

Д.А. Глозштейн, И.Г. Сидоркина
ФГБОУ ВО «Поволжский государственный технологический
университет», г.Йошкар-Ола

Ключевые слова: квантовая коммуникация, квантовый Интернет, квантовая запутанность, квантовая маршрутизация.

Квантовый Интернет — это передовая парадигма, которая использует уникальные свойства квантовых технологий для радикального изменения сетей связи. Улучшенная безопасность, увеличенная скорость и пропускная способность сети квантового Интернета приведут к появлению широкого спектра новых приложений и сервисов, для эффективной работы которых необходимо создать надежную инфраструктуру на сетевом уровне. Разработка квантовых протоколов существенно отличается от проектирования традиционных протоколов, поскольку она должна учитывать уникальные особенности квантовой физики и передачи информации. Однако реализация этих методов сопряжена со значительными трудностями на физическом уровне и крайне специфическими требованиями к аппаратуре.

Область квантовой коммуникации основана на синтезе идей квантовой механики и теории информации [1-2]. Способность квантовой коммуникации обеспечивать связь с безусловной безопасностью является основной движущей силой ее развития [3].

Квантовый Интернет предполагает использование теоретической и экспериментальной квантовой физики [4] и компьютерных наук для создания нового метода обработки и передачи информации. Он задумывался как сеть, которая может безопасно передавать квантовые данные, такие как квантовые ключи, квантовая запутанность и квантовые состояния на большие расстояния, без риска перехвата или модификации. Защищенная коммуникация стала возможной благодаря квантовому распределению ключей, при котором принципы квантовой механики позволяют обмениваться секретными ключами по общедоступному каналу с гарантированной безопасностью. Протоколы квантовой связи, как показано на рисунке 1, станут основой квантового Интернета [5].

Квантовый Интернет в его стандартной модели можно рассматривать как сеть, где каждый узел хранит кубиты в квантовом хранилище. Соединения или связующие звенья между узлами составляют квантовый канал. Этот канал может генерировать квантовую запутанность между кубитами, которые находятся в узлах на обоих концах этого канала. Такая структура называется сетью квантовой памяти [6]. Основопологающим

предположением в этой модели является практичность выполнения двухкубитных вентилей между любой парой кубитов, размещенных в одном узле. Кроме того, предполагается, что каждому узлу назначается заранее определенное количество блоков памяти, соответствующее каждому каналу, который к нему подключается.



Рисунок 1 - Базовая схема квантового распределения ключей

Наиболее полное представление о квантовом Интернете можно отразить в трех моделях сетевой архитектуры:

1. Стек ван Метера [7] основан на парах ЭПР и опирается на два ключевых протокола — очищение запутанности и обмен запутанностью, которые рекурсивно применяются ко всем пяти уровням стека.

2. Стек Венер [8] представляет собой многоуровневую модель квантовых сетей, основанную на двусторонней запутанности, описываемую в формате пяти уровней.

3. Стек Дюра [9] основан на многосторонних запутанных состояниях, которыми используются для выполнения запросов узлов, и формализуется на четырех уровнях. В рамках [10] стек был дополнен реальной моделью квантовой сети, содержащей запутанное состояние с квантовым регистром управления, отвечающим за кодирование выполняемой задачи.

Отличительной особенностью модели Дюра является то, что, в отличие от других архитектур, она использует многостороннюю запутанность для значительного роста производительности сети.

Важной особенностью модели ван Метера является возможность распознавания многосторонней запутанности. Несмотря на то, что эта модель была одним из первых предложений по формализации квантовых сетей, ее основные положения все еще актуальны, и она может быть частично интегрирована в более общую модель Дюра [9].

Основная особенность модели Венер заключается в том, что она является первой попыткой удовлетворить потребность во взаимодействии

между различными аппаратными реализациями, за счет внедрения на канальном уровне подуровня аппаратной абстракции (HAL).

Несмотря на специфические особенности, все три модели признают запутанность ключевым ресурсом квантового Интернета. С этой целью модель ван Метера предлагает четкое разграничение [11] для уровней распределения запутанности: а) между узлами сети посредством одиночных переходов, б) по маршрутам с несколькими переходами между промежуточными узлами и в) между конечными устройствами.

Модель Дюра определяет физический уровень как ориентированный на однократное запутывание. Канальный уровень распределяет многостороннюю запутанность между узлами сети, для чего выполняются операции на внешних и промежуточных узлах. Уровень связности определяет каналы длиной в один переход, а также промежуточные узлы.

Также в модели Дюра учитывается различие между локальным и межсетевым взаимодействием [9]: узлы находятся в одной сети, когда они используют одно и то же начальное многостороннее состояние. Хотя это различие нельзя напрямую ввести в другие модели, основанные на двусторонней запутанности, можно распространить эту идею на модель Венер путем использования концепции аппаратной абстракции — сеть определяется как набор узлов, использующих одну и ту же аппаратную платформу. Это расширение может быть также применено к модели ван Метера, используя концепцию квантовой рекурсивной сетевой архитектуры [12]. Кроме того, среди моделей, основанных на парах ЭПР, существует четкая граница между уровнями, реализующими квантовые и уровнями, которые используют только классическую коммуникации.

Список использованных источников

1. Gisin, N., Thew, R.: Quantum communication. *Nat. Photonics* 1(3), 165–171 (2007). <https://doi.org/10.1038/nphoton.2007.22>
2. Bennett, C.H., Shor, P.W. Quantum information theory. *IEEE Trans. Inf. Theor.* 44(6), 2724–2742 (1998). <https://doi.org/10.1109/18.720553>
3. Kumar, A., Garhwal, S.: State-of-the-art survey of quantum cryptography. *Arch. Comput. Methods Eng.* 28(5), 3831–3868 (2021). <https://doi.org/10.1007/s11831-021-09561-2>
4. Rozenman, G.G., Peisakhov, A., Zadok, N.: Dispersion of organic exciton polaritons—a novel undergraduate experiment. *Eur. J. Phys.* 43(3), 035301 (2022). <https://doi.org/10.1088/1361-6404/ac50fd>
5. Wehner, S., Elkouss, D., Hanson, R.: Quantum internet: a vision for the road ahead. *Science* 362(6412), eaam9288 (2018). <https://doi.org/10.1126/science.aam9288>
7. Simon, C.: Towards a global quantum network. *Nat. Photonics* 11(11), 678–680 (2017). <https://doi.org/10.1038/s41566-017-0032-0>
8. R. Van Meter, T. D. Ladd, W. J. Munro, K. Nemoto, System design for a long-line quantum repeater, *IEEE/ACM Transactions on Networking* 17 (3) (2008) pp. 1002–1013.
9. Kozłowski, A. Dahlberg, S. Wehner, Designing a quantum network protocol, in: *Proc. of the 16th International Conference on Networking Experiments and Technologies*, 2020, pp. 1–16.

10. A. Pirker, W. Dür, A quantum network stack and protocols for reliable entanglement-based networks, *New Journal of Physics* 21 (3) (2019) 033003.

11. J. Miguel-Ramiro, A. Pirker, W. Dür, Genuine quantum networks with superposed tasks and addressing, *npj Quantum Information* 7 (2021) 135.

12. L. Aparicio, R. Van Meter, H. Esaki, Protocol design for quantum repeater networks, in: *AINTEC '11: Proc. of the 7th Asian Internet Engineering Conference*, 2011, pp. 73–80.

13. R. Van Meter, J. Touch. Recursive quantum repeater networks, *NII Journal* (2011) pp. 65–79.

Глозштейн Даниил Александрович, аспирант каф. ИБ, GlozstejnDA@volgatech.net

Сидоркина Ирина Геннадьевна, профессор, д.т.н., заведующая каф. ИБ, igs592000@mail.ru

УДК: 347

К ВОПРОСУ О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Ахмадиева В.Ф., Ахмадиева В.Ф., Яппаров Р.М.

ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа

В индустриальном обществе быстрыми темпами набирает обороты развитие технологий и расширяется сфера применения электронных средств в качестве способа обмена информацией, растёт актуальность вопросов по защите конфиденциальной информации. Лицензирование деятельности по технической защите конфиденциальной информации выступает ключевым инструментом обеспечения безопасности информации. Лицензирование и его основные концепции будут рассмотрены нами в представленной статье.

Лицензирование деятельности по технической защите конфиденциальной информации — это процедура, предусматривающая выдачу специального разрешения на осуществление определенных видов деятельности, которая направлена на обеспечение защиты конфиденциальной информации от неправомерного доступа, использования и распространения [1].

Согласно законодательству, такая лицензия выдается Федеральной службой по техническому и экспортному контролю, выполняющая контроль за соблюдением правил, установленных законодательством, в части обеспечения безопасности конфиденциальной информации с ограниченным доступом [2].

Важнейшим элементом концепции являются строгие требования, предъявляемые к лицензиату. Законодательство содержит определенные условия, которым необходимо удовлетворять в случае наличия лицензии на защиту конфиденциальной информации. Эти требования могут характеризоваться наличием трудового стажа и специального образования