scientific reports

OPEN

High-dimensional quantum key distribution implemented with biphotons

Comfort Sekga[1], Mhlambululi Mafu[2]✉ & Makhamisa Senekane[3,4]

We present a high-dimensional measurement device-independent (MDI) quantum key distribution (QKD) protocol employing biphotons to encode information. We exploit the biphotons as qutrits to improve the tolerance to error rate. Qutrits have a larger quantum system; hence they carry more bits of classical information and have improved robustness against eavesdropping compared to qubits. Notably, our proposed protocol is independent of measurement devices, thus eliminating the possibility of side-channel attacks. Also, we employ the finite key analysis approach to study the performance of our proposed protocol under realistic conditions where finite resources are used. Furthermore, we simulated the secret key rate for the proposed protocol in terms of the transmission distance for different fixed amounts of signals. The results prove that this protocol achieves a considerable secret key rate for a moderate transmission distance of 90 km by using 10^{16} signals. Moreover, the expected secret key rate was simulated to examine our protocol's performance at various intrinsic error rate values, $Q = (0.3\%, 0.6\%, 1\%)$ caused by misalignment and instability due to the optical system. These results show that reasonable key rates are achieved with a minimum data size of about 10^{14} signals which are realizable with the current technology. Thus, implementing MDI-QKD using finite resources while allowing intrinsic errors due to the optical system makes a giant step forward toward realizing practical QKD implementations.

Quantum key distribution (QKD) is a procedure for establishing symmetric cryptographic keys between legitimate participants by distributing quantum states[1]. In principle, QKD provides information-theoretic security, guaranteed by quantum mechanical laws[2]. Notably, QKD has developed from mere theoretical security proofs to commercial applications over the past two decades. However, practical QKD has yet to attain its full deployment owing to security lapses in the theoretical security proofs that arise from certain assumptions about the sources or devices belonging to Alice and Bob[3]. For example, QKD protocols depend on trusted device scenarios, i.e., it is assumed that no information is leaked from the transmitters or the senders, which is very challenging to guarantee in practice. This creates a gap between theory and experimental implementations, opens loopholes, and leads to various possible attacks on the QKD systems[4]. Moreover, during implementations, QKD protocols depend on trusted device scenarios, and this assumption allows the protocols to achieve effective rates. Unfortunately, this provides an opportunity for harmful attacks, such as the side-channel attacks[5]. As a result, besides the enormous theoretical and experimental quantum cryptography progress, some work remains before fully deploying QKD in commercial applications. Hence, the device-independent (DI) QKD provides an improved security degree compared to conventional QKD schemes by lessening the number of assumptions required concerning the physical devices used[6].

The security of the DI-QKD depends on the violation of Bell inequalities[7]. However, the DI-QKD needs the loophole-free Bell experiments, making it impossible to realize using existing technologies. Recent demonstrations of various attacks highlight this on practical QKD systems[5]. As a result, the measurement device-independent (MDI) QKD provides an improved practical solution intrinsically insensitive to entire attacks caused by side channels. These attacks target a measurement device and remove the detection-associated security loopholes[8,9]. Furthermore, the participating parties are connected by an untrusted relay for an MDI-QKD, leading to a considerable gain in transmission distances compared to the traditional QKD schemes. Thus, this makes these set-ups ideally suitable for quantum networks. Moreover, some experimental demonstrations using

[1]Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana. [2]Department of Physics, Case Western Reserve University, Cleveland, OH 44106, USA. [3]Institute for Intelligent Systems, University of Johannesburg, Johannesburg 2006, South Africa. [4]National Institute for Theoretical and Computational Sciences, Gauteng 2006, South Africa. ✉email: mhlambululi.mafu@case.edu

MDI-QKD have been conducted in Refs.[10,11]. However, the practical MDI-QKD still experiences relatively low key rates compared to the conventional BB84 protocol due to the requirement of Bell-state measurements. Apart from these advances, adopting QKD widely has been a challenge, and it has been demonstrated that large-scale deployment will likely require chip-based devices for improved performance, miniaturization, and enhanced functionality[12–18]. Most significantly, these integrated photonic chips offer numerous benefits such as low cost, low power consumption, and well-established batch fabrication techniques[19].

To encode information in a QKD protocol, the parties must choose a certain degree of freedom, for instance, polarization or phase properties of single-photon as quantum states[1,20]. This means one classical bit of information is encoded onto each quantum state, resulting in limited secret key rates[21]. As a result, high dimensional encoding presents a promising solution to address the limitation of low secret key rates in QKD[22]. High dimensional quantum systems allow the communicating parties in QKD to encode information beyond one bit per signal[23]. The secret key rate, which may be limited by inevitable factors such as losses in the channel, and source and detector flaws, can be significantly improved by high-dimensional encoding where each photon can encode up to $\log_2 d > 1$ bits. This allows a considerable amount of information to be sent in a given transmission of the signal in the channel. Notably, previous studies indicate that the resistance to noise of the protocols increases when one increases the dimension, both for one-way[24–26] and two-way post-processing[27]. Furthermore, compared to qubit operations, high dimensional quantum states are robust against noise due to the background and hacking attacks[24].

Qudits have been proven to be robust against quantum cloning compared to their qubit counterparts[28]. Thus, they are an excellent illustration of the effectiveness of high-dimensional quantum systems since they lead to higher error thresholds making it challenging for the eavesdropper to intercept a high-dimensional QKD scheme. Owing to this, the merits of several degrees of freedom have been examined for high dimensional QKD, which includes position-momentum[29], orbital angular momentum[23,30–33] and time energy[34–41] and MDI-QKDs employing high-dimensional quantum states[42–44]. Another approach to realizing high dimensional encoding is using biphotons corresponding to a pair of indistinguishable photons with qutrit (i.e., a three-level quantum system) representation. Biphotons or pairs of entangled photons form a two-photon light and constitute one of the most critical states of light in recent quantum information and quantum optics[45,46]. The generation, manipulation, and detection procedures for single-mode biphoton beams with linear optics have been demonstrated in Refs.[47–49].

We propose an MDI-QKD protocol that encodes information on qutrit states by exploiting the polarization state of single-mode biphoton field. Using biphotons as qutrits enhances the attainable secret key rate and security due to improved information capacity per photon and the high noise tolerance[45]. To examine the practicality of the proposed protocol, we investigate the finite-key bounds against the general attacks based on entropic uncertainty relations. Moreover, this security analysis pertains to the implementation using the decoy states. This enables the proposed protocol to be secure against Photon-Number-Splitting (PNS) attacks[1]. For the finite-key study, the statistical fluctuations are catered by leveraging the large deviation theory, particularly the multiplicative Chernoff bound[50]. This bound provides the tightest bounds on estimated parameters for the high-loss regime. More recently, a similar work on three-dimensional MDI-QKD was proposed by Jo et al.[51]. Their proposed protocol exploits the time bin entangled qutrit states to encode information and employs a tripartite qutrit discrimination setup. The setup relies on a tritter and non-destructive photon number measurements to filter the states for Bell state measurements. Conversely, our proposed MDI-QKD protocol utilizes the Mach Zehnder interferometer to generate biphoton states and the Brown Twiss schemes to achieve Bell state measurements. While the scheme in Ref.[51] is more efficient in terms of fewer resources used in Charlie's measurement site; it involves non-destructive measurements, which may open up a possibility of side-channel attacks. Another noticeable difference is that our work considers finite key analysis and studies the performance of the qutrit MDI-QKD under realistic conditions by determining the key rate as a function of transmission distance. The work in Ref.[51] only provides tolerable error bounds that allow one to distill a secure key. Therefore, apart from this introduction, the following section describes the proposed protocol, while the next section provides the security proof based on the entropic uncertainty principle. After that, we simulate the performance of our protocol to demonstrate its feasibility and conclude this paper.

Protocol definition

Biphotons. The pure polarization state for a single-mode biphoton field is expressed according to the following[45,47]:

$$|\Phi\rangle = c_1|2,0\rangle + c_2|1,1\rangle + c_3|0,2\rangle, \tag{1}$$

where $c_i = |c_i|e^{i\phi_i}$ are complex amplitudes. The notation $|n_h, n_v\rangle$ represents a state that consists of n photons in the horizontal (h) mode as well as n photons in the vertical (v) polarization mode. Therefore, from Eq. (1), we can observe that a biphoton has a three-level quantum system (qutrit) representation, hence its use for ternary quantum information encoding. To realize the QKD protocol, one needs at least two mutually unbiased bases (MUB) from available $d + 1$ MUBs. The two orthonormal bases $\mathscr{M}_1 = |\phi\rangle_i$, where $i \in \{0, 1, 2\}$ and $\mathscr{M}_2 = |\Phi\rangle_j$, where $j \in \{0, 1, 2\}$ for a 3-dimensional Hilbert space $\mathscr{H}_3$ are considered mutually unbiased when all pairs of basis vectors $|\phi\rangle_i$ and $|\Phi\rangle_j$ satisfies

$$|\langle\phi_i|\Phi_j\rangle|^2 = \frac{1}{3}. \tag{2}$$

For biphotons, the standard basis is expressed in terms of the orthonormal states $|\alpha\rangle = |2, 0\rangle$, $|\beta\rangle = |0, 2\rangle$ and $|\gamma\rangle = |1, 1\rangle$. The states $|2, 0\rangle$ and $|0, 2\rangle$ represent type-I phase matching, while $|1, 1\rangle$ corresponds to type II phase

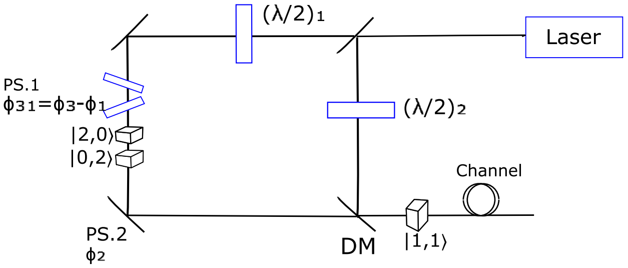

Figure 1. Mach–Zehnder interferometer set up used by Alice and Bob for biphoton state preparation. The laser beam is pumped towards a non-symmetric beam-splitter that transmits 2/3 and reflects 1/3 of the beam through the long and short arms. The $(\lambda/2)_i$ represents the halve wave plates for manipulating the amplitude, c_i of the states. The phase shifters (PS. 1 and PS. 2) introduce relative phases between the states. The DM denotes the dichroic mirror, which transmits two biphotons created using type I non-linear crystals from the long arm of the interferometer and reflect the pump from the short arm towards the type II non-linear crystal for the creation of state $|1,1\rangle$.

matching, and one can obtain these biphoton fields through spontaneous parametric down-conversion (SPDC). The other three MUBs are realized from the superposition of the basis vectors as follows

$$|\acute{\alpha}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + |\gamma\rangle) \tag{3}$$

$$|\acute{\beta}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega|\beta\rangle + \omega^2|\gamma\rangle) \tag{4}$$

$$|\acute{\gamma}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega^2|\beta\rangle + \omega|\gamma\rangle), \tag{5}$$

$$|\bar{\alpha}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + \omega|\gamma\rangle) \tag{6}$$

$$|\bar{\beta}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega|\beta\rangle + |\gamma\rangle) \tag{7}$$

$$|\bar{\gamma}\rangle = \frac{1}{\sqrt{3}}(\omega|\alpha\rangle + |\beta\rangle + |\gamma\rangle), \tag{8}$$

and

$$|\tilde{\alpha}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + \omega^2|\gamma\rangle) \tag{9}$$

$$|\tilde{\beta}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega^2|\beta\rangle + |\gamma\rangle) \tag{10}$$

$$|\tilde{\gamma}\rangle = \frac{1}{\sqrt{3}}(\omega^2|\alpha\rangle + |\beta\rangle + |\gamma\rangle), \tag{11}$$

where $\omega = \exp(i2\pi/2)$. In our scenario, to realize high dimensional encoding with biphotons, we propose an MDI-QKD protocol exploiting two Fourier transformed bases, $\mathscr{M}_1 = \{|\acute{\alpha}\rangle, |\acute{\beta}\rangle, |\acute{\gamma}\rangle\}$ and $\mathscr{M}_2 = \{|\bar{\alpha}\rangle, |\bar{\beta}\rangle, |\bar{\gamma}\rangle\}$.

Preparation of states. Alice (Bob) starts by randomly preparing qutrit states from two mutually unbiased bases $\mathscr{M}_1 = \{|\acute{\alpha}\rangle, |\acute{\beta}\rangle, |\acute{\gamma}\rangle\}$ and $\mathscr{M}_2 = \{|\bar{\alpha}\rangle, |\bar{\beta}\rangle, |\bar{\gamma}\rangle\}$. The biphoton states $\{|\acute{\alpha}\rangle, |\bar{\alpha}\rangle\}$, $\{|\acute{\beta}\rangle, |\bar{\beta}\rangle\}$ and $\{|\acute{\gamma}\rangle, |\bar{\gamma}\rangle\}$ are assigned bit values 0, 1 and 2, (the value 2 is converted to binary digit during sifting to obtain two bits per signal) respectively. The states are prepared using a Mach–Zehnder interferometer consisting of 3 arms and appropriate non-linear crystals in each arm. This is illustrated in Fig. 1.

The laser beam is pumped onto a non-symmetric beamsplitter that transmits two-thirds of the beam through the interferometer's long arm and reflects the other beam via the short arm. The beam in the long arm is pumped towards the type I non-linear crystals for generating states $|2,0\rangle$ and $|0,2\rangle$ resulting in a superposition

State	$\lvert c_1\rvert$	$\lvert c_2\rvert$	$\lvert c_3\rvert$	ϕ_1	ϕ_2	ϕ_3
$\lvert\acute{\alpha}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	0	0
$\lvert\acute{\beta}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	120°	−120°
$\lvert\acute{\gamma}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	−120°	120°
$\lvert\acute{\alpha}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	120°	0	0
$\lvert\bar{\beta}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	120°	0
$\lvert\bar{\gamma}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	0	120°

Table 1. The parameter settings for biphoton states from two mutually unbiased bases used in our QKD scheme. The complex amplitudes $|c_i|$ are realized through the use of half-wave plates. The ϕ_i are realized by use of phase shifters.

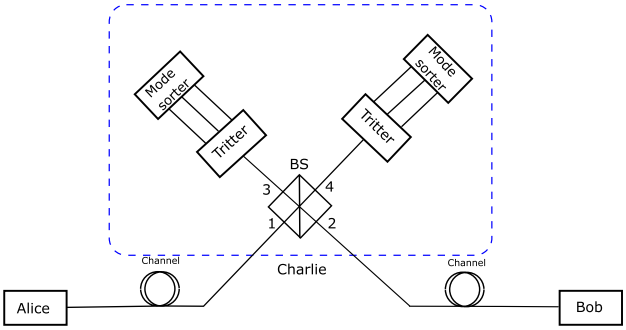

Figure 2. The generic measurement set up for our proposed MDI-QKD. Alice and Bob start by preparing the biphoton states from two mutually unbiased bases and send them through the unsecured channel to Charlie. Charlie allows the states to interfere in the symmetric beam-splitter (BS) upon receiving the states. The photons are directed towards the tritter and eventually detected in the Brown Twiss scheme (mode sorter).

$$|\Phi\rangle = c_1|2,0\rangle + e^{i\phi_{31}}c_3|0,2\rangle, \tag{12}$$

with $e^{i\phi_{31}}$ representing the relative phase between the states realized through phase shifters. The half-wave plate is used for manipulating the amplitudes of these states. A cut-off flitter is employed to remove the pump. After passing through the filter, the states arrive at the piezoelectric translator, where the phase shift, ϕ_2, is introduced between the superposition of states defined in Eq. (12) and the state $|1,1\rangle$. The reflected beam traveling through the short arm is guided towards the half-wave plate to control the amplitude corresponding to the state $|1,1\rangle$. The pump is reflected at the dichroic mirror towards the type II non-linear crystals to create the state $|1,1\rangle$. The type I biphotons from the long arm of the interferometer is transmitted via the dichroic mirror. Thus, at the interferometer's output, we have the superposition of three basic states in Eq. (1), which are then propagated through the insecure channel to the measurement site. Different states from two mutually unbiased are produced by adjusting the phase shifters and halve wave plates according to Table 1.

Measurement. Charlie allows the biphotons from Alice and Bob to interfere in a symmetric beam-splitter upon receiving the states. As a result, the Hong Ou Mandel effect occurs (see Fig. 2). The beam-splitter action can be described as follows.Let us assume Alice's biphoton state at the input arm of the beam-splitter is denoted by $|\psi\rangle_1$, then its transformation can be described as

$$a_1^\dagger|\psi\rangle_1 \rightarrow \frac{1}{\sqrt{2}}(|\psi\rangle_3 + |\overline{\psi}\rangle_4). \tag{13}$$

Similarly if Bob's state at the input arm is $|\acute{\psi}\rangle_2$ then the action of the beam-splitter is described as

$$a_2^\dagger|\acute{\psi}\rangle_2 \rightarrow \frac{1}{\sqrt{2}}(|\overline{\acute{\psi}}\rangle_3 - |\acute{\psi}\rangle_4), \tag{14}$$

where $a_i^\dagger$ denotes the creation operator and $|\bar{x}\rangle$ is the reflected state. The overall beam-splitter transformations are described as

$$\begin{aligned}|\psi\rangle_1|\acute{\psi}\rangle_2 &\xrightarrow{BS} \frac{1}{\sqrt{2}}(|\psi\rangle_3+|\overline{\psi}\rangle_4)\otimes\frac{1}{\sqrt{2}}(|\overline{\acute{\psi}}\rangle_3-|\acute{\psi}\rangle_4)\\ &=\frac{1}{\sqrt{2}}(|\psi\rangle_3|\overline{\acute{\psi}}\rangle_3-|\psi\rangle_3|\acute{\psi}\rangle_4+|\overline{\psi}\rangle_4|\overline{\acute{\psi}}\rangle_3-|\overline{\psi}\rangle_4|\acute{\psi}\rangle_4)\\ &=\frac{1}{\sqrt{2}}(|\Psi^+\rangle+|\Psi^-\rangle)\end{aligned} \tag{15}$$

where

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|\psi\rangle_3|\overline{\acute{\psi}}\rangle_3-|\overline{\psi}\rangle_4|\acute{\psi}\rangle_4) \tag{16}$$

and

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|\overline{\psi}\rangle_4|\overline{\acute{\psi}}\rangle_3-|\psi\rangle_3|\acute{\psi}\rangle_4). \tag{17}$$

The subscripts 1, 2, and 3, 4 denote a beam-splitter's input and output ports, respectively. According to the Hong Ou Mandel interference, identical photons will leave the beam-splitter from a similar output port, and distinguishable photons from both input ports of the beam-splitter will exit in both output ports. Let Alice and Bob choose a similar biphoton states $|\acute{\alpha}_A\rangle$ and $|\acute{\alpha}_B\rangle$, respectively. Therefore, based on the Hong Ou Mandel interference, the state $|\Psi^-\rangle$ in Eq. (17) will disappear, and the resultant state is

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|\acute{\alpha}_A\rangle_3|\overline{\acute{\alpha}_B}\rangle_3-|\overline{\acute{\alpha}_B}\rangle_4|\acute{\alpha}_A\rangle_4). \tag{18}$$

Therefore, identical biphotons will always appear in the same output arm of BS (3rd arm or 4th arm). Otherwise, if Alice and Bob prepare opposite biphotons, both $|\Psi^-\rangle$ and $|\Psi^-\rangle$ will exist, and there is a non-zero probability that the biphotons will exit at both output arms of the BS. The photons that exit the beam-splitter are transmitted toward the three input-output ports beam-splitter (tritter). The photons are directed toward the two non-polarizing beam-splitters to separate them into three channels from each output of the symmetric beam-splitter connected to each input of the two tritters (see Fig. 3). The probability of photons exiting through any of the output ports of the tritter is governed by the unitary matrix

$$\mathscr{U}=\frac{1}{\sqrt{3}}\begin{pmatrix}1 & 1 & 1\\ 1 & e^{i2\pi/3} & e^{i4\pi/3}\\ 1 & e^{i4\pi/3} & e^{i8\pi/3}\end{pmatrix}. \tag{19}$$

In a case where each input of the tritter is injected with biphoton state, the resultant output state after the evolution induced by $\mathscr{U}$ is given by

$$|1,1,1\rangle \xrightarrow{\mathscr{U}} \sqrt{\frac{2}{3}}|3,0,0\rangle-\frac{1}{\sqrt{3}}|1,1,1\rangle, \tag{20}$$

where $|1,1,1\rangle$ corresponds to one biphoton state in each input or output of the tritter, and $|3,0,0\rangle$ represents three biphoton states exiting through one output port and no photons in the other two output ports. The output ports of each tritter are linked with three biphoton mode sorters. At the output of each tritter, the biphoton states from Alice and Bob, are directed towards the Brown Twiss schemes which are tuned to measure the standard basis biphoton modes $|\alpha\rangle, |\beta\rangle$ and $|\gamma\rangle$. Each Brown Twiss scheme made up of polarization filters in the arms. The filters comprise a pair of phase-plates and a polarization analyzer used to realize the polarization states of single-photons creating the biphoton. Each Brown Twiss scheme is tuned to detect a certain polarization state of biphoton by setting wave plates ($\lambda/4$ plate, $\lambda/2$ plate) to angle positions that realize desired polarization and setting polarization analyser to allow the desired polarization to pass through. Different angle settings for wave plates are shown in Table 2. When a Brown Twiss scheme is tuned to the settings for detection of specific polarization states, the orthogonal biphoton states cannot result in coincidence detection. For instance, in the Brown Twiss scheme used to detect $|\beta\rangle$ biphoton mode, there are two detectors for the horizontal polarization contributions from Alice and Bob's biphoton states which are labelled as D_{HA} and D_{HB}. Furthermore, there are two detectors for measuring the vertical polarization contributions of biphoton states from Alice and Bob labelled as D_{VA} and D_{VB} as shown in Fig. 3. Similarly, appropriate parameters are set in the filters of both arms of the Brown Twiss scheme for detecting other states to allow coincidence detection. Note that states prepared by Alice and Bob are a superposition of the three basic states $|\alpha\rangle, |\beta\rangle$ and $|\gamma\rangle$. Therefore, a successful Bell state measurement in the Brown Twiss scheme corresponds to the observation of precisely 12 detectors being triggered; for instance, D_{H1A}, D_{H1B}, D_{H2A} and D_{H2B} (associated with $|\alpha\rangle_L$ biphoton mode), D_{H3A}, D_{H3B}, D_{V4A} and D_{V4B} (associated with $|\beta\rangle_L$ biphoton mode) and D_{V5A}, D_{V5B}, D_{V6A} and D_{V6B} (associated with $|\gamma\rangle_L$ biphoton mode). These measurement results can be simplified in terms of Bell measurements as $\frac{1}{\sqrt{2}}(D_{\alpha_L}D_{\beta_L}D_{\gamma_L}+D_{\alpha_R}D_{\beta_R}D_{\gamma_R})$ which represent a click in detectors on the left-hand side for $|\alpha\rangle, |\beta\rangle$ and $|\gamma\rangle$ modes (i.e.,D_{α_L} denotes coincidence detection in detectors of $|\alpha\rangle$ mode) or a click on the right-hand side for $|\alpha\rangle, |\beta\rangle$ and $|\gamma\rangle$ modes detectors. A conclusive result is given by click in detectors of the mode sorters on the left-hand side or the right-hand side only.

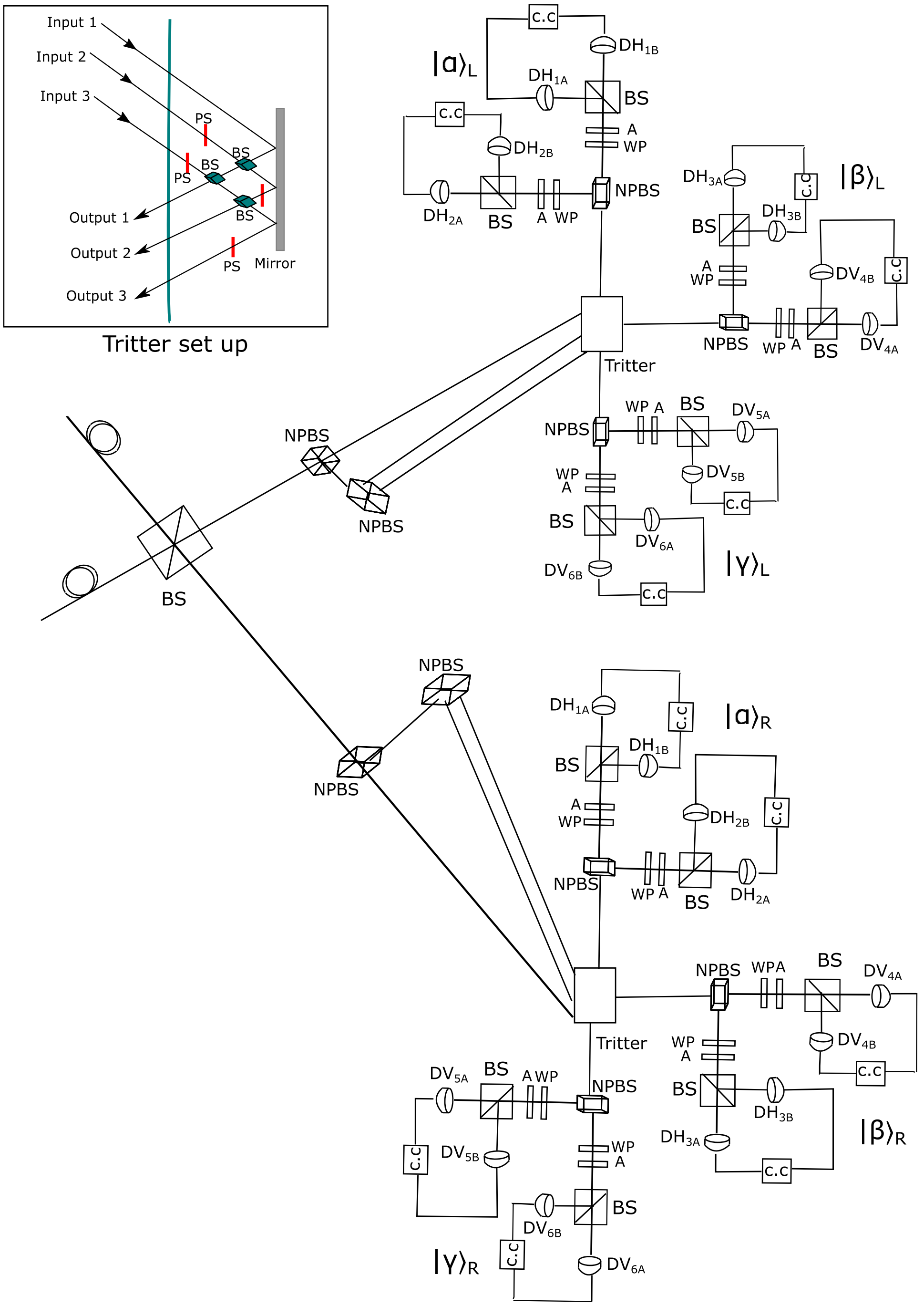

Figure 3. Illustration of the measurement set up at Charlie's site. The incoming biphotons interfere in the beam-splitter (BS) and exit through either of two output ports towards the two non-symmetric beam-splitter (NPBS), where they are further split into three channels and directed towards the tritter. The tritter setup shown in the upper left is a three-input-output port splitter. It comprises three conventional beam-splitters (BS), four-phase shifters (PS), and a mirror. The output ports of the tritter are linked with three Brown Twiss schemes for detecting the three basic states $|\alpha\rangle, |\beta\rangle$, and $|\gamma\rangle$. Each Brown Twiss scheme consists of a non-symmetric beam-splitter (NPBS), wave plates (WP), polarization analyser (A), and detectors ($D\mathbf{P}_i$) where $\mathbf{P} \in \{H, V\}$ represents polarization mode and subscript i denotes single photons forming biphotons. The abbreviation c.c corresponds to coincident counting or detection.

The other Bell state measurements result in inconclusive measurement results, e.g., $\frac{1}{\sqrt{2}}(D_{\alpha_L}D_{\beta_L}D_{\gamma_R} + D_{\alpha_R}D_{\beta_R}D_{\gamma_L})$. The results are provided in Table 3.

Wave plate		$\|\alpha\rangle$		$\|\beta\rangle$		$\|\gamma\rangle$
	H	H	H	V	V	V
$\lambda/4$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$
$\lambda/2$	$\frac{\pi}{8}$	$\frac{\pi}{8}$	$\frac{\pi}{8}$	$-\frac{\pi}{8}$	$-\frac{\pi}{8}$	$-\frac{\pi}{8}$

Table 2. The parameter settings for wave plates in the Brown Twiss schemes.

States sent by Alice and Bob	Charlie's measurement results							
	$D_{\alpha_L} D_{\beta_L} D_{\gamma_L}$	$D_{\alpha_R} D_{\beta_R} D_{\gamma_R}$	$D_{\alpha_L} D_{\beta_L} D_{\gamma_R}$	$D_{\alpha_L} D_{\beta_R} D_{\gamma_R}$	$D_{\alpha_L} D_{\beta_R} D_{\gamma_L}$	$D_{\alpha_R} D_{\beta_L} D_{\gamma_L}$	$D_{\alpha_R} D_{\beta_L} D_{\gamma_R}$	$D_{\alpha_R} D_{\beta_R} D_{\gamma_L}$
$\|\acute{\alpha}\rangle$ or $\|\bar{\alpha}\rangle$	Conclusive	Conclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive
$\|\acute{\beta}\rangle$ or $\|\bar{\beta}\rangle$	Conclusive	Conclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive
$\|\acute{\gamma}\rangle$ or $\|\bar{\gamma}\rangle$	Conclusive	Conclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive	Inconclusive

Table 3. The possible Bell state measurement results in the Brown Twiss scheme mode sorting.

Sifting. Alice and Bob post select states prepared using the same basis when Charlie reports a conclusive event and discards the rest of the data. A conclusive event corresponds to a case where there is a coincidence detection in three Brown Twiss schemes (linked to the same tritter) for three different basis states $|\alpha\rangle, |\beta\rangle$ and $|\gamma\rangle$. This occurs when Alice and Bob have prepared the same biphoton state. We define the set $\mathscr{K}$ comprising of biphoton signals if Alice and Bob selected the key basis $\mathscr{M}_1$ and Charlie gets a successful measurement. Similarly, $\mathscr{C}$ is a set of post-selected signals from measurement basis $\mathscr{M}_2$, which are used for monitoring the presence of an adversary. The protocol repeats the first steps until the sifting conditions $|\mathscr{K}| \geq n$ and $|\mathscr{C} \ | \geq m$ are met for all N signals prepared by Alice and Bob.

Parameter estimation. The participating parties, Alice and Bob, make use of the random bits obtained from $\mathscr{K}$ to create a raw key consisting of bit strings K_A and K_B. Then, they compute the average error $\frac{1}{|\mathscr{C} \ |} \sum a_i \oplus b_i$ where a_i and b_i are Alice and Bob's bit values.

Error correction. The information reconciliation scheme is performed, which leaks at least leak_{EC} bits of classical error-correction data. Alice evaluates a bit string (i.e., a hash) measuring length $\log_2(1/\varepsilon_{\text{cor}})$ using a random universal$_2$ hash function to K_A. Then, Alice transmits the choice of the function, including the hash to the receiver, Bob. When the hash of K_B does not match the hash of K_A, the protocol is aborted.

Privacy amplification. During this step, Alice uses a random universal$_2$ hash function for extracting the length ℓ bits of secret key S_A from K_A. Bob exploits a similar hash function for extracting the key S_B of length ℓ from K_B.

Security analysis

We consider the realistic scenarios where participating parties exchange finite signals N and determine the statistical fluctuations of finite-size key effects. The security analysis follows the proofs provided in Refs.[52–56] based on a universally composable framework. The protocol creates a pair of key bit strings $\mathsf{S_A}$ for Alice and $\mathsf{S_B}$ for Bob. These key bit strings measure length ℓ and must satisfy the correctness and secrecy requirements so that the protocol can be considered secure. Based on the composability requirement, the QKD protocol is considered to be correct when $\mathsf{S_A} = \mathsf{S_B}$ for any eavesdropping attack. Thus, the ε_{cor}-correct protocol differs from a correct one according to the error probability, ε_{cor}, where $\Pr[\mathsf{S_A} \neq \mathsf{S_B}] \leq \varepsilon_{\text{cor}}$. Therefore, the CQ state, $\rho_{\mathsf{S_A}E}$ is Δ-secret when

$$\min_{\rho_E} \frac{1}{2} ||\rho_{\mathsf{S_A}E} - \rho_U \otimes \rho_E||_1 \leq \Delta, \tag{21}$$

where $\rho_{\mathsf{S_A}E}$ is the classical-quantum (CQ) state, which represents the correlation between Alice's key bit string S_A and Eve's quantum state ρ_E, and ρ_U corresponds to the completely mixed state on the key space.

Since we consider signals generated using spontaneous parametric down-conversion (SPDC) sources that sometimes emit at least one photon pair, our protocol is susceptible to photon number splitting (PNS) attacks. Therefore, we apply the decoy states technique analysis. With the decoy-state approach, Alice prepares photons at random by using the three different intensities (μ, ν, ω) with μ denoting the signal state intensity, ν for decoy states, and ω represents the vacuum states[57]. These intensities are generally chosen according to the following probabilities $P_\mu > P_\nu > P_\omega$ whereby P_μ, P_ν, and P_ω represent signal, decoy and vacuum states. Accordingly, signal states attained with the intensity μ are utilized to generate the final secure key. Finally, the decoy-states acquired based on intensity ν are used to bound the knowledge of Eve about the key. Therefore, the key rate of the $\varepsilon_{\text{sec}} + \varepsilon_{cor}$-MDI protocol with biphotons is expressed as

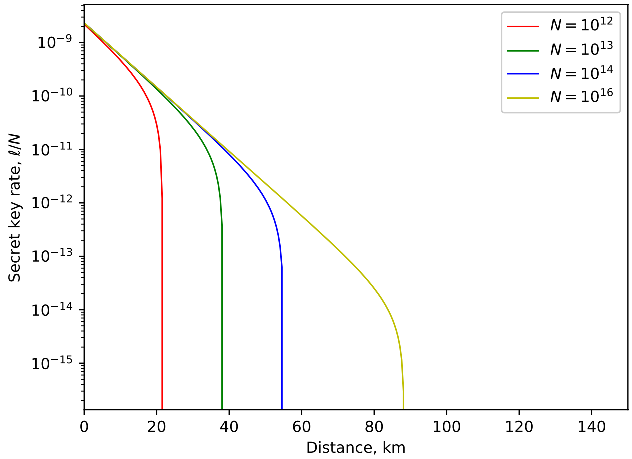

Figure 4. Illustration of the secret key rate (in logarithmic scale) in terms of the transmission distance (km), for a fixed amount of signals $N = 10^{12}$, $N = 10^{13}$, $N = 10^{14}$ and $N = 10^{16}$.

$$\frac{\ell}{N_{\text{total}}} = q\left[Q^{1,1}_{\mu_a\mu_b,\mathscr{M}_1}(\log_2 3 - h_3(e^{1,1U}_{\mathscr{M}_2})) - \text{leak}_{EC} - \log_2\frac{2}{\varepsilon_{\text{cor}}} - 2\log_2\frac{4}{\varepsilon_{\text{sec}}}\right], \tag{22}$$

with $q = \frac{N_\mu p_\kappa^2}{N_{\text{total}}}$, N_μ represents the amount of detected signals prepared according to the intensity μ. In contrast, p_κ denotes the probability of measuring in the key basis $\mathscr{M}_1$ and N_{total} is the total amount of exchanged signals. The term $Q^{1,1}_{\mu_a\mu_b,\mathscr{M}_1}$ represents the gain of biphotons prepared by Alice and Bob in the key basis $\mathscr{M}_1$ with intensities μ_a and μ_b, respectively. Accordingly, the term $e^{1,1U}_{\mathscr{M}_2}$ denotes the upper bound on the error rate emanating from single-photon components in the non-key basis $\mathscr{M}_2$ and leak_{EC} represents the quantity of information leaked to Eve in the error correction step which equals to $N_\mu f_{\text{EC}} h_3(E_{\mu_a\mu_b\mathscr{M}_1})$. Here f denotes the efficiency due to error correction and $h_3(x)$ is the entropy corresponding to three-dimensional quantum states given by $h_3(x) = -x\log_2(\frac{x}{2}) - (1-x)\log_2(1-x)$. Finally, the correction terms $\log_2(1/\varepsilon_{\text{cor}})$ and $2\log_2(4/\varepsilon_{\text{sec}})$ correspond to the bits of information lost through computation of universal hash function during error correction step and the privacy amplification. The applicable parameters in Eq. (22) are derived in Appendix A.

Simulation results

We present the analysis of the behavior of the secret key rate in Eq. (22). The simulation results correspond to a fibre-based QKD scheme where the expected key rate is maximized by using the following experimental values where fiber loss coefficient 0.2 dB/km, detector efficiency $\eta = 14.5\%$, single-photon detector dark count rate $P_d = 1.7 \times 10^{-6}$, error correction efficiency $f_{EC} = 1.22$, signal states mean photon number $\mu = 0.6$ and optimal probability p_z for the key basis is 0.95 Ref.[58].

Figure 4 depicts the expected secret key rate corresponding to each pulse (i.e., ℓ/N) in terms of the transmission distance between the participating parties, Alice and Bob, for various amounts of signals N. The simulation result demonstrates the feasibility of our proposed protocol in the finite-key regime. Notably, we obtain a fairly reasonable transmission distance of 90 km with realistic 10^{16} photon signals. For comparison purposes, we provide the plot for key rate against transmission distance for our proposed biphoton MDI-QKD and the qubit-based MDI-QKD[55] in Fig. 5. The results indicate that qubit-based MDI-QKD slightly outperforms our proposed biphoton QKD in terms of maximum transmission and achievable key rates. However, it is worth highlighting that the biphoton MDI-QKD provides a higher bit error rate tolerance compared to the qubit-based MDI-QKD. For example, it has previously been demonstrated in Ref.[45,59] that biphoton-based QKD protocols can tolerate an error rate of about 17.7% to distill a secure key. In contrast, the best qubit-based one-way QKD can only tolerate up to 14.1% in the error rate[45]. Therefore, we highlight that owing to its ability to tolerate a higher quantum bit error rate, the biphoton MDI-QKD can still be considered a reliable candidate for key distribution purposes, particularly over short transmission distances with low losses in the channel. Notably, we remark that the means to create and detect biphoton optical fields have long been successfully investigated[47,60–62]. Furthermore, using comparable schemes the experimental results show that the biphoton states can be realized with high fidelity that ranged from 98.3 % to 99.8%, clearly demonstrating the feasibility of biphoton QKD. Most significantly, the advent of superconducting nanowire single-photon detectors has demonstrated detection efficiency of about 93%[63]. Thus, by harnessing these new technologies, the detection inefficiencies contributed by our detection system, which detectors in our scheme could contribute, can be drastically reduced, resulting in improved key rates. In Fig. 6, we present the performance expected secret key rate (per pulse) ℓ/N given as a function of the number of signals N for various values of the intrinsic error rate: $Q = (0.3\%, 0.6\%, 1\%)$ owing to the misalignment and the optical system's instability at a distance of 50 km. We show that a minimum data size of about 10^{14} signals (attainable current hardware in practical QKD systems) is required to produce a provably secure secret key.

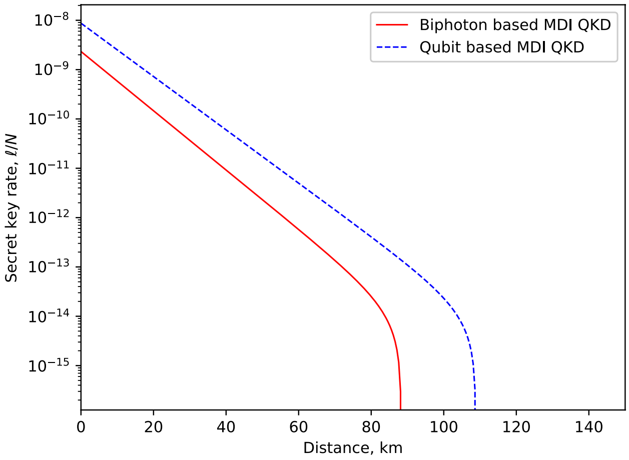

Figure 5. Illustration of the secret key rate (in logarithmic scale) in terms of the transmission distance (km) for our proposed biphoton MDI-QKD and the qubit-based MDI-QKD proposed in Ref.[55] for a fixed amount of signals $N = 10^{16}$.

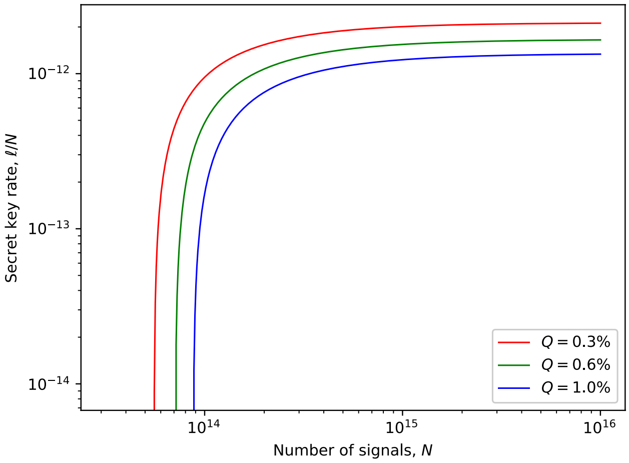

Figure 6. The secret key rate (in logarithmic scale) in terms of the number of signals N, for intrinsic misalignment errors 0.3%, 0.6%, and 1%.

Conclusion

We presented a high-dimensional QKD protocol employing biphotons to encode information. The biphotons were exploited as qutrits to improve the secret key rate. This is because qutrits carry more bits of classical information and have improved robustness against eavesdropping compared to qubits. Moreover, the secret key rate for the MDI-QKD proposed protocol was simulated regarding the transmission distance for different fixed amounts of signals. These results prove that this protocol achieves a considerable secret key rate for a moderate transmission distance of 90 km by using 10^{16} signals. Also, the expected secret key rate was simulated to examine our protocol's performance at various intrinsic error rate values, $Q = (0.3\%, 0.6\%, 1\%)$ caused by misalignment and instability due to the optical system. These results show that reasonable key rates are achieved with a minimum data size of about 10^{14} signals which are realizable with the current technology. Therefore, the proposed protocol is crucial for realizing practical QKD implementations.

Data availability

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Appendix

A: Estimation of key rate parameters

We evaluate gains and quantum bit error rates by considering the conditional probabilities for the coincidence detection of n-photon pairs in the Brown Twiss scheme. In terms of the basis state $|\alpha\rangle$, the yield is given by

$$Y^{\alpha}_{n,n} = [1-(1-Y_{0D_{H1A}})(1-\eta_{D_{H1A}}t)^n][1-(1-Y_{0D_{H1B}})(1-\eta_{D_{H1B}}t)^n] \\ \times [1-(1-Y_{0D_{H2A}})(1-\eta_{D_{H2A}}t)^n][1-(1-Y_{0D_{H2B}})(1-\eta_{D_{H2B}}t)^n], \tag{23}$$

where Y_0 is the background count rate, D_{H1A}, D_{H1B}, D_{H2A} and D_{H2B} correspond to detectors for measuring horizontally polarized states in the Brown Twiss scheme. The terms t and η represent channel transmittance and detection efficiencies. The yield for photon pairs that correspond to state $|\beta\rangle$ is given by

$$Y^{\beta}_{n,n} = [1-(1-Y_{0D_{H3A}})(1-\eta_{D_{H3A}}t)^n][1-(1-Y_{0D_{H3B}})(1-\eta_{D_{H3B}}t)^n] \\ \times [1-(1-Y_{0D_{V4A}})(1-\eta_{D_{V4A}}t)^n][1-(1-Y_{0D_{V4B}})(1-\eta_{D_{V4B}}t)^n], \tag{24}$$

where D_{H3A}, D_{H3B}, D_{V4A}, and D_{V4B} correspond to detectors for measuring horizontal and vertical polarized states, respectively, in the Brown Twiss scheme. Similarly, the detection probability for the n-photon pair corresponding to $|\gamma\rangle$ is

$$Y^{\gamma}_{n,n} = [1-(1-Y_{0D_{V5A}})(1-\eta_{D_{V5A}}t)^n][1-(1-Y_{0D_{V5B}})(1-\eta_{D_{V5B}}t)^n] \\ \times [1-(1-Y_{0D_{V6A}})(1-\eta_{D_{V6A}}t)^n][1-(1-Y_{0D_{V6B}})(1-\eta_{D_{V6B}}t)^n], \tag{25}$$

D_{V5A}, D_{V5B}, D_{V6A}, and D_{V6B} correspond to detectors for measuring vertically polarized states in the Brown Twiss scheme. Therefore, the overall yield is given by

$$Y_{n,n} = Y^{\alpha}_{n,n} Y^{\beta}_{n,n} Y^{\gamma}_{n,n}. \tag{26}$$

From these results, the gain for states prepared from key basis comprising of n-photon pairs is given by

$$Q^{n,n}_{\mu_a\mu_b,\mathscr{M}_1} = Y_{n,n}P(n_a)P(n_b), \tag{27}$$

where $P(n_a)$ and $P(n_b)$ denotes the probabilities for Alice and Bob's SPDC sources to emit n_a-photon and n_b -photon pairs. This probability is expressed as

$$P(n) = \frac{(n+1)(\frac{\mu}{2})^n}{(1+\frac{\mu}{2})^{n+2}}. \tag{28}$$

The gain corresponding to single-photon contributions is then given by

$$Q^{1,1}_{\mu_a\mu_b,\mathscr{M}_1} = \frac{4Y_{1,1}\mu_a\mu_b}{(2+\mu_a+\mu_b)^3}. \tag{29}$$

In addition, we have the overall gain expressed as

$$Q_{\mu_a\mu_b,\mathscr{M}_1} = \sum_{n}^{\infty} Q^{n,n}_{\mu_a\mu_b,\mathscr{M}_1}, \tag{30}$$

and the QBER, $E_{\mu_a\mu_b,\mathscr{M}_1}$ is expressed as

$$E_{\mu_a\mu_b,\mathscr{M}_1} Q_{\mu_a\mu_b,\mathscr{M}_1} = \sum_{n=0}^{\infty} e_{n,n} Q^{n,n}_{\mu_a\mu_b,\mathscr{M}_1}, \tag{31}$$

where the error rate of the n-photon pairs from Alice and Bob, $e_{n,n}$ is expressed as

$$e_{n,n} = e^{\alpha}_{n,n} + e^{\beta}_{n,n} + e^{\gamma}_{n,n}. \tag{32}$$

The error rate for the n-photon pair corresponding to the state $|\alpha\rangle$ given by

$$e^{\alpha}_{n,n} = [e_0(Y_{0D_{H1A}}Y_{0D_{H1B}} + Y_{0D_{H1A}}\eta_{D_{H1B}} + Y_{0D_{H1B}}\eta_{D_{H1A}} + Y_{0D_{H2A}}Y_{0D_{H2B}} \\ + Y_{0D_{H2A}}\eta_{D_{H2B}} + Y_{0D_{H2B}}\eta_{D_{H2A}}) + e_d(\eta_{D_{H1A}}\eta_{D_{H1B}} + \eta_{D_{H2A}}\eta_{D_{H2B}})] \div Y^{\alpha}_{n,n} \tag{33}$$

The error rates e^{β}_n and e^{γ}_n associated with the detection of states $|\beta\rangle$ and $|\gamma\rangle$, respectively are analogously obtained as

$$e^{\beta}_{n,n} = [e_0(Y_{0D_{H3A}}Y_{0D_{H3B}} + Y_{0D_{H3A}}\eta_{D_{H3B}} + Y_{0D_{H3B}}\eta_{D_{H3A}} + Y_{0D_{V4A}}Y_{0D_{V4B}} \\ + Y_{0D_{V4A}}\eta_{D_{V4B}} + Y_{0D_{V4B}}\eta_{D_{V4A}}) + e_d(\eta_{D_{H3A}}\eta_{D_{H3B}} + \eta_{D_{V4A}}\eta_{D_{V4B}})] \div Y^{\beta}_{n,n} \tag{34}$$

$$e^{\gamma}_{n,n} = [e_0(Y_{0D_{V5A}}Y_{0D_{V5B}} + Y_{0D_{V5A}}\eta_{D_{V5B}} + Y_{0D_{V5B}}\eta_{D_{V5A}} + Y_{0D_{V6A}}Y_{0D_{V6B}} \\ + Y_{0D_{V6A}}\eta_{D_{V6B}} + Y_{0D_{V6B}}\eta_{D_{V6A}}) + e_d(\eta_{D_{V5A}}\eta_{D_{V5B}} + \eta_{D_{V6A}}\eta_{D_{V6B}})] \div Y^{\gamma}_{n,n} \tag{35}$$

Finally, the upper bound on the error rate measured in the complimentary basis used to approximate the phase error rate on the key basis is given by

$$e^{1,1U}_{\mathscr{M}_2} = \frac{E_{\nu_a\nu_b,\mathscr{M}_2}\mathrm{Q}_{\nu_a\nu_b,\mathscr{M}_2}e^{2\nu} - e_0 Y_0}{Y^L_{1,1}\nu^2}, \tag{36}$$

where

$$Y^L_{1,1} = \frac{P(\mu_a|2)P(\mu_b|2)[\mathrm{Q}_{\nu_a\nu_b,\mathscr{M}_2} - P(\nu_a|0)P(\nu_b|0)Y_0] - P(\nu_a|2)P(\nu_b|2)[\mathrm{Q}_{\mu_a\mu_b,\mathscr{M}_1} - P(\mu_a|0)P(\mu_b|0)Y_0]}{P(\mu_a|2)P(\mu_b|2)P(\nu_a|1)P(\nu_b|1) - P(\mu_a|1)P(\mu_b|1)P(\nu_a|2)P(\nu_b|2)}. \tag{37}$$

In above equation $P(\lambda|n) = \frac{(n+1)(\frac{\lambda}{2})^n}{(1+\frac{\lambda}{2})^{n+2}}$ with $\lambda \in \{\mu, \nu\}$ and *n* denotes number of photons.B: Secrecy

Let the system $\tilde{\mathsf{E}}$ represent information collected by Eve on Alice and Bob's bit strings K_A and K_B, respectively, up to the error correction step. By applying the privacy amplification based on the universal class-two hash function, we generate a Δ-secret key of length ℓ, and

$$\Delta \leq 2\varepsilon + \frac{1}{2}\sqrt{2^{\ell - \mathrm{H}^{\varepsilon}_{\min}(\mathsf{K}_A|\tilde{\mathsf{E}})}}, \tag{38}$$

where $\mathrm{H}^{\varepsilon}_{\min}(\mathsf{K}_A|\tilde{\mathsf{E}})$ represents the smooth min-entropy, which corresponds to the average probability which an adversary guesses K_A correctly using an optimal strategy through having an access to $\tilde{\mathsf{E}}$. Let $\nu = \frac{1}{2}\sqrt{2^{\ell - \mathrm{H}^{\varepsilon}_{\min}(\mathsf{K}_A|\tilde{\mathsf{E}})}}$, then the secret key length, ℓ is given by

$$\ell = \mathrm{H}^{\varepsilon}_{\min}(\mathsf{K}_A|\tilde{\mathsf{E}}) - 2\log_2\left(\frac{1}{2\nu}\right). \tag{39}$$

During error correction, Alice and Bob reveal bits of information equals to $\mathrm{leak}_{EC} + \log_2\left(\frac{2}{\varepsilon_{\mathrm{cor}}}\right)$ to an eavesdropper. Therefore, we have that

$$\mathrm{H}^{\varepsilon}_{\min}(\mathsf{K}_A|\tilde{\mathsf{E}}) \geq \mathrm{H}^{\epsilon}_{\min}(\mathsf{K}_A|\mathsf{E}) - \mathrm{leak}_{EC} + \log_2\left(\frac{2}{\varepsilon_{\mathrm{cor}}}\right), \tag{40}$$

where E is Eve's information prior to error correction step. Since our analysis is based on decoy states, K_A can be written in terms of $\mathsf{K}^1_A\mathsf{K}^m_A$ and this represents the bit strings owing to single photons and multi-photons events. Through using the generalized chain rule for smooth entropies, we have that

$$\begin{aligned}\mathrm{H}^{\epsilon}_{\min}(\mathsf{K}_A|\mathsf{E}) &\geq \mathrm{H}^{\delta_1}_{\min}(\mathsf{K}^1_A|\mathsf{K}^m_A\mathsf{E}) + \mathrm{H}^{\delta_3}_{\min}(\mathsf{K}^m_A|\mathsf{E}) - 2\log_2\left(\frac{1}{\delta_2}\right) - 1\\ &\geq \mathrm{H}^{\delta_1}_{\min}(\mathsf{K}^1_A|\mathsf{K}^m_A\mathsf{E}) - 2\log_2\left(\frac{1}{\delta_2}\right) - 1,\end{aligned} \tag{41}$$

and here the second inequality is based on the fact that $\mathrm{H}^{\delta_3}_{\min}(\mathsf{K}^m_A|\mathsf{E}) \geq 0$. Next, we provide bound for $\mathrm{H}^{\delta_1}_{\mathrm{Twissmin}}(\mathsf{K}^1_A|\mathsf{K}^m_A\mathsf{E})$ by using the uncertainty relations for the smooth entropies. To achieve this, we use a gendankenexperiment where Alice and Bob prepare all their states in the basis $\mathscr{M}_2$ even when they choose the $\mathscr{M}_1$ basis. In this hypothetical protocol, the bit strings obtained from measurements in the complementary basis, C_A and C_B of length ℓ replace the keys K_A and K_B. The smooth min-entropy is expressed as

$$\begin{aligned}\mathrm{H}^{\delta_1}_{\min}(\mathsf{K}^1_A|\mathsf{K}^m_A\mathsf{E}) &\geq n_{1,1\mu} - \mathrm{H}^{\varepsilon}_{\max}(\mathsf{C}_A|\mathsf{C}_B)\\ &= n_{1,1\mu}[1 - h(e^{1,1}_{\mathscr{M}_2})],\end{aligned} \tag{42}$$

where $n_{1,1\mu} = N_\mu p^2_\kappa \mathrm{Q}^{1,1}_{\mu_a\mu_b,\mathscr{M}_1}$ denotes the sifted raw key size obtained from the single photon occurances.

Finally, we combine all the terms which represent errors for min-entropies and error probabilities due to parameter estimation discussed in previous section. Thus, the secrecy is given by

$$\varepsilon_{\mathrm{sec}} = 2\varepsilon + 2\delta_1 + \delta_2 + \nu + \varepsilon_1 + \varepsilon_2. \tag{43}$$

Here, ε_1 and ε_2 represent error probabilities for estimating the single photon events as well as the phase error rate. The error term is set to a common value ε and $\varepsilon_{\mathrm{sec}} = 8\varepsilon$. The final key length ℓ is obtained using the results from Eqs. (40) to (42) and invoking the secrecy requirement from Eqs. (43) in (39). Then, the final derived formula is written as

$$\ell = N_\mu p^2_\kappa\left[\mathrm{Q}^{1,1}_{\mu_a\mu_b,\mathscr{M}_1}(\log_2 3 - h_3(e^{1,1U}_{\mathscr{M}_2})) - \mathrm{leak}_{EC} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{4}{\varepsilon_{\mathrm{sec}}}\right]. \tag{44}$$

Received: 9 August 2022; Accepted: 18 January 2023
Published online: 21 January 2023

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).

2. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
3. Mafu, M. & Senekane, M. Security of quantum key distribution protocols, in *Advanced Technologies of Quantum Key Distribution* (IntechOpen, 2018).
4. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).
5. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
6. McKague, M. Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices. *New J. Phys.* **11**, 103037 (2009).
7. Hänggi, E. Device-independent quantum key distribution. arXiv preprint. arXiv:1012.3878 (2010).
8. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
9. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **87**, 012320 (2013).
10. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
11. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
12. Sibson, P. *et al.* Chip-based quantum key distribution. *Nat. Commun.* **8**, 1–6 (2017).
13. Wei, K. *et al.* High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X* **10**, 031030 (2020).
14. Semenenko, H. *et al.* Chip-based measurement-device-independent quantum key distribution. *Optica* **7**, 238–242 (2020).
15. Zhao, P., Zhou, L., Zhong, W. & Sheng, Y.-B. Faithful entanglement distribution using quantum multiplexing in noisy channel. *EPL (Europhys. Lett.)* **135**, 40001 (2021).
16. Cao, L. *et al.* Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems. *Phys. Rev. Appl.* **14**, 011001 (2020).
17. Kwek, L.-C. *et al.* Chip-based quantum key distribution. *AAPPS Bull.* **31**, 1–8 (2021).
18. Liu, Q. *et al.* Advances in chip-based quantum key distribution. *Entropy* **24**, 1334 (2022).
19. Orieux, A. & Diamanti, E. Recent advances on integrated quantum communications. *J. Opt.* **18**, 083002 (2016).
20. Sekga, C. & Mafu, M. Tripartite quantum key distribution implemented with imperfect sources. *Optics* **3**, 191–208 (2022).
21. Molina-Terriza, G., Torres, J. P. & Torner, L. Management of the angular momentum of light: preparation of photons in multidimensional vector states of angular momentum. *Phys. Rev. Lett.* **88**, 013601 (2001).
22. He, C., Shen, Y. & Forbes, A. Towards higher-dimensional structured light. *Light Sci. Appl.* **11**, 1–17 (2022).
23. Mafu, M. *et al.* Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88**, 032305 (2013).
24. Bechmann-Pasquinucci, H. & Peres, A. Quantum cryptography with 3-state systems. *Phys. Rev. Lett.* **85**, 3313 (2000).
25. Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
26. Reimer, C. *et al.* High-dimensional one-way quantum processing implemented on d-level cluster states. *Nat. Phys.* **15**, 148–153 (2019).
27. Nikolopoulos, G. M. & Alber, G. Security bound of two-basis quantum-key-distribution protocols using qudits. *Phys. Rev. A* **72**, 032320 (2005).
28. Navez, P. & Cerf, N. J. Cloning a real d-dimensional quantum state on the edge of the no-signaling condition. *Phys. Rev. A* **68**, 032313 (2003).
29. Howell, J. C., Bennink, R. S., Bentley, S. J. & Boyd, R. W. Realization of the Einstein–Podolsky–Rosen paradox using momentum- and position-entangled photons from spontaneous parametric down conversion. *Phys. Rev. Lett.* **92**, 210403 (2004).
30. Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
31. Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
32. Wang, F. *et al.* Towards practical high-speed high dimensional quantum key distribution using partial mutual unbiased basis of photon's orbital angular momentum. arXiv preprint. arXiv:1801.06582 (2018).
33. Bouchard, F. *et al.* Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2**, 111 (2018).
34. Tittel, W., Brendel, J., Zbinden, H. & Gisin, N. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.* **84**, 4737 (2000).
35. Thew, R. T., Acin, A., Zbinden, H. & Gisin, N. Bell-type test of energy-time entangled qutrits. *Phys. Rev. Lett.* **93**, 010503 (2004).
36. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. arXiv preprint. arXiv:0512080 (2005).
37. Ali-Khan, I., Broadbent, C. J. & Howell, J. C. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.* **98**, 060503 (2007).
38. Mower, J. *et al.* High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A* **87**, 062322 (2013).
39. Nunn, J. *et al.* Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Opt. Express* **21**, 15959–15973 (2013).
40. Bunandar, D., Zhang, Z., Shapiro, J. H. & Englund, D. R. Practical high-dimensional quantum key distribution with decoy states. *Phys. Rev. A* **91**, 022336 (2015).
41. Niu, M. Y., Xu, F., Shapiro, J. H. & Furrer, F. Finite-key analysis for time-energy high-dimensional quantum key distribution. *Phys. Rev. A* **94**, 052323 (2016).
42. Jo, Y. & Son, W. Key-rate enhancement using qutrit states for quantum key distribution with askew aligned sources. *Phys. Rev. A* **94**, 052316 (2016).
43. Hwang, W.-Y., Su, H.-Y. & Bae, J. N-dimensional measurement-device-independent quantum key distribution with n+ 1 uncharacterized sources: zero quantum-bit-error-rate case. *Sci. Rep.* **6**, 1–3 (2016).
44. Dellantonio, L., Sørensen, A. S. & Bacco, D. High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces. *Phys. Rev. A* **98**, 062301 (2018).
45. Bregman, I., Aharonov, D., Ben-Or, M. & Eisenberg, H. Simple and secure quantum key distribution with biphotons. *Phys. Rev. A* **77**, 050301 (2008).
46. Chekhova, M. Polarization and spectral properties of biphotons, in *Progress in Optics*, vol. 56, 187–226 (Elsevier, 2011).
47. Bogdanov, Y. I. *et al.* Qutrit state engineering with biphotons. *Phys. Rev. Lett.* **93**, 230503 (2004).
48. Burlakov, A. V. & Chekhova, M. V. Polarization optics of biphotons. *J. Exp. Theor. Phys. Lett.* **75**, 432–438 (2002).
49. Maslennikov, G., Zhukov, A., Chekhova, M. & Kulik, S. Practical realization of the quantum cryptography protocol exploiting polarization encoding in the qutrits. arXiv preprint. arXiv:0305115 (2003).
50. Chernoff, H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.* **23**, 493–507 (1952).
51. Jo, Y., Bae, K. & Son, W. Enhanced bell state measurement for efficient measurement-device-independent quantum key distribution using 3-dimensional quantum states. *Sci. Rep.* **9**, 1–11 (2019).
52. Yin, H.-L. & Chen, Z.-B. Finite-key analysis for twin-field quantum key distribution with composable security. *Sci. Rep.* **9**, 1–9 (2019).

53. Mafu, M., Garapo, K. & Petruccione, F. Finite-size key in the Bennett 1992 quantum-key-distribution protocol for Rényi entropies. *Phys. Rev. A* **88**, 062306 (2013).
54. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 1–6 (2012).
55. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 1–7 (2014).
56. Mafu, M., Garapo, K. & Petruccione, F. Finite-key-size security of the Phoenix-Barnett-Chefles 2000 quantum-key-distribution protocol. *Phys. Rev. A* **90**, 032308 (2014).
57. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
58. Wei, Z. *et al.* Decoy-state quantum key distribution with biased basis choice. *Sci. Rep.* **3**, 1–4 (2013).
59. Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 030301 (2010).
60. Moreva, E., Maslennikov, G., Straupe, S. & Kulik, S. Realization of four-level qudits using biphotons. *Phys. Rev. Lett.* **97**, 023602 (2006).
61. Goldberg, A. Z. Quantum polarimetry. *Prog. Opt.* **67**, 185–274 (2022).
62. Ma, P.-C., Chen, G.-B., Li, X.-W. & Zhan, Y.-B. Cyclic controlled remote state preparation in the three-dimensional system. *Laser Phys. Lett.* **19**, 115204 (2022).
63. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photonics* **7**, 210–214 (2013).

Author contributions

Conceptualization, C.S. and M.M.; methodology, C.S.; software, C.S.; validation, C.S. and M.M.; formal analysis, C.S., M.M. and M.S; writing—original draft preparation, C.S.; writing—review and editing, M.M.; supervision, M.M.; project administration, M.M.; funding acquisition, M.S. All authors have read and agreed to the published version of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to M.M.

Reprints and permissions information is available at www.nature.com/reprints.

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