Performance analysis of quantum key distribution based on air-water channel*

ZHOU Yuan-yuan (周媛媛)** **and ZHOU Xue-jun** (周学军)
Electronic Engineering College, Naval University of Engineering, Wuhan 430033, China

(Received 5 January 2015)

Considering the air-water interface and ocean water's optical attenuation, the performance of quantum key distribution (QKD) based on air-water channel is studied. The effects of photons' various incident angles to air-water interface on quantum bit error rate (QBER) and the maximum secure transmission distance are analyzed. Taking the optical attenuation of ocean water into account, the performance bounds of QKD in different types of ocean water are discussed. The simulation results show that the maximum secure transmission distance of QKD gradually reduces as the incident angle from air to ocean water increases. In the clearest ocean water with the lowest attenuation, the maximum secure transmission distance of photons far exceeds the the working depth of underwater vehicles. In intermediate and murky ocean waters with higher attenuation, the secure transmission distance shortens, but the underwater vehicle can deploy other accessorial methods for QKD with perfect security. So the implementation of OKD between the satellite and the underwater vehicle is feasible.
Document code: A **Article ID:** 1673-1905(2015)02-0149-4
DOI 10.1007/s11801-015-5004-3

"Quantum secure communication of China Beijing Shanghai line" project has been started, which proves a great leap of quantum key distribution (QKD)[1] from experiment to application[2]. In recent years, many theoretical and experimental researches have been carried out towards the development of practical QKD systems based on optical fibers[3-14] and free-space[15-17]. However, people have higher expectations that the quantum secure communication can completely improve the underwater communication. Marco Lanzagorta[18] presented a good idea that QKD can be implemented between the satellite and the underwater vehicle to construct a two-way laser communication link with perfect security, and theoretically proved that the implementation of BB84 QKD protocol between two users submerged in ocean water was feasible. Ref.[19] analyzed the influence of the transmission rates of different photon components on quantum bit error rate (QBER) of QKD between different media. However, other than the influence of air-water interface, there is much challenge confronted by the photon signals from air to ocean water, such as the larger optical attenuation of ocean water, various noise and quantum efficiency of photodetector.

In this paper, synthetically considering the influence of the air-water interface and the optical attenuation of the ocean water on QKD, the maximum secure transmission distances of BB84 QKD in different types of water are analyzed, and a more comprehensive demonstration for the feasibility of implementing OKD between the satellite and the underwater vehicle is provided.

As shown in Fig.1, there is an incident ray with wave vector $\boldsymbol{k}$ from the medium with refractive index n_1 to the medium with refractive index n_2, and the angle of refraction is γ.

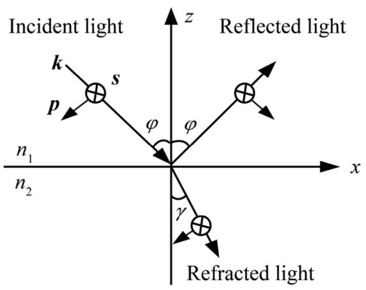

Fig.1 Schematic diagram of the photons transmitting between different media

Then we define t_p and t_s to be the amplitude transmittances of $\boldsymbol{s}$ component and $\boldsymbol{p}$ component, respectively. According to Fresnel formula[20], t_p and t_s can be expressed as

$$t_p = \frac{2\sin\gamma\cos\phi}{\sin(\phi+\gamma)\cos(\phi-\gamma)}\,, \tag{1}$$

$$t_s = \frac{2\sin\gamma\cos\phi}{\sin(\phi+\gamma)}\,. \tag{2}$$

* This work has been supported by the National High Technology Research and Development Program of China (No.2011AA7014061).
** E-mail: zyy_hjgc@aliyun.com

As shown in Eqs.(1) and (2), $t_p=t_s$ is with ϕ=0° and $0<t_s<t_p$ is with 0°<ϕ<90°. There is no phase change in the refracted light. A photon state with a certain polarization is projected to ***s*** direction and ***p*** direction, and $a|\boldsymbol{p}\rangle+b|\boldsymbol{s}\rangle$ is gained, where a and b are complex numbers. Then, the photon state of transmitted light changes to $at_p|\boldsymbol{p}\rangle+bt_s|\boldsymbol{s}\rangle$. It is known that t_p and t_s are not equal in general. Therefore, the polarizations of the photons with $ab\neq0$ will change.

Under ideal condition, the photon-state changes of two pairs of orthogonal bases before and after transformation will cause bit error. The bit error rate of a pair of basis vectors of $|\boldsymbol{\alpha}\rangle$ and $|\boldsymbol{\beta}\rangle$ can be given as

$$Q_{\alpha\beta}=\frac{\left(\langle\boldsymbol{\alpha}|\boldsymbol{\beta}'\rangle\right)^2+\left(\langle\boldsymbol{\beta}|\boldsymbol{\alpha}'\rangle\right)^2}{\left(\langle\boldsymbol{\alpha}|\boldsymbol{\alpha}'\rangle\right)^2+\left(\langle\boldsymbol{\beta}|\boldsymbol{\beta}'\rangle\right)^2+\left(\langle\boldsymbol{\alpha}|\boldsymbol{\beta}'\rangle\right)^2+\left(\langle\boldsymbol{\beta}|\boldsymbol{\alpha}'\rangle\right)^2},\tag{3}$$

where $|\boldsymbol{\alpha}'\rangle$ and $|\boldsymbol{\beta}'\rangle$ denote the polarizations after $|\boldsymbol{\alpha}\rangle$ and $|\boldsymbol{\beta}\rangle$ transmissions, respectively.

Considering the most typical case, we choose the four states $|\boldsymbol{p}\rangle$, $|\boldsymbol{s}\rangle$, $(|\boldsymbol{p}\rangle+|\boldsymbol{s}\rangle)/\sqrt{2}$ and $(|\boldsymbol{p}\rangle-|\boldsymbol{s}\rangle)/\sqrt{2}$ corresponding to the H, V, + and – in BB84 protocol. Through the interface of different media, the former two states keep unchanged, but the later two states will change to

$$\left(t_p|\boldsymbol{p}\rangle+t_s|\boldsymbol{s}\rangle\right)/\sqrt{t_p^2+t_s^2},\tag{4}$$

$$\left(t_p|\boldsymbol{p}\rangle-t_s|\boldsymbol{s}\rangle\right)/\sqrt{t_p^2+t_s^2}.\tag{5}$$

Eqs.(4) and (5) show that the transformation is not unitary. So the transformation will lead to the rise of bit error rate and finally influence the key generation rate and the secure transmission distance.

According to Eq.(3), $|\boldsymbol{p}\rangle$ and $|\boldsymbol{s}\rangle$ keep unchanged, so bit error rate does not change and can be defined as 0. However, the bit error rate caused by the transformation of $(|\boldsymbol{p}\rangle+|\boldsymbol{s}\rangle)/\sqrt{2}$ and $(|\boldsymbol{p}\rangle-|\boldsymbol{s}\rangle)/\sqrt{2}$ can be given by

$$Q_p=\frac{\left(t_p-t_s\right)^2}{2\left(t_p^2+t_s^2\right)}.\tag{6}$$

Subsequently, the performance of QKD under water is analyzed. After transmitting through the air-water interface, the photon signals go into seawater and arrive at the underwater vehicles. The underwater photon communication system can be influenced by optical attenuation, various noises, quantum efficiency of photodetector and so on. Here, the influence of optical attenuation in seawater on QKD is mainly considered.

For convenience, the ocean waters have been divided into Jerlov water types[21] that approximately share the same optical properties. The Jerlov water types under consideration in our discussion and their respective attenuation coefficients χ_c for light with λ=480 nm are given in Tab.1.

Tab.1 Approximate values of the total attenuation coefficient χ_c for the three main types of Jerlov ocean water for λ=480 nm

Jerlov type	Description	χ_c (m^{-1})
I	Clearest	0.03
II	Intermediate	0.18
III	Murkiest	0.30

It is important to emphasize that the attenuation coefficients in Tab.1 are only approximations for a certain wave. Indeed, the optical properties of ocean water tend to change with depth, seasonal changes and weather effects. In what follows, we assume that the quoted value for the attenuation coefficient is constant over the entire water column above the underwater vehicle.

QBER is an important quantity used to quantify the security of the QKD system[22-24]. It decides the key generation rate of QKD directly. For a typical BB84 QKD system, the QBER is given as

$$QBER=\frac{I_{dc}+\frac{R_d A\Delta t'\lambda\Delta\lambda\Omega}{4hc\Delta t}}{\frac{u\eta}{2\Delta t}e^{-\chi_c r}+2I_{dc}+\frac{R_d A\Delta t'\lambda\Delta\lambda\Omega}{2hc\Delta t}},\tag{7}$$

where I_{dc} is the dark current, Ω is the field of view of the detector, h is Planck's constant, c is the speed of light, η is the quantum efficiency of the detector, χ_c is the attenuation coefficient, R_d is the irradiance of the environment, $\Delta\lambda$ is the filter spectral width, Δt is the bit period, $\Delta t'$ is the receiver gate time, A is the receiver aperture, and u is the mean photon number per pulse.

The final key generation rate can be given by

$$R=1-H_2\left(Q_b\right)-H_2\left(Q_p\right),\tag{8}$$

where Q_b and Q_p correspond to the QBER and phase error rate based on the same measurement basis, and $H_2(Q_b)$ and $H_2(Q_p)$ are the binary Shannon information entropy functions given by $H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x)$. Here, when photon signals transmit through air-water interface, Q_b is considered to be unchangeable and defined as 0 under ideal condition, and Q_p can be calculated by Eq.(6). However, when photon signals are under water, Q_b is given by Eq.(7), and Q_p is equal to 0.

The simulation does not consider the transmission of photon signals in air, and the emphasis is on the courses from air to water and in water. We use the parameters shown in Tab.2 to characterize the underwater optical communication system[18]. The refractive indices of two media are n_1=1 and n_2=1.33.

Fig.2 shows phase error rate Q_p as a function of the incident angle ϕ. The phase error rate is Q_p=0 with the incident angle ϕ=0°. Q_p gradually increases with the increase of ϕ, and reaches the maximum of 0.019 5 with ϕ=90°.

In Fig.3, the phase error rate Q_p is chosen as the maximum of 0.019 5. Then, it is the worst influence of the air-water interface on the photon transmission in water. Fig.3 shows that the maximum secure transmission distance is obtained as about 281 m in the clearest ocean water (Jerlov type I). However, the maximum secure transmission distances in intermediate (Jerlov type II) and murky (Jerlov type III) ocean waters are 46 m and 28 m, respectively. It is worthwhile to mention that most of the underwater operations require a range of about 100 m and are carried out in deep blue waters which correspond very closely to Jerlov Type I ocean waters. It is obvious that 281 m is far beyond the working deepness of the underwater vehicles. Even though the underwater vehicle is in intermediate and murky ocean waters, it can deploy a small buoy to carry the optical transmitter and receiver for transmitting and receiving messages with perfect security.

Tab.2 Parameters for characterizing the underwater optical communication system

Parameter	Value	Parameter	Value
ϕ	10°	Ω	$2\pi(1-\cos\phi)$
λ	480 nm	$\Delta\lambda$	0.12×10^{-9} nm
Δt	35 ns	$\Delta t'$	200 ps
R_d	0.012 5	η	0.3
u	0.1 Hz	I_{dc}	60 Hz
A	30 cm^2		

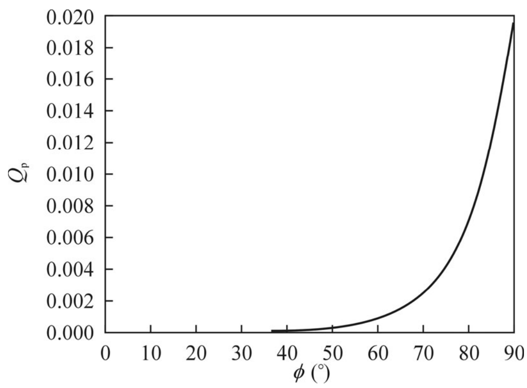

Fig.2 The phase error rate Q_p as a function of the incident angle ϕ

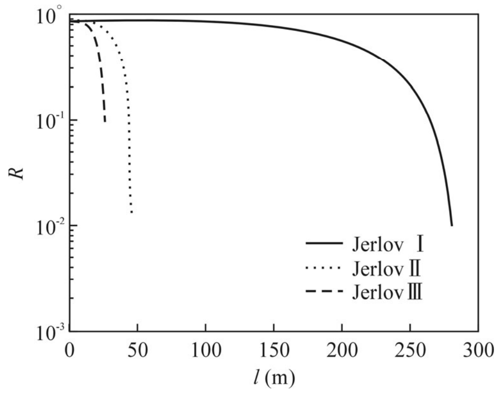

Fig.3 The key generation rate as a function of the transmission distance in three types of Jerlov waters

From Fig.4, we can see that the maximum secure transmission distance of QKD gradually reduces as the incident angle ϕ increases. In the clearest ocean water, the maximum secure transmission distance can be most up to 421 m, and is not less than 281 m. In intermediate and murky ocean waters, the variation ranges of the maximum secure transmission distance are from 70 m to 47 m and from 42 m to 28 m, respectively.

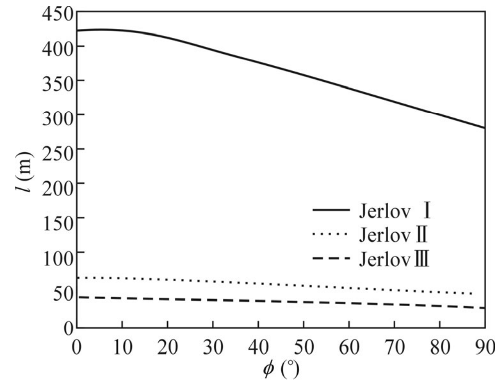

Fig.4 The maximum secure transmission distance as a function of the incident angle ϕ in three types of Jerlov waters

In summary, in this paper, we consider synthetically the influence of air-water interface and ocean water's optical attenuation on the performance of QKD in the transmission process of photon signals from air to ocean water, analyze the effects of photons' various incident angles to air-water interface on QBER and the maximum secure transmission distance, and discuss the performance bounds of OKD in different types of ocean waters considering the optical attenuation of ocean water. The simulation results show that the maximum secure transmission distance of QKD gradually reduces with the increase of the incident angle from air to ocean water. Considering the optical attenuation of the ocean water, the maximum secure transmission distance of photons can be most up to 421 m and is not less than 281 m in the clearest ocean water with lower attenuation. The transmission distance is superduper for the underwater vehicles carried out in deep blue waters which correspond very closely to the clearest ocean water. In intermediate and murky ocean waters with higher attenuation, the variation ranges of the maximum secure transmission distance are from 70 m to 47 m and from 42 m to 28 m, respectively. In the later two types of waters, the underwater vehicle can also deploy other accessorial methods for QKD with perfect security. So the implementation of OKD between the satellite and the underwater vehicle is feasible. A more detailed feasibility study, which includes a very precise characterization of the ocean foam, electromagnetic and scattering properties of oceanic waters, as well as their effect on the quantum channels, will be our next research focus.

References

[1] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, IEEE International Conference on Computers, Syetems and Signal Processing **175**, (1984).

[2] CNII, http://www.cnii.com.cn/broadband/2014-05/13/content 1360888. htm.

[3] H. K. Lo, C. Marcos and Q. Bing, Physical Review Letters **108**, 130503 (2012).

[4] F. H. Xu, B. Qi, Z. L. Liao and H. K. Lo, Applied Physics Letters **103**, 061101 (2013).

[5] Y. Y. Zhou, H. Q. Zhang, X. J. Zhou and P. G. Tian, Acta Physica Sinica **62**, 200302 (2013). (in Chinese)

[6] H. Q. Zhang, Y. Y. Zhou, X. J. Zhou and P. G. Tian, Optoelectronics Letters **9**, 389 (2013).

[7] Y. Y. Zhou, X. J. Zhou, P. G. Tian and Y. J. Wang, Chinese Physics B **22**, 010305 (2013).

[8] Y. Y. Zhou and X. J. Zhou, Acta Physica Sinica **60**, 100301 (2011). (in Chinese)

[9] Y. Y. Zhou, X. J. Zhou and J Gao, Optoelectronics Letters **6**, 396 (2010).

[10] Y. Y. Zhou and X. J. Zhou, Optoelectronics Letters **7**, 389 (2011).

[11] H. P. Hu, J. D. Wang, Y. X. Huang, S. H. Liu and W. Lu, Acta Physica Sinica **59**, 287 (2010). (in Chinese)

[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).

[13] S. L. Zhang, X. B. Zou, C. F. Li, C. H. Jin and G. C. Guo, Chinese Science Bulletin **54**, 1863 (2009).

[14] J. Yang, B. J. Xu, X. Peng and H. Guo, Physics Letters A **85**, 052302 (2012).

[15] T. Schmitt-Manderbach, H. Weier, M. Fürs, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter, Physical Review Letters **98**, 010504 (2007).

[16] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson and C. M. Simmons, Physical Review Letters **81**, 03283 (1998).

[17] M. Aspelmeyer, H. R. BÖhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther and A. Zeilinger, Science **301**, 5633 (2003).

[18] M. Lanzagorta, Underwater Communications, New York: Morgan & Claypool Publishers, 44 (2012).

[19] F. Zhou, H. L. Yong, D. D. Li, J. Yin, J. G. Ren and C. Z. Peng, Acta Physica Sinica **63**, 140303 (2014). (in Chinese)

[20] K. H. Zhao, X. H. Zhong, Optics, Beijing: Peking University Press, 248 (1984). (in Chinese)

[21] N. G. Jerlov, Marine Optics, Second Edition, Holand: Elsevier Science, 7 (1976).

[22] H. K. Lo, X. F. Ma and K. Chen, Physical Review Letters **94**, 230504 (2005).

[23] X. F. Ma, B. Qi, Y. Zhao and H. K. Lo, Physics Letters A **72**, 012326 (2005).

[24] Q. Wang, X. B. Wang and G. C. Guo, Physics Letters A **75**, 012312 (2007).