

КВАНТОВЫЕ ПОВТОРИТЕЛИ В СИСТЕМАХ КВАНТОВОЙ СВЯЗИ QUANTUM REPEATERS IN QUANTUM COMMUNICATION SYSTEMS

Камалов Н.Р., студент 4 курса факультета компьютерных наук
ФГБОУ ВО «Воронежский
государственный университет», Воронеж,
Россия

Kamalov N.R., 4th year student of the
Computer Science Faculty
FSBEI HE «Voronezh State University»,
Voronezh, Russia

Клинских А.Ф., доктор физико-
математических наук, профессор,
профессор
ФГБОУ ВО «Воронежский
государственный университет», Воронеж,
Россия

Klinskikh A.F., DrSc in Physics and
Mathematics, Professor, Professor
FSBEI HE «Voronezh State University»,
Voronezh, Russia

Аннотация. В работе рассмотрена архитектура квантового повторителя на основе явления квантовой телепортации с реализацией максимально запутанных состояний Белла. Приведены алгоритмы квантовой очистки по протоколам Беннета и Дойча. В результате реализована схема квантового повторителя с тремя узлами и операциями обмена запутанностью. Проведена симуляция квантовых сигналов с помощью пакета Qiskit.

Ключевые слова: квантовый повторитель, квантовая очистка, состояние Белла, кубит, обмен запутанностью.

Abstract. The paper considers the architecture of a quantum repeater based on the phenomenon of quantum teleportation with the implementation of the most entangled Bell states. Algorithms for quantum purification according to the Bennett and Deutsch protocols are given. As a result, a quantum repeater scheme with three nodes and entanglement exchange operations has been implemented. Quantum signals were simulated using the Qiskit package.

Keywords: modernization, timber industry, innovative potential

Введение

Квантовые технологии и коммуникации в настоящий момент являются наиболее перспективными и прорывными в таком активно развивающемся секторе экономики, как цифровая связь. Особенно квантовые коммуникации востребованы в сфере защиты информационно-телекоммуникационных сетей, информации финансового сектора, госорганов и высокотехнологичных компаний.

Принцип работы квантовых коммуникационных сетей (quantum networks) базируются на законах квантовой механики. Безопасность передачи данных реализуется с помощью алгоритмов квантового распределения ключей (КРК, quantum key distribution – QKD), используются волоконно-оптические системы передачи квантовых состояний фотонов [1,2]. Развитие квантовых коммуникаций существенно приближает ученых к практическому

созданию квантового компьютера. Несмотря на то, что пока полномасштабный квантовый компьютер – это чисто гипотетическое устройство, его реализация может наступить в результате давно ожидаемого прорыва, в том числе и в технологиях квантовых коммуникаций. Общая концепция такого устройства основана на теории квантовых вычислений с использованием квантовых алгоритмов [3-8]. На настоящий момент проблема реализации квантового канала коммуникации связана с квантово-механическими ограничениями. Протоколы требуют существования квантовой запутанности между передающей и принимающей сторонами. При этом, сама запутанность является хрупким ресурсом и сильно искажается шумом, из-за чего длина затухания канала невелика. Кроме того, классические повторители решают проблему потерь сигнала простым усилением или измерением и регенерацией входного сигнала, которая невозможна ввиду теоремы о запрете клонирования. Также декогеренция ограничивает возможности измерения состояний квантовых систем без разрушения их информационного содержания. Обход вышеописанных ограничений позволит на практике использовать новые возможности коммуникации, такие как квантовая телепортация и устойчивая к взлому квантовая криптография. Следует отметить, что эти возможности не имеют классического аналога в реализации.

В статье предлагается возможная реализация схемы квантового повторителя, позволяющая разделить весь канал связи на множество небольших сегментов, длина каждого из которых меньше длины затухания канала.

Для достижения цели необходимо решить следующие задачи:

- Разобрать принцип действия квантового повторителя, основанного на явлении телепортации с использованием максимально запутанных состояний Белла.
- Изучить протоколы квантовой очистки и алгоритм обмена запутанностью между элементами канала связи.
- Реализовать схему квантового повторителя для последующего моделирования.

Обоснование принципа действия квантового повторителя

Фундаментальным элементом квантовой схемы является кубит. Это двумерная квантовая система с ортонормальными базисными состояниями $|0\rangle$ и $|1\rangle$ (известными как вычислительный базис):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

где α и β – комплексные коэффициенты, означающие амплитуду вероятности, то есть $|\alpha|^2 + |\beta|^2 = 1$.

Вообще говоря, запутанность – это невозможность представления системы 2-х кубитов в виде тензорного произведения. Степень запутанности определяется значением определителя матрицы плотности. Стандартными запутанными состояниями двухкубитовой системы AB являются максимально запутанные состояния Белла $|\Phi_{\pm}\rangle$ и $|\Psi_{\pm}\rangle$, которые выражаются в терминах состояний вычислительного базиса.

Для состояния Белла определитель матрицы плотности максимален и равен $1/4$, это означает что кубит запутан с другим.

Существенной проблемой состояний Белла, генерируемых схемой распределения запутанности между двумя удаленными узлами, является то, что они не совершенны. Хотя потери можно уменьшить путем многократного повторения схемы, в таких системах будут возникать и другие ошибки.

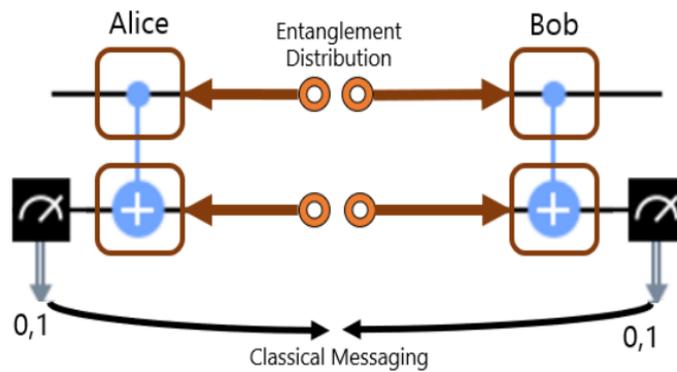
В рассматриваемом случае ошибки, связанные с несовершенными локальными операциями, будут уменьшать верность выбранной нами связи с состоянием $|\Phi^+\rangle$, транслируя их соответствующим трем другим элементам состояния Белла.

В данной работе решается задача генерирования заранее известного извлекаемого состояния Белла с более высокой точностью из множества несовершенных копий с помощью процесса квантовой очистки.

Протокол очистки Беннета предполагает, что две копии Bell-состояния уже установлены между узлами ретранслятора, которые могут иметь низкую точность. На каждом узле обе стороны применяют операцию CNOT между двумя кубитами, сохраняя соответствующие кубиты каждой пары в качестве управляющего и целевого, соответственно. Затем целевые кубиты измеряются в вычислительном базисе $|0\rangle, |1\rangle$. Наконец, результаты измерений передаются по классическому каналу между узлами (см. рис. 1а). Неизмеренное состояние контрольных кубитов сохраняется, только если результаты измерений целевых кубитов совпадают (т.е. оба равны нулю (0,0) или единице (1, 1)). В этом случае очистка проходит успешно. Результирующее состояние неизмеренного кубита будет иметь более высокую точность, если исходная точность обеих пар была больше 50% и наши локальные операции (CNOT и проективные измерения) достаточно точны. Если результаты измерений не совпадают (т.е. (0,1) или (1,0)) то протокол очистки не удался, и нужно начинать все сначала со свежими запутанными состояниями.

Протокол Беннета страдает от двух основных недостатков. Для его работы, во-первых, начальное состояние должно быть в форме Вернера. Во-вторых, требуется много раундов очистки, чтобы получить состояние Вернера с верностью выше 99%, если начать с набора низковерных соединений. Дойч решил эти проблемы путем модификации протокола Беннета. Состояние двухуровневой квантовой системы можно представить в виде единичного вектора в трехмерном пространстве. Он называется блоховским вектором состояния, а сфера, на которой он находится, называется блоховской сферой. Унитарная операция $R_x(\theta)$ представляет собой поворот блоховского вектора относительно оси x на угол θ . В матричной нотации она изображена на рис. 1б. Эта процедура приводит к теоретическому увеличению достоверности примерно в 100 раз по сравнению с алгоритмом Беннета. Более того, начальные состояния пар Белла не обязательно должны иметь форму Вернера.

Использование распределения запутанности с последующей квантовой очисткой позволяет разработать механизм для создания высокоточного состояния Белла между соседними узлами ретранслятора. Затем необходимо сформировать механизм для соединения отдельных связей вместе, чтобы создать дальнюю запутанную связь. Для решения этой задачи возьмем две пары в состоянии Белла, соединённые друг с другом в состоянии $|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34}$, где метки 1, 2, 3, 4 обозначают местоположение кубитов, из которых узлы (1, 2), (2, 3) и (3, 4) являются смежными. Когда выполняется измерение состояния Белла между кубитами 2 и 3, оно переводит кубиты 1 и 4 в состояние $|\Phi^+\rangle_{14}$ до операции коррекции Паули I, Z, X, Y в



a)

$$R_x(\theta) = \begin{bmatrix} \cos(\theta/2) & -i \sin(\theta/2) \\ -i \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

b)

Рисунок 1 – Схема протокола очистки запутанности Беннета-Дойча

Entanglement Swapping

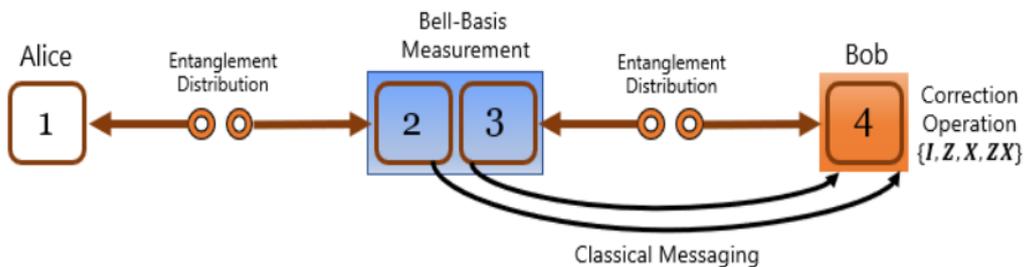


Рисунок 2 – Обмен запутанностью

зависимости от результата измерения. По сути, это эквивалентно протоколу телепортации, но в этом случае кубиты, состояние которых должно быть передано, запутываются с другими кубитами. Например, если две пары в состоянии Белла, соединённые друг с другом в состоянии $|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34}$, где метки 1, 2, 3, 4 обозначают местоположение кубитов, из которых узлы (1, 2), (2, 3) и (3, 4) смежные, то будет выполняться измерение состояния Белла между кубитами 2 и 3, и оно переведет кубиты 1 и 4 в состояние $|\Phi^+\rangle_{14}$ до операции коррекции Паули I, Z, X, Y в зависимости от результата измерения (см. рис. 2).

Реализация схемы квантового повторителя

Создание запутанностей между узлом и концами ретранслятора реализуется в схеме, представленной на рисунке 3. На первом этапе четыре кубита на своих квантовых регистрах $\det(\sigma)$ на кубите $q_3 = 0$. Затем кубиты q_0 и q_1 запутаны в состоянии Белла, а q_2 и q_3 нет, $\det(\sigma)$ на кубите $q_3 = 0$. Наконец запутанность q_0 и q_1 стимулирует образование запутанности q_2 и q_3 , $\det(\sigma)$ на кубите $q_3 = 1/4$, таким образом, он разделяет запутанность с кубитом другого регистра.

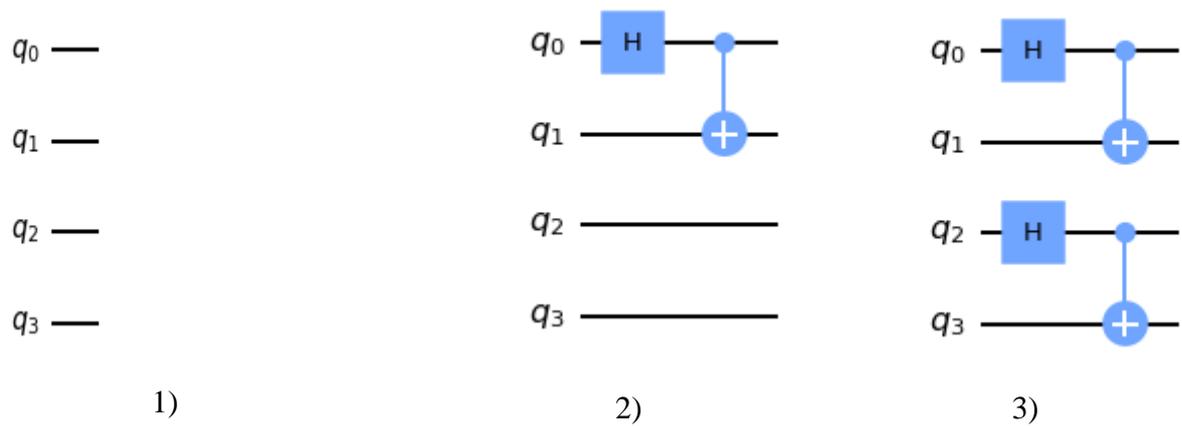


Рисунок 3 – Схема формирования запутанностей между узлом и концами ретранслятора

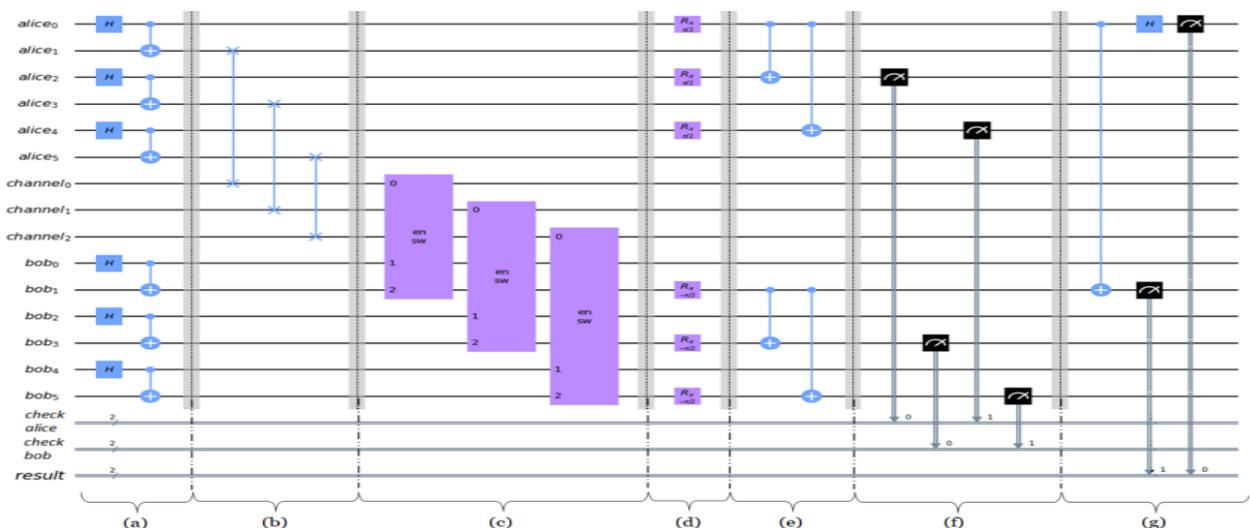


Рисунок 4 – Полная схема предлагаемой архитектуры квантового повторителя.

- (а) Подготовка состояний Белла, (б) Передача запутанных кубитов в канал,
- (с) Обмен запутанностью, (д) Операция коррекции Дойча, (е) Протокол очистки Беннета,
- (ф) Измерение и классический обмен сообщениями,
- (г) Измерение в базисе Белла для проверки верности запутанности

Таким образом, на первом шаге схемы между соседними узлами повторителя создается несколько Bell-пар путем распределения запутанности. После создания достаточного их количества при необходимости выполняется очистка запутанности (один или несколько раз) для повышения верности связи. Затем два соседних канала с высокой верностью соединяются с помощью протокола обмена запутанностью, чтобы создать канал вдвое длиннее исходного. Далее квантовая очистка снова выполняется на более длинных связях, созданных на шаге 1. За этим снова следует обмен запутанностью для создания еще более длинных связей. Таким образом, шаги 1 и 2 повторяются до тех пор, пока между Алисой и Бобом (см. рис. 2) не будет создана запутанная связь требуемой верности. Если очистка или обмен запутанными связями не удастся на каком-либо этапе, мы должны начать эту часть снова с шага 1. После завершения всего цикла операций между двумя сторонами будет установлена прочная и надежная запутанная связь (см. рис. 4).

Заключение

Таким образом, в статье Разобраны основы схемы квантового повторителя, реализованной на максимально запутанных состояниях Белла на базе систематизации протоколов квантовой очистки и схемы обмена запутанностью между элементами канала. Реализована схема квантового повторителя.

СПИСОК ЛИТЕРАТУРЫ

1. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels / С.Н. Bennett, G. Brassard, С. Crépeau, R. Jozsa, А. Peres, W.K. Wootters // Physical Review Letters. – 1993. – Vol. 70. – P. 1895–1899. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.70.1895>.
2. Shor, P.W. Algorithms for quantum computation: discrete logarithms and factoring / P.W. Shor // Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 Nov. 1994. – IEEE Computer Society Press, 1994. – P. 124–134. – URL: <https://ieeexplore.ieee.org/document/365700>.
3. Манин, Ю.И. Вычислимое и невычислимое / Ю.И. Манин. – Москва : Советское радио, 1980. – 128 с.
4. Манин, Ю.И. Доказуемое и недоказуемое / Ю.И. Манин. – Москва : Советское Радио, 1979. – 88 с.
5. Фейнман, Р.Ф. Внизу полным-полно места: приглашение в новый мир физики / Р.Ф. Фейнман // Российский химический журнал. – 2002. – Т. XLVI, № 5. – С. 4-7.
6. Weisner, S. Conjugate coding / S. Weisner // Association for Computing Machinery, Special Interest Group in Algorithms and Computation Theory. – 1983. – Т. 15. – С. 78–88.
7. Холево, А.С. Квантовая информатика : прошлое, настоящее, будущее / А.С. Холево // В мире науки. – 2008. – № 7. – С. 68-75.
8. Biggest quantum computer / Geek.com. – URL: <https://www.geek.com/chips/biggest-quantum-computer-to-date-544054/> (дата обращения: 11.08.2019).