

泡沫覆盖不规则海面的空-水量子密钥分发

王澍**, 周媛媛*, 周学军***, 张政, 陈霄

海军工程大学电子工程学院, 湖北 武汉 430033

摘要 基于光子量子特性, 综合考虑泡沫粒径分布、散射系数、泡沫层厚度及入射角、风速的影响, 建立了一种泡沫-不规则海面的复合模型。给出了空-水量子密钥分发(QKD)系统的误码率公式, 结合蒙特卡罗算法模拟研究了各参量对光子偏振量子态、QKD 误码率及传输距离的影响, 分析了泡沫-不规则海面下 4 强度 BB84 空-水 QKD 系统的性能。研究表明, 偏振误码率随泡沫层厚度、散射系数、光源入射角的增大而增大; 风速增大导致空-水 QKD 系统的量子误码率增大, 安全传输距离减小; 随着泡沫层厚度的增大, 空-水 QKD 系统的密钥生成率和安全传输距离减小。当泡沫层厚度增至 6 cm 并考虑最大偏振误码率时, 最大安全距离由 144 m 降至 101.3 m, 但仍满足水下航行器 100 m 的安全潜深要求。

关键词 量子光学; 量子密钥分发; 泡沫-不规则海面; 空-水信道; Mie 散射; 蒙特卡罗; 误码率

中图分类号 O431.2

文献标识码 A

doi: 10.3788/AOS201838.1027002

Air-Water Quantum Key Distribution on Irregular Sea Surface Covered with Foams

Wang Lian**, Zhou Yuanyuan*, Zhou Xuejun***, Zhang Zheng, Chen Xiao

Department of Electric Engineering, Naval University of Engineering, Wuhan, Hubei 430033, China

Abstract A foam-irregular-sea-surface hybrid model is established based on the quantum properties of photons and with the consideration of the influences of the foam particle size distribution, scattering coefficient, foam layer thickness, incident angle and wind speed. The error rate formula for an air-water quantum key distribution (QKD) system is obtained. Combining with the Monte Carlo algorithm, the influence of each parameter on the photon polarization state, QKD error rate and transmission distance is simulated and discussed. The performance of the four-intensity BB84 air-water QKD system under the foam-irregular-sea-surface is analyzed. The research results show that, the polarization error rate increases with the increase of the foam layer thickness, scattering coefficient and light incident angle. Besides, the increase of wind speed leads to the rise of the quantum bit error rate of the air-water QKD system and the reduction of the secure transmission distance. Meanwhile, the key generation rate and the secure transmission distance of the air-water QKD system decrease as the foam layer thickness increases, and the maximum secure distance is reduced from 144 m to 101.3 m when the foam layer thickness increases to 6 cm and the maximum polarization error rate is considered, but it still satisfies the requirement of the 100 m safety depth for the underwater vehicles.

Key words quantum optics; quantum key distribution; foam-irregular-sea-surface; air-water channel; Mie scattering; Monte Carlo; error rate

OCIS codes 270.5565; 270.5568; 010.4450

1 引 言

量子密钥分发^[1](QKD)基于量子力学的基本原理, 具有经典密码学无法企及的无条件安全性。随着水下通信需求的日益突显, 在卫星或机载平台(空)与水下航行器(水)之间建立大容量、远距离、大

潜深、高速率、双向通、实时通和完美安全的通信链路成为亟待解决的问题。Lanzagorta^[2]提出了在空-水之间建立经典激光和量子两条信道的方案, 前者用来实现大容量、即时的双向信息传输, 后者用来实现 QKD, 以保障经典激光通信完美安全。Lanzagorta 等^[2-3]理论验证了在水下信道实施 QKD

收稿日期: 2018-03-15; 修回日期: 2018-05-02; 录用日期: 2018-05-16

基金项目: 国家自然科学基金(61302099)

* E-mail: yzhou516@163.com; ** E-mail: 15623529329@163.com; *** E-mail: Liuzh531@163.com

的可行性。赵士成等^[4-5]分析了水下量子通信的误码率和安全传输距离。金贤敏等实现了全球首个水下量子通信实验^[6],发现光子偏振量子态在高散射和高损耗的海水中仍可保持良好的量子特性,为空-水 QKD 的进一步研究提供了有力依据。

然而,关于空-水信道中最为复杂的空-水界面(海面)对 QKD 性能的影响研究鲜有报道。目前针对空-水界面的光通信研究主要以经典激光为对象,主要关注于海面电磁散射、光功率衰减、辐射传输等方面^[7-9],未深入到光量子的范畴。周飞等^[10]在海面光滑平静的假设条件下,对不同介质间的 QKD 性能进行了分析,但实际海面每时每刻都在发生变化,不仅存在高低不等、长短不齐的不规则波动,还会出现泡沫覆盖在海面的情况。Xu 等^[11-12]分析了不规则海面和海面泡沫粒子对 QKD 系统误码率的影响,但未将两者结合起来建立统一模型, QKD 的性能分析也不够充分。

本文将海面覆盖的离散泡沫粒子的体散射与实际不规则海面的折射作用相结合,综合考虑泡沫粒子粒径分布、散射系数、泡沫层厚度、光源入射角及海洋风速等因素的影响,运用 Mie 理论、改进的体积散射函数及菲涅耳定理,建立了一种泡沫-不规则海面的体-面复合模型。基于此复合模型,通过蒙特卡罗算法,对传输光子偏振变化和 4 强度诱骗态 BB84 空-水 QKD 系统进行了数值仿真和性能分析。

2 泡沫-不规则海面的复合模型与分析

在空-水 QKD 的下行链路中,光信号从大气入射到海水中,必须穿越空-水界面(海面)。但实际海面受潮汐、风暴潮、海啸及海浪的影响总在不规则变化。潮汐、风暴潮和海浪产生的波长远大于 QKD 光信号的波长,故可忽略其影响;海浪主要由海风引起,且在一定风速作用下破碎波会产生泡沫层,因此风速是影响空-水 QKD 性能的一个重要参量。为分析空-水 QKD 下行信道的传输特性,必须先建立统一的空-水界面模型。

如图 1 所示,假设初始入射光的入射角为 θ_0 ,垂直水面的坐标轴为 z 轴,入射光子与泡沫层(厚度为 d)的泡沫粒子发生一次或多次碰撞,发生散射、吸收、移动,存活下来的光子再穿过不规则海面,发生反射和折射作用后射入海水中,最终由 QKD 系统探测接收。海面泡沫主要由水汽泡组成,因此将泡沫粒子等效为外层水膜、内层空气核的球形分层模型,如图 2 所示,其中 a 为内半径, b 为外半径,

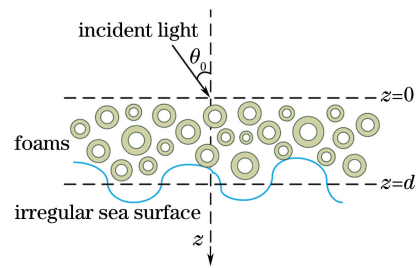


图 1 泡沫-不规则海面的复合模型

Fig. 1 Foam-irregular-sea-surface hybrid model

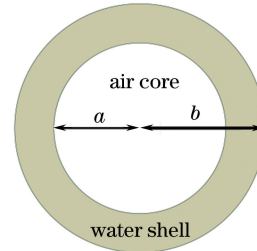


图 2 泡沫粒子结构

Fig. 2 Structure of foam particle

其粒径分布满足伽玛分布^[13]。

2.1 泡沫粒子的 Mie 散射分析

海面泡沫粒子的尺寸远大于入射光波长,因此运用 Mie 散射理论^[14]对球形分层的泡沫粒子进行散射特性分析。空-水 QKD 常用光子偏振态进行编码,故采用斯托克斯(Stokes)矢量来表示光子的偏振信息。当入射光子与泡沫粒子碰撞产生散射时,光子的偏振态、传播方向及振幅相位都会发生变化,也会影响不规则海面的入射角度,因此需得到光子经泡沫-不规则海面散射后的 Stokes 矢量,以分析实际海面对空-水 QKD 性能的影响。

根据以往的观测和实验结果^[15-16]可知,海面泡沫粒子的数量分布与海洋风速有关,单位体积内的粒子数 n_0 可表示为

$$n_0 = \frac{f_s}{4\pi b^3/3}, \quad (1)$$

式中 f_s 为体积占空比,其表达式为

$$f_s = \frac{0.01\exp(0.06U_{19.5}) - 0.011}{d}, \quad U_{19.5} > 2 \text{ m} \cdot \text{s}^{-1}, \quad (2)$$

式中 $U_{19.5}$ 为距离海面 19.5 m 处的风速。粒子数与粒径分布共同影响泡沫粒子的散射系数和衰减系数。

入射光经泡沫粒子单次散射后,光子态可表示为 $S' = MS$, 其中 $S = (I, Q, U, V)^T$ (I 为总光强, Q 为线偏振光水平分量与垂直分量间的差值, U 为线偏振光 45° 分量与 135° 分量的差值, V 为圆偏振光左旋和右旋的差值, T 代表求转置)为散射前的光子

态; \mathbf{M} 为穆勒 (Mueller) 矩阵, 表示粒子的散射作用。 \mathbf{M} 中的各元素可由散射振幅函数 S_1 、 S_2 求出, S_1 和 S_2 是关于散射角 θ 的函数, 其表达式为

$$\begin{aligned} S_1(\theta) &= \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)} (a_n \pi_n + b_n \tau_n), \\ S_2(\theta) &= \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)} (a_n \tau_n + b_n \pi_n), \end{aligned} \quad (3)$$

式中 n 表示第 n 次散射, 参量 π_n 、 τ_n 的表达式分别为

$$\pi_n = \frac{dP_n \cos \theta}{d \cos \theta}, \quad \tau_n = \frac{dP_n^{(1)} \cos \theta}{\theta}, \quad (4)$$

式中 $P_n \cos \theta$ 为第一类 Legendre 函数, $P_n^{(1)} \cos \theta$ 为一阶 n 次连带 Legendre 函数; a_n 和 b_n 分别为该空心分层泡沫粒子的 Mie 散射系数, 其表达式为

$$a_n = \frac{[\sigma j_n(\sigma)]' [j_n(\zeta) + B_n(\zeta, \chi) y_n(\zeta)] - \{[\zeta j_n(\zeta)]' + B_n(\zeta, \chi) [\zeta y_n(\zeta)]'\} j_n(\sigma)}{[\sigma h_n(\sigma)]' [j_n(\zeta) + B_n(\zeta, \chi) y_n(\zeta)] - \{[\zeta j_n(\zeta)]' + B_n(\zeta, \chi) [\zeta y_n(\zeta)]'\} h_n(\sigma)}, \quad (5)$$

$$b_n = \frac{[\sigma j_n(\sigma)]' \zeta [j_n(\zeta) + A_n(\zeta, \chi) y_n(\zeta)] - \{[\zeta j_n(\zeta)]' + A_n(\zeta, \chi) [\zeta y_n(\zeta)]'\} \sigma^2 j_n(\sigma)}{[\sigma h_n(\sigma)]' \zeta^2 [j_n(\zeta) + B_n(\zeta, \chi) y_n(\zeta)] - \{[\zeta j_n(\zeta)]' + B_n(\zeta, \chi) [\zeta y_n(\zeta)]'\} h_n(\sigma)}, \quad (6)$$

式中 $A_n(\zeta, \chi)$ 、 $B_n(\zeta, \chi)$ 已由文献[17-18]给出; 参量 $\sigma = k'b$ 、 $\zeta = k_b b$ 、 $\chi = k_a a$ 、 k' 为介质波数, k_b 和 k_a 分别为壳、核的波数; $y_n(\zeta)$ 为 Neumann 函数; $j_n(\sigma)$ 和 $h_n(\sigma)$ 分别为第一类 Bessel 球函数和半整数阶第二类 Hankel 函数。

若要获得光子散射后的偏振信息即 Stokes 矢量, 必须先确定其散射角。 散射角可由体积散射函数求出, 常用于水中光传输研究的 Mie 体积散射函数有 Henyey-Greenstein (HG) 函数^[19] 和 Fournier-Forand (FF) 函数^[20], 但前者不能获得不对称因子 g , 后者不能得到反函数解析解。 为克服上述缺陷, 采用修正 HG 函数和 FF 函数结合的方法来确定散射角, 即利用修正 HG 函数得到散射角表达式, 由 FF 函数积分归一化获得不对称因子 g 。

泡沫粒子的体积散射函数由修正 HG 函数表示, 再求解其反函数, 可得散射角为

$$\theta = \begin{cases} \arccos \left\{ \frac{1}{2g} \left[(1+g^2) - \frac{(1-g^2)^2}{(1-g+2g\omega_1)^2} \right] \right\}, & 0 < \theta \leq \frac{\pi}{2} \\ \arccos \left\{ \frac{1}{2g} \left[\frac{(1-g^2)^2}{(1-g+2g\omega_1)^2} - (1+g^2) \right] \right\}, & \frac{\pi}{2} < \theta \leq \pi \end{cases} \quad (7)$$

式中随机数 $\omega_1 \in [0, 1]$ 服从均匀分布, 不对称因子 g 由 FF 函数计算得出:

$$g = \frac{\int_0^\pi F(\theta) \cos \theta d\theta}{\int_0^\pi F(\theta) d\theta}, \quad (8)$$

式中 $F(\theta)$ 为 FF 函数, 其表达式为

$$F(\theta) = \frac{1}{4\pi(1-\delta)^2\delta^v} \times \left\{ v(1-\delta) - (1-\delta^v) + \frac{4}{u^2} [\delta(1-\delta^v) - v(1-\delta)] \right\} - \frac{1-\delta_\pi^v}{16\pi(1-\delta_\pi)^2\delta_\pi^v} (3\cos^2\theta - 1), \quad (9)$$

式中 $v = \frac{3-\epsilon}{2}$ 、 $\delta = \frac{u^2}{3(n'-1)^2}$ 、 $\delta_\pi = \frac{4}{3(n'-1)^2}$ 、 $u = 2\sin\left(\frac{\theta}{2}\right)$; ϵ 为散射体尺度分布的特征参数; n' 为散射体与周围介质的相对折射率。

2.2 泡沫-不规则海面的传输性能分析

假设光束初始入射角为 θ_0 , 方向角为 ϕ_0 , 入射点为 o , 建立三维坐标系 $oxyz$, 如图 3 所示, 光束经过泡沫粒子的 m 次散射后, 穿过泡沫层到达不规则海面。 光子最终到达不规则海面时对应的 Stokes 矢量为

$$\mathbf{S}_m = \mathbf{R}(\gamma_m)\mathbf{M}(\theta_m)\mathbf{R}(\phi_m)\cdots\mathbf{R}(\gamma_1)\mathbf{M}(\theta_1)\mathbf{R}(\phi_1)\mathbf{R}(\phi_0)\mathbf{S}, \quad (10)$$

式中 $\mathbf{R}(\gamma_i)$ 和 $\mathbf{R}(\phi_i)$ ($i=1, \dots, m$) 分别为关于角度 γ_i 或 ϕ_i 的旋转矩阵, γ_i 为 Stokes 矢量从第 i 次的

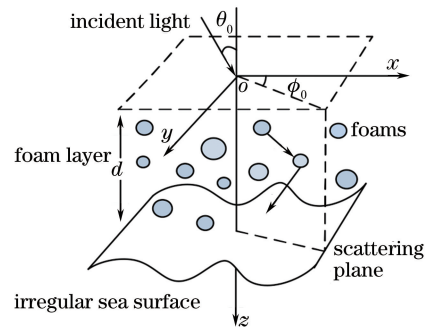


图 3 泡沫-不规则海面的光束传输示意图
Fig. 3 Schematic of beam transmission on foam-irregular-sea-surface

散射平面旋转回 xoz 面的夹角, ϕ_i 为第 i 次散射的方向角, θ_i 为第 i 次散射角。

经过整个泡沫层的 m 次散射后, 光子偏振变化的偏转角为

$$\phi_m = \arccos \left[\frac{\mathbf{S}_m \cdot \mathbf{S}_0}{|\mathbf{S}_m| |\mathbf{S}_0|} \right], \quad (11)$$

式中 $\mathbf{S}_0 = \mathbf{R}(\phi_0)\mathbf{S}$ 。光子在最后一次散射后的传输方向为 $\mathbf{D}_m = (u_{x_m}, u_{y_m}, u_{z_m})^T$, 其中

$$\begin{cases} u_{x_m} = \sin \theta_m \cos \phi_m \\ u_{y_m} = \sin \theta_m \sin \phi_m, \quad |u_{z_{m-1}}| \leq 0.9999 \\ u_{z_m} = \frac{u_{z_{m-1}}}{|u_{z_{m-1}}|} \cos \phi_m \end{cases}, \quad (12)$$

$$\begin{cases} u_{x_m} = \frac{\sin \theta_m (u_{x_{m-1}} u_{z_{m-1}} \cos \phi_m - u_{y_{m-1}} \sin \phi_m)}{\sqrt{1 - u_{z_{m-1}}^2}} + u_{x_{m-1}} \cos \theta_m \\ u_{y_m} = \frac{\sin \theta_m (u_{y_{m-1}} u_{z_{m-1}} \cos \phi_m + u_{x_{m-1}} \sin \phi_m)}{\sqrt{1 - u_{z_{m-1}}^2}} + u_{y_{m-1}} \cos \theta_m, \quad |u_{z_{m-1}}| > 0.9999 \\ u_{z_m} = -\sin \theta_m \cos \phi_m \sqrt{1 - u_{z_{m-1}}^2} + u_{z_{m-1}} \cos \theta_m \end{cases}, \quad (13)$$

式中 $\mathbf{D}_{m-1} = (u_{x_{m-1}}, u_{y_{m-1}}, u_{z_{m-1}})^T$ 为此次散射前光子的运动方向。

因此, 光子穿过泡沫层后, 射入不规则海面的入射角为

$$\alpha_0 = \arccos \left(\frac{\mathbf{D}_m \cdot \mathbf{Z}}{|\mathbf{D}_m| |\mathbf{Z}|} \right), \quad (14)$$

式中 $\mathbf{Z} = (0, 0, 1)^T$ 。

此外, 海面受海风吹动形成海浪, 呈现出不规则的空-水界面, 这势必会引起界面法线的偏离, 改变入射光的传播方向。如图 4 所示, α_0 为入射光经泡沫层后到达平静海面的入射角, α_1 、 α_2 分别为不规则海面的实际入射角和折射角, β 为不规则海面引起的法线偏离角, 即法线方向与 z 轴的夹角, 称为

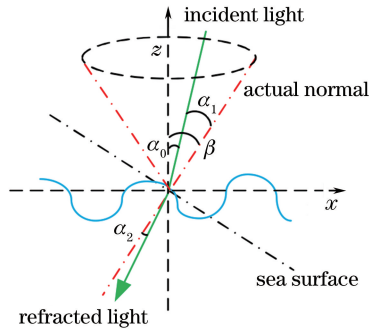


图 4 不规则海面的光束传输示意图

Fig. 4 Schematic of beam transmission on irregular sea surface

俯仰角, 且有 $\alpha_0, \alpha_1, \alpha_2, \beta \in [0, \pi/2)$ 。假设反射光束已超出水下探测器的统计分布范围, 未予以考虑。

根据 Cox 和 Munk 提出的一定风速下海面法线俯仰角的经验归一化概率密度公式^[21], 有

$$p(\beta) = \frac{2}{\kappa^2} \exp(-\tan^2 \beta / \sigma^2) \tan \beta \sec^2 \beta, \quad (15)$$

式中 $\kappa^2 = 0.003 + 0.00512U$, U 为风速 (m/s)。对概率密度进行采样, 可得相应的俯仰角为

$$\beta = \tan^{-1} (\sqrt{-\sigma^2 \ln \xi}), \quad (16)$$

式中随机数 $\xi \in (0, 1]$ 。

不规则海面的实际入射角 $\alpha_1 = |\alpha_0 \pm \beta|$, 再根据折射定理^[22]求得折射角 α_2 为

$$\alpha_2 = \arcsin(n_1 \sin \alpha_1 / n_2), \quad (17)$$

式中 n_1 、 n_2 分别为大气和海水的折射率。

若初始入射光束为线偏振光, 则穿过整个泡沫-不规则海面的透射光束仍为线偏振光。由菲涅耳公式可求出一定入射角下反射和透射的振幅、强度、振动取向等, 结合折射定理可得不规则海面的透射率为

$$T_1 = \frac{1}{2} \left| \frac{\sin 2\alpha_1 \sin 2\alpha_2}{\sin^2(\alpha_1 + \alpha_2)} \times \frac{1 + \cos^2(\alpha_1 - \alpha_2)}{\cos^2(\alpha_1 - \alpha_2)} \right|. \quad (18)$$

海面泡沫的存在也会对空-水界面的透射率产生影响, 透射率与风速 U 也有关, 两者关系为

$$T_2 = \begin{cases} 1 - 1.2 \times 10^{-7} \times U^{3.3}, & U \leq 9 \text{ m} \cdot \text{s}^{-1} \\ 1 - 1.2 \times 10^{-7} \times U^{3.3} \times (0.225U - 0.99), & U \geq 9 \text{ m} \cdot \text{s}^{-1} \end{cases}. \quad (19)$$

因此, 泡沫-不规则海面的总透射率为

$$T = T_1 T_2. \quad (20)$$

入射光穿过泡沫-不规则海面后, 其偏振态的改变也会影响空-水 QKD 的性能。以 BB84 协议作为

空-水 QKD 方案,并设其相应的四个基矢态为 $|p\rangle$, $|s\rangle$, $(|p\rangle + |s\rangle)/\sqrt{2}$ 和 $(|p\rangle - |s\rangle)/\sqrt{2}$ 。由(11)式可知,光束射入泡沫层,在与泡沫粒子发生散射后光子基矢的偏振态最终发生 φ_m 角度的偏转。该光束到达不规则海面后,由于其界面折射光路不存在相位变化,故光子态 $c_1|p\rangle + c_2|s\rangle$ (c_1, c_2 为复数)在经不规则海面透射后变为 $c_1 t_p |p\rangle + c_2 t_s |s\rangle$,其中 t_p 和 t_s 分别为光束 p 分量(水平分量)和 s 分量(垂直分量)的振幅透射率,这显然也造成了光子偏振态的改变。由此可知,光子穿过泡沫-不规则海面的整个过程中,其偏振态的最终偏转角可表示为

$$\varphi' = \begin{cases} \left| \arctan \frac{t_p}{t_s} - \varphi_m \right|, & |p\rangle \text{ or } |s\rangle \\ \left| \arctan \frac{t_p}{t_s} - \frac{\pi}{4} - \varphi_m \right|, & \frac{|p\rangle + |s\rangle}{\sqrt{2}} \text{ or } \frac{|p\rangle - |s\rangle}{\sqrt{2}} \end{cases}, \quad (21)$$

式中 t_p, t_s 由菲涅耳公式求得:

$$t_p = \frac{2 \sin \alpha_2 \cos \alpha_1}{\sin(\alpha_1 + \alpha_2) \cos(\alpha_1 - \alpha_2)}, \quad (22)$$

$$t_s = \frac{2 \sin \alpha_2 \cos \alpha_1}{\sin(\alpha_1 + \alpha_2)}. \quad (23)$$

光子在通过检偏器进行测量时,其偏振态改变可能会引发错误检测,将此误码率视为偏振误码率 e_p ,主要用来衡量光子偏振变化对 QKD 系统的影响,其与偏转角度 φ' 有关^[23],表示为

$$e_p = \sin^2 \varphi'. \quad (24)$$

综上所述,入射光穿过泡沫-不规则海面后,其偏振态会发生改变,导致误码率增大。退偏比可直观描述光子偏振态的变化,保真度可度量量子态的相似程度,因此从这两个方面分析光子偏振态的变化情况。

3 基于泡沫-不规则海面的空-水 QKD 分析

为获得更好的系统性能,采用 4 强度诱骗态 BB84 QKD 方案进行空-水信道的密钥分发。在此方案中,发送端 Alice 具有 4 个不同强度的光源,其中 ρ_0 (真空态)、 ρ_x, ρ_y 用于制备诱骗态脉冲, ρ_z 用于制备信号态脉冲。 $\rho_l = \sum_k f_k^l |k\rangle \langle k|$ ($l = x, y, z$),其中 f_k^l 为对应的光子数分布, $|k\rangle$ 为 k -光子态。

当 Alice 发射脉冲 ρ_l 时,空-水 QKD 系统的总计数率和误码表示为

$$S_l = \sum_{k \geq 0} f_k^l Y_k, \quad l = x, y, z, \quad (25)$$

$$T_l = E_l S_l = \sum_{k \geq 0} f_k^l t_k, \quad l = x, y, z, \quad (26)$$

式中 Y_k 为 k -光子 (k 为光子数)的计数率; E_l 为系统量子误码率(QBER); k -光子的误码数 $t_k = e_k Y_k$, e_k 为 k -光子对应的误码率。

不同于光纤信道,空-水信道 QKD 的误码率与环境背景光噪声、散射噪声、热噪声、探测器暗计数、接收孔径及视场等有关。根据文献[2],基于泡沫-不规则海面的复合模型,可得空-水 QKD 系统的 QBER 计算公式为

$$E_\mu = \frac{e_p \frac{\mu \eta}{4 \Delta t} \exp(-\chi_c L) + I_{dc} + \frac{R_d(\lambda) A \Delta t' \lambda \Delta \lambda \Omega}{4 h c \Delta t}}{\frac{\mu \eta}{2 \Delta t} \exp(-\chi_c L) + 2 I_{dc} + \frac{R_d(\lambda) A \Delta t' \lambda \Delta \lambda \Omega}{2 h c \Delta t}}, \quad (27)$$

式中传输信道和接收端探测器的全局传输效率 $\eta = T T_{AB} \eta_B$,其中 η_B 为接收端探测效率; $T_{AB} = \exp(-\chi_c L)$ 为海水信道的传输损耗(透射率),其中 χ_c 为衰减系数, L 为传输距离; μ 为平均光强; I_{dc} 为探测器暗计数; Ω 为探测器视场; $R_d(\lambda)$ 为环境辐照度; A 为接收孔径面积; $\Delta t'$ 为接收机选通时间; $\Delta \lambda$ 为谱线宽度; h 为普朗克常数; c 为真空光速; Δt 为光脉冲周期。

由参考文献[24]可知,空-水 QKD 系统的单光子计数率 Y_1 下界的通用公式为

$$Y_1 = \frac{f_2^y S_x - f_2^x S_y + (f_2^x f_0^y - f_2^y f_0^x) Y_0}{f_1^x f_2^y - f_1^y f_2^x}. \quad (28)$$

为简化运算,定义参量

$$G(i, j, k) = (g_i^x - g_j^x)(g_j^y - g_k^y) - (g_i^y - g_j^y)(g_j^x - g_k^x), \quad (29)$$

式中

$$g_m^l = \frac{f_m^l}{f_m^z}, \quad (m \geq 1, l = x, y, z, f = a, b, c). \quad (30)$$

易证明,若 $k - j \geq j - i \geq 0$,有

$$G(i, j, k) \geq 0. \quad (31)$$

在以往的 e_1 估计中,将所有误码都归结于单光子脉冲,由此得到一个粗略的 e_1 上界。所提方案利用 4 个不同强度脉冲来联合估计出更精确的 e_1 上界^[24],以提高空-水 QKD 系统的密钥生成率。

利用(26)式消除变量可得

$$t_1 = \bar{t}_1 + \sum_{k \geq 4} h_{t_1}(k) t_k, \quad (32)$$

式中 \bar{t}_1 为 t_1 的上界, $h_{t_1}(k)$ 为简化运算定义的参

量,其表达式分别为

$$\bar{t}_1 = \frac{(f_2^y f_3^z - f_2^z f_3^y)T_x - (f_2^x f_3^z - f_2^z f_3^x)T_y}{f_1^z f_2^z f_3^z G(1,2,3)} + \frac{(f_2^x f_3^y - f_2^y f_3^x)T_z + (f_2^x f_3^z - f_2^z f_3^x)f_0^y Y_0 e_0}{f_1^z f_2^z f_3^z G(1,2,3)} + \frac{(f_2^x f_3^y - f_2^y f_3^x)f_0^x + (f_2^x f_3^z - f_2^z f_3^x)Y_0 e_0}{f_1^z f_2^z f_3^z G(1,2,3)} Y_0 e_0, \quad (33)$$

$$h_{t_1}(k) = -\frac{G(2,3,k)}{G(1,2,3)}, \quad k \geq 4 \quad (34)$$

结合(31)式可知,只要 $k \geq 4$,则有 $h_{t_1}(k) \leq 0$ 。

(33)式即为 t_1 的上界,故 e_1 的上界为

$$\bar{e}_1 = \frac{\bar{t}_1}{\underline{Y}_1}, \quad (35)$$

式中 \underline{Y}_1 为 Y_1 的下界。

空-水 QKD 系统的最终密钥生成率为

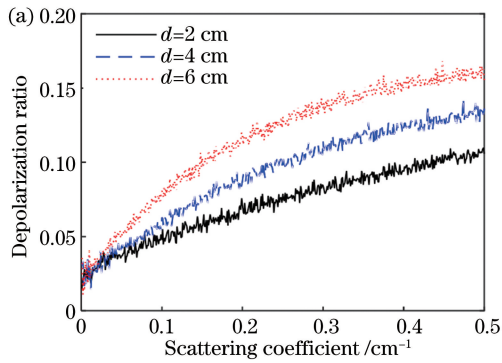
$$R \geq a_1^z \underline{Y}_1 [1 - H(\bar{e}_1)] - S^z f' H(E^z), \quad (36)$$

式中 S^z 和 E^z 为 Alice 端选择 z 态时对应的系统总计数率和误码率, f' 为实际纠错算法效率, $H_2(x) = -x \text{lb}(x) - (1-x) \text{lb}(1-x)$ 为二进制香农熵函数。

4 仿真结果与分析

海面泡沫粒子的粒径、位置分布、方向及海面不规则性都是随机的,使得光子散射和运动方向不确定,因此采用蒙特卡罗算法^[25]对光子穿越泡沫-不规则海面的密钥分发过程进行模拟;并通过数值仿真,比较分析了不同参数的实际海面对光子偏振态的影响,光源入射角与误码率之间的关系以及不同条件下泡沫-不规则海面对空-水 QKD 系统性能的影响。

这里侧重于建立泡沫-不规则海面的复合模型



并分析其对 QKD 性能的影响,未考虑大气信道的传输,主要对空-水界面及水下部分的 QKD 进行仿真分析。主要实验参数^[2,26]见表 1,泡沫粒子的平均外半径取为 $250 \mu\text{m}$,水膜平均厚度为 $20 \mu\text{m}$,采用 Jerlov I 型水体,并最优化信号态强度。

表 1 主要仿真参数

Table 1 Main simulation parameters

Parameter	Value	Parameter	Value
ϕ	10°	Ω	$2\pi(1 - \cos \phi)$
λ / nm	480	$\Delta\lambda / \text{nm}$	0.12
$\Delta t / \text{ns}$	35	$\Delta t' / \text{ps}$	200
A / cm^2	30	η_B	0.3
I_{dc} / Hz	60	χ_c / m^{-1}	0.03

光源垂直射入泡沫-不规则海面时,水平线偏振光和 45° 线偏振光在不同泡沫层厚度 ($d = 2, 4, 6 \text{ cm}$) 条件下到达海面光子的退偏比和保真度与海面散射系数之间的关系分别如图 5、6 所示。可以看出,无论发射哪种线偏振光,海面泡沫层厚度或散射系数的增大均会导致光子退偏比的增大和保真度的减小。以水平线偏振光为例,在散射系数为 0.5 cm^{-1} 、泡沫层厚度由 2 cm 增至 6 cm 时,光子退偏比 $R' \leq 0.11$ 变为 $R' \leq 0.16$,保真度 $F' \geq 97.6\%$ 变为 $F' \geq 95.8\%$,这将引入偏振误码率。主要原因一方面是散射系数的增大使光子在一定厚度的泡沫层内的随机移动步长减小;另一方面是海面泡沫层厚度增加。这两个因素都会增大光子与泡沫粒子的碰撞机率,使散射次数增多。球形粒子的单次散射虽不产生退偏,但其多重散射容易产生退偏现象,因此散射次数的增多会增大光子退偏程度,减小保真度。此外,散射系数与泡沫粒子的粒径和数量分布相关,光子偏振态的变化会受这两个因素的影响。两种线偏振光的偏振变化范围相近,说明两者引起

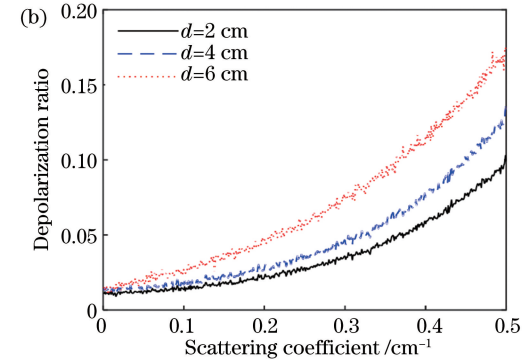


图 5 不同泡沫层厚度下光子退偏比与散射系数的关系曲线。(a)水平线偏振;(b) 45° 线偏振

Fig. 5 Photon depolarization ratio versus scattering coefficient under different foam layer thicknesses.

(a) Horizontal linear polarization; (b) 45° linear polarization

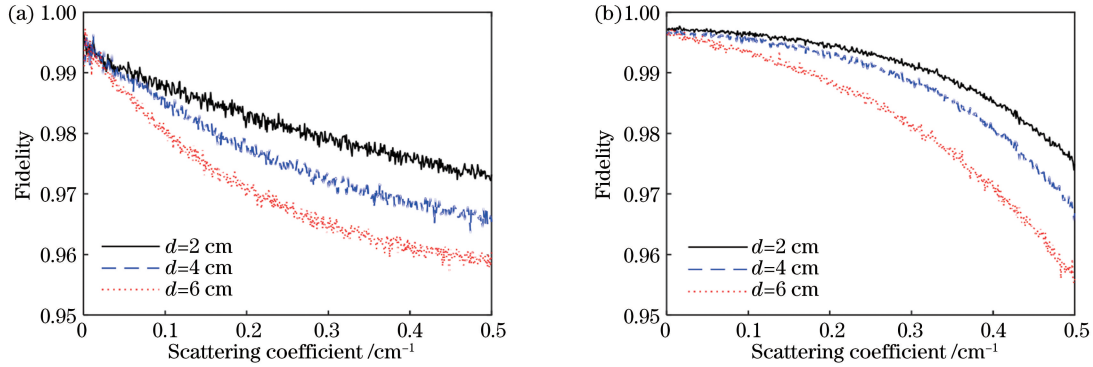


图 6 不同泡沫层厚度下光子保真度与散射系数的关系曲线。(a)水平线偏振;(b) 45°线偏振
Fig. 6 Photon fidelity versus scattering coefficient under different foam layer thicknesses.

(a) Horizontal linear polarization; (b) 45° linear polarization

的偏振误差率大小相近,因此可随机选择偏振基矢态进行量子密钥的编码传输。

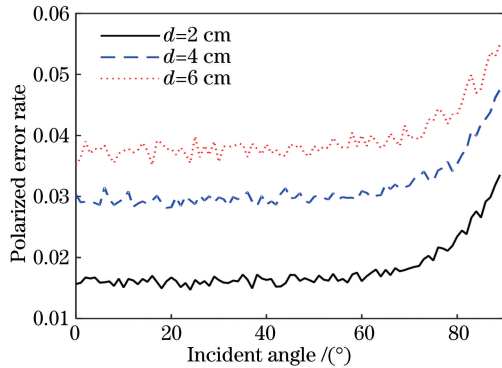


图 7 不同泡沫层厚度下偏振误差率与入射角间的关系
Fig. 7 Polarization error rate versus incident angle under different foam layer thicknesses

图 7 所示为光源以不同角度射入泡沫-不规则海面时,在不同泡沫层厚度条件下光束穿过海面复合模型所引起的偏振误差率与入射角间的关系。可以看出,海面泡沫层厚度的增大会导致偏振误差率的增大。这是因为光子穿越泡沫-不规则海面时,泡沫层厚度的增大使光子散射次数增多,增大了光子偏振态的变化,也就增大了击中错误检测器的概率,使误码率增大。入射角增大也会导致偏振误差率的增大,在入射角小于 50°时,偏振误差率波动不大;在入射角超过 50°后,偏振误差率随入射角的增大急速增大。这是由于光子碰撞大部分发生的是前向小角度散射,根据文献[10]的分析可知,入射角较大时误码率才开始较快地增大,因此在入射角大于 50°时,由不规则海面引入的误码率才会急剧增大。

图 8 所示为光源垂直入射时,在不同风速(0 m/s,无风;5 m/s,微风;10 m/s,劲风;20 m/s,大风;40 m/s,暴风)条件下量子误码率与传输距离

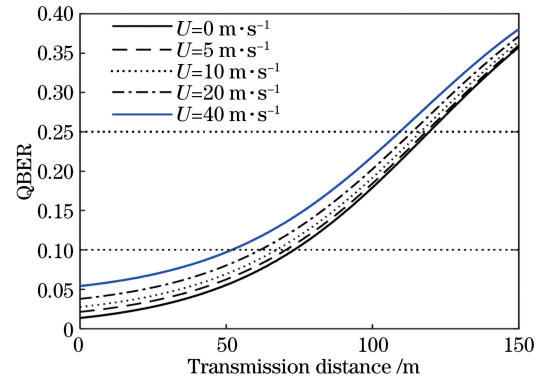


图 8 不同风速下 QBER 与传输距离间的关系
Fig. 8 QBER versus transmission distance under different wind speeds

的关系。信号态的平均光强取 0.1。可以看出,海洋风速会影响量子密钥传输的安全距离和量子误码率,且最大安全传输距离随着风速的增大而减小。这是因为风速增大使泡沫-不规则海面所含的泡沫粒子增多,散射系数和随机起伏程度增大,导致散射次数和实际法线偏离的角度增大,这不仅会增大偏振误差率,也会减小整个界面的透射率,影响空-水 QKD 的传输性能。若只考虑简单的截听-重发攻击即最低安全界限 $f_{\text{QBER}} = 0.25$,当风速从 0 m/s 增至 40 m/s 时,最大安全距离从 118 m 减小为 107.8 m。若考虑各类复杂强大的攻击即最高安全界限 $f_{\text{QBER}} = 0.1$,相应的最大安全距离由 73.4 m 减小至 52 m。由于潜艇和 underwater 航行器的安全潜深为 100 m,故此时可采用拖拽浮标等辅助手段来实现空-水 QKD。

在最优化信号态强度并考虑由泡沫-不规则海面引起的最大偏振误差率条件下,不同泡沫层厚度下密钥生成率与传输距离之间的关系如图 9 所示。可以看出,海面泡沫层厚度的增大不仅导致 QKD 的安全传输距离减小,而且会造成系统的密钥生成

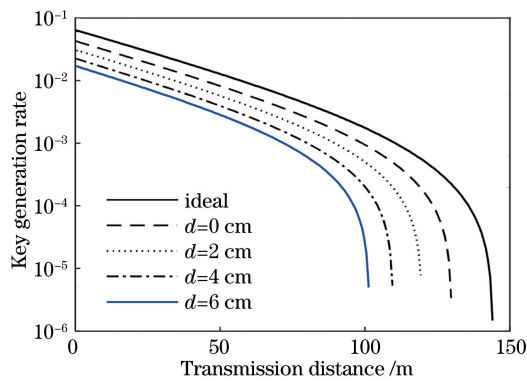


图9 不同泡沫层厚度下密钥生成率与传输距离间的关系
Fig. 9 Key generation rate versus transmission distance under different foam layer thicknesses

率减小。这是因为随着泡沫层厚度的增大,泡沫粒子和散射次数增多,加大了光子偏振态的变化程度,降低了光子击中正确检测器的概率。泡沫对光子也有一定吸收作用,虽其影响不如散射作用明显,但也会减小光子的接收数量。光子传输过程中海水衰减也会造成误码率的增大。在不考虑泡沫-不规则海面的影响即理想情况下,QKD系统的最大安全距离约为144 m;在无泡沫但海面不规则情况($d=0$ cm)下,最大安全距离为129.8 m;在泡沫层厚度为6 cm的情况下,最大安全距离可达101.3 m,仍满足水下航行器100 m的安全潜深要求。这说明基于空-水信道的QKD具有一定的可行性。

5 结 论

针对实际泡沫覆盖的随机波动的不规则海面,综合考虑泡沫粒径分布、散射系数、泡沫层厚度、入射角及海洋风速的影响,从光量子角度,运用Mie理论、修正HG与FF函数结合的方法及菲涅耳定理,建立了一种适用于空-水QKD的泡沫-不规则海面的体-面复合模型。基于此模型,采用蒙特卡罗算法,研究了不同泡沫层厚度条件下泡沫-不规则海面的泡沫粒径分布和散射系数对光子偏振态的影响以及该海面引入的偏振误码率随入射角的变化关系。结合4强度BB84协议,分析了不同风速下空-水QKD系统的量子误码率与安全传输距离间的关系,研究了泡沫-不规则海面对空-水QKD系统的密钥生成率和传输距离的影响。仿真结果表明,泡沫覆盖的不规则海面改变了光子偏振态,散射系数越大,光子退偏程度越高,保真度越小,偏振误码率越大;偏振误码率也随着光源入射角和泡沫层厚度的增大而增大,且在入射角超过 50° 后急剧增大;风速会对

泡沫-不规则海面的泡沫粒径分布、散射系数、界面不规则程度及透射率造成影响,故风速增大使得空-水QKD系统的量子误码率增大,安全传输距离减小;在最大偏振误码率的条件下,随着泡沫层厚度的增大,空-水QKD系统的密钥生成率和安全传输距离逐渐减小,若不考虑泡沫-不规则海面的影响,最大安全距离约为144 m,而当泡沫层厚度增大至6 cm时,最大安全距离可达101.3 m,仍满足潜艇和 underwater 航行器100 m安全潜深的要求。这不仅验证了空-水QKD系统的理论可行性,而且对未来构建空-水一体的量子通信链路具有一定的参考价值。

参 考 文 献

- [1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [J]. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984, 560: 175-179.
- [2] Lanzagorta M. Underwater communications [M]. New York: Morgan & Claypool Publisher, 2012: 45-48.
- [3] Uhlmann J, Lanzagorta M, Venegas-Andraca S E. Quantum communications in the maritime environment[C]. MTS/IEEE Oceans Conference, 2015: 15798695.
- [4] Zhao S C, Shi P, Li W D, *et al.* Simulation and QBER analysis of underwater quantum communication[J]. Periodical of Ocean University of China, 2016, 46(2): 131-137.
赵士成, 史鹏, 李文东, 等. 水下量子通信的数值模拟及误码率分析[J]. 中国海洋大学学报, 2016, 46(2): 131-137.
- [5] Shi P, Zhao S C, Gu Y J, *et al.* Channel analysis for single photon underwater free space quantum key distribution[J]. Journal of the Optical Society of America A, 2015, 32(3): 349-356.
- [6] Ji L, Gao J, Yang A L, *et al.* Towards quantum communications in free-space seawater[J]. Optics Express, 2017, 25(17): 19795-19806.
- [7] Liang Y, Guo L X. Study of the electromagnetic scattering from the rough sea surface with bubbles/foams by the modified two-scale method[J]. Acta Physica Sinica, 2009, 58(9): 6158-6166.
梁玉, 郭立新. 气泡/泡沫覆盖粗糙海面电磁散射的修正双尺度法研究[J]. 物理学报, 2009, 58(9): 6158-6166.
- [8] Qi X, Han X E. Study about laser scattering characteristics of rough sea surface with foams[J]. Acta Optica Sinica, 2015, 35(8): 0829003.

- 元晓, 韩香娥. 覆盖泡沫粗糙海面的激光散射特性研究[J]. 光学学报, 2015, 35(8): 0829003.
- [9] Li X Z, Miao X C, Qi X, *et al.* Laser atmosphere seawater channel transmission characteristics under complicate sea conditions[J]. *Acta Optica Sinica*, 2018, 38(3): 0301002.
李祥震, 苗希彩, 元晓, 等. 复杂海况下激光大气-海水信道传输特性研究[J]. 光学学报, 2018, 38(3): 0301002.
- [10] Zhou F, Yong H L, Li D D, *et al.* Study on quantum key distribution between different media[J]. *Acta Physica Sinica*, 2014, 63(14): 140303.
周飞, 雍海林, 李东东, 等. 基于不同介质间量子密钥分发的研究[J]. 物理学报, 2014, 63(14): 140303.
- [11] Xu H B, Zhou Y Y, Zhou X J. The performance analysis of quantum key distribution based on an irregular air-water interface[C]. *IEEE International Conference on Information Management*, 2017: 358-361.
- [12] Xu H B, Zhou Y Y, Zhou X J. Effect of sea foam on polarized photons scattering[J]. *Laser & Optoelectronics Progress*, 2017, 54(12): 122901.
徐华彬, 周媛媛, 周学军. 海面泡沫对偏振光子的散射影响[J]. 激光与光电子学进展, 2017, 54(12): 122901.
- [13] Villarino R, Camps A, Vall-llossera M, *et al.* Sea foam effects on the brightness temperature at L-band[J]. *Proceedings of IEEE International Geoscience and Remote Sensing Symposium*, 2003, 5: 3076-3078.
- [14] Zhang Y L, Wang Y M, Huang A P. Influence of suspended particles in Mie theory on underwater laser transmission[J]. *Chinese Journal of Lasers*, 2018, 45(5): 0505002.
张莹璐, 王英民, 黄爱萍. 米氏理论下悬浮粒子对水下激光传输的影响[J]. 中国激光, 2018, 45(5): 0505002.
- [15] Wu J. Bubble flux and marine aerosol spectra under various wind velocities [J]. *Journal of Geophysical Research Oceans*, 1992, 97(C2): 2327-2333.
- [16] Qi X. Propagation characteristics of laser beam traversing the air-sea interface with foams [D]. Xi'an: Xidian University, 2015: 46-48.
元晓. 泡沫覆盖气-海界面的激光传输特性研究[D]. 西安: 西安电子科技大学, 2015: 46-48.
- [17] Wu Z S, Wang Y P. Electromagnetic scattering for multilayered sphere: Recursive algorithms[J]. *Radio Science*, 1991, 26(6): 1393-1401.
- [18] Tsang L, Ding K H, Zhang G, *et al.* Backscattering enhancement and clustering effects of randomly distributed dielectric cylinders overlying a dielectric half space based on Monte-Carlo simulations [J]. *IEEE Transactions on Antennas and Propagation*, 1995, 43(5): 488-499.
- [19] Wei A H, Zhao W, Han B, *et al.* Simulative study of optical pulse propagation in water based on Fournier-Forand and Henyey-Greenstein in volume scattering functions [J]. *Acta Optica Sinica*, 2013, 33(6): 0601003.
魏安海, 赵卫, 韩彪, 等. 基于 Fournier-Forand 和 Henyey-Greenstein 体积散射函数的水中光脉冲传输仿真分析[J]. 光学学报, 2013, 33(6): 0601003.
- [20] Freda W, Piskozub J. Improved method of Fournier-Forand marine phase function parameterization [J]. *Optics Express*, 2007, 15(20): 12763-12768.
- [21] Gjerstad K I, Stamnes J J, Hamre B, *et al.* Monte Carlo and discrete-ordinate simulations of irradiances in the coupled atmosphere-ocean system[J]. *Applied Optics*, 2003, 42(15): 2609-2622.
- [22] Gooch J W. *Snell's law*[M]. New York: Springer, 2011: 673-675.
- [23] Fung C H F, Qi B, Tamaki K, *et al.* Phase-remapping attack in practical quantum-key-distribution systems[J]. *Physical Review A*, 2007, 75(3): 032314.
- [24] Zhou Y H, Yu Z W, Wang X B. Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100% [J]. *Physical Review A*, 2014, 89(5): 052325.
- [25] Sun X M, Wang H H, Shen J. Study on two Monte Carlo simulation programs of polarization lidar depolarization by water cloud[J]. *Acta Optica Sinica*, 2017, 37(1): 0101002.
孙贤明, 王海华, 申晋. 两种模拟水云对偏振激光雷达退偏振的蒙特卡罗方法研究[J]. 光学学报, 2017, 37(1): 0101002.
- [26] Wang Q, Zhang C H, Wang X B. Scheme for realizing passive quantum key distribution with heralded single-photon sources [J]. *Physical Review A*, 2016, 93(3): 032312.