

ТЕНДЕНЦИИ РАЗВИТИЯ КВАНТОВЫХ КОММУНИКАЦИЙ

Развитие квантовых коммуникаций

Ю.В.Курочкин

Актуальность исследования, разработки и внедрения квантовых технологий не снижается уже много десятилетий. Первый этап развития и внедрения в практику квантовых технологий позволил создать лазеры, высокоскоростную оптическую связь, интернет, нанофотонику и многие другие применения, кардинально изменившие окружающий мир. В последние десятилетия мы наблюдаем стремительное развитие нового этапа квантовых технологий, отличающегося движением к познанию и применению квантовых свойств одиночных атомов и фотонов. Общепринято деление квантовых технологий на три больших направления: квантовые вычисления, квантовые коммуникации и квантовые сенсоры. Работы по этим направлениям регулярно публикуются в журнале «Квантовая электроника».

В этом номере журнала представлена подборка статей, посвященных сегодняшним тенденциям развития квантовых коммуникаций. Основное направление здесь – квантовая криптография, или квантовое распределение ключей. Центральной идеей последнего является теорема о запрете клонирования [1], которая состоит в том, что произвольное квантовое состояние невозможно копировать, не внося искажений. На практике это означает, что если информация передается неортогональными состояниями одиночного фотона, то попытка извлечь информацию приведет к конечному уровню ошибок. Квантовая теория информации в свою очередь позволила связать верхний предел доли перехваченной информации с уровнем ошибок [2]. С помощью одиночных фотонов передается именно ключ – случайная последовательность битов, который потом можно использовать для защиты информации. Если уровень ошибок говорит о перехвате ключа, то он просто не используется для передачи полезной информации. При этом перехватчику предоставляется возможность использовать любые технологии будущего, не противоречащие законам квантовой механики. Это значит, что квантовые состояния можно не только измерять и пересылать, но и производить неразрушающие измерения [3] и условные манипуляции. Первым и самым распространенным протоколом передачи информации является BB84 [4], преимущество которого состоит в наличии строгого доказательства стойкости. Наличие протоколов с нестрогим доказательством секретности [5] открывает широкие возможности для развития теории квантовых коммуникаций. Оптические реализации даже одного протокола могут очень сильно различаться: например, квантовые состояния в оптоволоконных линиях могут кодироваться как поляризацией [6], так и фазой [7] фотона, что открывает большой простор для экспериментальных работ.

Ю.В.Курочкин. Международный центр квантовой оптики и квантовых технологий, Россия, 143025 Москва, Сколково, ул. Новая, 100; e-mail: y.kurochkin@gmail.com

Поступила в редакцию 10 апреля 2020 г.

Прикладные решения на основе квантовых коммуникаций уже используются государственными органами, банками, телекоммуникационными и энергетическими компаниями. Несмотря на значительный прогресс, все еще сохраняются значительные ограничения как по дальности передачи кубит, так и по скорости генерации квантовых ключей. Эти ограничения часто носят фундаментальный характер, и для их преодоления требуются новые идеи и научные разработки. Именно по этой причине квантовые коммуникации продолжают исследоваться и развиваться в университетах и научных центрах всего мира. Следующим этапом развития могут стать квантовые сети на основе повторителей [8], по которым квантовый сигнал будет передаваться на большие расстояния через промежуточные узлы без измерения. Для реализации таких сетей требуются протокол обмена запутанностью и квантовая память, в которой недавно произошел значительный научный прорыв [9]. Это направление развития в свою очередь требует новых методов приготовления и измерения квантовых состояний, в том числе запутанных состояний [10], и новых доказательств стойкости протоколов.

Поддержка развития квантовых технологий на государственном уровне в последние годы не только возросла, но и стала целевой. Так, в Китае уже построена квантовая сеть Пекин–Шанхай, в ЕС стартовала большая программа поддержки исследований [11], в России квантовые технологии целевым образом поддерживаются в рамках федерального проекта «Цифровые технологии» [12], программы поддержки действуют в Англии и США.

Публикуемая подборка статей посвящена преимущественно теоретическим исследованиям в области квантовой теории информации. Тем не менее мы постарались не обойти вниманием экспериментальные исследования, которые могут быть важны для реализации систем квантовых коммуникаций.

1. Wootters W.K., Zurek W.H. *Nature*, **299**, 802 (1982).
2. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dušek M., Lütkenhaus N., Peev M. *Rev. Modern Phys.*, **81** (3), 1301 (2009).
3. Fedorov I.A., Ulanov A.E., Kurochkin Y.V., Lvovsky A.I. *Optica*, **2** (2), 112 (2015).
4. Bennett C.H., Brassard G., in *Proceedings of International Conference on Computers, Systems & Signal Processing* (Bangalore, India: IEEE, 1984, p. 175).
5. Kurochkin Y. *Intern. Soc. Opt. Photon.*, 5833, 213 (2005).
6. Duplinskiy A., Ustimchik V., Kanapin A., Kurochkin V., Kurochkin Y. *Opt. Express*, **25** (23), 28886 (2017).
7. Dynes J., Yuan Z., Plews A., Takahashi R., Doi K., Tam W., Sharpe A., Kujiraoka M. *J. Lightwave Technol.*, **36** (16), 3427 (2018).
8. Duan L.M., Lukin M.D., Cirac J.I., Zoller P. *Nature*, **414** (6862), 413 (2001).
9. Bhaskar M.K., Riedinger R., Machielse B., Levonian D.S., Nguyen C.T., Knall E.N., Lukin M.D. *Nature*, **580**, 60 (2020).
10. Fedorov I.A., Ulanov A.E., Kurochkin Y.V., Lvovsky A.I. *Opt. Lett.*, **42** (1), 132 (2017).
11. <https://qt.eu/>.
12. <https://digital.ac.gov.ru/support/#analytics>.