\mathcal{K}$ clicks and $\mathcal{J}$ does not, when conditioned by an idler detector for mode $\mathcal{Q}$ click is

$$\begin{aligned} \text{Pr}_{S:\mathcal{K}|I:Q}(\theta_T) &= \text{Tr}(\hat{\rho}_{S|I:Q}(\hat{1}_{\mathcal{K}} - |0\rangle\langle 0|_{\mathcal{K}}) \otimes |0\rangle\langle 0|_{\mathcal{J}}), \\ &= \frac{1}{\mathcal{N}_I \text{Pr}_{I:Q} \mathcal{N}_{S|I:Q}} \left(c_0 \text{vac}(\mathcal{Q}) \text{vac}(\mathcal{K}) + c_1 (q_2(\theta_T) a_{\mathcal{J}|0} + q_1(\theta_T) a_{\mathcal{K}|1}) \right). \end{aligned} \quad (\text{A19})$$

The click probability when both the signal detector for mode $\mathcal{K}$ and $\mathcal{J}$ clicks, when conditioned by an idler detector for mode $\mathcal{Q}$ click is

$$\begin{aligned} \text{Pr}_{S:\mathcal{J},\mathcal{K}|I:Q}(\theta_T) &= \text{Tr}(\hat{\rho}_{S|I:Q}(\hat{1}_{\mathcal{J}} - |0\rangle\langle 0|_{\mathcal{J}}) \otimes (\hat{1}_{\mathcal{K}} - |0\rangle\langle 0|_{\mathcal{K}})), \\ &= \frac{1}{\mathcal{N}_I \text{Pr}_{I:Q} \mathcal{N}_{S|I:Q}} \left(c_0 \text{vac}(\mathcal{Q}) \text{vac}(\mathcal{J}, \mathcal{K}) + c_1 (q_2(\theta_T) a_{\mathcal{J},\mathcal{K}|1} + q_1(\theta_T) a_{\mathcal{K},\mathcal{J}|1}) \right). \end{aligned} \quad (\text{A20})$$

The click probability for Eve when neither signal detector for the modes in the set $\mathcal{L} \in \{\mathcal{J}, \mathcal{K}\}$ clicks is

$$\begin{aligned} \text{Pr}_{S0:\mathcal{L}|I:Q}(\theta_T) &= \text{Tr}(\hat{\rho}_{S|I:Q}|0\rangle\langle 0|_{\mathcal{J}} \otimes |0\rangle\langle 0|_{\mathcal{K}}), \\ &= \frac{1}{\mathcal{N}_I \text{Pr}_{I:Q} \mathcal{N}_{S|I:Q}} \left(c_0 \text{vac}(\mathcal{Q}) \text{vac}_0(\mathcal{J}, \mathcal{K}) + c_1 (q_2(\theta_T) a_{\mathcal{J},\mathcal{K}|0} + q_1(\theta_T) a_{\mathcal{K},\mathcal{J}|0}) \right). \end{aligned} \quad (\text{A21})$$

The corresponding click probability for Alice is not considered, as Alice does not include her signal detector no-click events for her detection statistics, whereas the situation of Eve not resending a photon is relevant to what Alice (does and does not) receive.

As described earlier in this paper, Eve generates a single-photon corresponding to what she measures and she then sends this single-photon to Alice's signal detectors. We denote this as $\mathcal{J}_{\epsilon}$. There is the unnormalised state after the basis elements have been separated and noise in-

cluded at Alice's signal detector sub-system $\hat{\rho}_{S:\mathcal{J}|\mathcal{J}_{\epsilon}}^{\text{UNNORM}}$, which is normalised by $\mathcal{N}_{\epsilon} = \text{Tr}(\hat{\rho}_{S:\mathcal{J}|\mathcal{J}_{\epsilon}}^{\text{UNNORM}})$. Where this normalisation factor is defined as

$$\mathcal{N}_{\epsilon} = \cos^2(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2, \bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2) + \sin^2(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2, \bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2). \quad (\text{A22})$$

The resultant normalised state (where we have once again excluded off-diagonal terms) is

$$\begin{aligned}\hat{\rho}_{S:\mathcal{J}|E:\mathcal{J}_e} &= \frac{\hat{\rho}_{S:\mathcal{J}|E:\mathcal{J}_e}^{\text{UNNORM}}}{\mathcal{N}_e}, \\ &= \frac{1}{\mathcal{N}_e} \left(\cos^2(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2, \bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2) + \sin^2(\theta_T) \hat{\phi}(\bar{n}_{B:\mathcal{K}}, |t_{\mathcal{K}}|^2, \bar{n}_{B:\mathcal{J}}, |t_{\mathcal{J}}|^2) \right).\end{aligned}\quad (\text{A23})$$

The state (Eq. A23) thus depends on the relative basis angle and basis choice of Eve, where $\mathcal{J}_e$ corresponds to the mode $\mathcal{J}$ (as seen by Alice) when $\theta_T = 0$. The following click probabilities are for when Eve's resent light is incident upon Alice's signal detector subsystem. Hence, the click probability when the signal detector for mode $\mathcal{J}$ clicks and $\mathcal{K}$ does not click (when a single-photon $\mathcal{J}_e$ is sent) is

$$\begin{aligned}\text{Pr}_{S:\mathcal{J}|E:\mathcal{J}_e}(\theta_T) &= \text{Tr}(\hat{\rho}_{S:\mathcal{J}|E:\mathcal{J}_e}(\hat{1}_{\mathcal{J}} - |0\rangle\langle 0|_{\mathcal{J}}) \otimes |0\rangle\langle 0|_{\mathcal{K}}), \\ &= \frac{1}{\mathcal{N}_e} (\cos^2(\theta_T) a_{\mathcal{J}|1} + \sin^2(\theta_T) a_{\mathcal{K}|0}).\end{aligned}\quad (\text{A24})$$

The click probability when the signal detector for $\mathcal{K}$ clicks and $\mathcal{J}$ does not click is

$$\begin{aligned}\text{Pr}_{S:\mathcal{K}|E:\mathcal{J}_e}(\theta_T) &= \text{Tr}(\hat{\rho}_{S:\mathcal{J}|E:\mathcal{J}_e}(\hat{1}_{\mathcal{K}} - |0\rangle\langle 0|_{\mathcal{K}}) \otimes |0\rangle\langle 0|_{\mathcal{J}}), \\ &= \frac{1}{\mathcal{N}_e} (\cos^2(\theta_T) a_{\mathcal{J}|0} + \sin^2(\theta_T) a_{\mathcal{K}|1}).\end{aligned}\quad (\text{A25})$$

The click probability when the signal detector for both $\mathcal{J}$ and $\mathcal{K}$ clicks is

$$\begin{aligned}\text{Pr}_{S:\mathcal{J},\mathcal{K}|E:\mathcal{J}_e}(\theta_T) &= \text{Tr}(\hat{\rho}_{S:\mathcal{J}|E:\mathcal{J}_e}(\hat{1}_{\mathcal{K}} - |0\rangle\langle 0|_{\mathcal{K}}) \otimes (\hat{1}_{\mathcal{J}} - |0\rangle\langle 0|_{\mathcal{J}})), \\ &= \frac{1}{\mathcal{N}_e} (\cos^2(\theta_T) a_{\mathcal{J},\mathcal{K}|1} + \sin^2(\theta_T) a_{\mathcal{K},\mathcal{J}|1}).\end{aligned}\quad (\text{A26})$$

5. Alice

We define the untampered correct coincidence, wrong coincidence and double coincidence contributions from Alice in this section. The total angle is zero $\theta_T = 0$ for

these contributions as there is no relative basis angle and Alice always chooses the correct basis (therefore there will not be a $\frac{\pi}{4}$ shift). Therefore, we omit the θ_T notation for the contributions from Alice. The Alice contribution correct coincidence probability is

$$\text{Pr}_c^{\mathfrak{A}} = \frac{1}{2} \left(\sum_{\substack{i=1 \\ i \neq j}}^2 \text{Pr}_{I:\mathcal{X}_{+,i}} \text{Pr}_{S:\mathcal{X}_{+,j}|I:\mathcal{X}_{+,i}} + \sum_{i=1}^2 \text{Pr}_{I:\mathcal{X}_{\times,i}} \text{Pr}_{S:\mathcal{X}_{\times,i}|I:\mathcal{X}_{\times,i}} \right).\quad (\text{A27})$$

The Alice contribution wrong coincidence probability is

$$\text{Pr}_w^{\mathfrak{A}} = \frac{1}{2} \left(\sum_{i=1}^2 \text{Pr}_{I:\mathcal{X}_{+,i}} \text{Pr}_{S:\mathcal{X}_{+,i}|I:\mathcal{X}_{+,i}} + \sum_{\substack{i=1 \\ i \neq j}}^2 \text{Pr}_{I:\mathcal{X}_{\times,i}} \text{Pr}_{S:\mathcal{X}_{\times,j}|I:\mathcal{X}_{\times,i}} \right).\quad (\text{A28})$$

The Alice contribution double coincidence probability is

$$\text{Pr}_{wc}^{\mathfrak{A}} = \frac{1}{2} \left(\sum_{\substack{i=1 \\ i \neq j}}^2 \text{Pr}_{I:\mathcal{X}_{+,i}} \text{Pr}_{S:\mathcal{X}_{+,i},\mathcal{X}_{+,j}|I:\mathcal{X}_{+,i}} + \sum_{\substack{i=1 \\ i \neq j}}^2 \text{Pr}_{I:\mathcal{X}_{\times,i}} \text{Pr}_{S:\mathcal{X}_{\times,i},\mathcal{X}_{\times,j}|I:\mathcal{X}_{\times,i}} \right).\quad (\text{A29})$$

6. Eve

In this section we define the correct, wrong and double coincidence contributions from Eve upon Alice's sig-

nal detector. The Eve contribution correct coincidence probability is

7. Noise-only

As mentioned earlier, we assume that both channels have the same background noise. This section details the click probabilities when there is no object present. I.e. the background noise click probabilities. The background noise contribution correct coincidence click probability is

$$\begin{aligned} \Pr_c^B &= \frac{1}{2} \sum_{\substack{i=1 \\ i \neq j}}^2 \Pr_{I:\mathcal{X}_{+,i}} \text{vac}(\mathcal{X}_{+,j}) + \\ &+ \frac{1}{2} \sum_{i=1}^2 \Pr_{I:\mathcal{X}_{\times,i}} \text{vac}(\mathcal{X}_{\times,i}). \end{aligned} \quad (\text{A33})$$

The background noise contribution wrong coincidence click probability is

$$\begin{aligned} \Pr_w^B &= \frac{1}{2} \sum_{i=1}^2 \Pr_{I:\mathcal{X}_{+,i}} \text{vac}(\mathcal{X}_{+,i}) + \\ &+ \frac{1}{2} \sum_{\substack{i=1 \\ i \neq j}}^2 \Pr_{I:\mathcal{X}_{\times,i}} \text{vac}(\mathcal{X}_{\times,j}). \end{aligned} \quad (\text{A34})$$

The background noise contribution double coincidence click probability is

$$\begin{aligned} \Pr_{wc}^B &= \frac{1}{2} \sum_{\substack{i=1 \\ i \neq j}}^2 \Pr_{I:\mathcal{X}_{+,i}} \text{vac}(\mathcal{X}_{+,j}, \mathcal{X}_{+,i}) + \\ &+ \frac{1}{2} \sum_{\substack{i=1 \\ i \neq j}}^2 \Pr_{I:\mathcal{X}_{\times,i}} \text{vac}(\mathcal{X}_{\times,i}, \mathcal{X}_{\times,j}). \end{aligned} \quad (\text{A35})$$

8. BB84-inspired system

We compare our QI system with similar system which has a single-mode coherent state

$$\hat{\rho}_\alpha = e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |n\rangle\langle n| \quad (\text{A36})$$

as its light source, where we exclude off-diagonal terms due to the detectors we consider. The use of a weak coherent state is commonplace in a prepare-and-measure BB84 QKD system, therefore we refer to this QSI system as the BB84-inspired system. The architecture of this system is identical for the light Eve sends towards Alice and is similar to Fig. 1 sans the idler detector sub-system. This state of light has Poissonian photon statistics and we assume that the mean photon number $\bar{n}_\alpha = |\alpha|^2$ is small enough to ensure that there are no multi-photon contributions, where α is the amplitude of the coherent state. Therefore, the probability of the BB84-inspired system light source with 2-photons is negligible

$$P(2) = e^{-|\alpha|^2} \frac{|\alpha|^4}{2} \approx 0. \quad (\text{A37})$$

We truncate the single-mode coherent state such that it only has vacuum and single-photon contributions, therefore we must renormalise with the factor $\mathcal{N}_\alpha = \text{Tr}(e^{|\alpha|^2} \sum_{n=0}^1 \frac{|\alpha|^{2n}}{n!} |n\rangle\langle n|)$. The resulting state for the BB84-inspired system is

$$\hat{\rho}'_\alpha = c_0^\alpha |0\rangle\langle 0|_{\mathcal{Q}} + c_1^\alpha |1\rangle\langle 1|_{\mathcal{Q}}, \quad (\text{A38})$$

where $c_0^\alpha = \frac{e^{|\alpha|^2}}{\mathcal{N}_\alpha}$ and $c_1^\alpha = \frac{e^{|\alpha|^2} |\alpha|^2}{\mathcal{N}_\alpha}$ and as this is a prepare-and-measure scheme we have selected $\mathcal{Q}$ as the mode Alice sends her photon in. Alice's truncated state in terms of the basis $(\mathcal{J}, \mathcal{K})$ of the signal detectors (where once again $\theta_T = 0$ if it is for the untampered light pathway) is

$$\hat{\rho}'_\alpha = c_0^\alpha |0\rangle\langle 0|_{\mathcal{J}} \otimes |0\rangle\langle 0|_{\mathcal{K}} + c_1^\alpha (\cos^2(\theta_T) |1\rangle\langle 1|_{\mathcal{J}} \otimes |0\rangle\langle 0|_{\mathcal{K}} + \sin^2(\theta_T) |0\rangle\langle 0|_{\mathcal{J}} \otimes |1\rangle\langle 1|_{\mathcal{K}}). \quad (\text{A39})$$

This (unnormalised) state after the inclusion of noise and loss at the signal detector sub-system is

$$\begin{aligned} \hat{\rho}_{S:\alpha}^{\text{UNNORM}} &= c_0^\alpha \hat{\rho}_{\mathcal{J}}^B(|r_{\mathcal{J}}|^2 \bar{n}_{B,\mathcal{J}}) \otimes \hat{\rho}_{\mathcal{K}}^B(|r_{\mathcal{K}}|^2 \bar{n}_{B,\mathcal{K}}) + \\ &+ c_1^\alpha \left(\cos^2(\theta_T) \hat{\phi}(\bar{n}_{B,\mathcal{J}}, |t_{\mathcal{J}}|^2, \bar{n}_{B,\mathcal{K}}, |t_{\mathcal{K}}|^2) + \sin^2(\theta_T) \hat{\phi}(\bar{n}_{B,\mathcal{K}}, |t_{\mathcal{K}}|^2, \bar{n}_{B,\mathcal{J}}, |t_{\mathcal{J}}|^2) \right), \end{aligned} \quad (\text{A40})$$

after which we normalise this state, which results in $\hat{\rho}_{S:\alpha} = \hat{\rho}_{S:\alpha}^{\text{UNNORM}} / \mathcal{N}_{S:\alpha}$, where $\mathcal{N}_{S:\alpha} = \text{Tr}(\hat{\rho}_{S:\alpha}^{\text{UNNORM}})$. The following click probabilities apply for Eve or Alice's signal detectors (if it is untampered light incident at Alice's detectors). The click probability where the signal detector for mode $\mathcal{J}$ clicks and $\mathcal{K}$ does not is

$$\begin{aligned} \Pr_{S:\mathcal{J}|\alpha:\mathcal{Q}} &= \text{Tr}(\hat{\rho}_{S:\alpha} (\hat{1}_{\mathcal{J}} - |0\rangle\langle 0|_{\mathcal{J}}) \otimes |0\rangle\langle 0|_{\mathcal{K}}), \\ &= \frac{1}{\mathcal{N}_{S:\alpha}} \left(c_0^\alpha \text{vac}(\mathcal{J}) + c_1^\alpha (\cos^2(\theta_T) a_{\mathcal{J}|1} + \sin^2(\theta_T) a_{\mathcal{K}|0}) \right). \end{aligned} \quad (\text{A41})$$

The click probability where the signal detector for mode $\mathcal{K}$ clicks and $\mathcal{J}$ does not is

$$\begin{aligned} \text{Pr}_{\text{S};\mathcal{K}|\alpha;\mathcal{Q}} &= \text{Tr}(\hat{\rho}_{\text{S};\alpha}(\hat{1}_{\mathcal{K}} - |0\rangle\langle 0|_{\mathcal{K}}) \otimes |0\rangle\langle 0|_{\mathcal{J}}), \\ &= \frac{1}{\mathcal{N}_{\text{S};\alpha}} \left(c_0^\alpha \text{vac}(\mathcal{K}) + c_1^\alpha (\cos^2(\theta_{\text{T}}) a_{\mathcal{J}|0} + \sin^2(\theta_{\text{T}}) a_{\mathcal{K}|1}) \right). \end{aligned} \quad (\text{A42})$$

The click probability where the signal detector for both mode $\mathcal{J}$ and $\mathcal{K}$ clicks is

$$\begin{aligned} \text{Pr}_{\text{S};\mathcal{J},\mathcal{K}|\alpha;\mathcal{Q}} &= \text{Tr}(\hat{\rho}_{\text{S};\alpha}(\hat{1}_{\mathcal{J}} - |0\rangle\langle 0|_{\mathcal{J}}) \otimes (\hat{1}_{\mathcal{K}} - |0\rangle\langle 0|_{\mathcal{K}})), \\ &= \frac{1}{\mathcal{N}_{\text{S};\alpha}} \left(c_0^\alpha \text{vac}(\mathcal{J}, \mathcal{K}) + c_1^\alpha (\cos^2(\theta_{\text{T}}) a_{\mathcal{J},\mathcal{K}|1} + \sin^2(\theta_{\text{T}}) a_{\mathcal{K},\mathcal{J}|1}) \right). \end{aligned} \quad (\text{A43})$$

For click probability when neither of Eve's signal detectors for the modes in a set $\mathcal{L} \in \{\mathcal{J}, \mathcal{K}\}$ clicks is

$$\begin{aligned} \text{Pr}_{\text{S}0;\mathcal{L}|\alpha;\mathcal{Q}}(\theta_{\text{T}}) &= \text{Tr}(\hat{\rho}_{\text{S};\alpha}|0\rangle\langle 0|_{\mathcal{J}} \otimes |0\rangle\langle 0|_{\mathcal{K}}), \\ &= \frac{1}{\mathcal{N}_{\text{S};\alpha}} \left(c_0^\alpha \text{vac}_0(\mathcal{J}, \mathcal{K}) + c_1^\alpha (q_2(\theta_{\text{T}}) a_{\mathcal{J},\mathcal{K}|0} + q_1(\theta_{\text{T}}) a_{\mathcal{K},\mathcal{J}|0}) \right). \end{aligned} \quad (\text{A44})$$

The Alice's signal detector click probabilities when Eve's resent light is incident are the same for the BB84-inspired system as the QI system, as Alice's state of light does not affect the fact that Eve sends out a single photon in a mode instructed by her measurement. However, the click probabilities of contributions from Eve, Alice and noise will differ from the QI system. To note, the mode we prepare $\alpha : \mathcal{X}_{+/\times,i}$ is correlated with the signal detector mode $\text{S} : \mathcal{X}_{+/\times,i}$, for example. Hence, starting with Alice (and omitting the θ_{T} term), the Alice contribution correct coincidence click probability is

$$\text{Pr}_{\text{c}}^{\mathfrak{A};\alpha} = \frac{1}{4} \sum_{i=1}^2 (\text{Pr}_{\text{S};\mathcal{X}_{+,i}|\alpha;\mathcal{X}_{+,i}} + \text{Pr}_{\text{S};\mathcal{X}_{\times,i}|\alpha;\mathcal{X}_{\times,i}}). \quad (\text{A45})$$

The Alice contribution wrong coincidence click probability is

$$\text{Pr}_{\text{w}}^{\mathfrak{A};\alpha} = \frac{1}{4} \sum_{\substack{i=1 \\ i \neq j}}^2 (\text{Pr}_{\text{S};\mathcal{X}_{+,j}|\alpha;\mathcal{X}_{+,i}} + \text{Pr}_{\text{S};\mathcal{X}_{\times,j}|\alpha;\mathcal{X}_{\times,i}}). \quad (\text{A46})$$

Furthermore, the Alice contribution double coincidence click probability is

$$\text{Pr}_{\text{wc}}^{\mathfrak{A};\alpha} = \frac{1}{4} \sum_{\substack{i=1 \\ i \neq j}}^2 (\text{Pr}_{\text{S};\mathcal{X}_{+,i},\mathcal{X}_{+,j}|\alpha;\mathcal{X}_{+,i}} + \text{Pr}_{\text{S};\mathcal{X}_{\times,i},\mathcal{X}_{\times,j}|\alpha;\mathcal{X}_{\times,i}}). \quad (\text{A47})$$

We now move onto Eve, and the Eve contribution correct coincidence click probability is

$$\begin{aligned} \text{Pr}_{\text{c}}^{\mathfrak{E};\alpha}(\theta) &= \frac{1}{4} \sum_{\substack{i=1 \\ i \neq j}}^2 \left(r (\text{Pr}_{\text{S};\mathcal{X}_{+,i}|\text{E};\mathcal{Y}_{+,i}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{+,i}|\alpha;\mathcal{X}_{+,i}}(\theta_{\text{T}}) + \text{Pr}_{\text{S};\mathcal{X}_{+,i}|\text{E};\mathcal{Y}_{+,j}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{+,j}|\alpha;\mathcal{X}_{+,i}}(\theta_{\text{T}})) + \right. \\ &\quad + (1-r) (\text{Pr}_{\text{S};\mathcal{X}_{+,i}|\text{E};\mathcal{Y}_{\times,i}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{\times,i}|\alpha;\mathcal{X}_{+,i}}(\theta_{\text{T}}) + \text{Pr}_{\text{S};\mathcal{X}_{+,i}|\text{E};\mathcal{Y}_{\times,j}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{\times,j}|\alpha;\mathcal{X}_{+,i}}(\theta_{\text{T}})) + \\ &\quad + r (\text{Pr}_{\text{S};\mathcal{X}_{\times,i}|\text{E};\mathcal{Y}_{+,i}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{+,i}|\alpha;\mathcal{X}_{\times,i}}(\theta_{\text{T}}) + \text{Pr}_{\text{S};\mathcal{X}_{\times,i}|\text{E};\mathcal{Y}_{+,j}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{+,j}|\alpha;\mathcal{X}_{\times,i}}(\theta_{\text{T}})) + \\ &\quad + (1-r) (\text{Pr}_{\text{S};\mathcal{X}_{\times,i}|\text{E};\mathcal{Y}_{\times,i}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{\times,i}|\alpha;\mathcal{X}_{\times,i}}(\theta_{\text{T}}) + \text{Pr}_{\text{S};\mathcal{X}_{\times,i}|\text{E};\mathcal{Y}_{\times,j}}(\theta_{\text{T}}) \text{Pr}_{\text{S};\mathcal{Y}_{\times,j}|\alpha;\mathcal{X}_{\times,i}}(\theta_{\text{T}})) + \\ &\quad + \text{vac}(\mathcal{X}_{+,i}) (r \text{Pr}_{\text{S}0;\mathcal{Y}_{+}|\alpha;\mathcal{X}_{+,i}}(\theta_{\text{T}}) + (1-r) \text{Pr}_{\text{S}0;\mathcal{Y}_{+}|\alpha;\mathcal{X}_{+,i}}(\theta_{\text{T}})) + \\ &\quad \left. + \text{vac}(\mathcal{X}_{\times,i}) (r \text{Pr}_{\text{S}0;\mathcal{Y}_{+}|\alpha;\mathcal{X}_{\times,i}}(\theta_{\text{T}}) + (1-r) \text{Pr}_{\text{S}0;\mathcal{Y}_{\times}|\alpha;\mathcal{X}_{\times,i}}(\theta_{\text{T}})) \right). \end{aligned} \quad (\text{A48})$$

The Eve contribution wrong coincidence click probability is

$$\begin{aligned}
\Pr_w^{\mathcal{E}:\alpha}(\theta) = & \frac{1}{4} \sum_{\substack{i=1 \\ i \neq j}}^2 \left(r(\Pr_{S:\mathcal{X}_{+,j}|E:\mathcal{Y}_{+,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,i}|\alpha:\mathcal{X}_{+,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{+,j}|E:\mathcal{Y}_{+,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,j}|\alpha:\mathcal{X}_{+,i}}(\theta_T)) + \right. \\
& + (1-r)(\Pr_{S:\mathcal{X}_{+,j}|E:\mathcal{Y}_{\times,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,i}|\alpha:\mathcal{X}_{+,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{+,j}|E:\mathcal{Y}_{\times,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,j}|\alpha:\mathcal{X}_{+,i}}(\theta_T)) + \\
& + r(\Pr_{S:\mathcal{X}_{\times,j}|E:\mathcal{Y}_{+,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,i}|\alpha:\mathcal{X}_{\times,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{\times,j}|E:\mathcal{Y}_{+,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,j}|\alpha:\mathcal{X}_{\times,i}}(\theta_T)) + \\
& + (1-r)(\Pr_{S:\mathcal{X}_{\times,j}|E:\mathcal{Y}_{\times,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,i}|\alpha:\mathcal{X}_{\times,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{\times,j}|E:\mathcal{Y}_{\times,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,j}|\alpha:\mathcal{X}_{\times,i}}(\theta_T)) + \\
& + \text{vac}(\mathcal{X}_{+,j})(r \Pr_{S0:\mathcal{Y}_{+}|\alpha:\mathcal{X}_{+,i}}(\theta_T) + (1-r) \Pr_{S0:\mathcal{Y}_{\times}|\alpha:\mathcal{X}_{+,i}}(\theta_T)) + \\
& \left. + \text{vac}(\mathcal{X}_{\times,j})(r \Pr_{S0:\mathcal{Y}_{+}|\alpha:\mathcal{X}_{\times,i}}(\theta_T) + (1-r) \Pr_{S0:\mathcal{Y}_{\times}|\alpha:\mathcal{X}_{\times,i}}(\theta_T)) \right). \tag{A49}
\end{aligned}$$

The Eve contribution double coincidence click probability is

$$\begin{aligned}
\Pr_{wc}^{\mathcal{E}:\alpha}(\theta) = & \frac{1}{4} \sum_{\substack{i=1 \\ i \neq j}}^2 \left(r(\Pr_{S:\mathcal{X}_{+,i},\mathcal{X}_{+,j}|E:\mathcal{Y}_{+,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,i}|\alpha:\mathcal{X}_{+,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{+,i},\mathcal{X}_{+,j}|E:\mathcal{Y}_{+,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,j}|\alpha:\mathcal{X}_{+,i}}(\theta_T)) + \right. \\
& + (1-r)(\Pr_{S:\mathcal{X}_{+,i},\mathcal{X}_{+,j}|E:\mathcal{Y}_{\times,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,i}|\alpha:\mathcal{X}_{+,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{+,i},\mathcal{X}_{+,j}|E:\mathcal{Y}_{\times,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,j}|\alpha:\mathcal{X}_{+,i}}(\theta_T)) + \\
& + r(\Pr_{S:\mathcal{X}_{\times,i},\mathcal{X}_{\times,j}|E:\mathcal{Y}_{+,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,i}|\alpha:\mathcal{X}_{\times,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{\times,i},\mathcal{X}_{\times,j}|E:\mathcal{Y}_{+,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{+,j}|\alpha:\mathcal{X}_{\times,i}}(\theta_T)) + \\
& + (1-r)(\Pr_{S:\mathcal{X}_{\times,i},\mathcal{X}_{\times,j}|E:\mathcal{Y}_{\times,i}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,i}|\alpha:\mathcal{X}_{\times,i}}(\theta_T) + \Pr_{S:\mathcal{X}_{\times,i},\mathcal{X}_{\times,j}|E:\mathcal{Y}_{\times,j}}(\theta_T) \Pr_{S:\mathcal{Y}_{\times,j}|\alpha:\mathcal{X}_{\times,i}}(\theta_T)) + \\
& + \text{vac}(\mathcal{X}_{+,i}, \mathcal{X}_{+,j})(r \Pr_{S0:\mathcal{Y}_{+}|\alpha:\mathcal{X}_{+,i}}(\theta_T) + (1-r) \Pr_{S0:\mathcal{Y}_{\times}|\alpha:\mathcal{X}_{+,i}}(\theta_T)) + \\
& \left. + \text{vac}(\mathcal{X}_{\times,i}, \mathcal{X}_{\times,j})(r \Pr_{S0:\mathcal{Y}_{+}|\alpha:\mathcal{X}_{\times,i}}(\theta_T) + (1-r) \Pr_{S0:\mathcal{Y}_{\times}|\alpha:\mathcal{X}_{\times,i}}(\theta_T)) \right). \tag{A50}
\end{aligned}$$

The background noise contribution for BB84-inspired differs from QI also. The background noise correct coincidence click probability is equal to the wrong coincidence click probability and it is

$$\Pr_c^{\text{B}:\alpha} = \Pr_w^{\text{B}:\alpha} = \frac{1}{4} \sum_{i=1}^2 \left(\text{vac}(\mathcal{X}_{+,i}) + \text{vac}(\mathcal{X}_{\times,i}) \right). \tag{A51}$$

The background noise double coincidence click probability is

$$\begin{aligned}
\Pr_{wc}^{\text{B}:\alpha} = & \frac{1}{4} \sum_{\substack{i=1 \\ i \neq j}}^2 \left(\text{vac}(\mathcal{X}_{+,i}, \mathcal{X}_{+,j}) + \right. \\
& \left. + \text{vac}(\mathcal{X}_{\times,i}, \mathcal{X}_{\times,j}) \right). \tag{A52}
\end{aligned}$$

The real and false channel for the BB84 system is de-

fined as the QI system is, albeit with an appropriate substitution of the Alice/Eve/noise coincidence probabilities.

Appendix B: Proof

If Alice measures that both $\hat{\Pr}_w^{\mathfrak{A}/\mathfrak{F}} - \Pr_w^{\text{B}} > 0$, then she chooses the channel with the larger k-factor to be the one which contains her own light $k_{\mathfrak{A}} > k_{\mathfrak{F}}$. By definition, Alice's measurement of the false channel infers that $\Pr_c^{\text{B}} - \Pr_c^{\mathcal{E}} > \Pr_w^{\mathcal{E}} - \Pr_w^{\text{B}} > 0$.

We prove that $k_{\mathfrak{A}} > k_{\mathfrak{F}}$ is true by contradiction. Assume that $k_{\mathfrak{F}} > k_{\mathfrak{A}}$, using the k-factor definitions we can restate this as $k_{\mathfrak{F}} > k_{\mathfrak{F}} + g$, where g is a constant defined as

$$g = \frac{(\Pr_c^{\mathfrak{A}} - \Pr_c^{\text{B}})(\Pr_w^{\mathcal{E}} - \Pr_w^{\text{B}}) - (\Pr_c^{\mathcal{E}} - \Pr_c^{\text{B}})(\Pr_w^{\mathfrak{A}} - \Pr_w^{\text{B}})}{(\Pr_w^{\mathcal{E}} - \Pr_w^{\text{B}}) \left((\Pr_w^{\mathfrak{A}} - \Pr_w^{\text{B}}) + \frac{p_{\mathfrak{A}}}{1-p} (\Pr_w^{\mathcal{E}} - \Pr_w^{\text{B}}) \right)}, \tag{B1}$$

we can prove by contradiction as $k_{\mathfrak{F}} \not> k_{\mathfrak{F}} + g$ if $g >$

0, which can be done by showing that the numerator

and denominator of g are both positive. If we show that $\Pr_c^{\mathcal{A}}(0 < \xi < 1) - \Pr_c^{\mathcal{B}} > 0$, then the numerator of g is guaranteed to be positive as $\Pr_w^{\mathcal{A}} - \Pr_w^{\mathcal{B}} \leq 0$. The denominator of g equals the product of the denominators of $k_{\mathcal{F}}$ and $k_{\mathcal{A}}$, and if $\Pr_c^{\mathcal{A}}(0 < \xi < 1) - \Pr_c^{\mathcal{B}} > 0$ was shown, then the denominator of g must be positive, as $k_{\mathcal{A}} > 0$ and $k_{\mathcal{F}} > 0$.

Appendix C: Monte-Carlo

We have a M.C. simulation for the system we describe. This numerical approach means we can find the covariance of the noise contribution and the object present distribution which allows us to analyse the noise-reduced distributions. Instead of relying upon analysis with the expectation values only.

The number of idler clicks is a Poisson random variable

dictated by the idler click probability. The rest of the random variables in our simulation are conditionally dependent upon the number of idler clicks. If there has been enough simulation runs our resultant statistics matches with the analytic approach for the noise-reduced distributions to use the expected number of idler clicks. We do not consider the probability of interception p or probability of $p_{\mathcal{F}/\mathcal{A}}$ false/real channel interception as a random variable, as the dependence between the real and false channel is negligible when the background noise is much greater than the signal (from Alice and Eve) contribution $\bar{n} \ll \bar{n}_B$. We simulate the dependence of the random variable for the noise distribution and the object present distribution by using the same seed random number when sampling for both of these random variables. It is from this simulated dependence we can calculate the covariance. However, in practice, the clicks that originate from Alice/Eve or noise cannot be distinguished and so this dependence can only be calculated via our M.C. simulation.

-
- [1] S. Lloyd, *Science* **321**, 1463 (2008).
 - [2] S. H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, *Phys. Rev. Lett.* **101**, 253601 (2008).
 - [3] R. Nair and M. Gu, *Optica* **7**, 771 (2020).
 - [4] S. Guha and B. I. Erkmen, *Phys. Rev. A* **80**, 52310 (2009).
 - [5] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, *Phys. Rev. Lett.* **114**, 80503 (2015).
 - [6] Q. Zhuang, Z. Zhang, and J. H. Shapiro, *J. Opt. Soc. Am. B* **34**, 1567 (2017).
 - [7] E. D. Lopaeva, I. R. Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, *Phys. Rev. Lett.* **110**, 153603 (2013).
 - [8] J. Zhao, A. Lyons, A. C. Ulku, H. Defienne, D. Faccio, and E. Charbon, *Opt. Express* **30**, 3675 (2022).
 - [9] D. G. England, B. Balaji, and B. J. Sussman, *Phys. Rev. A* **99**, 23828 (2019).
 - [10] H. Liu, B. Balaji, and A. S. Helmy, *IEEE T. Aero. Elec. Sys.* **56**, 3529 (2020).
 - [11] H. Yang, W. Roga, J. D. Pritchard, and J. Jeffers, *Opt. Express* **29**, 8199 (2021).
 - [12] H. Yang, N. Samantaray, and J. Jeffers, *Phys. Rev. Appl.* **18**, 34021 (2022).
 - [13] S. Frick, A. McMillan, and J. Rarity, *Opt. Express* **28**, 37118 (2020).
 - [14] H. Kuniyil, H. Ozel, H. Yilmaz, and K. Durak, *J. Opt. (U. K.)* **24**, 105201 (2022).
 - [15] T. Gregory, P.-A. Moreau, E. Toninelli, and M. J. Padgett, *Sci. Adv.* **6**, eaay2652 (2020).
 - [16] T. Gregory, P.-A. Moreau, S. Mekhail, O. Wolley, and M. J. Padgett, *Sci. Rep.* **11**, 21841 (2021).
 - [17] R. J. Murchie, J. D. Pritchard, and J. Jeffers, *Phys. Rev. Appl.* **21**, 64008 (2024).
 - [18] M. P. Mrozowski, R. J. Murchie, J. Jeffers, and J. D. Pritchard, *Opt. Express* **32**, 2916 (2024).
 - [19] M. Malik, O. S. Magaña-Loaiza, and R. W. Boyd, *Appl. Phys. Lett.* **101**, 241103 (2012).
 - [20] W. Roga and J. Jeffers, *Phys. Rev. A* **94**, 32301 (2016).
 - [21] X. Yao, X. Liu, L. You, Z. Wang, X. Feng, F. Liu, K. Cui, Y. Huang, and W. Zhang, *Phys. Rev. A* **98**, 63816 (2018).
 - [22] Y.-B. Zhao, W.-L. Zhang, D. Wang, X.-T. Song, L.-J. Zhou, and C.-B. Ding, *Chin. Phys. B* **28**, 104203 (2019).
 - [23] J. Heo, J. Kim, T. Jeong, Y. S. Ihn, D. Y. Kim, Z. Kim, and Y. Jo, *Optica* **10**, 1461 (2023).
 - [24] T. Jennewein, R. Tannous, W. Wu, D. Sinar, S. Vinet, A. Kirillova, S. Sajeed, A. Ling, and C. Perumangatt, in *Optica Quantum 2.0 Conference and Exhibition* (Optica Publishing Group, 2023) p. QW3A.2.
 - [25] D. Wang, J.-Y. Zhao, Y.-C. Wang, L.-J. Zhou, and Y.-B. Zhao, *Sci. Rep.* **14**, 22058 (2024).
 - [26] J. Heo, T. Jeong, N. H. Park, and Y. Jo, *APL Photonics* **9**, 076111 (2024).
 - [27] S. Johnson, J. Rarity, and M. Padgett, *Sci. Rep.* **14**, 11579 (2024).
 - [28] T. P. Espinoza, S. C. Carrasco, J. Rogan, J. A. Valdivia, and V. S. Malinovsky, *Phys. Rev. Res.* **6**, 43214 (2024).
 - [29] Y. Wang, G. Smith, and A. May, *Secure quantum ranging* (2025).
 - [30] C. H. Bennett and G. Brassard, *Theor. Comput. Sci.* **560**, 7 (2014).
 - [31] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptol.* **5**, 3 (1992).
 - [32] B. Huttner and A. K. Ekert, *J. Mod. Opt.* **41**, 2455 (1994).
 - [33] J. N. Blakely and S. D. Pethel, *Phys. Rev. Res.* **4**, 23178 (2022).
 - [34] J. N. Blakely, S. D. Pethel, K. R. Stewart, and K. Jacobs, *arXiv:quant-ph/2410.08353* (2024).
 - [35] M. Curty and N. Lütkenhaus, *Phys. Rev. A* **69**, 42321 (2004).
 - [36] J. G. Skellam, *J. R. Stat. Soc.* **109**, 296 (1946).

[37] D. Karlis and I. Ntzoufras,
J. R. Stat. Soc., Series D **52**, 381 (2003).
[38] W. K. Wootters and B. D. Fields,
Ann. Phys. (N.Y.) **191**, 363 (1989).

[39] A. Maccarone, K. Drummond, A. McCarthy, U. K. Stein-
lehner, J. Tachella, D. A. Garcia, A. Pawlikowska, R. A.
Lamb, R. K. Henderson, S. McLaughlin, Y. Altmann,
and G. S. Buller, Opt. Express **31**, 16690 (2023).