Source Engineering for Quantum Key Distribution with Noisy Photon-Added Squeezed States

Andrea Giani[*], Moe Z. Win[†], and Andrea Conti[*]

[*]Department of Engineering and CNIT, University of Ferrara, Via Saragat 1, 44122 Ferrara, Italy
(e-mail: andrea.giani@unife.it, a.conti@ieee.org)
[†]Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139 USA
(e-mail: moewin@mit.edu)

ICC 2023 - IEEE International Conference on Communications | 978-1-5386-7462-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICC45041.2023.10279710

***Abstract*—Quantum key distribution (QKD) is a key enabler toward unconditionally secure communications. The imperfections exhibited by non-ideal sources degrade the QKD performance. This raises the problem of engineering the employed quantum states to mitigate the impairments caused by such imperfections. This paper proposes to employ noisy photon-added squeezed states (PASSs) as QKD sources for the decoy-state protocol. First, noisy PASSs are characterized in the Fock space. Then, noisy PASSs are engineered for the decoy-state protocol. Finally, the performance of the decoy-state protocol with engineered noisy PASSs are quantified in a variety of settings.**

***Index Terms*—Quantum key distribution, quantum state engineering, photon-added squeezed state, quantum noise.**

I. Introduction

Quantum key distribution (QKD) [1] allows two entities, namely Alice and Bob, to generate and exchange secure keys for establishing unconditionally secure communications even in the presence of an eavesdropper, namely Eve [2]–[4]. The unconditional security relies on the exploitation of the peculiar properties of quantum mechanics [5]–[8]. While the original Bennett-Brassard 1984 (BB84) protocol considers an ideal single-photon source (SPS), applications with non-ideal sources have been developed with satisfactory performance [9]–[18]. The metrics typically used for assessing the performance of the BB84 protocol are the secure transmission distance and the secure key generation rate. However, in some practical scenarios, imperfections exhibited by quantum systems can be exploited by Eve to gain information about the key, thus compromising the communication security. In particular, when Alice employs a non-ideal source (i.e., not behaving as an ideal SPS), the BB84 is susceptible to a photon-number-splitting (PNS) attack [19]–[21]. Therefore, characterizing the BB84 protocol performance is difficult when accounting for both the employed QKD sources and the imperfections of the communication systems.

In the literature, the BB84 protocol has been investigated and its unconditional security has been proven [5]–[8]. To overcome the security challenges caused by the use of a non-ideal SPS, the decoy-state protocol was proposed [22]–[25], and characterized for several noiseless sources, namely coherent and weak coherent states [22]–[27], modified coherent states [28], heralded single-photon states [29]–[31], and single photon-added coherent states [32]. However, a general approach to engineer a variety of QKD sources for the decoy-state protocol is still missing.

This paper proposes the use of noisy photon-added squeezed states (PASSs) as QKD sources for the decoy-state protocol.[1] The fundamental questions related to the use of noisy PASSs for QKD are: how does the noise in state preparation affect QKD performance; and how to engineer noisy PASSs for QKD? The answers to these questions provide insights to engineer non-ideal sources for mitigating impairments that degrade QKD performance. The goal of this paper is to improve the performance of the decoy-state protocol by engineering noisy PASSs used as QKD sources. The key contributions can be summarized as follows: (i) characterize noisy PASSs in the Fock space; (ii) describe the decoy-state protocol with noisy PASSs; and (iii) quantify the performance of the decoy-state protocol employing engineered noisy PASSs.

The remaining sections are organized as follows: Section II describes the decoy-state protocol and defines noisy PASSs. Section III characterizes noisy PASSs in the Fock space. Section IV describes the decoy-state protocol with engineered noisy PASSs. Section V presents the case studies. Finally, Section VI gives our conclusions.

Notations: Operators are denoted by uppercase letters. For example, an operator is denoted by $\boldsymbol{X}$. The sets of complex numbers and of positive integer numbers are denoted by $\mathbb{C}$ and $\mathbb{N}$, respectively. For $z \in \mathbb{C}$: $|z|$ denotes the absolute value; z^* denotes the complex conjugate; and $\imath = \sqrt{-1}$. The trace and the adjoint of an operator are denoted by $\mathrm{tr}\{\cdot\}$ and $(\cdot)^\dagger$, respectively. The annihilation and the creation operators are denoted by $\boldsymbol{A}$ and $\boldsymbol{A}^\dagger$, respectively. The displacement operator with parameter $\mu \in \mathbb{C}$ is $\boldsymbol{D}_\mu = \exp\left\{\mu\boldsymbol{A}^\dagger - \mu^*\boldsymbol{A}\right\}$. The squeezing operator with parameter $\zeta \in \mathbb{C}$ is $\boldsymbol{S}_\zeta = \exp\left\{\frac{1}{2}\zeta(\boldsymbol{A}^\dagger)^2 - \frac{1}{2}\zeta^*\boldsymbol{A}^2\right\}$. The squeezing parameter $\zeta \in \mathbb{C}$ can equivalently be written as $\zeta = re^{\imath\varphi}$, with $r \geqslant 0$ and $-\pi < \varphi \leqslant \pi$. For $z, z_0 \in \mathbb{C}$, $z \to z_0$ denotes the limit as z approaches z_0. The hyperbolic sine and the hyperbolic cosine are denoted by $\sinh(x)$ and $\cosh(x)$, respectively. The Hermite polynomial of degree n is denoted by $H_n(x)$. The adjugate of a matrix is denoted by $\mathrm{adj}(\cdot)$.

[1] PASSs affected by thermal noise during state preparation are referred to as noisy PASSs.

978-1-5386-7462-8/23/$31.00 ©2023 IEEE

II. Preliminaries

This section provides some preliminaries used in the remainder of the paper.

A. Decoy-State Protocol

In practical BB84 implementations, Alice's non-ideal source exhibits a non-zero probability of emitting multi-photon states. In such condition, Eve can retain extra photons by performing a PNS attack, without changing the physical characteristics of the states, thus gathering information about the key. Unfortunately, the PNS technique compromises the BB84 unconditional security when the quantum channel does not exhibit sufficiently small losses [8], [19]–[21]. To cope with this security challenge, the decoy-state protocol was proposed [22]–[25]. The idea of the decoy-state protocol is that Alice employs additional states, namely decoy states, with different intensities (i.e., mean numbers of photons). Such decoy states are randomly interleaved with the signal states used for encoding information in the original BB84 protocol. Signal and decoy states are indistinguishable as they differ only in their intensity. Therefore, when performing a PNS attack, Eve introduces a deviation from the expected statistical characteristics of both signal and decoy states. Consequently, when Alice communicates to Bob in which positions she sent the decoy states, they can compare the expected statistical characteristics of the decoy states with the measured ones and detect Eve. Achieving adequate performance of the decoy-state protocol requires to properly choose both signal and decoy states. In particular, it is desirable to employ signal states with sub-Poissonian photon number statistics to reduce both vacuum and multi-photon emission probabilities while increasing the single-photon probability.[2]

B. Noisy Photon-Added Squeezed States

Given a quantum state $\boldsymbol{\varXi}$, the associated photon-added state is obtained by performing $k \in \mathbb{N}$ times the photon-addition operation on $\boldsymbol{\varXi}$, and it is defined as

$$\boldsymbol{\varXi}(k) = \frac{(\boldsymbol{A}^\dagger)^k \boldsymbol{\varXi} \boldsymbol{A}^k}{N_k} \tag{1}$$

where $N_k = \operatorname{tr}\{(\boldsymbol{A}^\dagger)^k \boldsymbol{\varXi} \boldsymbol{A}^k\}$ is the associated normalization constant. A noisy PASS is obtained from (1) by using $\boldsymbol{\varXi} = \boldsymbol{D}_\mu \boldsymbol{S}_\zeta \boldsymbol{\varXi}_{\mathrm{th}} \boldsymbol{S}_\zeta^\dagger \boldsymbol{D}_\mu^\dagger$, which is the squeezed-displaced thermal state [33], [34], and $\boldsymbol{\varXi}_{\mathrm{th}}$ is the thermal state whose Fock representation is given by

$$\boldsymbol{\varXi}_{\mathrm{th}} = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n| \,. \tag{2}$$

In (2), $\bar{n} = (\exp\{\hbar\omega/(k_{\mathrm{B}}T)\} - 1)^{-1}$ is the mean number of thermal photons determined by the Planck's law once the angular frequency ω of the electromagnetic field and the absolute temperature T are given, while $\hbar$ and k_{B} are the reduced Planck constant and the Boltzmann constant, respectively. Therefore, a noisy PASS is defined as

$$\boldsymbol{\varXi}(k,\mu,\zeta,\bar{n}) = \frac{(\boldsymbol{A}^\dagger)^k \boldsymbol{D}_\mu \boldsymbol{S}_\zeta \boldsymbol{\varXi}_{\mathrm{th}} \boldsymbol{S}_\zeta^\dagger \boldsymbol{D}_\mu^\dagger \boldsymbol{A}^k}{N_k(\mu,\zeta,\bar{n})} \tag{3}$$

where $N_k(\mu,\zeta,\bar{n}) = \operatorname{tr}\{(\boldsymbol{A}^\dagger)^k \boldsymbol{D}_\mu \boldsymbol{S}_\zeta \boldsymbol{\varXi}_{\mathrm{th}} \boldsymbol{S}_\zeta^\dagger \boldsymbol{D}_\mu^\dagger \boldsymbol{A}^k\}$ is the associated normalization constant. The influence of the noise in state preparation depends on the intensity $\bar{n}$ of the thermal state. Notice that (3) generalizes multiple sub-classes of quantum states, which can be obtained for specific values of k, μ, ζ, and $\bar{n}$. Specifically, a noisy PASS turns into a: (i) noisy photon-added coherent state [35], when $\zeta \to 0$; (ii) photon-added squeezed thermal state, when $\mu = 0$; (iii) noisy coherent state, when $\zeta \to 0$ and $k = 0$; (iv) coherent state, when $k = 0$, $\zeta \to 0$, and $\bar{n} = 0$; and (v) photon-added displaced squeezed vacuum state, when $\bar{n} = 0$. Therefore, noisy PASSs can be engineered by tuning k, μ, and ζ.

III. Characterization of Noisy PASSs

Engineering noisy PASSs requires to characterize them in the Fock space. This section provides the Fock representation, photon number distribution, and mean number of photons of a noisy PASS. The following lemma provides the Fock representation of a noisy PASS.

Lemma 1 (Fock representation of a noisy PASS): The Fock representation of a noisy PASS is found to be as in (4) shown at the top of the next page, where

$$A = 1 + \bar{n} + (2\bar{n}+1)\sinh(r)^2 \tag{5a}$$
$$B = (2\bar{n}+1)e^{\imath\varphi}\sinh(r)\cosh(r) \tag{5b}$$
$$C = \frac{\bar{n}(\bar{n}+1)}{\bar{n}^2 + (\bar{n}+\frac{1}{2})(1+\cosh(2r))} \tag{5c}$$
$$D = -\frac{e^{\imath\varphi}(\bar{n}+\frac{1}{2})\sinh(2r)}{\bar{n}^2 + (\bar{n}+\frac{1}{2})(1+\cosh(2r))} \tag{5d}$$
$$E = \frac{\frac{\mu}{2} + (\bar{n}+\frac{1}{2})(\mu\cosh(2r) - \mu^* e^{\imath\varphi}\sinh(2r))}{\bar{n}^2 + (\bar{n}+\frac{1}{2})(1+\cosh(2r))} \tag{5e}$$
$$p = \min\{n,m\} - k \geqslant 0 \,. \tag{5f}$$

Proof: Given a Fock state $|n\rangle$, $n \in \mathbb{N}$, from the definition of $\boldsymbol{A}$ and $\boldsymbol{A}^\dagger$, we have

$$\boldsymbol{A}^k|n\rangle = \sqrt{\frac{n!}{(n-k)!}}|n-k\rangle, \quad \text{for } k \leqslant n \tag{6a}$$
$$(\boldsymbol{A}^\dagger)^k|n\rangle = \sqrt{\frac{(n+k)!}{n!}}|n+k\rangle \,. \tag{6b}$$

Therefore, by using (6) in (3), we obtain

$$\langle n|\boldsymbol{\varXi}(k,\mu,\zeta,\bar{n})|m\rangle = \frac{\sqrt{n!\,m!}}{N_k(\mu,\zeta,\bar{n})\sqrt{(n-k)!\,(m-k)!}} \times\langle n-k|\boldsymbol{D}_\mu \boldsymbol{S}_\zeta \boldsymbol{\varXi}_{\mathrm{th}} \boldsymbol{S}_\zeta^\dagger \boldsymbol{D}_\mu^\dagger|m-k\rangle. \tag{7}$$

By using [33, eqs. (4.4), (4,23), and (5.2)] together with (5) in (7), we obtain (4). □

[2] Multi-photon states can be exploited by Eve to perform a PNS attack, while vacuum states reduce the secure key generation rate.

$$\langle n|\boldsymbol{\Xi}(k,\mu,\zeta,\bar{n})|m\rangle = \frac{\sqrt{(n!\,m!)}}{N_k(\mu,\zeta,\bar{n})\,(n-k)!\,(m-k)!\sqrt{\left(A^2-|B|^2\right)}}\exp\left(-\frac{A\,|\mu|^2-\frac{1}{2}\left[B(\mu^*)^2+B^*\mu^2\right]}{A^2-|B|^2}\right)$$

$$\times\sum_{i=0}^{p}\binom{n-k}{i}\binom{m-k}{i}\,i!\,C^i\,H_{n-k-i}\left(\frac{E}{\sqrt{2D}}\right)H_{m-k-i}\left(\frac{E^*}{\sqrt{2D^*}}\right)\left(\frac{D}{2}\right)^{\frac{n-k-i}{2}}\left(\frac{D^*}{2}\right)^{\frac{m-k-i}{2}} \quad (4)$$

The normalization constant in (3) is found to be

$$N_k(\mu,\zeta,\bar{n}) = (-1)^k\exp\left(\frac{1}{2}\boldsymbol{x}^{\mathrm{T}}\boldsymbol{M}\boldsymbol{x}\right)$$
$$\times\frac{\partial^{2k}}{\partial x_1^k\,\partial x_2^k}\exp\left(-\frac{1}{2}\boldsymbol{x}^{\mathrm{T}}\boldsymbol{M}\boldsymbol{x}\right)$$

where $\boldsymbol{x} = (\det\{\boldsymbol{C}\})^{-1}(\operatorname{adj}(\boldsymbol{ZCZ}))^{\mathrm{T}}\boldsymbol{Z}\boldsymbol{\mu}$ and $\boldsymbol{M} = \boldsymbol{XZCZ}$, with

$$\boldsymbol{X} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \quad \boldsymbol{Z} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \quad \boldsymbol{\mu} = \begin{bmatrix}\mu & \mu^*\end{bmatrix}^{\mathrm{T}}$$
$$\boldsymbol{C} = \left(\bar{n}+\frac{1}{2}\right)\begin{bmatrix}\cosh(2r) & \sinh(2r)e^{-\imath\varphi}\\ \sinh(2r)e^{\imath\varphi} & \cosh(2r)\end{bmatrix}+\frac{1}{2}\boldsymbol{I}\,.$$

From (4), the photon number distribution of a noisy PASS is defined as $P_n(k,\mu,\zeta,\bar{n}) \triangleq \langle n|\boldsymbol{\Xi}(k,\mu,\zeta,\bar{n})|n\rangle$.

Fig. 1 shows the photon number distribution of a noiseless ($\bar{n}=0$) and noisy ($\bar{n}=0.1$) PASS for different values of k, μ, and ζ.[3] It can be first noticed that for $k=1$, both noiseless and noisy PASSs (Fig. 1c and Fig. 1d, respectively) exhibit probability zero of vacuum ($n=0$) emission due to the photon-addition operation. Furthermore, it can be observed that for both $k=0$ and $k=1$, the photon number distribution of a noisy PASS (Fig. 1b and Fig. 1d, respectively) deviates from that one of a noiseless PASS (Fig. 1a and Fig. 1c, respectively). This is caused by non-vacuum components of the thermal state that increase multi-photon probabilities. In particular, two situations can be distinguished. In the first one, when $k=0$, the noisy PASS (Fig. 1b) benefits from the thermal noise and exhibits a higher single-photon probability and a lower vacuum emission probability compared to a noiseless PASS (Fig. 1a). In the second situation, when $k=1$, a noisy PASS (Fig. 1d) exhibits a lower single-photon probability and higher multi-photon probabilities compared to a noiseless PASS (Fig. 1c). Therefore, engineering noisy PASSs for QKD applications requires to properly tune k, μ, and ζ to shape the photon number distribution of both signal and decoy states.

The following lemma provides the mean number of photons of a noisy PASS.

Lemma 2 (Mean number of photons of a noisy PASS): The mean number of photons of a noisy PASS is found to be

$$\bar{n}_{\mathrm{p}}(k,\mu,\zeta,\bar{n}) \triangleq \langle\boldsymbol{A}^\dagger\boldsymbol{A}\rangle = \frac{N_{k+1}(\mu,\zeta,\bar{n})}{N_k(\mu,\zeta,\bar{n})}-1\,. \quad (8)$$

Proof: From the Cahill-Glauber anti-normal ordering expansion [36, eq. (5.12)] with $s=1$, $t=-1$, and $m=n$, we have

$$(\boldsymbol{A}^\dagger)^n\boldsymbol{A}^n = \sum_{j=0}^{n}(-1)^j\,j!\binom{n}{j}^2\boldsymbol{A}^{n-j}(\boldsymbol{A}^\dagger)^{n-j}. \quad (9)$$

Consider a noisy PASS $\boldsymbol{\Xi}(k,\mu,\zeta,\bar{n})$, by using (9) together with the cyclical property of the trace operator, we have

$$\begin{aligned}\langle(\boldsymbol{A}^\dagger)^n\boldsymbol{A}^n\rangle &\triangleq \operatorname{tr}\{\boldsymbol{\Xi}(k,\mu,\zeta,\bar{n})(\boldsymbol{A}^\dagger)^n\boldsymbol{A}^n\}\\ &= \sum_{j=0}^{n}(-1)^j\,j!\binom{n}{j}^2\\ &\quad\times\operatorname{tr}\left\{\frac{(\boldsymbol{A}^\dagger)^{n+k-j}\boldsymbol{D}_\mu\boldsymbol{S}_\zeta\boldsymbol{\Xi}_{\mathrm{th}}\boldsymbol{S}_\zeta^\dagger\boldsymbol{D}_\mu^\dagger\boldsymbol{A}^{n+k-j}}{N_k(\mu,\zeta,\bar{n})}\right\}\\ &= \frac{1}{N_k(\mu,\zeta,\bar{n})}\sum_{j=0}^{n}(-1)^j j!\binom{n}{j}^2 N_{n+k-j}(\mu,\zeta,\bar{n})\,.\end{aligned} \quad (10)$$

In accordance with the definition of mean number of photons, (8) is obtained by using (10) with $n=1$. □

IV. Decoy-State Protocol with Noisy PASSs

This section describes the communication system and the decoy-state protocol with noisy PASSs, and provides the lower bound for the secure key generation rate.

A. Communication System

The adopted communication system is in accordance with [20] and briefly described in the following.

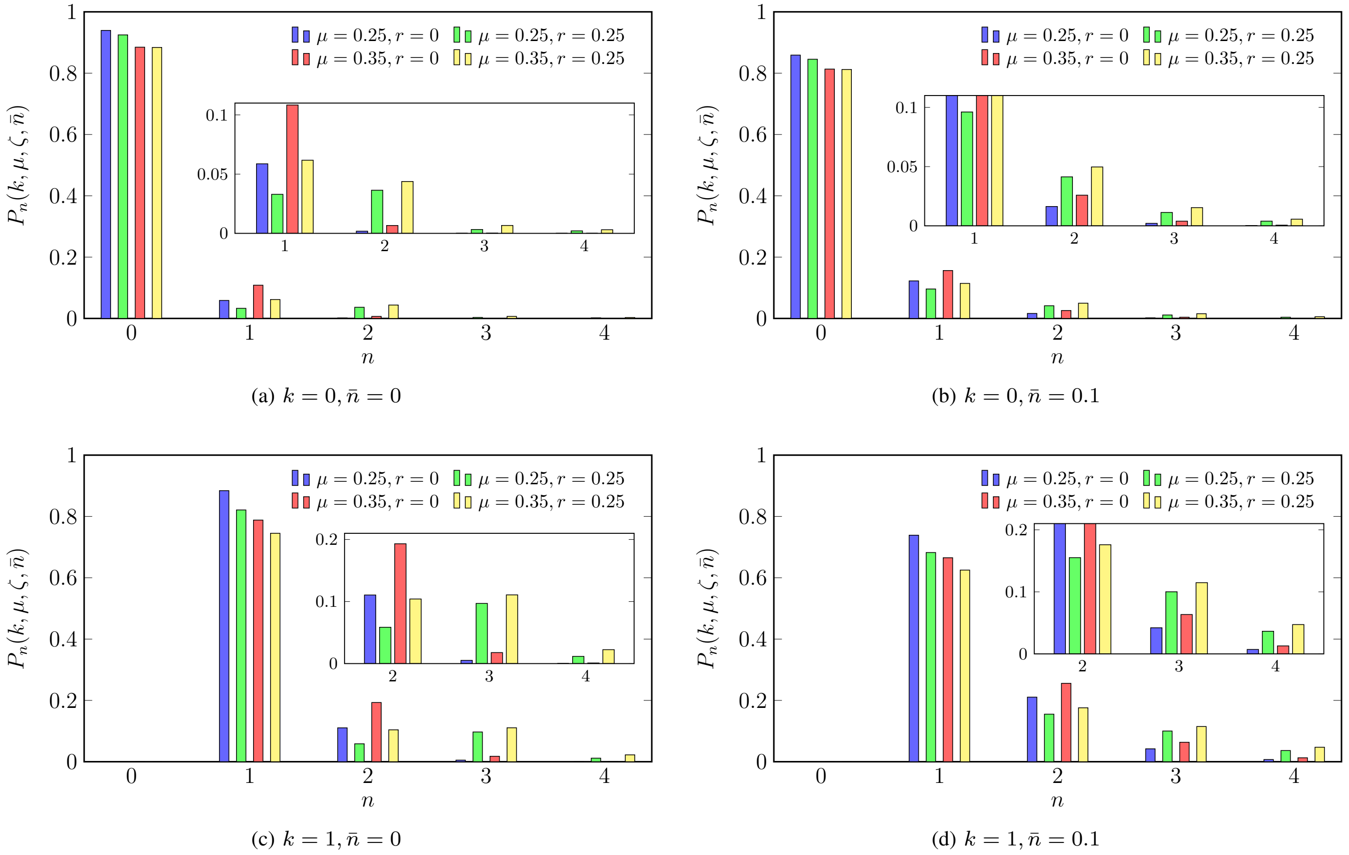
Source: Alice's source emits noisy PASSs that can be engineered by tuning k, μ, and ζ. Signal and decoy states are characterized by a mean number of photons $\bar{n}_{\mathrm{p}}(k,\mu,\zeta,\bar{n})$ and $\bar{n}_{\mathrm{p}}(k,\mu',\zeta',\bar{n})$, respectively, with $\bar{n}_{\mathrm{p}}(k,\mu,\zeta,\bar{n}) > \bar{n}_{\mathrm{p}}(k,\mu',\zeta',\bar{n})$. The associated photon number distributions are denoted by $P_n(k,\mu,\zeta,\bar{n})$ and $P_n(k,\mu',\zeta',\bar{n})$, respectively.

Quantum channel: the quantum channel is an optical fiber characterized by its transmittance $\eta_{\mathrm{c}} = 10^{-\alpha L/10}$, where α is the loss coefficient, and L is the length of the optical fiber.

Detection system: Bob's detection system consists of threshold detectors that discriminate between vacuum and n-photon states, $n \geqslant 1$, and it is characterized by its transmittance $\eta_{\mathrm{B}} = \eta_{\mathrm{d}}\,\varepsilon_{\mathrm{d}}$, where η_{d} and ε_{d} are the internal transmittance and the efficiency of the optical detectors, respectively.

For a n-photon state, $n \geqslant 1$, assuming independence in the behavior of the photons, the associated overall transmittance is $\eta_n = 1-(1-\eta)^n$, where $\eta = \eta_{\mathrm{c}}\,\eta_{\mathrm{B}}$.

[3] Although μ and ζ are complex values, they are plotted for some real values.



(a) $k = 0, \bar{n} = 0$

(b) $k = 0, \bar{n} = 0.1$

(c) $k = 1, \bar{n} = 0$

(d) $k = 1, \bar{n} = 0.1$

Fig. 1: Photon number distribution for different values of k, μ, and r: (a) noiseless PASS with $k = 0$, (b) noisy PASS with $k = 0$, (c) noiseless PASS with $k = 1$, and (d) noisy PASS with $k = 1$.

B. Noisy PASSs Engineering for the Decoy-State Protocol

Since only a few decoy states are sufficient for practical implementations [24], [25], the characterization of the decoy-state protocol is provided for a single decoy state.

The overall gains for signal and decoy noisy PASSs are respectively defined as

$$Q \triangleq \sum_{n=0}^{\infty} Y_n P_n(k, \mu, \zeta, \bar{n}) \tag{11}$$

$$Q' \triangleq \sum_{n=0}^{\infty} Y_n P_n(k, \mu', \zeta', \bar{n}) \tag{12}$$

where $Y_n = Y_0 + \eta_n - Y_0\,\eta_n$ is the conditional probability of Bob's detection given that Alice sent a n-photon state, and Y_0 is the background rate. The overall quantum bit error rates for signal and decoy noisy PASSs are respectively defined as

$$Q_{\mathrm{b}} = R_{\mathrm{e}}\, Q \triangleq \sum_{n=0}^{\infty} e_n Y_n P_n(k, \mu, \zeta, \bar{n}) \tag{13}$$

$$Q'_{\mathrm{b}} = R'_{\mathrm{e}}\, Q' \triangleq \sum_{n=0}^{\infty} e_n Y_n P_n(k, \mu', \zeta', \bar{n}) \tag{14}$$

where R_{e} and R'_{e} are the associated total error rates, $e_n = (Y_0/2 + e_{\mathrm{det}}\,\eta_n)/Y_n$ is the error rate associated with a n-photon state, and e_{det} is a parameter related to the stability of the detection system. As mentioned above, both signal and decoy states are engineered by tuning k, μ, and ζ. Therefore, it is necessary to establish the state engineering domain, i.e., the set in which k, μ, and ζ can be chosen for engineering the noisy PASSs. To this aim, we define

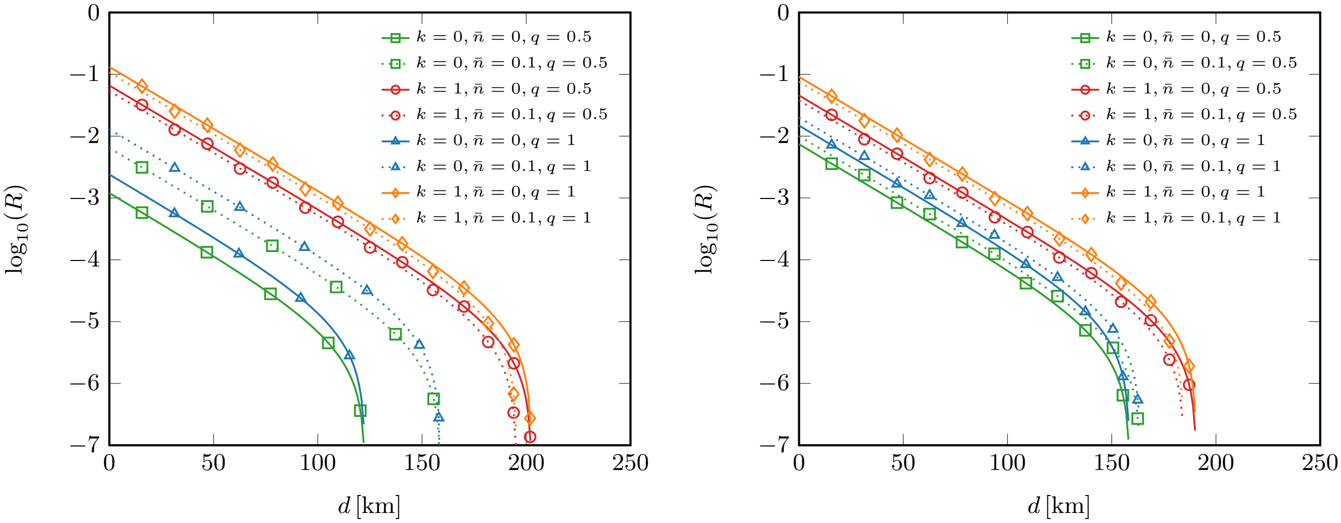
$$\mathcal{D}_{\mathrm{p}}^{(k)} \triangleq \left\{(\mu, \zeta, \mu', \zeta') \in \mathbb{C}^4 : \bar{n}_{\mathrm{p}}(k, \mu, \zeta, \bar{n}) > \bar{n}_{\mathrm{p}}(k, \mu', \zeta', \bar{n})\right\}$$
$$\mathcal{D}_{g}^{(k)} \triangleq \left\{(\mu, \zeta, \mu', \zeta') \in \mathbb{C}^4 : g(k, \mu, \zeta, \mu', \zeta', \bar{n}) \geqslant 0\right\}$$

where

$$g(k, \mu, \zeta, \mu', \zeta', \bar{n}) = \frac{P_n(k, \mu, \zeta, \bar{n})}{P_n(k, \mu', \zeta', \bar{n})} - \frac{P_{n-1}(k, \mu, \zeta, \bar{n})}{P_{n-1}(k, \mu', \zeta', \bar{n})} \tag{15}$$

for $n \geqslant k+1$. In particular, $\mathcal{D}_{\mathrm{p}}^{(k)}$ is the domain in which signal noisy PASSs exhibit higher intensities than decoy ones, while $\mathcal{D}_{g}^{(k)}$ is the domain in which (15) is positive. From (4), it can be noticed that only $k = 0$ and $k = 1$ are admissible. Therefore, by considering both signal and decoy states obtained by performing the same number of photon-addition operations k, the state engineering domain is defined as

$$\mathcal{D}_{\mathrm{eng}}^{(k)} \triangleq \mathcal{D}_{\mathrm{p}}^{(k)} \cap \mathcal{D}_{g}^{(k)}, \text{ for } k \in \{0, 1\}\,.$$



(a) $\mu = 0.15$, $r = 0.1$, $\mu' = 0.05$, $r' = 0.05$

(b) $\mu = 0.45$, $r = 0.2$, $\mu' = 0.35$, and $r' = 0.1$

Fig. 2: Secure key generation rate for different values of k, $\bar{n}$, and q: (a) $\mu = 0.15$, $r = 0.1$, $\mu' = 0.05$, $r' = 0.05$, and (b) $\mu = 0.45$, $r = 0.2$, $\mu' = 0.35$, and $r' = 0.1$. For a fair comparison, the considered state engineering domain is $\mathcal{D}_{\text{eng}}^{(0)} \cap \mathcal{D}_{\text{eng}}^{(1)}$.

It is worth remarking that in $\mathcal{D}_{\text{eng}}^{(k)}$ noisy PASSs can be specialized for engineering multiple classes of QKD sources, including some already characterized in the literature as special cases. This makes noisy PASSs suitable to engineer QKD sources for various applications in different scenarios. Moreover, such state engineering approach can be easily extended to an arbitrary number of decoy states.

C. Secure Key Generation Rate

The secure key generation rate is lower bounded by [24]

$$R \geqslant q\left\{-Q\, f_{\text{e}}\, H_2(R_{\text{e}}) + P_1(k,\mu,\zeta,\bar{n})\, Y_1[1-H_2(e_1)]\right\} \quad (16)$$

where q is the sifting efficiency of the protocol ($q = 1/2$ for the standard BB84, and $q \simeq 1$ for the efficient BB84), f_{e} is the bidirectional error correction efficiency, and $H_2(\cdot)$ is the binary Shannon entropy function. For quantum states in $\mathcal{D}_{\text{eng}}^{(k)}$, from (15) we obtain

$$P_n(k,\mu,\zeta,\bar{n}) \geqslant \frac{P_2(k,\mu,\zeta,\bar{n})}{P_2(k,\mu',\zeta',\bar{n})} P_n(k,\mu',\zeta',\bar{n}) \,. \quad (17)$$

By using (17) in (11), the following inequality holds

$$Q \geqslant Y_0 P_0(k,\mu,\zeta,\bar{n}) + Y_1 P_1(k,\mu,\zeta,\bar{n}) + \frac{P_2(k,\mu,\zeta,\bar{n})}{P_2(k,\mu',\zeta',\bar{n})} \sum_{n=2}^{\infty} Y_n P_n(k,\mu',\zeta',\bar{n}) \,. \quad (18)$$

Therefore, by using (12) in (18), Y_1 is lower bounded by (19) shown at the top of the next page. Analogously, from (14), e_1 is upper bounded by

$$e_1 \leqslant \frac{R'_{\text{e}}\, Q' - \frac{1}{2} Y_0 P_0(k,\mu',\zeta',\bar{n})}{Y_1 P_1(k,\mu',\zeta',\bar{n})} \,. \quad (20)$$

The lower bound for the secure key generation rate, on the engineering domain, is obtained by using (13), (19), and (20) in (16).

V. Case Study

This section presents a case study to quantify the secure key generation rate of the decoy-state protocol employing engineered noisy PASSs in an optical fiber-based quantum communication system.

In accordance with the communication system described in Sec. IV, we consider an optical fiber operating at $\lambda = 1550$ nm, with loss coefficient $\alpha = 0.2$ dB/km. The numerical results are obtained by setting $T = 4$ K, $\eta_{\text{B}} = 0.145$, $Y_0 = 3 \times 10^{-6}$, $e_{\text{det}} = 1.5 \times 10^{-3}$, and $f_{\text{e}} = 1.1$. The secure key generation rate R is evaluated for two different scenarios: (i) $\mu = 0.15$, $r = 0.1$, $\mu' = 0.05$, and $r' = 0.05$; and (ii) $\mu = 0.45$, $r = 0.2$, $\mu' = 0.35$, and $r' = 0.1$. In both scenarios, R is computed for $k = 0, 1$, $\bar{n} = 0, 0.1$, $q = 1/2$, for the standard BB84, and $q = 1$ (for simplicity) for the efficient BB84.

Fig. 2a shows the secure key rate R, for scenario (i), as a function of the transmission distance d. It can be noticed that for the same k and $\bar{n}$, efficient BB84 ($q = 1$) performs better than standard BB84 ($q = 1/2$). Furthermore, when $k = 1$, both protocols employing noiseless (solid line) and noisy (dotted line) PASSs, provide better performance compared to the case with $k = 0$. A similar behavior can be observed in Fig. 2b, which shows the secure key rate for scenario (ii). In this latter operating regime, the key rates for $k = 0$ and $k = 1$ are respectively higher and lower compared to the ones in Fig. 2a.

Fig. 2a and Fig. 2b also show that for $k = 1$, QKD performs better with noiseless PASSs. Surprisingly, for $k = 0$, QKD performs better with noisy PASSs. This can be attributed to the thermal noise respectively increasing and reducing the probability of emitting a single-photon and a vacuum state. Therefore, for $k = 0$, noisy PASSs can be engineered to exploit the thermal noise for improving the QKD performance.

$$Y_1 \geqslant \frac{Y_0[P_2(k,\mu',\zeta',\bar{n})P_0(k,\mu,\zeta,\bar{n}) - P_2(k,\mu,\zeta,\bar{n})P_0(k,\mu',\zeta',\bar{n})] + P_2(k,\mu,\zeta,\bar{n})\,Q' - P_2(k,\mu',\zeta',\bar{n})\,Q}{P_2(k,\mu,\zeta,\bar{n})P_1(k,\mu',\zeta',\bar{n}) - P_2(k,\mu',\zeta',\bar{n})P_1(k,\mu,\zeta,\bar{n})} \tag{19}$$

VI. Conclusion

This paper proposed to employ noisy PASSs as QKD sources for the decoy-state protocol. In particular, after characterizing PASSs accounting for noise in state preparation, it is shown how such states can be engineered to improve the performance of the decoy-state protocol. Noisy PASSs can be engineered by tuning k, μ, and ζ, which are the number of photon-addition operations, displacing parameter, and squeezing parameter, respectively. Specifically, noisy PASSs can be engineered only for $k = 0$ and $k = 1$. Numerical results show that, for $k = 1$, the thermal noise in state preparation degrades the QKD performance compared to the case with ideal state preparation. Surprisingly, for $k = 0$, QKD performs better in the presence of noisy state preparation due to the thermal noise increasing the single-photon probability and reducing the vacuum one. Therefore, for $k = 0$, noisy PASSs can be engineered to exploit the noise in state preparation. The findings of this paper provide insights in the engineering of non-ideal sources for improving the performance of the decoy-state protocol.

Acknowledgment

The fundamental research described in this paper was supported in part by the Office of Naval Research and in part by the MIT Institute for Soldier Nanotechnologies.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bangalore, IN, Dec. 1984, pp. 175–179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[3] L. Goldenberg, L. Vaidman, and S. Wiesner, "Quantum gambling," *Phys. Rev. Lett.*, vol. 82, no. 16, pp. 3356–3359, Apr. 1999.

[4] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.

[5] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[6] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.

[7] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inf. Comput.*, vol. 4, no. 5, pp. 325–360, Sep. 2004.

[8] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, May 2001.

[9] J. G. Rarity, P. R. Tapsterm, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, no. 1, p. 82, Oct. 2002.

[10] S. Guerrini, M. Chiani, and A. Conti, "Secure key throughput of intermittent trusted-relay QKD protocols," in *2018 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–5.

[11] R. J. Hughes, J. E. Nordholt, D. Derkacs, and P. G. Charles, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.*, vol. 4, no. 1, p. 43, Jul. 2002.

[12] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, no. 19, pp. 3762–3764, Apr. 2004.

[13] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, p. 075001, Jul. 2009.

[14] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, p. 190501, Nov. 2016.

[15] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Aug. 2017.

[16] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, p. 030501, Jan. 2018.

[17] C. Liorni, H. Kampermann, and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence," *New J. Phys.*, vol. 21, no. 9, p. 093055, Sep. 2019.

[18] T. Brougham and K. L. D. Oi, "Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD," *New J. Phys.*, vol. 24, no. 7, p. 075002, Aug. 2022.

[19] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug. 2000.

[20] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, no. 5, p. 052304, Apr. 2000.

[21] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New J. Phys.*, vol. 4, no. 1, p. 44, Jul. 2002.

[22] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, Aug. 2003.

[23] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230503, Jun. 2005.

[24] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, Jun. 2005.

[25] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, p. 012326, Jul. 2005.

[26] S.-H. Sun, M. Gao, H.-Y. Dai, P.-X. Chen, and C.-Z. Li, "Decoy state quantum key distribution with odd coherent state," *Chinese Phys. Lett.*, vol. 25, no. 7, p. 2358, Jul. 2008.

[27] Y. Li, W.-S. Bao, H.-W. Li, C. Zhou, and Y. Wang, "Passive decoy-state quantum key distribution using weak coherent pulses with intensity fluctuations," *Phys. Rev. A*, vol. 89, no. 3, p. 032329, Mar. 2014.

[28] Z.-Q. Yin, Z.-F. Han, F.-W. Sun, and G.-C. Guo, "Decoy state quantum key distribution with modified coherent state," *Phys. Rev. A*, vol. 76, no. 1, p. 014304, Jul. 2007.

[29] T. Horikiri and T. Kobayashi, "Decoy state quantum key distribution with a photon number resolved heralded single photon source," *Phys. Rev. A*, vol. 73, no. 3, p. 032331, Mar. 2006.

[30] Q. Wang, X.-B. Wang, and G.-C. Guo, "Practical decoy-state method in quantum key distribution with a heralded single-photon source," *Phys. Rev. A*, vol. 75, no. 1, p. 012312, Jan. 2007.

[31] Q. Wang *et al.*, "Experimental decoy-state quantum key distribution with a sub-Poissionian heralded single-photon source," *Phys. Rev. Lett.*, vol. 100, no. 9, p. 090501, Mar. 2008.

[32] D. Wang *et al.*, "Quantum key distribution with the single-photon-added coherent source," *Phys. Rev. A*, vol. 90, no. 6, p. 062315, Dec. 2014.

[33] P. Marian and T. A. Marian, "Squeezed states with thermal noise. I. Photon-number statistics," *Phys. Rev. A*, vol. 47, no. 5, pp. 4474–4486, May 1993.

[34] A. Giani, M. Z. Win, and A. Conti, "Quantum discrimination of noisy photon-subtracted squeezed states," in *GLOBECOM 2022 - 2022 IEEE Global Commun. Conf.*, Dec. 2022, pp. 5826–5831.

[35] S. Guerrini, M. Z. Win, M. Chiani, and A. Conti, "Quantum discrimination of noisy photon-added coherent states," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 469–479, Aug. 2020.

[36] K. E. Cahill and R. J. Glauber, "Ordered expansions in boson amplitude operators," *Phys. Rev.*, vol. 177, no. 5, pp. 1857–1881, Jan. 1969.