УДК 004.942+530.145.1

Актаева А.[1], Байкенов А.[2], Галиева Н.[3], Асанова К.[4], Байман Г.[5], Шатенова Г.[6]

[1]Алматинский технологический университет, г.Алматы, Казахстан
[2]Аламатинский университет энергетики и связи, г.Алматы, Казахстан
[3]Павлодарский государственный университет им.С.Торыайгырова, г.Павлодар, Казахстан
[4]Казахско-американский университет, г.Алматы, Казахстан
[5]Павлодарский государственный университет им. С.Торыайгырова, Павлодар, Казахстан
[6]Казахская академия транспорта и коммуникации им. М.Тынышбаева, г.Алматы, Казахстан

КВАНТОВАЯ ИНФОРМАЦИЯ: МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

АННОТАЦИЯ

В статье обсуждается значимость в современном информационном обществе информационных ресурсов, требующих надежных методов защиты от НСД.

Рассматривается структура и основные принципы технологии квантовой криптографии на основе свойств квантовых систем. Теоретическая разработка была экспериментально реализована авторами на установке для многоканальной сети передачи данных. Предложен метод повышения уровня информационной безопасности и защиты конфиденциальной информации путем квантовой телепортации на квантовых каналах лазерной связи.

КЛЮЧЕВЫЕ СЛОВА

Квантовая информация, квантовые каналы связи, энтропия фон Неймана, пропускная способность, АОЛС, кубит.

Aktaeva A.[1], Baikenov A.[2], Galieva N.[3], Asanova K.[4], Byman G.[5], Shatenova G.[6]

[1]Almaty technological university, Almaty, Kazakhstan
[2]Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
[3]S. Toraighyrov Pavlodar State University, Pavlodar, Kazakhstan
[4]Kazakh-American University, Almaty, Kazakhstan
[5]S. Toraighyrov Pavlodar State University, Pavlodar, Kazakhstan
[6]Kazakh Academy of Transport and Communication named after M. Tynyshpaev, Almaty, Kazakhstan

QUANTUM INFORMATION: METHODS OF PROTECTION INFORMATION

ABSTRACT

The most popular development tools of the quantum cryptography technology are compared, the structure and the basic principles of its work is considered. Also describes the structure and basic principles of quantum cryptography technology based on properties of quantum systems. Quantum information are a physical quantity characterizing changes occurring in the system during the interaction between the information flow and the external environment. Theoretical development has been experimentally realized by the authors at the facility for multi-channel data transmission network. In the article a method of increasing the level of information security and the protection of confidential information by the quantum teleportation of quantum channels laser communication are considered.

KEYWORDS

Quantum information, quantum communication channels, von Neumann entropy, bandwidth, FSO, qubit.

В настоящее время квантовая информатика представляет собой новую, быстро развивающуюся отрасль науки, связанную с использованием квантовых технологий для реализации принципиально новых методов инфо-телекоммуникации и вычислений: квантовая информация, квантовая информатика, квантовые каналы связи, квантовая криптография, квантовый компьютер [7].

Квантовая информация — это физическая величина, характеризующая изменения, происходящие в системе при взаимодействии информационного потока с внешним окружением.

Квантовая информация — это новый вид информации, который можно передавать, но нельзя размножать. Квантовый бит или кубит (qubit) описывается единичным вектором в двумерном комплексном векторном пространстве и представляет собой двухуровневую квантовую систему. В качестве кубитов могут выступать ионы, атомы, электроны, фотоны, спины атомных ядер, структуры из сверхпроводников и многие другие физические системы [7].

Классическая информация может быть «записана» в квантовом состоянии и передана через физический канал. Базис векторного пространства задается всего двумя единичными ортогональными векторами, обозначаемыми соответственно $|0\rangle$ и $|1\rangle$. В отличие от классического бита, квантовый бит может быть представлен произвольной суперпозицией базисных векторов состояния фотона $|\psi\rangle = a|H\rangle + b|V\rangle$ где, **a** и ***b***-произвольные комплексные числа, удовлетворяющие условию $|a|^2 + |b|^2 = 1$, может быть представлено, как и в случае спина, на блоховской сфере (рис.1) и однокубитовые операции представляют собой вращение вектора Блоха [7].

А квантовое состояние задаются неотрицательными, эрмитовыми операторами, дисперсии и ковариации наблюдаемых величин, а также является информационным ресурсом постольку, поскольку имеет статистическую неопределенность, и информация в неизвестном квантовом состоянии является квантовой информацией [23].

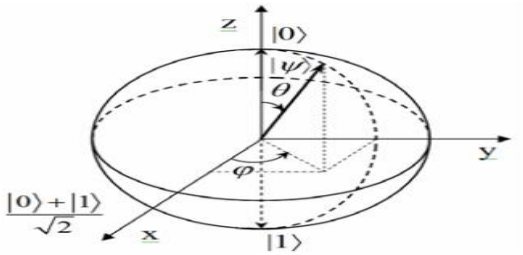

Рис. 1. Кубит на сфере Блоха

Квантовые состояния квантовой информаций обладают следующими свойствами:

1.*Суперпозиция*- состояния описываются линейной суперпозицией базисных соятояний;

2. *Интерференция* – результат измерений зависит от относительных фаз амплитуд в этих состояниях;

3. Сцепленность (entanglement) – полное знание о состоянии всей системы не соответствует такому же полному знанию о состоянии ее частей;

4. *Неклонируемость и статистическая неопределенность* – неизвестное квантовое состояние невозможно клонировать, а также наблюдать без его возмущения [29].

Развитие математической теории квантовых каналов передачи информации является актуальной фундаментальной проблемой. Квантовая теория информации - изучающая общие закономерности передачи, хранения и преобразования информации в системах, подчиняющихся законам квантовой механики и использует математические модели для исследования потенциальных возможностей таких систем, опираясь на методы некоммутативной теории вероятностей. В бесконечномерных - квантовых вероятностных системах канал характеризуется несколькими пропускными способностями, в зависимости от рода передаваемой классической или квантовой информации и дополнительных используемых ресурсов. Классическая пропускная способность определяет предельную скорость асимптотически безошибочной передачи классической информации. Протокол передачи классической информации предполагает кодирование классического сигнала состояниями на входе канала и декодирование на выходе, по которым производится оптимизация [22,29].

Простейший квантовый канал связи математически задается семейством (выходных или сигнальных) состояний S_x, где параметр x пробегает входной алфавит. Отображение $x \to S_x$ в сжатой форме содержит описание физического процесса, порождающего состояние S_x. Квантовый канал связи с двумя чистыми неортогональными состояниями где x = 0|1, причем S_1 когерентное состояние поля излучения лазера, а S_0 вакуумное состояние [23].

Теорема кодирования Шеннона характеризует пропускную способность классического канала связи, то есть предельную скорость асимптотически безошибочной передачи данных при длине сообщения, стремящейся к бесконечности. Теорема, которая дает выражение для классической пропускной способности квантового канала Ф, действующего в конечномерных гильбертовых пространствах:

$$C(\Phi) = \lim_{n\to\infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}),$$

$$C_\chi(\Phi) = \sup_{\{\pi_i, S_i\}} \left[H(\sum_i \pi_i S_i) - \sum_i \pi_i H(S_i) \right],$$

где H(S) — энтропия фон Неймана, а точная верхняя грань берется по всевозможным конечным входным ансамблям π = { π_i, S_i}, где { S_i } — состояния, { π_i } — соответствующие вероятности. Доказательство теоремы (неравенство ≥ в формуле (1)) основано на теореме кодирования для классически-квантового канала [24].

Квантовый канал связи предполагает наличие классического параметра *x*, пробегающего конечный или бесконечный алфавит *X* и отображение $x \in S_x$ в квантовые состояния на выходе канала. Классическая пропускная способность C такого канала Ÿ дается величиной и π = {π_x} — распределение вероятностей на *X*

$$C(\Upsilon) = \sup_\pi \chi(\pi),$$

$$\chi(\pi) = H\left(\sum_x \pi_x S_x\right) - \sum_x \pi_x H(S_x)$$

Обратные теоремы кодирования для классических пропускных способностей опираются на квантовую энтропийную границу, даюшую оценку сверху для информации Шеннона величиной X(π), т.е. оценку для количества классической информации, которую можно передать по квантовому каналу [24].

Другим типом классической пропускной способности является пропускная способность с использованием сцепленного состояния (*entanglement-assisted classical capacity*). Протокол передачи информации с использованием сцепленности предполагает, что системы A (передатчик) и B (приемник) имеют общее сцепленное состояние S_{ab} в качестве дополнительного ресурса. Использование сцепленности может дать возможность многократного увеличения скорости передачи для квантовых каналов с шумом и имеет место для ряда так называемых измерительных каналов, представляющих интерес для приложений новых технологий, таких как, квантовая томография и телепортация в конечномерном пространстве, оптическое гетеродинирование с ограничением на энергию входного сигнала и др.[5].

Пропускная способность с использованием сцепленности определяется как классическая пропускная способность, в которой производится оптимизация по всевозможным сцепленным состояниям и кодирующим каналам. Для классической пропускной способности с использованием сцепленности через квантовую взаимную информацию *I(S,Φ)*, а именно

$$C_{ea}(\Phi) = \max_S I(S, \Phi), \qquad I(S, \Phi) = H(S) + H(\Phi(S)) - H(\Phi \otimes \mathrm{Id}_R(|\psi_S\rangle\langle\psi_S|)),$$

где $|\psi_S\rangle\langle\psi_S|$ - очищение состояния S.

Принципиально другой характеристикой канала является его квантовая пропускная способность. Квантовое состояние само по себе является информационным ресурсом, и понятие квантовой пропускной способности связано с задачей асимптотически безошибочной передачи квантовых состояний по каналу с шумом. Соответствующий протокол предполагает использование кодирования на входе канала и декодирования на выходе. Теорема кодирования, дающая следующее выражение для квантовой пропускной способности конечномерного канала Q (Φ):

$$Q(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_S I_c(S, \Phi^{\otimes n}),$$

где $I_c(S, \Phi) = H(\Phi(S)) - H(\Phi \otimes \mathrm{Id}_R(|\psi_S\rangle\langle\psi_S|))$ - когерентная информация [22,24,29].

Квантовая энтропия определяет максимальную степень сжатия квантовых данных, т.е. количество квантовой информации.

При передаче классической информации (т. е. сообщения w = (x_1, . . ., x_n)) по квантовому каналу связи она записывается в квантовом состоянии S_w. Приемник производит квантовое измерение над состоянием на выходе канала связи, результатом которого являются значения w_0 = (y_1, . . ., y_n). Процесс передачи классической информации описывается диаграммой

$$w \xrightarrow{\text{кодирование}} S_w \xrightarrow{\text{канал}} S'_w \xrightarrow{\text{декодирование}} w'$$

Классическая пропускная способность канала *Φ* при применении квантовой теоремы кодирования определяется

$$C(\Phi) = \lim_{n\to\infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}), \qquad C_\chi(\Phi) = \max_{p_i, S_i} \left\{ H\left(\sum_i p_i \Phi[S_i]\right) - \sum_i p_i H(\Phi[S_i]) \right\}$$

А квантовый аналог Шенноновской формулы $C = \max_{\{p_x\}} I(X;Y)$, ,

где максимум берется по всевозможным распределениям на входе $\{p_x\}$ и описывается вероятностями переходов p(y|x) из входного алфавита X в выходной алфавит Y, т.е. условными вероятностями того, что принят символ y ∈ Y, при условии, что был послан символ x ∈ X. Если эта величина обладает свойством *аддитивности*, $C_\chi(\Phi \otimes n) = nC_\chi$ (Φ), то $C(\Phi) = C^{-}(\Phi)$. Аддитивность величины $C\chi(\Phi)$ означает, что использование сцепленных кодовых состояний не позволяет увеличить количество передаваемой классической информации [22,23,24,29].

Квантовая теория информации - система с «непрерывными переменными», основанная на принципах квантовой оптики. Особенно важными здесь являются гауссовские состояния, включающие когерентные и сжатые состояния, реализуемые в лазерах и нелинейных квантовых оптических устройствах, и соответствующий класс преобразователей квантовой информации – гауссовские каналы (сцепленность состояний, пропускные способности и другие характеристики), где роль квантовой степени свободы на выходе канала может также играть поляризация или направление спина. Например, двоичный оптический классически-квантовый канал может быть реализован следующим образом:

- если *x* = 0, то поле излучения находится в вакуумном состоянии;
- если *x* = 1, то лазер генерирует когерентное состояние [22,23,24,29].

Двоичный оптический классически-квантовый канал (беспроводной лазерный канал связи), основан на технологиях передачи инфракрасного излучения через воздушную или безвоздушную среду данных модулированным ИК-излучением. Атмосферные оптические линии связи (Free Space Optics) – это способ для организации надежных высокоскоростных беспроводных соединений в местах, где прокладка оптического кабеля затруднительна или невозможна. Пропускная способность канала определится выражением:

$$C = 1/\tau \cdot [1 + P \cdot \log P + (1 - P) \cdot \log(1 - P)],$$

где 1/τ – число двоичных символов, передаваемых по каналу АОЛС в секунду, P – вероятность ошибочного приема одного двоичного символа.

Скорость передачи информации для этого случая равна R=1/τ, а коэффициент снижения пропускной способности канала определится выражением:

$$\eta = 1 + P \cdot \log P + (1 - P) \cdot \log(1 - P).$$

Вероятность ошибочного приема одного двоичного символа зависит от метода модуляции сигнала [25].

Методом оптического мультиплексирования с ортогональным частотным разделением каналов (O-OFDM – Optical orthogonal frequency-division multiplexing) с квадратурной фазовой манипуляцией (QPSK – Quadrature Phase Shift Keying), на световой поток, излучаемый белыми светодиодами, происходит наложение данных при помощи модуляций. На практике метод O-OFDM реализуется при помощи алгоритма быстрого вычисления преобразования Фурье (FFT – Fast Fourier transform), то есть дискретного преобразования Фурье [22,23,24,29].

В сети VLC на светодиодах (Li-Fi), с использованием одного белого светодиода при бинарном сигнале в канале с аддитивным белым гауссовским шумом и высоком отношении сигнал/шум и использовании QPSK в сочетании с методом кодированного OFDM (COFMD – coded OFDM), который подразумевает канальное кодирование методом прямой коррекции ошибок (FEC - Forward Error Correction), а фундаментальный показатель качества цифровых систем - коэффициент вероятности ошибки на бит (BER – Bit Error Rate) составляет с $2 \cdot 10^{-5}$ от передатчика до приёмника [22,23,24,29].

Многоканальное решение обеспечивает увеличение дальности передачи информации, повышение надежности по сравнению с одноканальными вариантами. Применение предложенной системы позволяет расширить скоростной диапазон до гигабитных скоростей. На рисунке 2 схематично продемонстрирована многоканальная сеть передачи данных на базе комбинации технологии Li-Fi и технологии VFIR для обратной связи. При росте требований к скорости передачи информации телекоммуникационных систем, многоканальные АОЛС могут обеспечивать беспроводную передачу информации на уровне гигабитных скоростей — оптимальное решение для задач «последней мили» в нелицензированном диапазоне СВЧ.

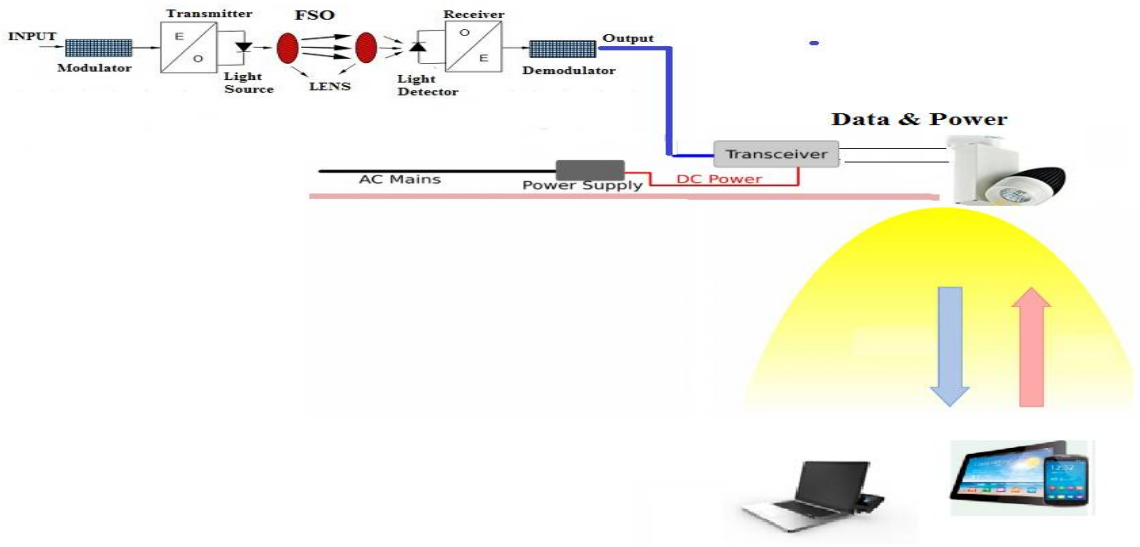

Рис.2. Многоканальная сеть передачи данных на базе комбинации технологии Li-Fi

Квантовый канал используется для передачи некоторого массива случайных битов квантовой информации - кубитов, реализованных в поляризационных степенях свободы светового поля, а открытый канал – для обсуждения. При передаче по квантовому каналу изначально линейно поляризованный свет станет в общем случае поляризованным эллиптически на выходе из-за возникающих температурных и фазовых флуктуаций показателя преломления. Несмотря на то, что степень поляризации сохраняется (имеется в виду случай, когда длина когерентности света L_{eff} намного превышает эффективную длину канала), любое чистое поляризационное состояние на выходе будет подвержено сильным флуктуациям. Основные состояния при таком способе кодирования имеют вид:

$$|\updownarrow\rangle \equiv |V\rangle, |\leftrightarrow\rangle \equiv |H\rangle,$$

$$|\square\ \rangle = \frac{1}{\sqrt{2}}\{|H\rangle + |V\rangle\},$$

$$|\square\ \rangle = \frac{1}{\sqrt{2}}\{|H\rangle - |V\rangle\}, |\circlearrowright\rangle$$

$$|L\rangle \equiv \frac{1}{\sqrt{2}}\{|H\rangle + i|V\rangle\}, |\circlearrowleft\rangle$$

$$|R\rangle \equiv \frac{1}{\sqrt{2}}\{|H\rangle - i|V\rangle\}.$$

Они соответствуют вертикальной, горизонтальной, диагональным и (право- и лево) циркулярным поляризациям однофотонных фоковских состояний [22].

Попыткой поиска ответов на квантовые вызовы в области обеспечения системы информационной безопасности и защиты информации является квантовая криптография. Упрощенная временная развертка событий в квантовой криптографии представлена на рисунке 3:

а) лазер генерирует световые импульсы, которые ослабляются до уровня фотон/импульс и посылаются через АОЛС получателю, где детектируются в ожидаемые моменты времени;

б) синхроимпульсы следуют с периодом T;

в) ослабленные до уровня фотон/импульс световые импульсы;

г) электрические импульсы, стробирующие детектор;

д) электрические импульсы на выходе детектора.

Темновые отсчеты возникают в случайные моменты времени и являются паразитным сигналом, который требуется учитывать при работе любой системы квантовой криптографии.

Основные усилия в этой области сосредоточены на задачах синтеза стойких к возможностям квантовых компьютеров криптографических алгоритмов и протоколов. Известно несколько протоколов распределения ключей на основе дискретных квантовых состояний. К настоящему времени предложено несколько десятков различных по назначению протоколов квантовой безопасной связи (BB84, ЭПР, B92(4+2), SARG04, CSS, ЛО-ЧУ, Гольденберга-Вайдмана, Коаши-Имото, Пинг-Понг и др.) [7].

В целом, протоколы квантовой криптографии можно разбить на две группы (рис.4). В первую входят протоколы квантовой криптографии, оперирующие с неортогональными

квантовыми состояниями. Во вторую – протоколы, основанные на так называемых перепутанных квантовых состояниях и проверке выполнения соотношений типа неравенства Белла.

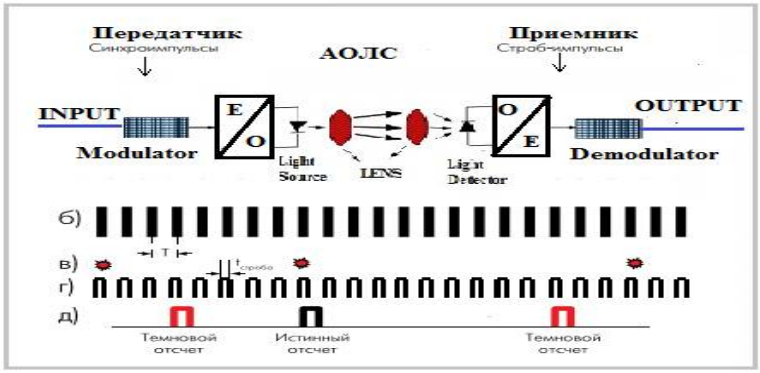

Рис. 3. Упрощенная временная развертка событий в квантовой криптографии

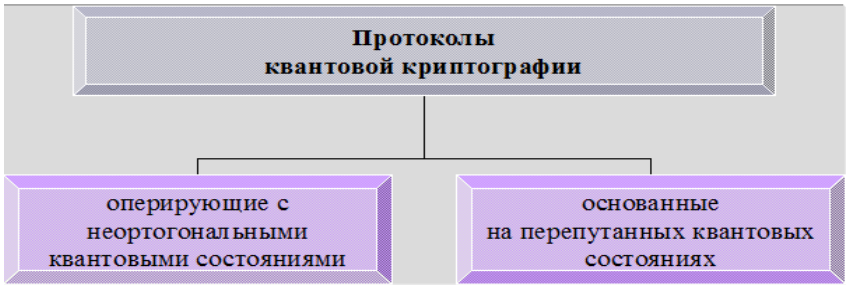

Рис.4. Группы протоколов квантовой криптографии

Наиболее известный протокол на перепутанных состояниях – протокол А.Экерта или E91. В основе отдельной группы протоколов квантовой криптографии лежит кодирование информации в квадратурные амплитуды моды квантованного электромагнитного поля [22,27,28, 29, 30].

В протоколе BB84 используется два или, три взаимно несмещенных базиса, состоящих из пары ортогональных состояний. Такие базисы удовлетворяют условию, что квадрат модуля скалярного произведения состояний из разных базисов равен обратной размерности гильбертова пространства:

$$\left|\left\langle \psi_i \middle| \varphi_i \right\rangle\right|^2 = 1/D,$$

в то время как для состояний из одного базиса скалярное произведение равно нулю:

$$\left\langle \psi_i \middle| \psi_j \right\rangle = 0 \ (i, j = 1, 2).$$

Так, при кодировании в поляризационных степенях свободы электромагнитного поля (D=2) можно составить три взаимно несмещенных базиса, которые образованы парами ортогональных поляризационных векторов:

вычислительный $\left(|\updownarrow\rangle \equiv |V\rangle, |\leftrightarrow\rangle \equiv |H\rangle\right)$,

диагональный $|\square\rangle \text{ B } \frac{1}{\sqrt{2}}\{|H\rangle \text{B} |V\rangle\}, |\square\rangle \text{ B } \frac{1}{\sqrt{2}}\{|H\rangle \text{B} |V\rangle\}$

циркулярный $|L\rangle \equiv \frac{1}{\sqrt{2}}\{|H\rangle + i|V\rangle\}, |R\rangle \equiv \frac{1}{\sqrt{2}}\{|H\rangle - i|V\rangle\}.$

Полная формализация достигается, если состояниям, соответствующим вертикальной и горизонтальной поляризациям света, сопоставить векторы в т.е. вычислительном базисе: $|H\rangle \to |1\rangle, |V\rangle \to |0\rangle$. Протокол BB84 является наиболее популярным протоколом квантовой криптографии [22,27,28, 29, 30].

Кроме квантового канала связи, по которому передающая и принимающая стороны обмениваются квантовыми состояниями – оптической линии связи – важным, неотъемлемым атрибутом квантовой криптографии является так называемый «открытый» канал связи. Открытым называется канал, если передаваемая по нему информация может быть доступна любому участнику протокола, в том числе злоумышленнику. Важным условием использования открытого канала в квантовой криптографии является невозможность изменить передаваемую по нему информацию.

Использование квантовой линии связи накладывает ограничение на возможность работы с поляризационной кодировкой, поскольку лазер обладает ощутимыми флуктуационными двулучепреломления. В силу этого для квантовой криптографии используется фазовая модуляция с интерферометрическими детектированием. Основополагающими принципами защиты данных в квантовых линиях связи являются невозможность копирования заранее неизвестного состояния отдельного квантового объекта и невозможность получения любой информации о квантовых состояниях этого объекта без их возмущения [7].

Квантовая телепортация - передача неизвестного квантового состояния на расстояние при помощи разделенной в пространстве и поделенной между двумя корреспондентами ЭПР-пары и классического канала связи. Квантовая телепортация, в отличие от плотного кодирования, происходит при отсутствии квантового канала связи, т.е. без передачи кубитов (рис.5).

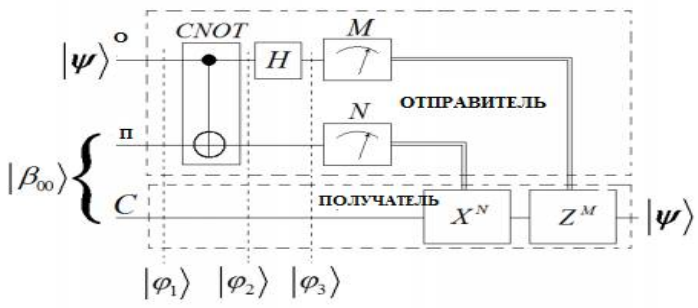

Рис. 5. Схема квантовой телепортации: одинарные линии- квантовые каналы связи ; двойные – классические [17]

Телепортация представляет собой идеальный способ передачи секретной информации, а также:

- процедура телепортации не нарушает теорему о неклонируемости;
- перенос квантовой информации от фотона к фотону может осуществляться на произвольные расстояние (более 144 км по открытой пространстве, 102 км -по оптическому волокну);
- телепортация не предполагает передачу информации о факте ее осуществления;
- классический канал (о факте передачи информации);
- если не проводить измерение состояний Белла и ограничиться проецированием на фермионное состояние, то телепортация будет успешно осуществлена в среднем один раз из четырех попыток [7].

Квантовая телепортация не дает возможности передавать информацию быстрее скорости света, как может показаться на первый взгляд, поскольку неотъемлемой частью протокола телепортации является передача информации по классическому каналу связи, а классический канал ограничен скоростью света (рис. 6).

Квантовая телепортация используемая в качестве некоторой базисной составляющей в квантовой схеме, открывает заманчивые возможности для решения этой и ряда других экспериментальных проблем, возникающих при реализации квантовых компьютеров, она позволяет осуществлять целый ряд квантовых логических операций, невозможных при использовании прямых унитарных операций. Формирование помехоустойчивых квантовых логических вентилей сводится в этом случае к приготовлению соответствующего вспомогательного запутанного состояния в схеме однокубитовой телепортации. [11].

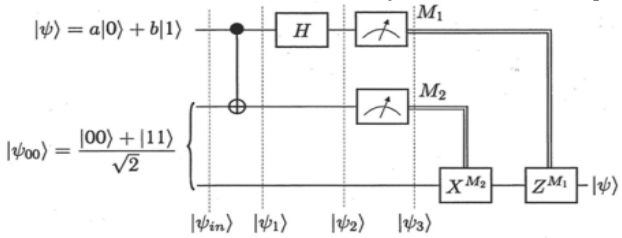

Рис.6 - Квантовая схема телепортации неизвестного состояния |Ψ>кубита [20]

Новые возможности инфракрасных лазеров для реализации квантовой телепортации состояний открывают преимущество в решении проблемы передачи легко разрушаемых суперпозиционных состояний на большие расстояния без потери ими когерентности.

Заключение

В связи с интенсивным развитием инновационных технологий особое значение приобретают исследования в электронике, создании интеллектуальных программных и аппаратных продуктов прикладной информатики и квантовых технологий. Квантовая информация и технологии, основанные на ее необычных свойствах, в будущем повлияют на основы и дальнейшее развитие информационного пространства, а широкое применение квантовых технологий предполагает научно-техническую революцию, масштабы которой очень трудно представить. Распространение технологии квантовой связи является одним из перспективных и в то же время реальных шагов в стратегических планах ряда стран Европы и США, Японии.

Теория квантовой информации кардинально изменит современные взгляды научного сообщества на основу системы информационной безопасности. Проведение экспериментов и исследований по обеспечению информационной безопасности представляет большой научный интерес по поиску решения основных задач и проблем, стоящих перед квантовыми криптографическими системами: задача детектирования единичных фотонов с высокой вероятностью в заданном квантовом состоянии при низком уровне ложных срабатываний, отсутствие управляемых источников одиночных фотонов, проблема увеличения дальности передачи и малая скорость генерации квантового ключа.

Применение квантовых технологий в области обеспечения системы информационной безопасности - одно из наиболее парадоксальных проявлений квантовой технологии, вызывающее в последние годы огромный интерес специалистов. в первую очередь, при передаче зашифрованных сообщений по двум т более каналам связи - квантовому и традиционному. Квантовая телепортация информации является одним из самых стремительно развивающихся прикладных направлений квантовой физики, и обеспечивает информирование о попытке перехвата передаваемой информации из-за необратимости коллапса волновой функции.

Исследования в области квантовой телепортации информации могут привести не только к положительным последствиям, но и отрицательным. Квантовая криптография, основанная на применении квантовой телепортации, в будущем заменит все используемые криптографические системы, и будет применяться наравне с обычными средствами инфотелекоммуникации. Актуальность и масштабность проблем, связанных с обеспечением информационной безопасности, с каждым днем будут возрастать, а развитие квантовой информации в ближайшем будущем принесет свои результаты и, возможно, приведет к существенному изменению научной картины мира в области ИТ.

Литература

1. Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // J. Stat. Phys. – 1980,V. 22, p. 563–591.
2. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer // Proc. Roy. Soc.- London,1985, V. A400,p. 96–117.
3. Cleve R., Ekert A., Macchiavello C., Mosca M. Quantum algorithms revisited // Phil. Trans. Royal Soc. - London,1998, V. A454,p. 339–354.
4. Turing A. On computable numbers with an application to the Entscheidungsproblem // Proc. LondonMath. Society. - 1937. - V. 42.–p. 230–265.
5. Гуревич И. Информационные характеристики физических систем.–М.:2009, 170 с.
6. Бауместер Д., Экерт А., Цайлингер А. Физика квантовой информации. -М.: Постмаркет, 2002.
7. Актаева А.. и др. Security of information: using of quantum technologies //International Journal of Open Information Technologies.-vol 4,№ 4, 2016, 40-48 pp., www.injoit.org.
8. Белокуров В.В., Тимофеевская О.Д., Хрусталев О.А. Квантовая телепортация – обыкновенное чудо. - Ижевск: РХД, 2000
9. Бройль Л. Революция в физике. -М: Атомиздат, 1965.
10. Валиев К.А. Квантовая информатика: компьютеры, связь и криптография.-М.: Вестник РАН, 2000.
11. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежда и реальность. -Ижевск: Регулярная и хаотическая динамика, 2001.
12. Гейзенберг В. Физика и философия.- М.:Наука,1989.
13. Кадомцев Б.Б. Динамика и информация.- М.:Успехи физических наук, 1999.
14. Клышко Д.Н. Физические основы квантовой электроники.-М.: Наука, 1986.
15. Мандель Л., Вольф Э. Оптическая когерентность и квантовая оптика. -М.: Физматлит, 2000.
16. Прескилл Дж. Квантовая информация и квантовые вычисления.-М.: РХД, 2008.
17. Холево А.С. Введение в квантовую теорию информации. – М.: МЦНМО, 2002.
18. Эйнштейн А., Подольский Б., Розен Н.// «Можно ли считать, что квантово-механическое описание физической реальности является полным?» //УФН, 1934, Том XVI, выпуск 4. - перевод – Любина А.Г., под редакцией Фока А.В..
19. Долгов В.А. и др. Криптографические методы защиты информации.-Хабаровск,2008.
20. Емельянов В.И. Квантовая физика: Биты и Кубиты.-М.:Изд.МГУ,2012.
21. Актаева А.У., Илипбаева Л.И. Инновационные технологии в системе информационной безопасности: квантовые технологии // Современные инновационные технологии и ИТ- образование.-2014, том 1, № 1(9), 320-326 стр.

22. Кулик С. Классическая криптография // ФОТОНИКА 2010,2, 36-41 стр.
23. Холево А.С Математические основы квантовой информатики.– М.:2016, 125 с.
24. Курочкин В.Л. Экспериментальная установка для квантовой криптографии с одиночными поляризованными фотонами//Журнал технической физики, 2005, том 75, № 6.
25. Глущенко Л.А., Моргунов К.К. Оценка защищенности информации в лазерных линиях связи //
26. http://sci-article.ru
27. http://works.tarefer.ru/71/100019/index.html
28. http://book.itep.ru/3/optic_32.htm
29. Килин С.Я Квантовая информация // Успехи физической науки, 1999, Том 169, №5.
30. http://tcode.tinro.ru/cryptography/src/38.pdf

References

1. Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // J. Stat. Phys. – 1980,V. 22, r. 563–591
2. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer // Proc. Roy. Soc.-London,1985, V. A400,r. 96–117.
3. Cleve R., Ekert A., Macchiavello C., Mosca M. Quantum algorithms revisited // Phil. Trans. Royal Soc. - London,1998, V. A454,p. 339–354.
4. Turing A. On computable numbers with an application to the Entscheidungsproblem // Proc. LondonMath. Society. - 1937. - V. 42.–r. 230–265.
5. Gurevich I. Informatsionnye kharakteristiki fizicheskikh sistem.–M.:2009, 170 s.
6. Baumester D., Ekert A., Tsaylinger A. Fizika kvantovoy informatsii. -M.: Postmarket, 2002.
7. Aktayeva A.U. Security of information: using of quantum technologies //International Journal of Open Information Technologies.-vol 4,№ 4, 2016, 40-48 pp.,www.injoit.org.
8. Belokurov V.V., Timofeevskaya O.D., Khrustalev O.A. Kvantovaya teleportatsiya – obyknovennoe chudo. - Izhevsk: RKhD, 2000.
9. Broyl' L. Revolyutsiya v fizike. -M: Atomizdat, 1965.
10. Valiev K.A. Kvantovaya informatika: komp'yutery, svyaz' i kriptografiya.-M.: Vestnik RAN, 2000.
11. Valiev K.A., Kokin A.A. Kvantovye komp'yutery: nadezhda i real'nost'. -Izhevsk: Regulyarnaya i khaoticheskaya dinamika, 2001.
12. Geyzenberg V. Fizika i filosofiya.- M.:Nauka,1989.
13. Kadomtsev B.B. Dinamika i informatsiya.- M.:Uspekhi fizicheskikh nauk, 1999.
14. Klyshko D.N. Fizicheskie osnovy kvantovoy elektroniki.-M.: Nauka, 1986.
15. Mandel' L., Vol'f E. Opticheskaya kogerentnost' i kvantovaya optika. -M.: Fizmatlit, 2000.
16. Preskill Dzh. Kvantovaya informatsiya i kvantovye vychisleniya.-M.: RKhD, 2008.
17. Kholevo A.S. Vvedenie v kvantovuyu teoriyu informatsii. – M.: MTsNMO, 2002.
18. Eynshteyn A., Podol'skiy B., Rozen N.// «Mozhno li schitat', chto kvantovo-mekhanicheskoe opisanie fizicheskoy real'nosti yavlyaetsya polnym?» //UFN, 1934, Tom XVI, vypusk 4. - perevod – Lyubina A.G., pod redaktsiey Foka A. V.
19. Dolgov V.A. i dr. Kriptograficheskie metody zashchity informatsii.-Khabarovsk,2008.
20. Emel'yanov V.I. Kvantovaya fizika: Bity i Kubity.-M.:Izd.MGU,2012.
21. Aktaeva A.U., Ilipbaeva L.I. Innovatsionnye tekhnologii v sisteme informatsionnoy bezopasnosti: kvantovye tekhnologii // Sovremennye innovatsionnye tekhnologii i IT- obrazovanie.-2014, tom 1, № 1(9), 320-326 str.
22. Kulik S. Klassicheskaya kriptografiya // FOTONIKA 2010,2, 36-41 str.
23. Kholevo A.S Matematicheskie osnovy kvantovoy informatiki.– M.:2016, 125 s.
24. Kurochkin V.L. Eksperimentalnaya ustanovka dlya kvantovoy kriptografii s odinochnymi polyarizovannymi fotonami//Zhurnal tekhnicheskoy fiziki, 2005, tom 75, № 6.
25. Glushchenko L.A., Morgunov K.K. Otsenka zashchishchennosti informatsii v lazernykh liniyakh svyazi //
26. http://sci-article.ru
27. http://works.tarefer.ru/71/100019/index.html
28. http://book.itep.ru/3/optic_32.htm
29. Kilin S.Ya Kvantovaya informatsiya // Uspekhi fizicheskoy nauki, 1999, Tom 169, №5
30. http://tcode.tinro.ru/cryptography/src/38.pdf

Поступила: 10.09.2016

Об авторах:

Актаева Алкена Умирбековна, доцент доцент кафедры «Информационные технологии» Алматинского технологического университета, dr.PhD, aaktaewa@list.ru;

Байкенов Олимжон Абдухакимович, доцент доцент кафедры ТКС Алматинского университета энергетики и связи, кандидат технических наук, baikenoff@yandex.ru;

Галиева Надежда Геннадьевна, исследователь НИЦ Павлодарского государственного университета им. С.Торыайгырова, MSc, nggaliyeva@gmail.com;

Асанова Карлыгаш, доцент Казахско-американский университет;

Байман Гульзагира, исследователь НИЦ Павлодарского государственного университета им. С.Торыайгырова, MSc, gbaiman@mail.ru;

Шатенова Гульмира, магистрант Казахской академии транспорта и коммуникации им. М.Тынышбаева, shatenova94@mail.ru.