

УДК 517.938

## Исследование модели реализации алгоритма квантового распределения ключей в турбулентной атмосфере\*

Фалеева М. П., Попов И. Ю.

Национальный исследовательский университет ИТМО

### 1. Введение

На сегодняшний день огромный интерес представляют исследования, связанные с разработкой линий связи, в основе которых лежат квантовые свойства света [1]- [2]. Безусловным преимуществом таких линий связи является высокая степень секретности передаваемой информации. Создание же квантовых каналов в свободном пространстве позволит решить вопрос передачи квантовой информации на расстояния, сравнимые с межконтинентальными, чего не позволяют достичь оптоволоконные каналы из-за сильного затухания сигналов [3]- [5]. Однако в настоящий момент накопленный материал в области изучения влияния турбулентной атмосферы на квантовую запутанность и осуществление квантовых алгоритмов далек до возможности реализации систем глобальной квантовой коммуникации.

### 2. Основное содержание работы

Построение математической модели открытого квантового канала в турбулентной атмосфере является достаточно сложной задачей. Турбулентность определяется совокупностью различных явлений атмосферы, таких как блуждание лучей, расширение лучей, сцинтилляция и декогерентность, которые порождают различные колебания атмосферных характеристик и случайные изменения параметров распространения электромагнитных волн. Мы рассмотрим только одно из явлений, явление блуждающего луча, которое порождает отклонение в начальном направлении распространения луча. Эффект блуждающего луча характерен для атмосферы со слабой турбулентностью, где он является преобладающим [6]. Изучим влияние данного эффекта на распространение света, который генерируется источником в виде гауссова пучка и отправляется на приемник. Вследствие турбулентности, пятно луча, падающего на круглую апертуру приемника, будет смещено относительно самой апертуры, и часть света не попадет на измерительную аппаратуру. Прошедший свет будет характеризоваться коэффициентом пропускания, который является случайной величиной, что вызвано случайной природой турбулентности. Для реализации кубитов мы используем моды гауссова пучка света:

$$\Psi_{mn}(x, y, z_{ap}, k) = \sqrt{\frac{2}{\pi W^2}} \exp\left(-((x-r)^2 + y^2) \left(\frac{1}{W^2} + \frac{ik}{2R}\right) + i(1+m+n)\phi\right) H_m\left(\frac{\sqrt{2}(x-r)}{W}\right) H_n\left(\frac{\sqrt{2}y}{W}\right), \quad (1)$$

---

\*Работа выполнена при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-31-90154

которые являются решениями параксиального уравнения Гельмгольца:

$$\left( i \frac{\partial}{\partial z} + \frac{1}{2k} \Delta_{\perp} + kn_1(x, y, z) \right) \Psi_{in/out}(x, y, z; k) = 0, \quad (2)$$

где  $\Delta_{\perp} = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$ ,  $W(z)$  - ширина пучка на расстоянии  $z$ ,  $R(z)$  - радиус кривизны волнового фронта,  $\phi(z_{ap})$  - фаза Гуи,  $z_{ap}$  - координата плоскости апертуры по оси  $Z$ ,  $H_m(\xi)$  - функции Эрмита-Гаусса.  $r$  - расстояние отклонения луча от центра апертуры.  $r$  является случайным параметром, распределение которого хорошо приближает распределения вероятностей Райса для случая слабой турбулентности.

Мы изучаем протокол квантового распределения ключей, основанный на запутанных парах кубитов (EPR-Protocol). Квантовое запутанное состояние (EPR-пара) генерируется источником. Далее каждый кубит отправляется через атмосферу по отдельному каналу получателям Алисе и Бобу и попадает на измерительную аппаратуру, состоящую из четырех идеальных детекторов в каждом канале, соответствующих измерению кубита в одном из двух базисов, состояния которых в совокупности неортогональны. После измерения Алиса и Боб связываются по классическому каналу и сравнивают базисы, в которых были измерены кубиты. Результаты, измеренные в разных базисах, отбрасывают, остальные формируют квантовый ключ. В результате передачи кубитов через турбулентную атмосферу возможно появление ошибок, в случае, когда и Алиса, и Боб получают одинаковое значение бита. Вероятность появления таких ошибок была рассчитана, и она задается следующим выражением:

$$P_{err} = \frac{1}{4} \left( \frac{T_{m_1 n_1}^2 T_{m_4 n_4}^2 - 2T_{m_1 n_1} T_{m_2 n_2} T_{m_3 n_3} T_{m_4 n_4} + T_{m_2 n_2}^2 T_{m_3 n_3}^2}{T_{m_1 n_1}^2 T_{m_4 n_4}^2 + T_{m_2 n_2}^2 T_{m_3 n_3}^2} \right), \quad (3)$$

где

$$\begin{aligned} T_{m,n}^2(r) &\approx \int_A |\Psi_{m,n}(\rho, \phi, z_{ap}; k_0)|^2 d\rho d\phi = \\ &= \frac{2}{\pi W^2} \exp\left(-\frac{2r^2}{W^2}\right) \int_0^a \rho \exp\left(-\frac{2\rho^2}{W^2}\right) \int_0^{2\pi} \exp\left(\frac{4\pi\rho \cos\phi}{W^2}\right) H_m^2\left(\frac{\sqrt{2}(\rho \cos\phi - r)}{W}\right) H_n^2\left(\frac{\sqrt{2}\rho \sin\phi}{W}\right) d\phi d\rho, \end{aligned}$$

$A$  - открытая область апертуры,  $a$  - радиус апертуры.

Значения вероятностей (3) были рассчитаны численно для разных наборов мод, кодирующих кубиты. Турбулентность атмосферы учтена путем генерации случайных значений расстояния отклонения луча. Выявлено, что правильный выбор мод, кодирующих кубиты, позволяет снизить вероятность ошибки до минимума (например, моды  $\Psi_{31}, \Psi_{32}, \Psi_{45}, \Psi_{64}$ ). В результате проведенного дополнительного исследования установлено, что такой набор мод также обеспечивает практически максимальное сохранение степени запутанности кубитов при передаче их через атмосферу на дальние расстояния, что указывает на важность контроля над изменением степени запутанности кубитов в процессе их передачи.

## Литература

1. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. Cambridge University Press, 2010. 676 p.
2. Mitschke F. Fiber Optics: Physics and Technology. Springer, Berlin, 2009. 301 p.
3. Zhang Sh., Shi J., Zhao J., Zhang H., Bao W. Entanglement performance of light through the composite free space channel // Optical and quantum electronics. 2021. Vol. 53. No. 2. pp. 81.

4. Vilmrotter V., Lau C.-W. Quantum detection theory for the free-space channel // IPN Progress Report. Vol. 142. pp. 146.
5. Agrawal G.P., Fiber optics and optical communications. New Jersey: John Wiley and Sons, 2020. 626 p.
6. Vasylyev D. Yu., Semenov A. A., Vogel W. Toward global quantum communication: beam wandering preserves nonclassicality // Phys. Rev. Lett. 2012. Vol. 108. pp. 220501.

MSC2020 81P70

## **Analysis of the quantum key distribution algorithm implementation model in turbulent atmosphere**

M. P. Faleeva, I. Yu. Popov

ITMO University