High-Dimensional Quantum Key Distribution in Quantum Access Networks

Osama Elmabrok, Mohsen Razavi, Tawfig Eltaif, and Khaled A. Alaghamri

Abstract—We investigate the use of high-dimensional quantum key distribution (HD-QKD) for wireless access to hybrid quantum-classical networks. We use $d$-dimensional time-phase encoded states to exchange a secret key between an indoor wireless user and the central office on the other end of the access network. We evaluate the performance in the case of transmitting quantum and classical signals over the same passive optical network by accounting for the impact of background noise induced by the Raman-scattered light on the QKD receiver. We also take into account the loss and background noise that occur in indoor environments as well as finite key effects in our analysis. By studying the system under nominal simulation conditions, we identify regimes of operation in which an HD-QKD system with $d = 4$ can outperform its qubit-based counterpart.

Index Terms—High-dimensional quantum key distribution (HD-QKD), optical wireless communications (OWC), decoy states.

I. INTRODUCTION

Quantum key distribution (QKD) provides cryptographic security based on the laws of quantum mechanics rather than computational complexity [1]. This can particularly be useful when long-term security is needed, as is the case in many scenarios where private data, such as medical records, may be shared via the Internet. As the common method for exchanging data by end users is via wireless access to communications networks, it would be useful for QKD systems to offer their services in the wireless mode as well [2], [3], [4]. The presence of high levels of background noise in wireless channels, even in indoor environments [5], is, however, a significant challenge in wireless QKD systems [6], resulting in low key rates. The use of high-dimensional QKD (HD-QKD) protocols is an intriguing option as they are known to offer higher resilience to noise than their qubit-based counterparts [7], [8], [9], [10]. This could particularly be useful, as we investigate here, for QKD systems that rely on wireless access to optical hybrid quantum-classical networks, i.e., where the optical access network is shared between quantum and classical applications.

QKD has seen a rapid growth over the past few years. It has shown versatility by being demonstrated over various types of links, including optical fiber [11], [12], free space [13], [14], satellite [15], [16], and even underwater links [17], [18]. It has also been demonstrated over hundreds of kilometers [19], [20], [21], and in coexistence with classical channels over an optical fiber [22], [23], [24]. The key generation rate, in all these cases, ought to increase for QKD to become more competitive and commercially viable.

HD-QKD provides a promising and efficient platform for overcoming some of the practical issues faced by present QKD systems [25], [26], [27], [28], [29], [30]. The efficiency is mainly due to its capacity of encoding multiple bits of information, $\log_2(d)$ for $d$-dimensional systems, on a single photon [31], as well as its more resilient to noise [7]. The same degrees of freedom used in qubit-based QKD systems can be employed in a high-dimensional quantum state space. In fact, various degrees of freedom of the photon, such as time-energy and time-bin encoding [32], [33], path encoding [34], time-path encoding [35], orbital angular momentum of light [27], [36], [37], frequency [29], [38], and frequency-time hybrid [39] have been demonstrated in HD-QKD systems. Each degree of freedom has its own benefits in terms of stability, control, and scalability, as well as its own challenges [7].

In this work, we examine the application of HD-QKD in quantum access networks. In our case, such networks comprise an indoor wireless link coupled to a fiber-based passive optical network (PON) catering both classical and quantum users. We employ the $d$-dimensional time-phase encoding scheme considered in [32], and analyse its performance in our hybrid setting. We analyse the effect of several sources of noise in our secret key analysis, such as the background noise caused by Raman-scattered light from classical channels. We also take into account the loss and background noise that occur in indoor environments [2], [5], [40]. We obtain the key generation rate by accounting for finite-size key effects for the three-intensity decoy-state protocol [41] considered in [32]. Our results suggest that a simple HD-QKD setup with $d = 4$ can already improve the performance of such QKD systems in certain practical regimes of interest, where finite-key effects are more pronounced.

The remainder of this paper is organized as follows. In Section II, the system is described, with its key-rate analysis presented in Section III. The numerical results are then discussed in Section IV, and Section V concludes the paper.

© 2024 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
II. SYSTEM DESCRIPTION

In this section, we describe the setup used to examine HD-QKD in hybrid quantum-classical access networks comprising indoor optical wireless channels and single-mode optical fibers; see Fig. 1. By utilizing time-phase encoding techniques, a total of \( N \) signals are transmitted from Alice to Bob. Alice is assumed to be in a windowless room of size \( X \times Y \times Z \), lit by an artificial light source. On the room’s floor, Alice uses a mobile device with a QKD transmitter that transmits light toward the ceiling, whereas Bob is assumed to be at the end of the access network in the central office. The signals sent by Alice are collected by a telescope, which is fixed at the center of the room’s ceiling, and coupled to a single-mode fiber to be sent to the central office. The classical channels are assumed to be bidirectional. The classical channels are assumed to be bidirectional. In our analysis, we focus on user 1 as the main example.

In Fig. 1, the telescope collects Alice’s signals, which are then coupled into a single-mode fiber and forwarded to the central office where the QKD measurements are performed. The wireless signals would suffer an extra coupling loss as a result of this coupling requirement. In this case, we assume that the telescope at the collection is properly aligned with the QKD source to ensure that a good portion of the power is received from the QKD source. This can be achieved by using additional beacon beams and steering mirrors based on micro-electromechanical systems (MEMS) [42]. In order to efficiently couple photons to the fiber, the effective field of view (FOV) at the collecting point should equal the numerical aperture of a single-mode fibre which would be roughly below \( 6^\circ \). In this setup, we use a \( d \)-dimensional time-phase encoding, which will be described in Section II-B. In the following, we model the wireless and wired parts of the link.

A. Channel Characterization

In this section, the two links in our setup, the wireless and fiber-based channels, are modelled in order to estimate the loss and background noise that may be introduced.

1) Indoor Optical Wireless Channel: Loss and background noise can make it difficult for a QKD system to function. Path loss is often severe in indoor environments partly because of beam spreading and alignment requirements, but also, in our case, because of coupling issues to the optical fiber. Background noise can also degrade the scheme’s performance by increasing the error rate. Using optical wireless communications (OWC) models, we estimate the path loss and the background noise sneaked into the QKD receiver. The channel DC gain, \( H_{DC} \) [43], [44], which estimates how much of the transmitted power is collected by the telescope in the room, is used to model the channel transmittance for the wireless link. For the line-of-sight link between the QKD transmitter and the telescope, this DC-gain is given by [43]:

\[
H_{DC} = \begin{cases} 
\frac{A(m_L+1)}{2\pi d^2} [\cos(\phi)]^{m_L} T_a(\psi) \times g(\psi) \cos(\psi), & 0 \leq \psi \leq \Psi_c, \\
0, & \text{elsewhere,}
\end{cases}
\]

where \( A \) is the effective area of the telescope and \( d \) is the distance between the QKD source and the telescope; \( \psi \) and \( \phi \) are, respectively, the incidence angle with reference to the receiver axis and the irradiance angle characterizing the relative location and orientation of the transmitter and telescope modules; \( T_a(\psi) \) is the optical filter transmission factor; \( m_L \) and \( g(\psi) \) are, respectively, the Lambert’s mode number used to identify the directivity of the QKD source beam and the concentrator gain, given by

\[
m_L = \frac{- \ln 2}{\ln \left( \cos \left( \Theta_{1/2} \right) \right)}
\]

and

\[
g(\psi) = \begin{cases} 
\frac{n^2}{\pi n^2(\Psi_c)^2}, & 0 \leq \psi \leq \Psi_c, \\
0, & \psi > \Psi_c,
\end{cases}
\]

where \( n \), \( \Psi_c \), and \( \Theta_{1/2} \) are, respectively, the refractive index of the concentrator, the telescope’s FOV, and the semi-angle at half power of the QKD light source. We neglect the reflected pulses from the walls, as they would arrive at a later time, and the employed beam is quite focused in our case.

In order to estimate the background noise in our window-less room, we calculate the noise induced by the artificial lamp using OWC models [5]. That would depend on the power spectral density (PSD) of the employed light source and the telescope’s FOV. Depending on the latter, we can limit the amount of background noise that may sneak into the QKD receiver. Here, we account for the reflected light from the walls and the floor that would be collected at the telescope using the same methodology described in [5].

2) Optical Fiber Link: As for the PON, we assume that arrayed waveguide grating (AWGs) are used to multiplex/demultiplex different wavelengths, and the loss for each AWG, in dB, is denoted by \( \Lambda \). QKD channels in a fiber link that is carrying classical data are mostly affected by the background noise caused by Raman scattering. Due to strong classical signals, the Raman noise would spread over a wide range of frequencies, and that would result in populating the QKD receivers with unwanted signals [45]. Based on their locations...
and the direction of light propagation, the receivers might be susceptible to forward and backward scattered light [46], whose intensity, at wavelength $\lambda_q$, is, respectively, given by [45], [47]

$$I_R^f (I, L, \lambda_d, \lambda_q) = I e^{-\alpha_r L} L \Gamma (\lambda_d, \lambda_q) \Delta \lambda$$

and

$$I_R^b (I, L, \lambda_d, \lambda_q) = I \left( 1 - e^{-2\alpha_r L} \right) \frac{\alpha_r}{2 \alpha_c} L \Gamma (\lambda_d, \lambda_q) \Delta \lambda.$$  \hspace{1cm} (5)

In (4) and (5), $I$ is the intensity of a classical signal at wavelength $\lambda_d$, $\Delta \lambda$ is the optical bandwidth of the QKD receiver and $\alpha_r$ is the loss coefficient of the fiber link; $L$ is the fiber length and $\Gamma (\lambda_d, \lambda_q)$ is the Raman cross section (per unit of fiber length and bandwidth), which can be measured experimentally. In this work, we have used the results reported in [45], [46] at $\lambda_d = 1550$ nm, so it can be adapted to any other wavelengths in the C band. We assume that the transmitted power $I$ is identical for all data channels and is set to guarantee a bit error rate (BER) of no more than $10^{-9}$ for such channels. The QKD receiver would then detect a total average number of photons per pulse, induced by forward and backward scattering, respectively, given by

$$\mu^f_R = \frac{\eta_{det} I_R^f \lambda_q T_d}{hc}$$

and

$$\mu^b_R = \frac{\eta_{det} I_R^b \lambda_q T_d}{hc},$$  \hspace{1cm} (7)

where $\eta_{det}$, $T_d$, and $h$, respectively, identify detectors’ quantum efficiency, the pulse duration, and Planck’s constant with $c$ being the speed of light in the vacuum.

**B. High-Dimensional Time-Phase Encoding**

We assume that the time-phase encoding technique presented in [32] is used in our setup. In this technique, there are $d$ temporal bins and the two employed bases are referred to as time and phase basis. The quantum eigenstates in the time and phase bases are, respectively, denoted by $|t_m\rangle$, $m = 0, \ldots, d-1$ and $|f_n\rangle = (1/\sqrt{d}) \sum_{m=0}^{d-1} e^{2\pi i mn/d} |t_m\rangle$, $n = 0, \ldots, d-1$, where $|t_m\rangle$ ideally refers to a single-photon state in the $m$th bin. Fig. 2 shows temporal states for $d = 4$. Each bin has a width $\tau$ and each signal encodes $\log_2(d)$ bits of information per photon. We assume that the time basis, $T$, is chosen with probability $p_T$, whereas the phase basis, $F$, is chosen with probability $p_F = 1 - p_T$. The data obtained in the time basis is used for secret key generation, whereas phase measurement data is used to monitor the presence of eavesdroppers to bound the information that may have leaked to them.

At Bob’s end, we use a possibly asymmetric beam splitter, with transmissivity $P_F$, to passively choose between time and phase basis measurement. The time basis measurement is simply done by time tagging the detection events at a single-photon detector. We use a tree of time-delay Mach-Zehnder interferometers, followed by single-photon detectors, to do phase-basis measurement; see Fig. 3 for the cases of $d = 2$ and $d = 4$. Note that in the phase basis, there is an intrinsic loss in the phase-basis decoder because of the side lobes created by the interferometers. This results in a decoding efficiency $\eta_d = 0.5$ for $d = 2$ and $\eta_d = 0.25$ for $d = 4$. In our system, we use the decoy-state version of the protocol where, instead of single photons, phase randomized weak coherent pulses (WCPs) are used. We use WCPs with three different intensities, $\mu_1$, $\mu_2$, and $\mu_3$, representing their mean number of photons.

While, in principle, one can choose higher dimensions for QKD systems, there are practical limitations that needs to be considered. For instance, the detection of time-bin states can be a challenging task, particularly, when photons are in a superposition of different time bins. This occurs in measuring high-dimensional phase states, whose detection remains challenging in terms of stability, efficiency, and flexibility.

**III. Key-Rate Analysis**

To guarantee that the failure rate of our HD-QKD system is below a certain secrecy parameter, the length of the final key, $l$,
needs to be smaller than the following expression [32], [41]:

\[
\log_2(d).\tilde{s}_{T,0} + \tilde{s}_{T,1} \left[ c_d - h_d(\lambda^{U}) \right] - \text{leak}_{EC} - \Delta_{FK},
\]

(8)

where \( \tilde{s}_{T,0} \) and \( \tilde{s}_{T,1} \) are the number of vacuum and single-photon detection events, respectively, in the time basis; \( c_d := - \log_2 \max | \langle f_{\eta} | t_m \rangle |^2 \). In our key rate analysis we assume that \( c_d = \log_2(d) \); \( \lambda^{U} \) is the upper bound on phase error rate in single photons in the phase basis, and \( h_d(x) \) is the Shannon entropy function in the \( d \)-dimensional case, given by \( h_d(x) := -x \log_2(x/(d-1)) - (1-x) \log_2(1-x) \). The number of bits sacrificed during error correction in (8) is computed by \( \text{leak}_{EC} = f h_d(e_T) n_T \), where \( f \) is the error correction inefficiency and \( e_T \) is the error rate in the time basis given by \( \frac{m_{T,1}}{2m_{T,1}} \), where \( m_{T,1} \) and \( m_{T,1} \) are, respectively, the number of total and incorrect detections observed by Bob when Alice encodes the quantum states in the time basis with an intensity \( T \); see Appendix A. Finally, by following the security proof presented in [32], [41], \( \Delta_{FK} = \log_2 \frac{d^2}{4} \) for \( d = 4 \) [32], and \( \Delta_{FK} = \log_2 \frac{d}{d^2} \) for \( d = 2 \) [41], corresponding to a total secrecy parameter of \( 22\beta \) in both cases. Appendix A shows how each of the above parameters can be calculated in the simulation scenario where no eavesdropper is present.

In the following section, we simulate the system under the nominal condition that no eavesdropper is present. In such nominal settings, the secret key length \( l \) mainly depends on the overall transmissivity of each link, \( \eta \), and the total background noise denoted by \( n_{bg} \). In Fig. 1, in the absence of an eavesdropper, the total Raman noise power that we consider in this work due to forward and backward scattering, at Bob 1 receiver, denoted, respectively, by \( I_f^v \) and \( I_f^b \), is given by

\[
I_f^v = \left[ I_R^v (I, I_0 + L_1, \lambda_{d_1}, \lambda_{q_1}) + \sum_{u=2}^{K} I_R^v (I e^{-\alpha_r L_a}, I_0, \lambda_{d_u}, \lambda_{q_1}) \right] 10^{-2 \Lambda / 10}
\]

(9)

and

\[
I_f^b = \left[ I_R^b (I, I_0 + L_1, \lambda_{d_1}, \lambda_{q_1}) + \sum_{u=2}^{K} I_R^b (I, I_0, \lambda_{d_u}, \lambda_{q_1}) \right] 10^{-2 \Lambda / 10},
\]

(10)

where \( L_0 \) is the total distance between the AWG box at the users’ side and the central office and \( L_a \) is the distance of the \( u \)th user to the same AWG in the access network. The total background noise per pulse at CO’s Bob 1 end is then given by

\[
n_{bg} = \eta_{det} \lambda_{q_1} T_d \left( I_f^v + I_f^b \right) + \eta_{det} \eta_{Pb} \eta_{fib} \eta_{coup},
\]

(11)

where \( \eta_{coup} \) is the additional air-to-fiber coupling efficiency; \( \eta_{b} \) [2], [5] is the indoor background noise induced by the bulb; \( \eta_{fib} \) is the optical fiber channel transmittance including the loss due to AWGs. The total channel transmittance between the QKD transmitter and receiver is given by \( \eta = H_{DC} \eta_{coup} \eta_{fib} \eta_{det} \), where \( \eta_{fib} \) is given by \( \eta_{fib} = e^{-\alpha_r (L_1 + L_0)} \times 10^{-2 \Lambda / 10} \) and \( \alpha_r \) is the loss coefficient of the fiber link.

IV. NUMERICAL ANALYSIS

In this section, we provide some numerical results for the setup shown in Fig. 1 under the nominal condition that no eavesdropper is present. The central wavelength for the quantum channels is given by \( \lambda_{ch} = \{ 1530.8 \text{ nm}, 1531.6 \text{ nm}, \ldots, 1555.62 \text{ nm} \} \) and that of classical channels is given by \( \lambda_{ch} = \{ 1560.4 \text{ nm}, 1561.2 \text{ nm}, \ldots, 1585.2 \text{ nm} \} \). We assume that \( \lambda_{q_1} = 1555.62 \text{ nm} \) and \( \lambda_{d_1} = 1585.2 \text{ nm} \). We consider a variable launch power for the classical channels to reduce the impact of Raman noise [2]. This corresponds to a \( -38.5 \text{ dBm} \) receiver sensitivity, ensuring a BER of \( 10^{-9} \) [49]. We assume that the fiber length from Alice’s location to AWG, \( L_1 \), is 500 meters, and that this value is the same for all other users. We assume that a full alignment is achieved between the QKD source and the telescope on the room ceiling in order to improve channel transmittance in the room. In this case, we assume that the semi-angle at half power of the QKD source, which is placed at a corner of the room’s floor, is \( 1^\circ \) and the telescope’s FOV is \( 6^\circ \). We compute the key generation rate with finite-size effects [32] using the decoy state approach of three intensities, \( \mu_1, \mu_2 \), and \( \mu_3 \).

Table I summarises the nominal parameter values used in our simulation. One point to highlight is that the values chosen for detectors’ efficiency and dark count mostly correspond to the available technology for single-photon avalanche photodiodes. If the noise in the system, or the decoding efficiency is worse than what is considered here, one can use superconducting nanowire single-photon detectors, which offer higher quantum efficiencies and much lower intrinsic dark count rates. Such detectors would allow us to achieve even higher key rates at high system clock rates of \( 2.5 \text{ GHz} \) for \( d = 4 \) and \( 5 \text{ GHz} \) for \( d = 2 \) with a nearly constant quantum bit error rate.

One main challenge of using OWC for QKD purposes is the existence of severe ambient light, which affects the scheme’s performance, particularly due to artificial light sources. In Fig. 4, the performance is assessed by varying the bulb’s PSD and computing the corresponding secret key rate when the repetition rate is at its maximum possible for a pulse duration of \( T_d = 100 \text{ ps} \). This

| Table I | NOMINAL VALUES USED FOR OUR SYSTEM PARAMETERS |
| --- | --- |
| Parameter | Nominal value |
| Room size, X,Y,Z | \( (4 \times 4 \times 3) \text{ m}^3 \) |
| Semi-angle at half power of the bulb, \( \Theta_1/2 \) | \( 70^\circ \) |
| Semi-angle at half power of the light source, \( \Phi_1/2 \) | \( 1^\circ \) |
| Receiver field of view, FOV | \( 6^\circ \) |
| Pulse duration, \( T_d \) | \( 100 \text{ ps} \) |
| \( \beta_1, \beta_2, \beta_3 \) | \( 0.54, 0.1, 0.5, 0.66, 0.9 \) |
| Security parameter, \( \beta \) | \( 0.0002, 0.44 \) |
| Air-to-fiber coupling efficiency, \( \eta_{coup} \) | \( 0.1 \) |
| Fiber attenuation coefficient, \( \alpha_r \) | \( 1.72 \times 10^{-7} \) |
| Loss due to each AWG, \( \Lambda \) | \( 2 \text{ dB} \) |
| Error correction inefficiency, \( f \) | \( 1.16 \) |
| Number of users, \( K \) | \( 32 \) |
| Dark count rate, \( n_{dc} \) | \( 10^{-7} \text{ (nm)}^{-2} \) |
| Misalignment probability, \( \epsilon_d \) | \( 0.033 \) |
| Quantum efficiency of detector, \( \eta_{det} \) | \( 0.3 \) |
corresponds to a repetition rate of 2.5 GHz for $d = 4$ and 5 GHz for $d = 2$ [32]. The estimated total background noise due to the bulb’s PSD is shown on the top x-axis in Fig. 4. More background noise in the channel means more errors would be generated, and, accordingly, at some point, no secret keys can be exchanged. The secret key rate is computed for $d = 2$ and $d = 4$ considering two different block lengths $N$, Fig. 4(a) shows the improvement in the key rate at low background noise levels when employing HD-QKD with $d = 4$, in comparison to $d = 2$ at the larger block size of $N = 5 \times 10^{11}$ at $L_0 = 5$ km. This corresponds to 100 s of data collection time at $d = 2$. The qubit-based system, however, offers a better performance at higher levels of background noise. The results change when we consider a lower block size of $N = 6.5 \times 10^{10}$ at $L_0 = 2$ km as shown in Fig. 4(b). In this case, when we have limited collection time, the HD system performs better across all viable PSD values. This suggests that the HD system is more resilient to statistical fluctuations caused by the finite-key analysis. Note that the number of bits sent by either of the two systems is the same for any fixed collection time. Also note that the block size only accounts for the time that quantum signals need to be exchanged; classical postprocessing steps can then be implemented offline, or in parallel with the transmission of the next quantum block.

Fig. 5 shows the secret key rate versus the total fiber length, $L_0 + L_1$, where the total channel loss in dB is shown on the top x-axis. This also accounts for the coupling efficiency, $\eta_{\text{coupl}}$, which is assumed to be 0.1 here; see Table I for all loss parameters. We see a similar behaviour as we saw in the previous figure regarding the length of the block size. In Fig. 5(a), the key rate is improved slightly at $d = 4$ when $N = 5 \times 10^{11}$, but the improvement is quite considerable over the entire range when we have a smaller number of data points corresponding to $N = 6.5 \times 10^{10}$. This interestingly shows that the resilience to errors for higher dimension systems is better pronounced when we account for finite key effects, especially when there are limitations with the data collection time. This is expected to be the case for the applications considered here where a wireless user would prefer to finish the key exchange process as soon as possible.

Finally, to shed more light into the above results, in Fig. 6, we have shown the quantum bit error rate (QBER) in both time and phase bases for the two block lengths considered in our analysis. It can be seen that in both cases the QBER in all graphs is higher for $d = 4$ than $d = 2$. This is not surprising as the HD system is more complex and more prone to errors. But, at the same time, the HD system is capable of tolerating more errors. Given that the statistical fluctuations would comparatively have a lower impact on large values of QBER, than the small values, it can then be understood why the system at $d = 4$ performs better at low values of block size $N$. This is because the upper bound we obtain for the QBER at $d = 4$, percentage wise, has less deviation from its nominal value than the low QBER of $d = 2$. This justifies our observation in Figs. 4 and 5.

V. CONCLUSIONS AND DISCUSSION

High-dimensional QKD systems are interesting options for boosting error tolerance and for improving the secret key generation rate. In this work, we examined HD-QKD in quantum
access networks considering the challenges of background noise, Raman scattering in optical fibers, and path loss. We considered a finite size of data to exchange secret keys between a wireless indoor user and a remote user located at the central office. HD-QKD turned out to be a promising solution for users in indoor environments who might want to use applications such as video conferencing in a convenient and safe manner. For such applications, an HD-QKD system with dimension four could be sufficient for obtaining a reasonable secure key rate over PONs. The key advantage could be in offering a lower required collection time for exchanging a key.

In general the choice of high-dimensional QKD versus qubit-based QKD requires additional considerations. The simplest methods for generating high-dimensional quantum states are time-energy and time-bin encodings. However, as the dimensions of quantum systems increase, there are other practical considerations that we need to account for. For instance, the dimensionality of the setup may increase. That could be a significant concern for certain applications [34]. The optimum dimension is eventually determined by the use-case scenario. Our results suggest that with a repetition rate of 2.5 GHz, and at nominal PON lengths of a few kilometers, a 4-bit system is sufficient for obtaining a secure key rate at the order of MB/s, which can be used to realize one-time pad encryption for video streaming [50].

Another consideration is whether the results of this work can be extended to an outdoor user or where the room is not windowless, or it has other sources of lighting. This certainly makes the implementation of the system more challenging as ambient light from the Sun and incandescent lamps cover a wide range of wavelengths. For instance, the spectral irradiance for the Sun is three orders of magnitude higher than that of the LED bulbs considered here. The QKD system may only work under daylight exposure if the receiver field of view is extremely narrow. Nevertheless, early work on daylight operation of intermodal QKD systems, which similarly rely on coupling light from free space to fiber, has already been reported [51], which makes the extension of this work to noisier environments more viable.

**APPENDIX A**

**KEY RATE ANALYSIS**

In this appendix, the relevant parameters for calculating the secret key generation rate, under the nominal condition of no eavesdropping, are obtained. In (8), \( \tilde{s}_{T,0} \) and \( \tilde{s}_{T,1} \) are the number of vacuum and single-photon detection events, respectively, in the time basis, and they are given by [32] and [41]:

\[
\tilde{s}_{T,0} = \max \left\{ \frac{\tau_0}{\mu_2 - \mu_3} \left( \frac{\mu_2 e^{\mu_3} n_{\mu_2,0}}{p_{\mu_2}} - \frac{\mu_3 e^{\mu_2} n_{\mu_3,0}}{p_{\mu_3}} \right), 0 \right\},
\]

(12)

and

\[
\tilde{s}_{T,1} = \max \left\{ \frac{\mu_1 \tau_1}{\mu_1 (\mu_2 - \mu_3) - (\mu_2^2 - \mu_3^2)} \times \left( \frac{e^{\mu_2} n_{\mu_2,1}}{p_{\mu_2}} - \frac{e^{\mu_3} n_{\mu_3,1}}{p_{\mu_3}} \right), 0 \right\},
\]

(13)

where \( n_{\mu,0} = n_{T,\mu} + \delta (n_{T,\beta}) \) with \( n_{T,\mu} \) being the number of detection events observed by Bob when Alice encodes the quantum states in the time basis with an intensity \( \mu \), and \( n_T = \sum_{\mu \in M} p_{\mu} n_{T,\mu} \) for \( \mu = (\mu_1, \mu_2, \mu_3) \). The deviation term is assumed to be \( \delta (n_{T,\beta}) = n_T / 2 \text{log}(1/\beta) \), following the Gaussian approximation (which is known to be closely following the more accurate bounds based on Chernoff inequality [52]).

In (8), \( \lambda_U \) is an upper bound on the phase error rate of single photons in the phase basis, and it is given by \( \lambda_U = Q + \xi \), where \( Q = \tilde{\nu}_{F,1} \) and \( \xi = \sqrt{\frac{(s_{T,1} + s_{F,1}) (s_{T,1} + 1)}{s_{F,1} (s_{T,1} + s_{F,1})^2}} \log \frac{2}{\sqrt{\pi}} \). In \( Q \) and \( \xi \), \( \tilde{\nu}_{F,1} \) is the number of detected signal photon states in the phase basis, and \( s_{T,1} \) is the number of erroneously detected single photons in the phase basis, and it is given by

\[
\tilde{\nu}_{F,1} = \frac{\tau_1}{\mu_2 - \mu_3} \left( \frac{e^{\mu_2} m_{\mu_2,0}}{p_{\mu_2}} - \frac{e^{\mu_3} m_{\mu_3,0}}{p_{\mu_3}} \right),
\]

(14)

where \( m_{\mu,0} = m_{T,\mu} + \delta (m_{T,\beta}) \) for \( \mu \in M \), is the number of errors associated with the phase basis when intensity \( \mu \) is used.

For \( d = 2 [41] \), \( \xi = \gamma (\beta, \frac{p_{\mu_1}}{s_{F,1}}, \tilde{s}_{F,1}, \tilde{s}_{T,1}) \), where \( \gamma (a, b, c, d) = \sqrt{\frac{(c + d) (1 - b) b}{c d (c + d) (c - b) b}} \).

In above equations, \( n_{T,\mu}, n_{F,\mu}, m_{T,\mu}, \) and \( m_{F,\mu} \), for \( \mu \in M \), are, respectively, given by

\[
n_{T,\mu} = p_{\mu} p_T N \left( 1 - e^{-\eta \mu} + d (n_{bg} + n_{dc}) \right),
\]

(15)

\[
n_{F,\mu} = p_{\mu} p_F N \left( 1 - e^{-\eta \mu} + d (n_{bg} + n_{dc}) \right),
\]

(16)

\[
m_{T,\mu} = p_{\mu} p_T N (\epsilon_d (1 - e^{-\eta \mu}) + (d - 1) (n_{bg} + n_{dc})),
\]

(17)

and

\[
m_{F,\mu} = p_{\mu} p_F N (\epsilon_d (1 - e^{-\eta \mu}) + (d - 1) (n_{bg} + n_{dc})),
\]

(18)

where we have neglected multiple-click events, \( p_F \) and \( p_T \) are, respectively, the probability of encoding in the phase and time bases; \( n_{bg} \) is the total background noise per pulse; \( n_{dc} \) is the dark count per pulse; \( \epsilon_d \) is misalignment error probability; and \( \eta \) is the channel transmittance.

**ACKNOWLEDGMENT**

All data generated in this paper can be reproduced by the provided methodology and equations.
REFERENCES

[1] S. Pirandola et al., “Advances in quantum cryptography,” Adv. Opt. Photon., vol. 12, no. 4, pp. 1012–1236, 2020.
[2] O. Elmabrok, M. Ghallai, and M. Razavi, “Quantum-classical access networks with embedded optical wireless links,” JOSA B, vol. 35, no. 3, pp. 487–499, 2018.

[3] S. Bahrami, O. Elmabrok, G. C. Lorenzo, and M. Razavi, “Resource optimization in quantum access networks,” in Proc. IEEE Int. Conf. Acoust. Speech Signal Process., 2019, pp. 7988–7992.

[4] O. Elmabrok and M. Razavi, “Quantum-classical access networks with embedded optical wireless links,” in Proc. IEEE GLOBECOM Conf., 2016, pp. 1–6.

[5] B. Fröhlich et al., “Long-distance quantum key distribution secure against coherent attacks,” Opt. Express, vol. 24, no. 20, pp. 22159–22168, 2016.

[6] H. Bechmann-Pasquinucci and W. Tittel, “Quantum cryptography using discrete-time quantum walks,” Sci. Adv., vol. 3, no. 11, 2017, Art. no. e1701491.

[7] F. Bouchard et al., “Quantum cryptography with twisted photons,” Phys. Rev. A, vol. 98, no. 1, 2018, Art. no. 010301.

[8] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, “High-dimensional quantum communication: Benefits, progress, and future challenges,” Adv. Quantum Technol., vol. 2, no. 12, 2019, Art. no. 1900038.

[9] S. Ecker et al., “Overcoming noise in entanglement distribution,” Phys. Rev. X, vol. 9, no. 4, 2019, Art. no. 041042.

[10] D. Bacco et al., “Boosting the secret key rate in a shared quantum and classical fibre communication system,” Commun. Phys., vol. 2, no. 1, pp. 1–8, 2019.

[11] J. Yin et al., “Satellite-based entanglement distribution over 1200 kilometers,” Science, vol. 356, no. 6343, pp. 1140–1144, 2017.

[12] J. Ali-Khan, C. J. Broadbent, and J. C. Howell, “Large-alphabet quantum key distribution using energy-time entangled bipartite states,” Phys. Rev. Lett., vol. 98, no. 6, 2007, Art. no. 060503.

[13] T. Giordani et al., “Experimental engineering of arbitrary qudit states with discrete-time quantum walks,” Phys. Rev. Lett., vol. 122, no. 2, 2019, Art. no. 020503.

[14] H.-L. Yin et al., “Measurement-device-independent quantum key distribution over a 2-km multicore fiber,” NPJ Quantum Inf., vol. 7, no. 1, pp. 1–6, 2021.

[15] J. Bavaresco et al., “Measurements in two bases are sufficient for certifying high-dimensional quantum entanglement,” Nature, vol. 546, no. 7660, pp. 622–626, 2017.

[16] F. Steinlechner et al., “Round-robin differential-phase-shift quantum key distribution with twisted photons,” Phys. Rev. A, vol. 98, no. 1, 2018, Art. no. 012301.

[17] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, “High-dimensional quantum communication: Benefits, progress, and future challenges,” Adv. Quantum Technol., vol. 2, no. 12, 2019, Art. no. 1900038.

[18] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, “Improved key-rate bounds for practical decoy-state quantum key distribution,” Quantum Sci. Technol., vol. 4, no. 3, 2019, Art. no. 035008.

[19] B. Da Lio et al., “Path-encoded high-dimensional quantum communication over 307km of optical fibre,” Nature Photon., vol. 9, no. 3, pp. 163–167, 2015.

[20] J. W. Wang et al., “Long-distance quantum key distribution over an outdoor underwater channel,” in Proc. IEEE Int. Conf. Acoust. Speech Signal Process., 2017, pp. 22563–22573, 2018.

[21] F. R. Gfeller and U. Bapst, “Wireless in-house data communication via diffuse infrared radiation,” Proc. IEEE, vol. 114, no. 11, pp. 1474–1486, Nov. 1979.

[22] M. Razavi, M. Bahrami, and J. A. Salehi, “Orthogonal frequency division multiplexed quantum key distribution in the presence of raman noise,” Quantum Opt., vol. 9090, pp. 190–196, 2016.

[23] I. Karakosta-Amarantidou et al., “Urban intermodal quantum key distribution,” Sci. Rep., vol. 9, no. 1, 2019, Art. no. 022307.

[24] J. M. Kahn and J. R. Barry, “Wireless infrared communications,” Proc. IEEE, vol. 85, no. 2, pp. 259–298, Feb. 1997.

[25] C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, “Concise protocol over deployed multicore fiber,” Nature Commun., vol. 15, no. 1, 2024, Art. no. 1651.

[26] B. Fröhlich et al., “Secure high-dimensional quantum key distribution based on wavelength-multiplexed time-bin encoding,” in Proc. CLEO: Sci. Innov., 2021, Paper STn1D–3.

[27] S. Bahrami, O. Elmabrok, G. C. Lorenzo, and M. Razavi, “Wavelength assignment in quantum access networks with hybrid wireless-fiber links,” JOSA B, vol. 36, no. 3, pp. B99–B108, 2019.

[28] I. Karakosta-Amarantidou et al., “Urban intermodal quantum key distribution,” Sci. Rep., vol. 9, no. 1, 2019, Art. no. 022307.

[29] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, “Improved key-rate bounds for practical decoy-state quantum key-distribution systems,” Phys. Rev. A, vol. 95, no. 1, 2017, Art. no. 012333, doi: 10.1103/PhysRevA.95.012333.