Performance analysis of inter-satellite round-robin differential-phase-shift quantum key distribution

Ziqing Wang1 · Robert Malaney1

Received: 13 April 2022 / Accepted: 7 September 2022 / Published online: 26 September 2022
© The Author(s) 2022

Abstract
As the vision of global-scale unconditional information security becomes gradually realized, the importance of inter-satellite quantum communications has been rapidly increasing. The recently proposed round-robin differential-phase-shift (RRDPS) quantum key distribution (QKD) protocol has attracted much attention not only due to its potential high error tolerance, but also due to its distinct feature that the information leakage can be bounded without monitoring signal disturbances. Despite many existing implementations over fiber-optic channels, the feasibility of RRDPS QKD over an inter-satellite channel is still unknown. Moreover, despite the current advances in orbital angular momentum (OAM) encoding and temporal mode (TM) encoding, most of the existing studies on RRDPS QKD are restricted to time-bin encoding. In this work, we remedy this situation by exploring the feasibility of performing RRDPS QKD using OAM encoding and TM encoding over an inter-satellite channel. Our results indicate that OAM encoding is preferable to time-bin encoding only under the circumstances where a low dimension and a large receiver aperture are used. However, we find that TM encoding is the best encoding scheme in RRDPS QKD over an inter-satellite channel. In particular, we show that TM encoding not only leads to the best performance and the largest feasible parameter range, but also, for the first time, enables all the theoretically available advantages of an increased dimension to be realized in the context of RRDPS QKD.

Keywords Inter-satellite quantum communications · Round-robin differential-phase-shift quantum key distribution · Orbital angular momentum · Temporal mode

Ziqing Wang
ziqing.wang1@unsw.edu.au

Robert Malaney
r.malaney@unsw.edu.au

1 School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia
1 Introduction

Satellite-based quantum key distribution (QKD) has been considered as a promising solution toward global-scale unconditional information security. Although quantum information can be encoded in any of the degrees of freedom (DoF) of a single photon, currently most real-world systems (e.g., [1, 2]) utilize polarization encoding, which limits the capacity of such systems due to an intrinsically bounded Hilbert space. There have been unceasing efforts to utilize high-dimensional DoF for quantum encoding. Specifically, the time bin, the orbital angular momentum (OAM), and the temporal mode (TM) of single photons have become three of the most promising candidates. During the past decade, the necessary ingredients, including controlled quantum state generation (see, e.g., [3–5]), quantum state manipulation (see, e.g., [6–8]), as well as high-efficiency selective measurement (see, e.g., [9–11]), for the use of these candidates in high-dimensional quantum information protocols have been extensively studied.

It is well known that QKD protocols of a higher dimension\(^1\) can provide benefits such as a better error tolerance [12]. The use of high-dimensional encoding enables two major classes of high-dimensional QKD protocols. As the natural extension of the conventional BB84 protocol, high-dimensional BB84 protocols can be achieved by encoding more than one bit of information per single photon. Extensive efforts have been devoted toward the use of time bins (e.g., [13, 14]), OAM (e.g., [15, 16]), and TMs (e.g., [17, 18]) of single photons in high-dimensional BB84 protocols. Another class of high-dimensional QKD protocols encodes only one bit of information per single photon, and the benefit of an enhanced error tolerance comes with the reduction in the transmitted information. For example, the protocol of [19] can tolerate an error rate of up to 50% in principle. However, just like most QKD protocols, this protocol requires the monitoring of signal disturbance in order to ensure security. It is intuitive that excessive disturbance monitoring, especially over a noisy quantum channel, may reduce the system efficiency and thus undermine the real-world practicability of a QKD protocol.

As another high-dimensional QKD protocol that conveys one bit per photon, the recently proposed round-robin differential-phase-shift (RRDPS) QKD protocol [20] also provides a high error tolerance (up to 50% in principle). A particularly interesting feature of this protocol is that the information leakage can be bounded regardless of the disturbance that Eve introduces to the quantum signals, making the disturbance monitoring unnecessary for security [20]. RRDPS QKD was originally proposed and has been mostly demonstrated using time-bin encoding with interferometer-based measurement devices over an optical fiber channel (see experiments in, e.g., [21–24]). Specifically, an RRDPS QKD system that generates a secret key over 50 km and tolerates a 29% bit error rate has been demonstrated with a passive interferometer configuration for measurement in [22]. A feasible distance of 90 km has also been demonstrated in [23] with an active interferometer configuration for measurement.

---

\(^1\) In this work, the word “dimension” refers only to the dimension of the single-photon signal states used in QKD, and not to our system-model parameters possessing units of length.
experiment has recently demonstrated RRDPS QKD over 140 km [25]. Furthermore, it can be argued that RRDPS QKD is feasible over an optical fiber channel of 200 km [20], and can tolerate a channel error rate close to 50% [26] under typical experimental settings. Despite the excellent scalability provided by the use of time bins, the generation and detection techniques for time-bin encoding usually require active stabilization, presenting a main technical challenge (see discussions in, e.g., [27]).

In principle, the implementation of RRDPS QKD is not restricted to time-bin encoding. Intuitively, the technical challenges associated with time-bin encoding can be eliminated by adopting other encoding schemes that do not require interferometer-based configurations for both state preparation and measurement, and this makes the OAM and TMs two possible candidates. Indeed, OAM-encoded RRDPS QKD over a short Free-Space Optical (FSO) channel has been demonstrated in a proof-of-principle experiment [27]. Although there exists no experimental demonstration of TM-encoded RRDPS QKD so far, the use of TM encoding in RRDPS QKD should also be feasible since the existing devices for TM-encoded quantum information protocols are able to achieve the same functions as their OAM counterparts (see reviews in, e.g., [28–30]). OAM-encoded (TM-encoded) RRDPS QKD can utilize the existing enabling technologies for OAM-encoded (TM-encoded) quantum information protocols, providing the advantages of an inherent stability and a high detection efficiency.

Currently, research on RRDPS QKD is still in its infancy. To the best of our knowledge, there exists no theoretical analysis or numerical investigation regarding the feasibility of RRDPS QKD within the context of satellite-based quantum communications. Regarding the use of other encoding schemes, the proof-of-principle experiment on OAM RRDPS QKD in [27] only considered an ideal circumstance with a perfect single-photon source (that does not give any multi-photon emission), no dark count at detectors, and no OAM-dependent channel loss; therefore, the real-world feasibility of OAM RRDPS QKD remains unclear. Furthermore, which encoding scheme achieves the best performance and/or the largest feasible parameter range in satellite-based RRDPS QKD is still unknown.

In this work, we close the above knowledge gaps by exploring the feasibility of performing RRDPS QKD using OAM encoding and TM encoding within the context of satellite-based quantum communications. Specifically, the performances achieved under different system parameter settings are investigated. For simplicity, we mainly focus on the scenario of inter-satellite quantum communications. Our novel contributions are as follows:

1. We extend the current performance analysis for time-bin-encoded RRDPS QKD (in, e.g., [20, 25]) to the scenarios where OAM encoding and TM encoding are used, respectively. Specifically, realistic system settings (including weak coherent pulses and nonzero detector dark count probabilities) are jointly considered in our performance analysis. For OAM encoding, the OAM-dependent diffraction loss is also taken into account.

2. We evaluate and compare the performances of inter-satellite RRDPS QKD of different dimensions, achieved with OAM encoding and TM encoding, under different settings of system parameters including beam-waist size, receiver-aperture size, and optical misalignment error. The performance of time-bin-encoded RRDPS
QKD, as well as the performance of polarization-encoded 2-dimensional decoy-state BB84 QKD, are also evaluated as benchmarks.

3. We further determine the potential improvements, in both the system performance and the feasible parameter range, provided by incorporating the decoy-state method into inter-satellite RRDPS QKD using OAM encoding and TM encoding.

Our main results are as follows: We find that it is feasible to perform RRDPS QKD over an inter-satellite channel using time-bin encoding, OAM encoding, as well as TM encoding. Specifically, we find that OAM encoding can outperform time-bin encoding in RRDPS QKD over an inter-satellite channel of an anticipated length under the circumstances where a low dimension and a large receiver aperture are used. However, the advantage of OAM encoding (over time-bin encoding) rapidly vanishes as the dimension increases and/or the size of receiver aperture decreases. We also find that an increased dimension leads to different consequences when different encoding schemes are used in inter-satellite RRDPS QKD. Interestingly, we find that TM encoding can be superior to both OAM encoding and time-bin encoding in RRDPS QKD over an inter-satellite channel. Specifically, we show that only TM encoding enables all the theoretically available advantages (i.e., a higher secret key rate, a better error tolerance, and a better loss tolerance) provided by an increased dimension in inter-satellite RRDPS QKD.

2 Operational procedures

We first use an ideal circumstance (where all prepared signals contain only one single photon) to illustrate the operational procedures of $d$-dimensional RRDPS QKD. Specifically, the transmitter (Alice) prepares a single-photon state

$$|\Psi\rangle := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} (-1)^{s_k} |k\rangle,$$

where $s_k \in \{0, 1\}$, and $\{|k\rangle\}_{k=1}^{d}$ denotes the set of $d$ standard basis states spanning a $d$-dimensional Hilbert space $\mathcal{H}_d$ (which is referred to as the encoding subspace).

Upon receipt of the signal, the receiver (Bob) randomly chooses an integer $r$ such that $1 \leq r \leq d - 1$. He then measures the phase difference between $|m\rangle$ and $|m + r\rangle$ ($m + r \leq d$). This is equivalent to projecting the incoming signal state onto the state $(|m\rangle \pm |m + r\rangle)/\sqrt{2}$. It is clear that two single-photon detectors are required to obtain a definitive result.

Equipped with two photon-number-resolving detectors, Bob retains only the events in which a single-photon click occurs at one of his detectors. Whenever this happens, Bob announces the random integers $\{m, r\}$ and records the measured phase difference as his sifted key bit $s_B$. Alice records $s_A = s_m \oplus s_{m+r}$ as her sifted key bit. If Bob receives $|\Psi\rangle$ without any disturbance, he learns $s_A$ without error.

In reality, however, the transmitted signal cannot be guaranteed to contain only one single photon. Furthermore, the eavesdropper (Eve) may also introduce disturbances and information leakage. In this work, we adopt an improved bound on the amount
of information leaked to Eve. Specifically, in $d$-dimensional RRDPS QKD, when the transmitted signal contains $n$ photons Eve’s information can be bounded by

$$I_{AE}(n; d) \leq I_{AE}^{upper}(n; d) = \text{Max}_{x_1, x_2, \ldots, x_{n+1}} \left\{ \frac{\sum_{a=1}^{n} \varphi((d-a)x_a, ax_a+1)}{d-1} \right\},$$

(2)

where nonnegative real parameters $\{x_a\}$ satisfy $\sum_{a=1}^{n+1} x_a = 1$ (note that, $\{x_a\}$ are fundamentally determined by Eve’s attack – the optimization over them is to ensure Eve obtains the maximum amount of information for a given pair of $\{n, d\}$), and $\varphi(x, y) = -x \log_2 x - y \log_2 y + (x+y) \log_2(x+y)$ [25]. This information bound can be evaluated effectively by solving a numerical optimization problem with $(n+1)$ nonnegative real parameters. It can be shown that $I_{AE}^{upper}(n; d) < 1$ for $n \leq d - 2$ [25], and following common practice (in, e.g., [31]) we set $I_{AE}^{upper}(n; d) = 1$ for $n \geq d - 1$. It is clear that $I_{AE}^{upper}(n; d)$ does not depend on the signal disturbance caused by Eve; therefore, RRDPS QKD does not require the monitoring of signal disturbance in order to ensure security.

3 Inter-satellite QKD

3.1 System model

Here we introduce the typical system model for inter-satellite QKD (illustrated in Fig. 1). Specifically, two communication parities, namely, Alice and Bob are both satellites, and they wish to share secret keys over an inter-satellite optical channel of distance $L$. We denote the beam-waist radius at the transmitter and the receiver-aperture radius as $w_0$ and $r_a$, respectively. We also denote the mean photon number per signal pulse, the central wavelength, the single-photon transmissivity, the detector dark count probability per signal pulse, and the optical misalignment error of the detection system as $\mu$, $\lambda_0$, $\eta$, $P_{\text{dark}}$, and $e_{\text{mis}}$, respectively. Unless otherwise specified, we set $w_0 = 15$ cm (following [16, 18]), $\lambda_0 = 1064$ nm (following [16, 18]), and $P_{\text{dark}} = 10^{-6}$ (following [25]).

3.2 General assumptions

Unless otherwise specified, our general assumptions are listed as follows:

- We assume that weak coherent pulses are used as signal pulses, and we assume that the photon number of the signal pulses follows a Poisson distribution.
- We assume that the transmitted signals in both time-bin-encoded RRDPS QKD and TM-encoded RRDPS QKD have the same fundamental Gaussian spatial profile. We assume that the transmitted signals in OAM-encoded RRDPS QKD contain Laguerre–Gaussian (LG) spatial modes with different OAM numbers $l$ and the same radial index $p = 0$ (for detailed descriptions of these LG modes, one can refer to our previous work [16]).
Fig. 1 System model for inter-satellite QKD

- We assume that both time-bin-encoded RRDPS QKD and OAM-encoded RRDPS QKD use exactly the same Gaussian temporal pulse shape. We assume that TM-encoded RRDPS QKD uses Hermite–Gaussian (HG) temporal modes2 (for detailed descriptions of these HG modes, one can refer to our previous work [18]).
- We assume a unit efficiency for quantum state preparation. We assume that all photon detectors are independent and have the same \( P_{\text{dark}} \) value. We further assume that all photon detectors have a unit efficiency.3
- We restrict ourselves to the infinite-key limit, and a reconciliation efficiency of 1.
- We assume that \( e_{\text{mis}} \) quantifies the collective effect of all types of errors such as system calibration errors, state preparation and measurement errors, channel errors, and all other imperfection-induced errors (e.g., tracking errors). Note that, the channel errors can be generally considered to be very small over an inter-satellite channel.4
- When the decoy-state method is incorporated into RRDPS QKD, we assume that infinite decoy states are used.5
- When the performance of 2-dimensional decoy-state BB84 QKD is evaluated as a benchmark, we assume that polarization encoding is used. We also assume that Bob uses threshold photon detectors which are independent and have the same specifications (including the \( P_{\text{dark}} \) value) as in RRDPS QKD.

Due to their spatial-mode nature, OAM basis states experience OAM-dependent diffraction during propagation, and such diffraction is more significant for a larger OAM number. As a result, in a specific QKD system the OAM basis state with a larger

---

2 Note that, the exact form of the temporal pulse shape is irrelevant in this work since the secret key rate has the unit bits/pulse.

3 For time-bin encoding, the overall detection efficiency is thus limited by non-interfering events due to the use of an interferometer for measurements (see discussions in Sect. 4.1.1). For OAM encoding and TM encoding the overall detection efficiency becomes 1 since no interferometer is needed (see discussions in Sect. 4.1.2).

4 In other types of satellite-based channels (e.g., satellite-to-Earth channels), the main contributors to channel errors include the arrival-time fluctuations (for time-bin encoding), the atmospheric optical turbulence (for OAM encoding), and the atmospheric chromatic dispersion (for TM encoding).

5 Note that, it has been shown that a practically feasible two-decoy-state configuration can achieve a performance that is very close to that of the infinite-decoy-state configuration in RRDPS QKD [31].
OAM number acquires a larger Gouy phase and suffers from a higher diffraction loss [32]. These two phenomena can modify the relative phases among the used OAM basis states, rendering OAM QKD over a long-distance FSO channel nonviable [33]. Due to the absence of atmospheric turbulence in space, we assume that the OAM-dependent Gouy phase is perfectly controlled or compensated for.\(^6\) This can be achieved by, e.g., applying a deterministic set of additional OAM-dependent phase patterns to the received signal. For the OAM-dependent diffraction loss, we assume that Bob applies a deterministic set of additional OAM-dependent losses to his received signal in order to equalize (i.e., reduce) the amplitudes of all lower-order OAM basis states to the amplitude of the highest-order OAM basis state in the received signal.\(^7\)

### 3.3 Channel loss

Based on our system model and assumptions, here we analyze the channel losses for RRDPS QKD systems utilizing different encoding schemes. Despite adopting the common notation “loss,” in calculations we mainly use the single-photon transmissivity \(\eta\) with the relation \(\text{Loss [dB]} = -10 \log_{10} \eta\).

For \(d\)-dimensional RRDPS QKD utilizing OAM encoding, \(\eta\) is given by [18, Eq. (A7) of Supplementary Material]

\[
\eta_{\text{OAM}} = 1 - \frac{\Gamma\left(1 + \left\lfloor \frac{d}{2} \right\rfloor, \frac{2r^2}{w_0^2 + (\alpha_L^2 \lambda w_0)^2}\right)}{\left\lfloor \frac{d}{2} \right\rfloor!},
\]

where \(\Gamma(\cdot, \cdot)\) is the (upper) incomplete Gamma function. The quantity \(\left\lfloor \frac{d}{2} \right\rfloor\) in the above equation represents the largest OAM number that should be used in \(d\)-dimensional OAM RRDPS QKD in order to give the highest transmissivity [18].

For any protocol (including the polarization-encoded 2-dimensional decoy-state BB84 QKD protocol investigated as a benchmark) whose transmitted signals have the fundamental Gaussian spatial profile, \(\eta\) is given by [18, Eq. (A9) of Supplementary Material]

\[
\eta_G = 1 - \exp\left(-\frac{2r^2}{w_0^2 + (\frac{\lambda L}{\pi w_0})^2}\right).
\]

\(^6\) Note that, this is viable and rather straightforward to implement (see discussions in, e.g., [27]).

\(^7\) Note that, both the set of additional OAM-dependent phase patterns (for Gouy phase compensation) and the required set of additional OAM-dependent losses (for amplitude equalization) can be easily estimated given the channel distance and other system settings (e.g., the beam-waist radius and the signal wavelength). Note, there exist additional compensation techniques aiming to counteract the effects of the OAM-dependent diffraction in long-distance quantum information protocols (see, e.g., [33]).
4 Performance analysis

In this section, we analyze the performance of RRDPS QKD protocols utilizing different encoding schemes in terms of the secret key rate. Specifically, we are interested in the secret key rate in \textit{bits per pulse}. We also analyze the performance of RRDPS QKD with the decoy-state method incorporated. The performance of polarization-encoded 2-dimensional decoy-state BB84 QKD is also investigated as a benchmark.

4.1 RRDPS QKD (without decoy-state method)

4.1.1 Time-bin encoding

When time-bin encoding is used, a projection onto the state $|m\rangle \pm |m + r\rangle / \sqrt{2}$ is generally achieved by a shift-type interferometer with a random delay $r$ (followed by a time-resolved photon detection). For a delay value $1 \leq r \leq d - 1$, both of Bob’s detectors open $d - r$ time windows to detect the incoming signal. Here, we provide an overview regarding the performance analysis of time-bin RRDPS QKD for completeness – details can be found in [25].

The gain (i.e., counting rate) for delay value $r$ (denoted as $Q_r$) can be calculated as

$$Q_r = (1 - P_{\text{dark}})^{2(d-r)-1} e^{-(d-r)\eta\mu} [(d-r)\eta\mu + 2(d-r)P_{\text{dark}}].$$  \hspace{1cm} (5)

The overall gain is then given by

$$Q = \frac{1}{d-1} \sum_{r=1}^{d-1} Q_r.$$

The overall quantum error rate $E$ is given by

$$E = \frac{1}{Q(d-1)} \sum_{r=1}^{d-1} E_r Q_r,$$

where

$$E_r Q_r = (1 - P_{\text{dark}})^{2(d-r)-1} e^{-(d-r)\eta\mu}$$

$$\times [(d-r)\eta\mu e_{\text{mis}} + (d-r)P_{\text{dark}}].$$  \hspace{1cm} (8)

Finally, the secret key rate is given by

$$R_{\text{RRDPS}}^{\text{TB}} = \frac{1}{d} \left[ Q \left[ 1 - h_2(E) \right] - e_{\text{src}} - (Q - e_{\text{src}}) I_{AE}^{\text{upper}}(v_{th}; d) \right].$$  \hspace{1cm} (9)
where

\[ e_{\text{src}} = 1 - \sum_{n=0}^{v_{\text{th}}} \frac{(d \mu)^n e^{-d \mu}}{n!}, \quad (10) \]

is the probability that the photon number of the transmitted signal is larger than the threshold photon number \( v_{\text{th}} \) [20]. In security analyses (see, e.g., [20]), it is assumed that (i) all transmitted signals with a photon number smaller than \( v_{\text{th}} \) give Eve the information \( I_{\text{AE}}^{\text{upper}}(v_{\text{th}}; d) \), and (ii) all transmitted signals with a photon number larger than \( v_{\text{th}} \) give Eve the maximum amount of information (i.e., one bit). Note that, the function \( h_2(\cdot) \) in Eq. (9) denotes the binary Shannon entropy, and this function is defined as \( h_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x) \). Note that both \( \mu \) and \( v_{\text{th}} \) should be optimized to maximize the secret key rate.

### 4.1.2 OAM encoding and TM encoding

When OAM encoding or TM encoding is used in RRDPS QKD, an interferometer is usually not needed for signal measurement. A projection onto the state \((|m\rangle \pm |m + r\rangle)/\sqrt{2}\) can be achieved by carefully designed devices. Such devices include the spatial light modulator for OAM encoding [27], and the quantum pulse gate for TM encoding (see, e.g., [29] for a comprehensive review). Furthermore, a detection efficiency of unity can, in principle, be achieved when carefully designed quantum state sorters are used (see discussions in, e.g., [27]). Note that, unlike the case of time-bin encoding, both of Bob’s detectors only need to open one time window to detect the incoming signal; therefore, the overall gain is given by

\[ Q = (1 - P_{\text{dark}})e^{-\eta \mu} (\eta \mu + 2 P_{\text{dark}}). \quad (11) \]

The overall quantum error rate \( E \) is given by \( E = EQ/Q \), where

\[ EQ = (1 - P_{\text{dark}})e^{-\eta \mu} (\eta \mu e_{\text{mis}} + P_{\text{dark}}). \quad (12) \]

The secret key rate is given by

\[ R^{\text{OAM/TM}}_{\text{RRDPS}} = Q \left[ 1 - h_2(E) \right] - e_{\text{src}} - (Q - e_{\text{src}}) I_{\text{AE}}^{\text{upper}}(v_{\text{th}}; d), \quad (13) \]

where

\[ e_{\text{src}} = 1 - \sum_{n=0}^{v_{\text{th}}} \frac{\mu^n e^{-\mu}}{n!}, \quad (14) \]

is the probability that the photon number of the transmitted signal is larger than \( v_{\text{th}} \) [20]. Note that both \( \mu \) and \( v_{\text{th}} \) should be jointly optimized to maximize the secret key rate.
4.2 RRDPS QKD with decoy-state method

In RRDPS QKD, the bound of information leakage can be given as a function of the number of photons contained within the transmitted signal. Recall the assumptions in Sect. 4.1 that (i) all transmitted signals with a photon number smaller than $v_{th}$ give Eve the information $I_{AE}^{upper}(v_{th}; d)$, and (ii) all transmitted signals with a photon number larger than $v_{th}$ give Eve the maximum amount of information (i.e., one bit). These assumptions may be overly pessimistic. Intuitively, it is natural to introduce the decoy-state method to improve the performance of RRDPS QKD by estimating the yields $\{Y_n\}$ of the transmitted signals with different photon numbers $\{n\}$ [34]. In this work, we assume that infinite decoy states are used (recall Sect. 3.2), and in the infinite-key limit this means that $\{Y_n\}$ can be estimated accurately. Although incorporating the decoy-state method in RRDPS QKD may require a more complicated setup, this does not change the fact that RRDPS QKD requires no signal disturbance monitoring to ensure security.

4.2.1 Time-bin encoding

Here, we provide an overview regarding the performance analysis of time-bin decoy-state RRDPS QKD for completeness – details can be found in [31]. For a delay value $1 \leq r \leq d - 1$, the yield of an $n$-photon transmitted signal is given by

$$Y_{nr} = \left(1 - \frac{d - r}{d} \eta \right)^{n-1} (1 - P_{\text{dark}})^{2(d-r)-1} \times \left[ \frac{d - r}{d} n \eta + 2 \left(1 - \frac{d - r}{d} \eta \right) (d - r) P_{\text{dark}} \right].$$

(15)

The mean yield of an $n$-photon transmitted signal is given by

$$Y_n = \frac{1}{d-1} \sum_{r=1}^{d-1} Y_{nr},$$

(16)

and the overall gain is given by

$$Q = \sum_{n=0}^{\infty} Y_n \frac{(d \mu)^n e^{-d \mu}}{n!}.$$  

(17)

The overall quantum error rate is given by

$$E = \frac{1}{Q(d-1)} \sum_{n=0}^{\infty} \sum_{r=1}^{d-1} E_{nr} Y_{nr} \frac{(d \mu)^n e^{-d \mu}}{n!},$$

(18)

For more discussions regarding incorporating the decoy-state method into RRDPS QKD, one can refer to, e.g., [26, 31].
where
\[
E_{nr} Y_{nr} = \left(1 - \frac{d - r}{d} \eta \right)^{n-1} (1 - P_{\text{dark}})^{2(d-r)-1} \times \left[ \frac{d - r}{d} n \eta \epsilon_{\text{mis}} + \left(1 - \frac{d - r}{d} \eta \right) (d - r) P_{\text{dark}} \right].
\] (19)

The secret key rate is then given by
\[
R_{\text{TB}}^{\text{RRDPS,DS}} = \frac{1}{d} \left[ Q [1 - h_2(E)] - \sum_{n=1}^{\infty} Y_n (d \mu)^n e^{-d \mu} I_{\text{AE}}^{\text{upper}} (n; d) \right].
\] (20)

Note that, \( \mu \) should be optimized to maximize the secret key rate.

### 4.2.2 OAM encoding and TM encoding

When OAM encoding or TM encoding is used in decoy-state RRDPS QKD, the yield of an \( n \)-photon transmitted signal is given by
\[
Y_n = (1 - \eta)^{n-1} (1 - P_{\text{dark}}) [n \eta + 2 (1 - \eta) P_{\text{dark}}],
\] (21)

and the overall gain is given by
\[
Q = \sum_{n=0}^{\infty} Y_n \mu^n e^{-\mu} n!.\] (22)

The overall quantum error rate is given by
\[
E = \frac{1}{Q} \sum_{n=0}^{\infty} E_n Y_n \mu^n e^{-\mu} \frac{n!}{n!}.
\] (23)

where
\[
E_n Y_n = (1 - \eta)^{n-1} (1 - P_{\text{dark}}) \left[ n \eta \epsilon_{\text{mis}} + (1 - \eta) P_{\text{dark}} \right].
\] (24)

The secret key rate is then given by
\[
R_{\text{OAM/TM}}^{\text{RRDPS}} = Q [1 - h_2(E)] - \sum_{n=1}^{\infty} Y_n \mu^n e^{-\mu} I_{\text{AE}}^{\text{upper}} (n; d).
\] (25)

Note that, \( \mu \) should be optimized to maximize the secret key rate.
4.3 Generalized decoy-state BB84 QKD

It is meaningful to use decoy-state BB84 QKD protocols as a benchmark. Specifically, in this work we adopt the generalized protocol in [35], and we assume the $d$-detector configuration for $d$-dimensional decoy-state BB84 QKD. Following [35], the yield of transmitted vacuum signals is given by

$$Y_0 = 1 - (1 - P_{\text{dark}})^d.$$  \hspace{1cm} (26)

The overall gain is given by

$$Q_\mu = Y_0 + 1 - e^{-\mu \eta}.$$  \hspace{1cm} (27)

The overall quantum error rate is given by

$$E_\mu = \frac{e_0 Y_0 + e_{\text{mis}} \left(1 - e^{-\mu \eta}\right)}{Y_0 + 1 - e^{-\mu \eta}}.$$  \hspace{1cm} (28)

The gain of single-photon transmitted signals is given by

$$Q_1 = (Y_0 + \eta) \mu e^{-\mu}.$$  \hspace{1cm} (29)

The quantum error rate of single-photon transmitted signals is given by

$$E_1 = \frac{e_0 Y_0 + e_{\text{mis}} \eta}{Y_0 + \eta}.$$  \hspace{1cm} (30)

The secret key rate is given by

$$R_{\text{BB84}}^{(d)} = Q_0 \log_2 d + Q_1 \left[\log_2 d - h_d \left(E_1\right)\right] - Q_\mu h_d \left(E_\mu\right),$$  \hspace{1cm} (31)

where $h_d(x) = -x \log_2[x/(d-1)] - (1-x) \log_2(1-x)$ is the $d$-dimensional modified Shannon entropy [35]. For a fair comparison, in Eq. (31) we have set the reconciliation efficiency to 1, and we consider the use of the efficient BB84 protocol following [35]. For the same reason, we also assume infinite decoy states. Note that, $\mu$ should be optimized to maximize the secret key rate.

5 Numerical results

In all figures, we use abbreviations in the figure legends for concise reasons. Specifically, in the figure legends we refer to time-bin encoding, TM encoding, OAM encoding, RRDPS QKD (without incorporating the decoy-state method), and RRDPS QKD (with the decoy-state method incorporated) as TB, OAM, TM, RRDPS, and DS RRDPS, respectively. Note that, the figure legend $[d = 2, \text{Benchmark}]$ represents polarization-encoded 2-dimensional decoy-state BB84 QKD protocol. When plotting
QKD performances against the receiver-aperture radius $r_a$, for a certain beam-waist radius $w_0$ we consider $r_a$ values ranging from $w_0$ to 1 m.

5.1 $L = 200$ km, $w_0 = 15$ cm

In Fig. 2, we plot the performances of inter-satellite RRDPS QKD at $L = 200$ km. Both the performances achieved without (Fig. 2a, c, e) and with (Fig. 2b, d, f) the decoy-state method incorporated are plotted. In each sub-figure, the performances achieved by different encoding schemes (i.e., time-bin encoding, OAM encoding, and TM encoding) using one of the three typical dimensions (i.e., $d = 8$, $d = 16$, and $d = 32$) are plotted against two system parameters (i.e., optical misalignment error $e_{\text{mis}}$ and receiver-aperture radius $r_a$). The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.

From all sub-figures of Fig. 2, we first observe that the QKD performance is reduced as $e_{\text{mis}}$ increases and/or $r_a$ decreases, and a larger $r_a$ value improves the error tolerance (especially when OAM encoding is used). We also observe that time-bin encoding and TM encoding both enable RRDPS QKD to achieve a better error tolerance than 2-dimensional decoy-state BB84 QKD (whose maximum tolerable error is $\sim 11\%$) over the inter-satellite channel even when the smallest $r_a$ value (i.e., $r_a = 15$ cm) is used. However, when OAM encoding is used, a much larger $r_a$ value is needed for RRDPS QKD to outperform 2-dimensional decoy-state BB84 QKD in terms of error tolerance over the inter-satellite channel. This observation can be explained by the fact that, under the same $r_a$ value OAM-encoded RRDPS QKD suffers from an OAM-dependent diffraction loss that can be much higher than the loss experienced by time-bin-encoded or TM-encoded RRDPS QKD.

Comparing Fig. 2(a, b), (c, d), and (e, f), we clearly observe that incorporating the decoy-state method in RRDPS QKD improves the secret key rate, error tolerance, and the feasible $r_a$ range over the inter-satellite channel when any of the encoding schemes is used. For example, incorporating the decoy-state method in RRDPS QKD reduces the minimum $r_a$ value necessary for OAM RRDPS QKD to outperform 2-dimensional decoy-state BB84 QKD in terms of error tolerance over the inter-satellite channel.

From all sub-figures of Fig. 2, we further observe that OAM encoding can outperform time-bin encoding under certain circumstances. Specifically, for $d = 8$ and $d = 16$, OAM encoding outperforms time-bin encoding when $r_a$ is sufficiently large. However, OAM encoding quickly becomes nonviable as $r_a$ becomes smaller due to the rapidly increasing OAM-dependent diffraction loss. Furthermore, for $d = 32$ OAM encoding leads to a very small feasible parameter range and hardly achieves any advantage over time-bin encoding due to the significant OAM-dependent diffraction loss for a large OAM number. Such observations indicate that OAM encoding may be preferable to time-bin encoding in inter-satellite RRDPS QKD only when $r_a$ is sufficiently large and/or the dimension $d$ is sufficiently low. Interestingly, from all sub-figures of Fig. 2 we find that TM encoding provides the best performance, the best error tolerance, and the largest feasible $r_a$ range. This indicates that TM encoding is preferable to both OAM encoding and time-bin encoding in inter-satellite RRDPS QKD.
Fig. 2 Performances of inter-satellite RRDPS QKD at $L = 200$ km. Both the performances achieved without (Fig. 2a, c, e) and with (Fig. 2b, d, f) the decoy-state method incorporated are plotted. In each subfigure, the performances achieved by different encoding schemes (i.e., time-bin encoding, OAM encoding, and TM encoding) using one of the three typical dimensions (i.e., $d = 8$, $d = 16$, and $d = 32$) are plotted against two system parameters (i.e., optical misalignment error $e_{\text{mis}}$ and receiver-aperture radius $r_a$). The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.

Since a higher dimension $d$ essentially reduces the information leakage to Eve, it is intuitive to think that increasing the dimension $d$ should provide improvements to RRDPS QKD over the inter-satellite channel. Although the system performances achieved with different dimensions are plotted in the sub-figures of Fig. 2, the consequences of increasing the dimension $d$ in inter-satellite RRDPS QKD are not explicitly
illustrated in these sub-figures. To remedy this situation, in Fig. 3 we re-plot the performances of inter-satellite RRDPS QKD at $L = 200$ km presented in Fig. 2. Specifically, in each sub-figure the performances achieved by one of the three encoding schemes (i.e., time-bin encoding, OAM encoding, and TM encoding) using all three typical dimensions (i.e., $d = 8$, $d = 16$, and $d = 32$) are plotted together against two system parameters (i.e., optical misalignment error $e_{\text{mis}}$ and receiver-aperture radius $r_a$) for a better comparison. Both the performances achieved without (Fig. 3a, c, e) and with (Fig. 3b, d, f) the decoy-state method incorporated are plotted. The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.

From the sub-figures of Fig. 3, we can clearly see that increasing the dimension $d$ leads to different consequences when different encoding schemes are used in inter-satellite RRDPS QKD. Specifically, when time-bin encoding (see Fig. 3a, b) or TM encoding (see Fig. 3e, f) is used, an increased dimension $d$ generally improves the error tolerance of inter-satellite RRDPS QKD. However, an increase in dimension $d$ can reduce the secret key rate of time-bin-encoded inter-satellite RRDPS QKD when $e_{\text{mis}}$ is sufficiently low and $r_a$ is sufficiently large. This can be explained by the fact that $d$-dimensional time-bin-encoded RRDPS QKD utilizes $d$ sequential pulses to generate one single bit (also recall the $1/d$ scaling factor in Eq. 9).

Figure 3c, d indicates that things are more complicated when OAM encoding is used. Specifically, without using the decoy-state method, increasing the dimension from $d = 8$ to $d = 16$ improves the error tolerance and reduces the feasible $r_a$ range at the same time. A further increase in dimension from $d = 16$ to $d = 32$ reduces both the error tolerance and the feasible $r_a$ range when OAM encoding is used. Furthermore, an increased dimension $d$ also leads to a lower QKD performance when $e_{\text{mis}}$ is sufficiently low. After using the decoy-state method, increasing the dimension $d$ seems to always improve the error tolerance; however, doing so will still cause a reduced feasible $r_a$ range and a lower secret key rate. These observations are all due to the increased OAM-dependent diffraction loss when a higher dimension is used.

5.2 $L = 200$ km, $w_0 = 5$ cm

Until now we have been setting the beam-waist radius to $w_0 = 15$ cm following our previous works [16, 18]. Despite not being unreasonably large, such a beam-waist radius is in fact larger than most of the used values in the existing implementations of satellite-based QKD. For example, the Micius quantum satellite features a 300-mm-aperture (in diameter) telescope that provides a near-diffraction-limited far-field divergence of $\sim 10 \mu$rad at $\sim 850$ nm [2]. Using this information, a beam-waist radius $w_0^{\text{Micius}} \approx 5.5$ cm (which is much smaller than our current setting $w_0 = 15$ cm) can be derived. In fact, our choice of a larger beam-waist radius essentially reduces the beam diffraction, making OAM-based quantum information protocol more feasible.

Note that, an increased dimension $d$ also improves the feasible $r_a$ range when time-bin encoding or TM encoding is used. However, this cannot be clearly observed in Figs. 2 and 3 since both time-bin-encoded and TM-encoded inter-satellite RRDPS QKD achieves positive secret key rates even under the smallest $r_a$ value. This is essentially due to the fact that the minimum loss ($\eta_{\text{TB}}^\min$ or $\eta_{\text{TM}}^\min$) at $L = 200$ km is not large enough. The feasibility of time-bin-encoded and TM-encoded inter-satellite RRDPS QKD in the high-loss regime is presented in Fig. 5.
Fig. 3 A re-plot of the performances of inter-satellite RRDPS QKD at $L = 200 \text{ km}$ presented in Fig. 2. Specifically, in each sub-figure the performances achieved by one of the three encoding schemes (i.e., time-bin encoding, OAM encoding, and TM encoding) using all three typical dimensions (i.e., $d = 8$, $d = 16$, and $d = 32$) are plotted together against two system parameters (i.e., optical misalignment error $e_{\text{mis}}$ and receiver-aperture radius $r_a$) for a better comparison. Both the performances achieved without (Fig. 3a, c, e) and with (Fig. 3b, d, f) the decoy-state method incorporated are plotted. The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.
To determine the feasibility of inter-satellite RRDPS QKD utilizing the existing operational platforms (e.g., the Micius quantum satellite), we adopt all settings of Fig. 3 except we change the beam-waist radius to $w_0 = 5$ cm to mimic the setting of the Micius quantum satellite. In Fig. 4, we plot the performances of inter-satellite RRDPS QKD at $L = 200$ km with $w_0 = 5$ cm. In each sub-figure, the performances achieved by one of the three encoding schemes (i.e., time-bin encoding, OAM encoding, and TM encoding) using all three typical dimensions (i.e., $d = 8$, $d = 16$, and $d = 32$) are plotted together against two system parameters (i.e., optical misalignment error $e_{\text{mis}}$ and receiver-aperture radius $r_a$). Both the performances achieved without (Fig. 4a, c, e) and with (Fig. 4b, d, f) the decoy-state method incorporated are plotted. The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.

From Fig. 4, we find that most of the observations made from Fig. 3 still hold. Comparing the sub-figures of Figs. 4 and 3 one by one, we can clearly see that the use of a smaller $w_0$ value reduces the QKD performance due to a higher diffraction loss. In terms of error tolerance and feasible $r_a$ range, we observe that time-bin encoding is more affected than TM encoding, and RRDPS QKD without incorporating the decoy-state method is more affected than RRDPS QKD with the decoy-state method incorporated. As expected, the results in Fig. 4c, d clearly indicate the detrimental impact imposed on OAM-encoded inter-satellite RRDPS QKD by a smaller $w_0$ value. Specifically, a very small feasible $r_a$ range can be achieved by OAM encoding even for $d = 8$, and no positive secret key rate can be achieved by OAM encoding for $d = 16$ and $d = 32$. This is due to the significant OAM-dependent diffraction loss caused by a smaller $w_0$ value. In order to utilize OAM encoding in inter-satellite RRDPS QKD, a larger beam-waist radius $w_0$ must be used.

### 5.3 The optimality of TM encoding

It can be seen from Fig. 2 that TM encoding outperforms both OAM encoding and time-bin encoding in terms of the secret key rate, the error tolerance, and the feasible $r_a$ range. Interestingly, both Figs. 3 and 4 also indicate that TM encoding (see Figs. 3e, f and 4e, f) is the only encoding scheme that gives a higher secret key rate, a better error tolerance, and a larger feasible $r_a$ range at the same time when the dimension $d$ increases. These observations indicate that TM encoding is superior to both OAM encoding and time-bin encoding in RRDPS QKD over an inter-satellite channel.

### 5.4 Performance against loss

In Figs. 2, 3, and 4, we have observed that both time-bin-encoded and TM-encoded RRDPS QKD achieved positive secret key rate over an $L = 200$ km inter-satellite channel even when the smallest receiver-aperture size is used. Although such an observation indicates that both time-bin encoding and TM encoding are promising paradigms for RRDPS QKD over a typical inter-satellite channel, none of the results in Figs. 2, 3, or 4 provide full information regarding the loss tolerance of time-bin-
Fig. 4 The performances of inter-satellite RRDPS QKD at $L = 200$ km. Here we set the beam-waist radius to $w_0 = 5$ cm in order to mimic the setting of the Micius quantum satellite [2]. In each sub-figure, the performances achieved by one of the three encoding schemes (i.e., time-bin encoding, OAM encoding, and TM encoding) using all three typical dimensions (i.e., $d = 8$, $d = 16$, and $d = 32$) are plotted together against two system parameters (i.e., optical misalignment error $e_{\text{mis}}$ and receiver-aperture radius $r_a$). Both the performances achieved without (Fig. 4a, c, e) and with (Fig. 4b, d, f) the decoy-state method incorporated are plotted. The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.
encoded and TM-encoded RRDPS QKD\(^\text{10}\). Specifically, some important questions yet to be answered are as follows.

1. Which encoding scheme gives the best loss tolerance in RRDPS QKD?
2. How does an increased dimension \(d\) affect the loss tolerance of time-bin-encoded and TM-encoded RRDPS QKD?
3. Can RRDPS QKD outperform 2-dimensional decoy-state BB84 QKD in terms of loss tolerance over an inter-satellite channel?

To answer all these questions, in Fig. 5 we plot the performances of inter-satellite RRDPS QKD achieved without (Fig. 5a, c, e) and with (Fig. 5b, d, f) the decoy-state method incorporated. In each sub-figure, the performances achieved by time-bin encoding and TM encoding using one of the three typical dimensions (i.e., \(d = 8\), \(d = 16\), and \(d = 32\)) are plotted together against the optical misalignment error \(e_{\text{mis}}\) and the total loss (in dB). The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.

From Fig. 5, we first clearly see that both time-bin encoding and TM encoding enable RRDPS QKD (of all considered dimensions) to outperform 2-dimensional decoy-state BB84 QKD in terms of error tolerance within their respective acceptable loss ranges. We also see that an increased dimension \(d\) improves the loss tolerance of RRDPS QKD when time-bin encoding or TM encoding is used. Specifically, without using the decoy-state method (see Fig. 5a, c, e), TM-encoded RRDPS QKD requires \(d = 32\) to achieve a level of loss tolerance similar to that of 2-dimensional decoy-state BB84 QKD (see Fig. 5e). However, it seems that such a level of loss tolerance cannot be achieved by time-bin-encoded RRDPS QKD even for \(d = 32\) (also see Fig. 5e). Comparing Fig. 5(a, b), (c, d), and (e, f), we clearly observe that incorporating the decoy-state method in RRDPS QKD improves both error tolerance and loss tolerance when time-bin encoding or TM encoding is used. Specifically, after incorporating the decoy-state method (see Fig. 5b, d, f), time-bin-encoded RRDPS QKD can achieve a level of loss tolerance similar to (although still slightly worse than) that of 2-dimensional decoy-state BB84 QKD. On the other hand, TM-encoded decoy-state RRDPS QKD only requires \(d = 8\) to outperform 2-dimensional decoy-state BB84 QKD in terms of loss tolerance (see Fig. 5b).

Interestingly, from all the sub-figures of Fig. 5 we clearly observe that TM encoding outperforms time-bin encoding in terms of secret key rate, error tolerance, as well as

\(^{10}\) Due to OAM-dependent diffraction, OAM-encoded RRDPS QKD intrinsically suffers from a higher loss than TM-encoded or time-bin-encoded RRDPS QKD of the same dimension under the same system settings. Since OAM encoding was involved in the performance comparison, in Figs. 2, 3, and 4 we have plotted our results against \(r_a\) (rather than loss) in order to faithfully capture the effect of OAM-dependent diffraction on OAM-encoded RRDPS QKD. Although the settings of Figs. 2, 3, and 4 reflect the typical scenarios of inter-satellite quantum communications, the corresponding losses suffered by time-bin-encoded and TM-encoded RRDPS QKD under these settings are not high enough for the investigation of the loss tolerance of time-bin-encoded and TM-encoded RRDPS QKD. In order to carry out such an investigation, we have to extend our attention to the high-loss regime that cannot be reached by the settings of Figs. 2, 3, and 4. Such a high-loss regime may be reached in a future nano-satellite scenario where extremely small beam-waist and receiver-aperture sizes have to be used (see, e.g., [36] for the size of an operational quantum nano-satellite). Since TM-encoded and time-bin-encoded RRDPS QKD suffer from the same amount of loss, we can straightforwardly plot our results against loss in Fig. 5, where OAM encoding is not involved in the performance comparison.
Fig. 5 Performances of inter-satellite RRDPS QKD achieved without (Fig. 5a, c, e) and with (Fig. 5b, d, f) the decoy-state method incorporated. In each sub-figure, the performances achieved by time-bin encoding and TM encoding using one of the three typical dimensions (i.e., $d = 8$, $d = 16$, and $d = 32$) are plotted together against optical misalignment error $e_{\text{mis}}$ and total loss (in dB). The performance of 2-dimensional decoy-state BB84 QKD is also plotted as a benchmark.

Loss tolerance in RRDPS QKD of all considered dimensions. This observation holds regardless of whether the decoy-state method is incorporated. It is also clear that TM encoding is the only one encoding method that enables all the theoretically available advantages (i.e., a higher secret key rate, a better error tolerance, and a better loss tolerance) provided by an increased dimension in RRDPS QKD at the same time.
6 Conclusions

Inter-satellite quantum communications have been considered as a crucial enabler of global-scale unconditional information security. The use of RRDPS QKD within the context of inter-satellite quantum communications not only provides a high error tolerance, but also potentially leads to a higher system efficiency and an improved real-world practicability due to the elimination of the need for signal disturbance monitoring. The use of novel (and increasingly mature) OAM encoding and TM encoding schemes eliminates the technical challenges associated with signal measurement in time-bin encoding (which is the default encoding scheme for RRDPS QKD), further improving the practical feasibility of RRDPS QKD. In this work, we explored the feasibility of performing inter-satellite RRDPS QKD utilizing OAM encoding and TM encoding schemes. We found that utilizing the OAM and TMs of single photons in RRDPS QKD is indeed feasible over a typical inter-satellite channel.

First, we extended the current performance analyses for time-bin-encoded RRDPS QKD (over a fiber-optic channel) to the scenarios where OAM encoding and TM encoding are used over an inter-satellite channel. We then evaluated and compared the performances of inter-satellite RRDPS QKD, of different dimension, achieved with OAM encoding and TM encoding, under different settings of system parameters. We also evaluated the performances of time-bin-encoded RRDPS QKD and polarization-encoded 2-dimensional decoy-state BB84 QKD as benchmarks. We further determined the potential improvements provided by incorporating the decoy-state method into inter-satellite RRDPS QKD using OAM encoding and TM encoding.

Our results indicated that OAM encoding is preferable to time-bin encoding only under the circumstances where a low dimension and a large receiver aperture are used. However, we found that TM encoding is the best encoding scheme in RRDPS QKD over an inter-satellite channel. In particular, we showed that TM encoding not only leads to the best performance and the largest feasible parameter range, but also, for the first time, enables all the theoretically available advantages of an increased dimension to be realized in the context of RRDPS QKD. Our results provide valuable insights into the practical implementation of high-error-tolerance low-overhead inter-satellite quantum communications utilizing currently available technologies.

The practical implementation of time-bin-encoded RRDPS QKD relies on the realization of a single-photon variable-delay interferometer for signal measurement. Since an interferometer is extremely susceptible to environmental disturbances, temperature fluctuations, and satellite-motion-induced Doppler shift, an active real-time stabilization system is usually needed. The active stabilization of fixed-delay interferometers for satellite-based quantum communications has been demonstrated (see, e.g., [37]). However, the practical implementation of time-bin-encoded RRDPS QKD of dimension \( d \) requires \( d \) (different) actively selectable delay paths in the variable-delay interferometer, and the simultaneous stabilization of all the delay paths has been considered a greater challenge (see discussions in, e.g., [38]). Although OAM encoding and TM encoding do not require an active interferometer-stabilization system (since no interferometer is needed), it should be pointed out that these encoding schemes also have their own technical challenges in practice. The well-known challenges regarding the real-world implementation of an OAM-encoded system include the alignment sen-
sitivity and physical size of the OAM quantum state sorter. One promising solution for this is a compact OAM quantum state sorter whose optical elements are integrated into a miniaturized optical platform with the help of advanced fabrication technologies (see demonstrations in, e.g., [39]). For TM encoding, the timing requirements may be very stringent due to the reliance on the spectral-temporal orthogonality of TMs. Considering the use of quantum pulse gates (based on the time-dependent nonlinear interaction between signal and pump pulses) for signal measurement, the synchronization of a TM-encoded system may be non-trivially dependent on the relative satellite motion. Such a timing challenge may be overcome by using weak coherent pilot pulses, which can serve as a timing reference and a pump pulse at the same time (see discussions in, e.g., [28]). It should be noted that the use of quantum pulse gates in TM encoding also requires arbitrary pulse shaping (of the pump pulse) and temperature stabilization (for the nonlinear crystal), and these requirements may add complexity to the design of a quantum satellite.

**Funding** Open Access funding enabled and organized by CAUL and its Member Institutions.

**Data availability** The data that support the findings of this study are available from the authors upon reasonable request.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

**References**

1. Chen, Y.A., Zhang, Q., Chen, T.Y., Cai, W.Q., Liao, S.K., Zhang, J., Chen, K., Yin, J., Ren, J.G., Chen, Z., Han, S.L., Yu, Q., Liang, K., Zhou, F., Yuan, X., Zhao, M.S., Wang, T.Y., Jiang, X., Zhang, L., Liu, W.Y., Li, Y., Shen, Q., Cao, Y., Lu, C.Y., Shu, R., Wang, J.Y., Li, L., Liu, N.L., Xu, F., Wang, X.B., Peng, C.Z., Pan, J.W.: An integrated space-to-ground quantum communication network over 4600 kilometres. Nature **589**(7841), 214–219 (2021). https://doi.org/10.1038/s41586-020-03093-8

2. Liao, S.K., Cai, W.Q., Liu, W.Y., Zhang, L., Li, Y., Ren, J.G., Yin, J., Shen, Q., Cao, Y., Li, Z.P., Li, F.Z., Chen, X.W., Sun, L.H., Jia, J.J., Wu, J.C., Jiang, X.J., Wang, J.F., Huang, Y.M., Wang, Q., Zhou, Y.L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.A., Liu, N.L., Wang, X.B., Zhu, Z.C., Lu, C.Y., Shu, R., Peng, C.Z., Wang, J.Y., Pan, J.W.: Satellite-to-ground quantum key distribution. Nature **549**(7670), 43–47 (2017). https://doi.org/10.1038/nature23655

3. Lukens, J.M., Islam, N.T., Lim, C.C.W., Gauthier, D.J.: Reconfigurable generation and measurement of mutually unbiased bases for time-bin qudits. Appl. Phys. Lett. **112**(11), 111102 (2018). https://doi.org/10.1063/1.5024318

4. Mirhosseini, M., Magaña-Loaiza, O.S., Chen, C., Rodenburg, B., Malik, M., Boyd, R.W.: Rapid generation of light beams carrying orbital angular momentum. Opt. Express **21**(25), 30196–30203 (2013). https://doi.org/10.1364/OE.21.030196

5. Ansari, V., Donohue, J.M., Brecht, B., Silberhorn, C.: Remotely projecting states of photonic temporal modes. Opt. Express **28**(19), 28295–28305 (2020). https://doi.org/10.1364/OE.395593

6. Pant, M., Englund, D.: High-dimensional unitary transformations and boson sampling on temporal modes using dispersive optics. Phys. Rev. A **93**, 043803 (2016). https://doi.org/10.1103/PhysRevA.93.043803
7. Gao, X., Krenn, M., Kysela, J., Zeilinger, A.: Arbitrary $d$-dimensional Pauli $X$ gates of a flying qudit. Phys. Rev. A 99, 023825 (2019). https://doi.org/10.1103/PhysRevA.99.023825
8. Ashby, J., Thiel, V., Allgaier, M., d’Ornellas, P., Davis, A.O.C., Smith, B.J.: Temporal mode transformations by sequential time and frequency phase modulation for applications in quantum information science. Opt. Express 28(25), 38376–38389 (2020). https://doi.org/10.1364/OE.410371
9. Jin, J., Agne, S., Bourgoin, J.P., Zhang, Y., Lütkenhaus, N., Jennewein, T.: Demonstration of analyzers for multimode photonic time-bin qubits. Phys. Rev. A 97, 043847 (2018). https://doi.org/10.1103/PhysRevA.97.043847
10. Mirhosseini, M., Malik, M., Shi, Z., Boyd, R.W.: Efficient separation of the orbital angular momentum eigenstates of light. Nat. Commun. 4(1), 2781 (2013). https://doi.org/10.1038/ncomms3781
11. Reddy, D.V., Raymer, M.G.: High-selectivity quantum pulse gating of photonic temporal modes using all-optical Ramsey interferometry. Optica 5(4), 423–428 (2018). https://doi.org/10.1364/OPTICA.5.000423
12. Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Security of quantum key distribution using $d$-level systems. Phys. Rev. Lett. 88, 127902 (2002). https://doi.org/10.1103/PhysRevLett.88.127902
13. Jin, J., Bourgoin, J.P., Tannous, R., Agne, S., Pugh, C.J., Kunz, K.B., Higgins, B.L., Jennewein, T.: Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel. Opt. Express 27(26), 37214–37223 (2019). https://doi.org/10.1364/OE.27.037214
14. Bouchard, F., England, D., Bustard, P.J., Heshami, K., Sussman, B.: Quantum communication with ultrafast time-bin qubits. PRX Quantum 3, 010332 (2022). https://doi.org/10.1103/PRXQuantum.3.010332
15. Chau, H.F.: Quantum key distribution using qudits that each encode one bit of raw key. Phys. Rev. A 92, 062324 (2015). https://doi.org/10.1103/PhysRevA.92.062324
16. Sasaki, T., Yamamoto, Y., Koashi, M.: Practical quantum key distribution protocol without monitoring signal disturbance. Nature 509(7501), 475–478 (2014). https://doi.org/10.1038/nature13303
17. Takesue, H., Sasaki, T., Tamaki, K., Koashi, M.: Experimental quantum key distribution without monitoring signal disturbance. Nat. Photonics 9(12), 827–831 (2015). https://doi.org/10.1038/nphoton.2015.173
18. Guan, J.Y., Cao, Z., Liu, Y., Shen-Tu, G.L., Pelc, J.S., Fejer, M.M., Peng, C.Z., Ma, X., Zhang, Q., Pan, J.W.: Experimental passive round-robin differential phase-shift quantum key distribution. Phys. Rev. Lett. 114, 180502 (2015). https://doi.org/10.1103/PhysRevLett.114.180502
19. Wang, S., Yin, Z.Q., Chen, W., Han, Y.G., Wang, R., Guo, G.C., Pan, J.W.: Experimental round-robin differential-phase-shift quantum key distribution with twisted photons. Phys. Rev. A 98, 010301 (2018). https://doi.org/10.1103/PhysRevA.98.010301
28. Brecht, B., Reddy, D.V., Silberhorn, C., Raymer, M.G.: Photon temporal modes: a complete framework for quantum information science. Phys. Rev. X 5, 041017 (2015). https://doi.org/10.1103/PhysRevX.5.041017

29. Ansari, V., Donohue, J.M., Brecht, B., Silberhorn, C.: Tailoring nonlinear processes for quantum optics with pulsed temporal-mode encodings. Optica 5(5), 534–550 (2018). https://doi.org/10.1364/OPTICA.5.000534

30. Karpiński, M., Davis, A.O.C., Sośnicki, F., Thiel, V., Smith, B.J.: Control and measurement of quantum light pulses for quantum information science and technology. Adv. Quantum Technol. 4(9), 2000150 (2021). https://doi.org/10.1002/qute.202000150

31. Wang, R., Yin, Z.Q., Wang, S., Chen, W., Guo, G.C., Han, Z.F.: Round-robin-differential-phase-shift quantum key distribution with monitoring signal disturbance. Opt. Lett. 43(17), 4228–4231 (2018). https://doi.org/10.1364/OL.43.004228

32. Padgett, M.J., Miatto, F.M., Lavery, M.P.J., Zeilinger, A., Boyd, R.W.: Divergence of an orbital-angular-momentum-carrying beam upon propagation. New J. Phys. 17(2), 023011 (2015). https://doi.org/10.1088/1367-2630/17/2/023011

33. Zhao, J., Mirhosseini, M., Braverman, B., Zhou, Y., Hashemi Rafsanjani, S.M., Ren, Y., Steinhoff, N.K., Tyler, G.A., Willner, A.E., Boyd, R.W.: Performance analysis of d-dimensional quantum cryptography under state-dependent diffraction. Phys. Rev. A 100, 032319 (2019). https://doi.org/10.1103/PhysRevA.100.032319

34. Lo, H.K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. 94, 230504 (2005). https://doi.org/10.1103/PhysRevLett.94.230504

35. Cañas, G., Vera, N., Cariñe, J., González, P., Cardenas, J., Connolly, P.W.R., Przysiezna, A., Gómez, E.S., Figueroa, M., Vallone, G., Villoresi, P., da Silva, T.F., Xavier, G.B., Lima, G.: High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers. Phys. Rev. A 96, 022317 (2017). https://doi.org/10.1103/PhysRevA.96.022317

36. Villar, A., Lohrmann, A., Bai, X., Vernoossen, T., Bedington, R., Perumangatt, C., Lim, H.Y., Islam, T., Reezwana, A., Tang, Z., Chandrasekara, R., Sachidananda, S., Durak, K., Wildfeuer, C.F., Griffin, D., Oi, D.K.L., Ling, A.: Entanglement demonstration on board a nano-satellite. Optica 7(7), 734–737 (2020). https://doi.org/10.1364/OPTICA.387306

37. Chapman, J.C., Graham, T.M., Zeitler, C.K., Bernstein, H.J., Kwiat, P.G.: Time-bin and polarization superdense teleportation for space applications. Phys. Rev. Appl. 14, 014044 (2020). https://doi.org/10.1103/PhysRevApplied.14.014044

38. Xu, Y., Lin, J., Li, Y.H., Dai, H., Liao, S.K., Peng, C.Z.: Active phase stabilization for the interferometer with 128 actively selectable paths. IEEE Trans. Nucl. Sci. 66(7), 1076–1080 (2019). https://doi.org/10.1109/TNS.2019.2921982

39. Ruffato, G., Girardi, M., Massari, M., Mafakheri, E., Sephton, B., Capaldo, P., Forbes, A., Romanato, F.: A compact diffractive sorter for high-resolution demultiplexing of orbital angular momentum beams. Sci. Rep. 8(1), 10248 (2018). https://doi.org/10.1038/s41598-018-28447-1

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.