Квантовые коммуникации

Н.Жизэн (Швейцария)

Перевод М.Х. Шульмана (shulman@dol.ru, www.timeorigin21.narod.ru)

---

arXiv:1507.05157 [quant-ph]

Quantum Communication

Nicolas Gisin,
University of Geneva, Switzerland

Современное состояние

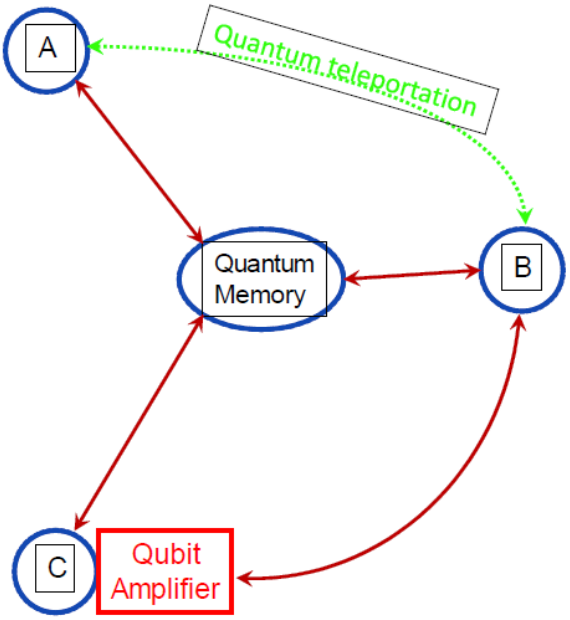
Квантовые коммуникации (Quantum Communication – QC) – это область знаний о передаче неизвестного квантового состояния из одного местоположения (скажем, от Алисы) в другое, удаленное от первого, местоположение (скажем, Бобу) [1]. Эта задача не является тривиальной из-за теоремы о невозможности квантового клонирования состояния, которая запрещает делать это так, как делается в классической физике.

С одной стороны, QC – чудесная вещь, т.к. позволяет нам распространять область запутывания на большие расстояния и, таким образом, устанавливать так называемые нелокальные корреляции, что подтверждается нарушениями неравенств Белла, т.е. такие корреляции, которые невозможно объяснить лишь локальными параметрами, распространяющимися в пространстве непрерывно.

С другой стороны, QC имеют огромный потенциал применения. Лучше всего известна задаче о распространении квантового ключа (Quantum Key Distribution – QKD), где использование запутывания гарантирует секретность ключа в криптографических приложениях. Другими примерами возможных приложений являются процессы, случайность которых гарантируется нарушением некоторого неравенства Белла. В самом деле, невозможно доказать случайность данной последовательности битов, но можно доказать, что некоторые процессы случайны, и известно, что случайные процессы продуцируют случайные последовательности битов. Следовательно, случайность переходит из математики в физику.

В QC необходимо использовать источники фотонов, средства кодирования некоторой квантовой информации (в виде квантовых битов или, кратко, кубитов), каналы передачи фотонов, обеспечивающих сохранение переносимой ими информации (например, поляризации или т.н. time-bin кубитов[1]), с возможностью телепортации информации и/или сохранения ее в квантовой памяти и, вероятно, детектор фотонов после анализатора, который позволяет восстановить квантовую информацию. Кроме того, QC эволюционирует от простой двусторонней связи к сложным сетям. Последнее требует, с фундаментальной точки зрения, лучшего понимания многочастичного запутывания и нелокальности, а с экспериментальной точки зрения глобального системного подхода с совершенной синхронизацией, сетевым управлением, процессами восстановления.

[1] См. https://en.wikipedia.org/wiki/Time-bin_encoding .



Quantum teleportation – квантовая телепортация

Quantum memory – квантовая память

Qubit Amplifier – усилитель кубитов

Текущие и будущие проблемы

QC сталкиваются со многими проблемами, которые простираются от индустриализации квантовых технологий до концептуальных вопросов теоретической физики, от оптики до материаловедения.

Источники: Помимо относительно простого случая двустороннего QKD, все задачи QC требуют источников запутанных фотонов. Сегодня такие источники основаны на спонтанном параметрическом преобразовании с понижением частоты, поэтому являются вероятностными. Следовательно, чтобы исключить генерацию нескольких пар фотонов, вероятность рождения одиночной пары поддерживается достаточно низкой, обычно от 1% до 0.1%. Более того, потери связи между нелинейными кристаллами, в которых рождаются фотоны, и оптоволокном оказываются критичными. Развитие доступных и детерминистических источников запутанных фотонов является важной задачей.

Квантовые каналы могут представлять собой либо космический вакуум, либо оптоволоконные кабели. Первый случай наиболее подходит для QC типа Земля-спутник и спутник-спутник; там главные проблемы заключаются в размере и весе телескопов [2]. Для волокон главной проблемой являются потери. Сегодня наилучшие оптоволокна имеют потери до 0.16 дБ/км, т.е. через 20 км более половины фотонов все еще сохраняются [3].

Квантовая телепортация: Этот замечательный процесс позволяет передавать квантовые состояния (т.е. квантовую информацию), используя заранее созданное запутывание в качестве канала. Квантовое состояние не передается вдоль какой-либо траектории в пространстве, но “телепортируется” отсюда туда. Кроме передачи запутывания, телепортация требует совместных измерений, еще одно квантовое свойство, не существующее в классической физике. Совместные измерения позволяют измерить относительные свойства двух систем, например выяснить, “являются ли состоянии поляризации анти-параллельными?”, не определяя информацию об их индивидуальных свойствах [4]. Следовательно, индивидуальные свойства при этом не возмущаются, но

корреляции между свойствами двух систем оказываются “квантово коррелированными”, т.е. запутанными. На практике два фотона смешиваются в светоделителе. Это работает, но требуется высокая стабильность, т.к. оба фотона должны быть неразличимы по всем параметрам. В частности, важна синхронизация, особенно когда фотоны пролетают большие расстояния перед встречей в светоделителе.

Более того, этот процесс вероятностный и работает в лучшем случае в половине случаев (при этом известно, когда он работает) [5]. Большой проблемой является существенное усовершенствование совместных измерений. Это, вероятно, требует передавать фотонные квантовые состояния с помощью твердотельных носителей (solids), чтобы совместное измерение осуществлялось с помощью степеней свободы, кодирующих квантовое состояние в твердотельных носителях, например, между двумя спинами. Кроме того, с чисто теоретической точки зрения, требуется лучшее понимание сущности совместных измерений, подобно абстрактной формулировке нелокальных корреляций.

Сигнальный (heralded) вероятностный усилитель кубитов также должен быть упомянут. Соответствующий процесс, восходящий к телепортации, позволяет увеличить вероятность присутствия фотона без возмущения кодируемого им кубита [6]. Проблема состоит в создании такого усилителя для больших расстояний (>10 км).

Детекторы: QC в основном осуществляются с использованием единичных фотонов, следовательно, требуются отличные детекторы единичных фотонов. Хотя следует сказать, что можно также использовать так называемые непрерывные параметры, например, импульсы сжатого света и гомодинные системы детектирования [7]. Недавно детекторы единичных фотонов получили значительное развитие, их растущая эффективность за пару лет от 20% достигла 80-90% благодаря сверхпроводящим системам детектирования [8]. В то же время нестабильность снизилась ниже чем до 100 пс. Однако еще остались некоторые значительные проблемы:

- упрощение/удешевление (в частности, при более высоких температурах, как минимум при 3 К, возможно, с применением высокотемпературной сверхпроводимости).
- повышение чувствительности детекторов к числу фотонов вплоть до нескольких десятков фотонов. Эта замечательная перспектива имеет, однако, смысл, только если эффективность детектирования равна не менее 95%.
- достижение 99-100% эффективности. Это кажется достижимым.

Устройства квантовой памяти позволяют обратимым образом и в нужный момент преобразовать фотонные квантовые состояния в некоторые атомные системы (и обратно) с большими временами когерентности [9]. Они нужны для синхронизации сложных квантовых сетей. *Они могут также переключать вероятностные источники в режим квази-детерминированности, обеспечивая их достаточно высокую эффективность*. Сегодня устройства квантовой памяти все еще являются лабораторными устройствами. Хотя все параметры – объем памяти, эффективность, надежность, полоса пропускания и возможность работы в мультимодовом режиме – были удовлетворительно продемонстрированы, каждая такая демонстрация использовала свою особенную систему. Следовательно, большой проблемой является является разработка системы, способной хранить 100 фотонных кубитов (например, 100 временных мод) в течение 1 секунды с

эффективностью 90% и надежностью около 95%. Это огромная проблема. Неясно, окажется ли лучшим решением использовать один естественный или искусственный атом в резонаторе или комплекс атомов (газ или легированные оптические кристаллы). Это требует совместного привлечения материаловедения и химии (в случае кристаллов), криогеники (низкие температуры представляются необходимыми для длительных времен хранения), спектроскопии и радиоволновой спин-эхотехники, оптики и электроники.

Многочастичное запутывание и нелокальность: будущие сложные квантовые сети будут рутинным образом продуцировать запутанные многочастичные состояния, чьи полные возможности еще должны быть прояснены. В случае 2-частичных, нелокальных корреляций это оказывается мощным ресурсом для некоторых замечательных процессов, называемых независимыми от устройства квантово-информационными процессами (Device Independent Quantum Information Processes (DIQIP) [10]. Аналогично, можно ожидать квантовых корреляций в сложных сетях, чтобы открыть новые возможности, которые еще предстоит создать.

QKD: Задача распространения квантового ключа является наиболее продвинутым приложением квантовых коммуникаций. Остальные задачи являются по большей части промышленными и коммерческими. Для промышленности задача QKD должна стать менее дорогой и использовать большие скорости (один Гб/с кажется недостижимым). Для коммерческих приложений должны быть переподготовлены специалисты по классической безопасности и криптографии, они должны понять потенциал квантовой физики и то, что их знания являются не устаревшими, но требующими дополнений: кванты не решают всех проблем, но обеспечивают гарантированную случайность и секретность. Следовательно, всегда надо будет сочетать их с классическими системами безопасности и криптографии.

Успехи науки и технологии по преодолению проблем

Наиболее значительные из упомянутых выше проблем требуют сочетание фотонных и твердотельных устройств, будь это применительно к детерминистическим устройствам, детекторам и устройствам квантовой памяти, и, вероятно, улучшенным совместным измерениям. Это базовая значительная проблема связана с интегрированными гибридными системами. В идеале все эти твердотельные устройства будут связаны со стандартными оптическими оптоволоконными коммуникационными кабелями и, следовательно, их легче будет включать в большие сети.

Заключительные замечания

Будущие квантовые сети будут похожи на сегодняшний интернет. Будут просто покупать компоненты и соединять их вместе с помощью оптических волокон под управлением и при синхронизации с помощью мощного программного обеспечения. Случайность и секретность появятся сами собой. Запутывание, нелокальность и телепортация получат широкое распространение, так что ими будут пользоваться дети. Немыслимые сегодня приложения станут разрастаться. Такая мечта станет возможной благодаря квантовым коммуникациям.

Ссылки

[1] European Roadmap for QIPC: http://qurope.eu
[2] T Scheidl *et al.,* New J. Phys. **15** 043008 (2013)
[3] B. Korzh *et al.,* Nature Photonics **9**, 163 (2015)
[4] C. Bennett et al., Phys. Rev. Lett. **70**, 1895 (1993)
[5] N. Lütkenhaus et al., PRA **59**, 3295 (1999)
[6] N. Gisin *et al*. Phys. Rev. Lett. **105**, 070501 (2010)
[7] C. Weedbrook, *et al.*, Rev. Mod. Phys. **84**, 621 (2012)
[8] F. Marsili *et al.,* Nature Photonics **7**, 210 (2013)
[9] C. Simon *et al.*, Eur. Phys. J. D **58**, 1 (2010)
[10] V. Scarani, Acta Phys. Slov. **62** 347 (2012)