CHIN. PHYS. LETT. Vol. 35, No. 9 (2018) 090302

Security Simulation of Continuous-Variable Quantum Key Distribution over Air-to-Water Channel Using Monte Carlo Method *

Cai-Lang Xie(谢才浪)[1], Ying Guo(郭迎)[1,2], Yi-Jun Wang(王一军)[1], Duan Huang(黄端)[1], Ling Zhang(张玲)[1]**

[1]*School of Information Science and Engineering, Central South University, Changsha 410083*
[2]*School of IOT Engineering, Taihu University, Wuxi 214064*

(Received 12 March 2018)

Considering the ocean water's optical attenuation and the roughness of the sea surface, we analyze the security of continuous-variable (CV) quantum key distribution (QKD) based air-to-water channel. The effects of the absorption and scattering on the transmittance of underwater quantum channel and the maximum secure transmission distance are studied. Considering the roughness of the sea surface, we simulate the performance bounds of CV QKD with different wind speeds using the Monte Carlo method. The results show that even if the secret key rate gradually reduces as the wind speed increases, the maximum transmission distance will not be affected obviously. Compared to the works regarding short-distance underwater optical communication, our research represents a significant step towards establishing secure communication between air platform and submarine vehicle.

PACS: 03.67.Dd, 03.67.Hk, 42.50.Ex DOI: 10.1088/0256-307X/35/9/090302

Quantum key distribution (QKD) provides a method to establish a secret shared key between two parties, traditionally called Alice and Bob. There are two available approaches of QKD that are employed to distribute secret keys, named as the discrete-variable QKD[1–4] and the continuous-variable (CV) QKD.[5–14] From a practical standpoint, the CV QKD has potential advantages due to its compatibility with the classical optical communication technologies. In a general CV-QKD system, the information is usually encoded in the quadrature of light with Gaussian modulation and sent through an insecure quantum channel to Bob. At Bob's side, the weak signal light is detected by interfering with a strong local oscillator (LO). Alice and Bob eventually extract a common string of the secret key after performing error correction and privacy amplification on the shared binary data. It is remarkable that the LO plays the role of the natural spatial and spectral filter,[15] which allows the system to run during the daytime.

The unconditionally secure quantum communications have so far been implemented in both fibers[16] and free-space air.[17] Recently, quantum communication over a seawater channel has attracted worldwide interest due to the commercial and secure considerations. The optical absorption and scattering properties of underwater media regarding underwater free space quantum channels have been investigated.[18] Moreover, the fact that quantum states can survive well after traveling through seawater has been demonstrated experimentally.[19] However, the light propagation in seawater is strongly affected by the absorption and scattering, which results in a very short communication distance.

Fortunately, the short-distance underwater quantum communication can be applied in some special and vital applications. For example, an encrypted message can be transmitted from a platform in air, such as a ground station, shape and aircraft to an underwater vehicle, even if it is close to the surface. In fact, the schemes of the optical mast based receiver and the buoy-based receiver have already been proposed.[20] However, the submarine may expose its location in these approaches, which brings a serious security flaw.

In this Letter, we focus on the CV QKD over an air-to-water channel and analyze its performance based on a rough sea surface. In this scheme, the secret keys are transmitted from free-space air to sea water directly. We first analyze the performance of the CV-QKD system which is only affected by optical absorption and scattering. The relationship between the transmittance and the coefficients of absorption and scattering is derived. Moreover, the roughness of the sea surface should also be considered to be a vital factor that causes deflection. Due to the randomness of the surface, the Monte Carlo method is employed to generate the slopes of wind-induced waves.[21] Combining the characters of free-space quantum channels, we evaluate the performance of the CV-QKD system. The results show that the roughness of the sea surface will reduce the secret key rate of CV QKD, but it will not reduce the transmission distance significantly, representing an important step towards the secure communication from air platform to underwater vehicles.

Firstly, considering the situation that the sea surface is flat, then the absorption and scattering are two main factors affecting light propagation through water. To define the total attenuation, absorption coefficient a and scattering coefficient b are introduced, both of which are the functions of the optical wavelength λ and chlorophyll concentration C.[22] The total attenuation coefficient c is defined as the sum of a and b,

$$a(\lambda) = [a_{\mathrm{w}}(\lambda) + 0.06 a_{\mathrm{c}}(\lambda) C^{0.65}][1 + 0.2 e^{-0.014(\lambda - 440)}],$$
$$b(\lambda) = 0.3 \frac{550}{\lambda} C^{0.62}, \quad c(\lambda) = a(\lambda) + b(\lambda), \tag{1}$$

*Supported by the National Natural Science Foundation of China under Grant No 61572529.
**Corresponding author. Email: lingzhang2017@foxmail.com
© 2018 Chinese Physical Society and IOP Publishing Ltd

where $a_{\rm w}(\lambda)$ is the absorption coefficient in ocean water, and $a_{\rm c}(\lambda)$ is the statistically derived chlorophyll specific absorption coefficient. Due to the existence of a blue-green optical window at the wavelength regime of 450–550 nm in seawater, we choose the light at 520 nm and numerically study the influence of propagation distance on the performance of CV QKD. The corresponding coefficients a, b, and c are listed in Table 1.

Table 1. Coefficient values of different water types at 520 nm.

Water types	$a\,(\mathrm{m}^{-1})$	$b\,(\mathrm{m}^{-1})$	$c\,(\mathrm{m}^{-1})$
Pure sea water	0.0405	0.0025	0.043
Clear ocean water	0.114	0.037	0.151
Coastal ocean water	0.179	0.219	0.398
Turbid harbor water	0.366	1.824	2.190

Table 2. Parameters for the security analysis of the CV-QKD system. All the variances and noises are in shot noise unit.

$V_{\rm A}$	ξ	η	$v_{\rm el}$	β	N	n	$\epsilon_{\rm PE}$
4	0.01	0.6	0.01	0.9	10^{10}	$10^{10}/2$	10^{-10}

Based on the assumption that the submarine vehicle is close to the sea surface, we could regard the seawater as a linear quantum channel. In a finite size analysis,[6] the secret key rate of the CV QKD against the collective attack reads

$$K = \frac{n}{N}[\beta I_{\rm AB} - S_{\rm BE}^{\epsilon_{\rm PE}} - \Delta(n)], \tag{2}$$

where $\frac{n}{N}$ is the ratio of the number of photons used to establish the secret key to the total number of photons exchanged by Alice and Bob, β is the reconciliation efficiency, the mutual information $I_{\rm AB}$ gives the amount of effective mutual information between Alice and Bob, $S_{\rm BE}^{\epsilon_{\rm PE}}$ is defined as the upper bound of the Holevo information compatible with probability $\epsilon_{\rm PE}$, and $\Delta(n)$ is a function corresponding to the privacy amplification. Here the mutual information $I_{\rm AB}$ can be calculated by

$$I_{\rm AB} = \frac{1}{2}\log_2\left(\frac{V+\chi_{\rm tot}}{1+\chi_{\rm tot}}\right), \tag{3}$$

where $\chi_{\rm tot} = \chi_{\rm ch} + \chi_{\rm Bob}/T$ is the total added noise referring to the input, $\chi_{\rm ch} = 1/T - 1 + \xi$ is the channel added noise, and $\chi_{\rm Bob} = [(1-\eta) + v_{\rm el}]/\eta$ is the detector added noise. The parameter ξ represents the excess noise while η and $v_{\rm el}$ correspond to the efficiency and electric noise of the detector, respectively. Here $T = e^{\rm cD}$ represents the transmittance of sea water with the attenuation coefficient c and the depth D. For the Gaussian modulated coherent state CV-QKD system, the variance $V = V_{\rm A} + 1$ with the modulated variance $V_{\rm A}$ at the Alice side. Based on the covariance matrix of the shared states between Alice and Bob,

$$\gamma_{\rm AB} = \begin{pmatrix} V\boldsymbol{I} & \sqrt{T(V^2-1)}\boldsymbol{Z} \\ \sqrt{T(V^2-1)}\boldsymbol{Z} & T(V+\chi_{\rm ch})\boldsymbol{I} \end{pmatrix}, \tag{4}$$

where $\boldsymbol{I} = \mathrm{diag}(1,1)$, $\boldsymbol{Z} = \mathrm{diag}(1,-1)$, the value of $S_{\rm BE}^{\epsilon_{\rm PE}}$ can also be estimated, and the privacy amplification function $\Delta(n)$ reads

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{\rm PA}), \tag{5}$$

where $\bar{\epsilon}$ and $\epsilon_{\rm PA}$ are the smoothing parameter and failure probability of the privacy amplification, respectively. Based on the corresponding parameters of the system in Table 2, which are standard in CV-QKD experiments. Figure 1 shows the secret key rate K of the CV QKD as a function of the transmission depth under water. The results show that the maximum secure transmission distance is around 80 m in the pure sea water, which may fit for the demand of practical air-to-water applications. However, the performance decreases sharply with the changes of the water quality conditions. For example, compared to the secure transmission distance of 80 m in pure sea water, the secure bounds are less than 20 m in the coastal ocean water. The worst achievable transmission distance in turbid harbor water is only a few meters. Fortunately, most of the air-to-water applications may run far from the coastline, which means that the water types of pure sea water and clear ocean water could be the closest conditions for practical implementations.

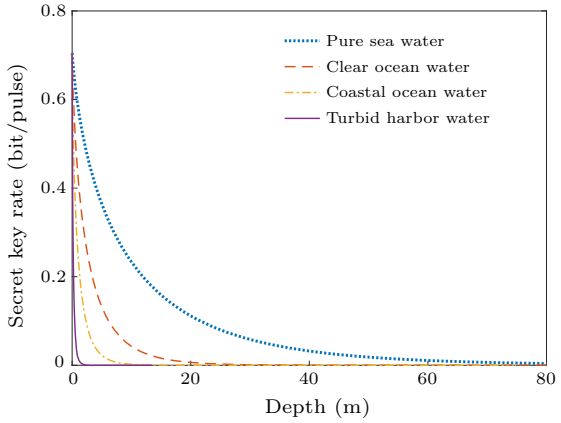

Fig. 1. The secret key rate as a function of the transmission depth in four typical water types.

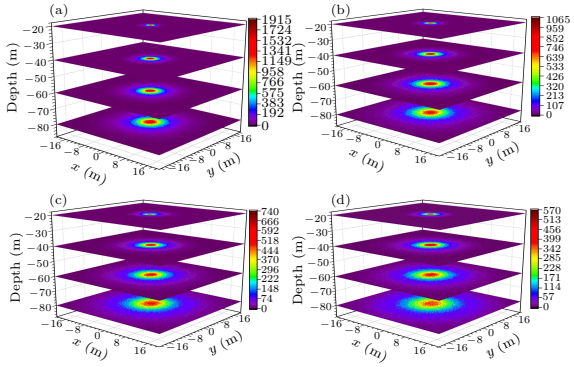

Fig. 2. The light intensity distribution derived from the rough sea surface at different depths of water. The wind speeds are set to (a) 3 m/s, (b) 6 m/s, (c) 9 m/s, and (d) 12 m/s, respectively. The total number of photons for the Monte Carlo simulation is 10^6.

However, from a practical point of view, the real sea surface will not be absolutely stable as a smooth flat surface but fluctuating in time due to many factors. The roughness of the sea surface is an important factor because it will cause the deflection of the propagation direction. Actually, there are three types of roughness, i.e., wind-induced waves, tidal caused by

gravity and centrifugal force, and tsunami caused by tectonic force. The tidal and tsunami types have a very small effect on CV QKD due to their long wavelengths. Therefore, we focus on the influence of wind-induced waves on the CV-QKD performance.

A general and widely used wave model was presented by Cox and Munk (CM).[21] It describes an approach for interpreting the statistics of the sun's glitter on the sea surface in terms of the statistics of the slope distribution. They found that the probability distribution of the cross-wind components is closely Gaussian and the up-wind components should be approximated with extra higher moments. The probability distribution of the rough sea surface slopes thus can be characterized by the Gram–Charlier distribution

$$\begin{aligned} p(Z_{\rm u}, Z_{\rm c}) = & \frac{1}{2\pi\sigma_{\rm u}\sigma_{\rm c}} \exp\Big[-\frac{1}{2}(Z_{\rm u}^2 + Z_{\rm c}^2)\Big] \\ & \times \Big[1 - \frac{1}{2}c_{21}Z_{\rm c}(Z_{\rm u}^2 - 1) \\ & - \frac{1}{6}c_{03}(Z_{\rm c}^3 - 3Z_{\rm c}) \\ & + \frac{1}{24}c_{40}(Z_{\rm u}^4 - 6Z_{\rm u}^2 + 3) \\ & + \frac{1}{4}c_{22}(Z_{\rm u}^2 - 1)(Z_{\rm c}^2 - 1) \\ & + \frac{1}{24}c_{04}(Z_{\rm c}^4 - 6Z_{\rm c}^2 + 3)\Big], \end{aligned} \tag{6}$$

and

$$Z_{\rm u} = \frac{\varepsilon_{\rm u}}{\sigma_{\rm u}}, Z_{\rm c} = \frac{\varepsilon_{\rm c}}{\sigma_{\rm c}}, \tag{7}$$

where $\varepsilon_{\rm u}$ and $\varepsilon_{\rm c}$ represent the up-wind and cross-wind of wave surface slopes with the variances $\sigma_{\rm u}^2$ and $\sigma_{\rm c}^2$, respectively. The corresponding parameters are estimated by

$$\begin{aligned} & \sigma_{\rm c}^2 = 0.003 + 1.92 \times 10^{-3} v, \ \sigma_{\rm u}^2 = 3.16 \times 10^{-3} v \\ & c_{21} = 0.01 - 0.0086v, \ c_{03} = 0.04 - 0.033v, \\ & c_{40} = 0.4, c_{22} = 0.12, \ c_{04} = 0.23, \end{aligned} \tag{8}$$

where v is the wind speed.

To obtain the angle of incidence $\theta_{\rm i}$ in the CM model, it is necessary to calculate the local surface slope ε in the direction $\theta_{\rm s}$ against the up-wind direction. They are linked by

$$\varepsilon = \sqrt{\varepsilon_{\rm u}^2 + \varepsilon_{\rm c}^2}, \ \theta_{\rm s} = \arctan\Big(\frac{\varepsilon_{\rm c}}{\varepsilon_{\rm u}}\Big). \tag{9}$$

The refraction angle $\theta_{\rm r}$ can be calculated by Snell's law expressed as $\theta_{\rm r} = \arcsin(\frac{\sin\theta_{\rm i} n_{\rm a}}{n_{\rm w}})$, where the refractive indices of air and water, $n_{\rm a}$ and $n_{\rm w}$, can be set to $n_{\rm a} = 1.000293$ and $n_{\rm w} = 1.34$, respectively. Figure 2 shows the light intensity distribution at the depths of 20 m, 40 m, 60 m, and 80 m. The Monte Carlo method is used to simulate the emitted and received photons. We can see that the beam spot becomes larger with the increasing transmission depth. This phenomenon can be explained from the geometry three-dimensional surface. Moreover, it is obvious that the higher speed wind causes worse deflection.

For the finite radius of the aperture, the light deflection will directly affect the efficiency of the detector. We define $\eta_{\rm def}$ to characterize the ratio of the received photons to total emitted photons. To evaluate $\eta_{\rm def}$, we integrate the photons over the receiver radius r based on the results of the above intensity distribution. Figure 3 illustrates $\eta_{\rm def}$ as functions of wind speed and depth. No matter whether the wind speed or depth increases, the efficiency $\eta_{\rm def}$ will decrease rapidly. For example, the detection efficiency is around 0.43 at the depth of 20 m but it achieves 0.05 at the depth of 80 m when the wind speed is 3 m/s. In the view of varying wind speed, the value of the efficiency is reduced from 0.43 to 0.18 as the wind speed increases from 3 m/s to 12 m/s at the depth of 20 m.

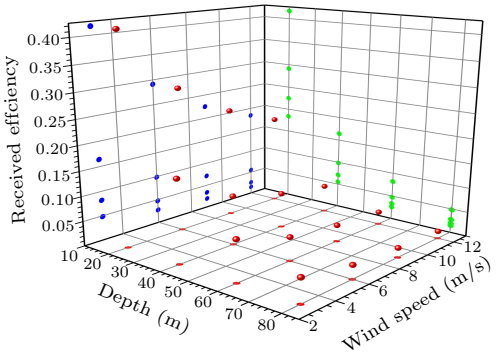

Fig. 3. The efficiency of the detector as a function of different wind speeds and depths. The wind speeds are set to 3 m/s, 6 m/s, 9 m/s and 12 m/s, and the depths are set to 20 m, 40 m, 60 m, and 80 m. The number of photons used for Monte Carlo simulation is 10^6 for each case and the radius of the receiver is 1 m.

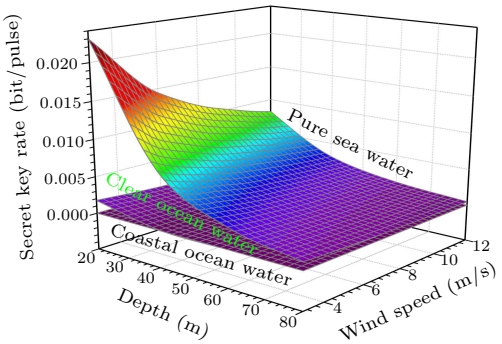

Fig. 4. The secret key rate as functions of depth and wind speed for three kinds of water types. The results from top to bottom represent the cases of pure sea water, clear ocean water, and coastal ocean water, respectively.

For an air channel, we mainly consider the important effects of beam wandering and broadening, caused by atmospheric turbulence. Compared to the linear quantum channel like a fiber whose transmittance could be easily obtained using transmission distance, the air channel is more complicated and probabilistic. Fortunately, based on the beam-spot radius W and the beam-deflection distance r, the transmittance of light in free-space air could be characterized by the log-negative Weibull distribution,[23–26] which

can be expressed as

$$P(T^{\rm air}) = \frac{2R^2}{\delta^2 \lambda T^{\rm air}} \left(2\ln\frac{T_0^{\rm air}}{T^{\rm air}}\right)^{\frac{2}{\lambda}-1} \exp\left[-\frac{R^2(2\ln\frac{T_0^{\rm air}}{T^{\rm air}})^{\frac{2}{\lambda}}}{2\delta^2}\right] \quad (10)$$

for $T^{\rm air} \in [0, T_0^{\rm air}]$, and $P(T^{\rm air}) = 0$ else. Here the notation $T_0^{\rm air}$ is the maximal transmission coefficient for the given beam-spot radius, λ and R represent the shape and scale parameters, respectively,

$$\lambda = 8\Phi \frac{\exp(-4\Phi) I_1(4\Phi)}{1-\exp(-4\Phi) I_0(4\Phi)} \times \left[\ln\left(\frac{2T_0^2}{1-\exp(-4\Phi) I_0(4\Phi)}\right)\right]^{-1},$$
$$R = a\left[\ln\left(\frac{2T_0^2}{1-\exp(-4\Phi) I_0(4\Phi)}\right)\right]^{-(1/\lambda)}, \quad (11)$$

where $\Phi = \frac{a^2}{W^2}$, a is the aperture radius, and I_n the modified Bessel function.

In the log-negative Weibull model, the beam-deflection distance depends on the Rice distribution with the variance δ^2. It is notable that the atmospheric transmittance is not constant but fluctuating in time, which has been discussed in the previous work.[27–29] Fortunately the transmitted quantum states could be governed by two parameters of the attenuation distribution, i.e., the mean value of transmittance $\langle T^{\rm air}\rangle$ and the mean of the square root of transmittance $\langle\sqrt{T^{\rm air}}\rangle$.

We now analyze the performance of the CV-QKD system under the influence of a rough sea surface. The emitted photons may not be collected perfectly but deflected out of the receiver aperture. Therefore, the transmittance of the air-to-water channel becomes $T' = \eta_{\rm def} T\langle T^{\rm air}\rangle$. The covariance matrix of the shared states (Eq. (4)) becomes

$$\gamma'_{\rm AB} = \begin{pmatrix} V\boldsymbol{I} & \gamma'_{12} \\ \gamma'_{21} & T'(V+\chi_{\rm ch})\boldsymbol{I} \end{pmatrix}, \quad (12)$$

where $\gamma'_{12} = \langle\sqrt{T^{\rm air}}\rangle\sqrt{\eta_{\rm def}T(V^2-1)}\boldsymbol{Z}$, and $\gamma'_{21} = \langle\sqrt{T^{\rm air}}\rangle\sqrt{\eta_{\rm def}T(V^2-1)}\boldsymbol{Z}$. Then the secret key rate of the CV QKD can be easily estimated using Eq. (2). Based on the approximation of $\delta^2 = 0.5$ and $W = 0.5$ (the aperture radius is normalized, i.e., $a = 1$), Fig. 4 shows the secret key rate at the depths from 20 m to 80 m and the wind speeds from 3 m/s to 12 m/s. The system could generate secret keys only in three kinds of water types, that is, pure sea water, clear ocean water, and coastal ocean water. Compared to the results based on the assumption that the surface is flat, even the performance of the CV QKD with a rough sea surface is worse than the case of a flat surface, there is a slight difference between their secure transmission distances. For example, in Fig. 1 the secret key will be around 0.1 bit/pulse for pure sea water at the depth of 20 m if the surface is flat. In Fig. 4 it decreases to 0.023 bit/pulse but still keeps positive at a depth of 80 m. This implies that the air-to-water CV-QKD system based on a rough sea surface which is close to the real condition is feasible. Furthermore, by combining with the satellite QKD technologies, it is possible to establish a global secure underwater communication network.

In summary, the performance of CV QKD based on the rough sea surface has been analyzed. According to the CM model, the relationship between speed wind and detection efficiency is derived. To be as close to the real sea surface as possible, different speeds of cross-wind and up-wind are generated using the Monte Carlo method. The results show that the secret key rate is related strongly to the water type, wind speed, and depth of submarine vehicle. The roughness of the sea surface could degrade the performance of the CV-QKD system, but has slight influence on the transmission distance. This means that the implementation of CV QKD between a sender upon the surface and a receiver under sea water is feasible. Our research has important significance in the future explorations regarding to the secure global underwater optical communication network. Moreover, the factors such as sea foam and floating organisms will also change the status of the sea surface and thus affect the performance of the CV-QKD system, which will become the follow-up research focus.

References

[1] Gisin N et al 2002 *Rev. Mod. Phys.* **74** 145
[2] Lo H K et al 2014 *Nat. Photon.* **8** 595
[3] Pirandola S et al 2015 *Nat. Photon.* **9** 397
[4] Sun S H et al 2010 *Opt. Lett.* **35** 1203
[5] Braunstein S L and van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[6] Leverrier A et al 2010 *Phys. Rev.* A **81** 062343
[7] Peuntinger C et al 2014 *Phys. Rev. Lett.* **113** 060502
[8] Guo Y et al 2018 *Phys. Rev.* A **97** 052326
[9] Kevin G et al 2017 *Optica* **4** 611
[10] Jouguet P et al 2013 *Nat. Photon.* **7** 378
[11] Gehring T et al 2015 *Nat. Commun.* **6** 8795
[12] Nathan W et al 2016 *Optica* **3** 634
[13] Liao Q et al 2018 *New J. Phys.* **20** 023015
[14] Bai Z L et al 2016 *Sci. Chin.-Phys. Mech. Astron.* **59** 614201
[15] Elser D et al 2009 *New J. Phys.* **11** 045014
[16] Marcikic I et al 2003 *Nature* **421** 509
[17] Bennett C H et al 1992 *J. Cryptology* **5** 3
[18] Shi P, Zhao S C, Gu Y J and Li W D 2015 *J. Opt. Soc. Am.* A **32** 349
[19] Ji L, Gao J, Yang A L, Feng Z, Lin X F, Li Z G and Jin X M 2017 *Opt. Express* **25** 19795
[20] Philip A H and Robert A L 2014 *Proc. SPIE* **9114** 9114
[21] Charles C and Walter M 1954 *J. Opt. Soc. Am.* **44** 838
[22] Kong M W, Wang J L, Chen Y F, Ali T, Sarwar R, Qiu Y, Wang S L, Han J and Xu J 2017 *Opt. Express* **25** 21509
[23] Zunino L, Gulich D, Funes G and Perez D G 2015 *Opt. Lett.* **40** 3145
[24] Berman G P, Chumak A A and Gorshkov V N 2007 *Phys. Rev.* E **76** 056606
[25] Jakeman E and Ridley K D 2007 *Waves Random Complex Media* **17** 405
[26] Vasylyev D Y, Semenov A A and Vogel W 2012 *Phys. Rev. Lett.* **108** 220501
[27] Vladyslav C U, Bettina H, Christian P, Christoffer W, Christoph M, Gerd L and Radim F 2012 *New J. Phys.* **14** 093048
[28] Dong R F, Lassen M, Heersink J, Marquardt C, Filip R, Leuchs G and Andersen U L 2010 *Phys. Rev.* A **82** 012312
[29] Guo Y, Xie C L, Liao Q, Zhao W, Zeng G H and Huang D 2017 *Phys. Rev.* A **96** 022320