***И.Д. Чхайло, И.Д. Трацевский, М.Б. Атманских***

*Тюменский государственный университет, г. Тюмень*

**УДК 003.26**

# МОДЕЛЬ МАРШРУТИЗАЦИИ ДЛЯ КВАНТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ

**Аннотация.** В работе описываются способ квантовой телепортации кубита, алгоритм Гровера, протокол квантового распределения ключей BB84. Исследуется способ создания на их основе топологии квантовых устройств с коммутацией пакетов. Описывается защищенный способ построения адресации устройств для коммутации пакетов.

**Ключевые слова:** топология «Звезда», маршрутизация, адресация, алгоритм Гровера, квантовые компьютеры.

**Введение**

Идея построения квантовых вычислений исследуется еще со второй половины XX века. Большой объем работ в этой области был связан с квантовыми алгоритмами, позволяющими эффективно решать некоторые задачи. К самым известным из ник относятся Алгоритм Дойча-Йожи [1], Алгоритм Гровера [2], Алгоритм Шора [3]. Также затрагивают вопрос квантовых вычислений, связанный с построением различных вычислимых функций, опираясь на построение различных вентилей и описания порождаемой ими системы функций [4].

Естественно, что в таком разрезе большой акцент делается на низкоуровневые задачи и методы, такие как организация памяти и теория информации [5], или, как сказано выше, конструирование различных числовых функций и алгоритмов. С другой стороны, получив эффективное преимущество перед классическими ЭВМ в области решения некоторых переборных задач, непосредственно связанных с криптостойкостью шифров, например, задача факторизации для RSA [6], остро встает вопрос о влиянии квантовых вычислительных машин (КВМ) на традиционную криптографию.

С другой стороны, оказываются обделены вниманием некоторые более высокоуровневые области современных вычислительных систем, такие как компьютерные сети. Целью данной работы является описание относительно простого метода скрытой адресации, предназначенной для соединения нескольких КВМ в одну сетевую топологию.

**Описание метода квантовой телепортации**

Простым и надежным каналом связи между двумя КВМ является метод квантовой телепортации кубита [7].

Пусть Алиса хочет передать Бобу некоторый кубит, находящийся в состоянии:

$$\varphi = a|0> + b|1>.$$

Для этого у Алисы и Боба должна быть возможность связываться по классическому каналу связи, а также они должны иметь по одному кубиту из запутанной пары (ЭПР-пары):

$$\psi_0 = \frac{1}{\sqrt{2}}(|00> + |11>).$$

Первым действием Алиса должна применить к кубиту $\varphi$ и к первому кубиту из $\psi_0$ (или, иначе говоря, к первым двум кубитам из $\varphi \otimes \psi_0$), следующие вентили:

$$(H \otimes I \otimes \mathrm{I})(\mathrm{CNOT} \otimes \mathrm{I})(\varphi \otimes \psi_0),$$

где $H$ – вентиль Адамара, задаваемый следующей матрицей:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix},$$

I – тождественное преобразование, задаваемое единичной матрицей:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

CNOT – двухкубитный вентиль «Контролируемое «ИЛИ»», задаваемый следующей матрицей:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Соответственно в силу запутанности второго и третьего кубитов некоторые изменения также произойдут и с третьим кубитом.

Далее Алиса производит измерение первых двух кубитов, получая пару классических бит, которые передает Бобу по открытому классическому каналу связи. В зависимости от полученной пары Боб производит одно из преобразований своего кубита:

00 – применяет I = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

01 – применяет X = $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$,

10– применяет Z = $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$,

11 – применяет Y = $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Таким образом, состояние кубита Боба по итогу проделанных манипуляций будет соответствовать исходному состоянию кубита Алисы.

В результате помимо незатруднительных унитарных преобразований, для телепортации одного кубита потребовалось раздать по кубиту из ЭПР-пары Алисе и Бобу, а также передать два бита по классическому каналу связи.

**Алгоритм Гровера**

Пусть имеется некоторая булева функция $f$ от $n$ переменных (то есть от $2^n$ возможных натуральных чисел в качестве аргумента) такая, что существует единственный набор $\bar{x}_i$ для которого $f(\bar{x}_i) = 1$.

Для нахождения этого набора на классическом компьютере потребуется порядка $O(2^n)$ операций, в то время как Алгоритм Гровера для КВМ справляется с этим всего за $O(\sqrt{2^n})$ [1].

Пусть $U_\alpha$ – такой унитарный оператор, который зеркально отражает все кет-векторы относительно гиперплоскости, перпендикулярной $\alpha$.

$|h>=\frac{1}{2^{\frac{n}{2}}}\sum_{i_1,i_2,\ldots,i_n=0}^{i_1,i_2,\ldots,i_n=1}x_j^{i_j}$, т.е. это равномерная суперпозиция всех состояний, получающаяся после применения преобразования Уолша-Адамара к нулевому состоянию.

Тогда Алгоритм Гровера состоит в применении оператора $G=-U_h\ U_{\bar{x}_i}$ к состоянию $|h>$ число раз, равное округлению числа $\frac{\pi 2^{\frac{n}{2}}}{4}$ к целому, т.е. $O(\sqrt{2^n})$ раз. Таким образом, амплитуда кет-вектора, соответствующего решению уравнения, увеличивается почти до единицы, а вероятность при измерении в конце получить неправильный вектор, равна примерно $\frac{1}{2^n}$.

**Квантовый протокол распределения ключей BB84**

Данный протокол позволяет Алисе и Бобу генерировать некоторый общий набор бит, измерять вероятность того, что данные биты были прослушаны, а также то, что канал связи прослушивается.

Для организации протокола Алисе и Бобу требуется канал связи, способный передавать кубиты (квантовые канал связи), а также классический канал связи. Перед началом работы Алиса и Боб выбирают и согласуют два базиса для измерения кубитов такие, что

$$|0_*>=\frac{1}{\sqrt{2}}(|0_+>+|1_+>),$$

$$|1_*>=\frac{1}{\sqrt{2}}(|0_+>-|1_+>),$$

То есть базисы повернуты друг относительно друга на $\frac{\pi}{4}$. Кет-векторы $|0_*>$ и $|1_*>$ кодируют 0 и 1 в первом базисе, а $|0_+>$ и $|1_+>$ кодируют их во втором базисе соответственно.

Далее Алиса случайным образом выбирает набор бит и для каждого из них случайным образом выбирает базис, в котором он будет закодирован. Далее она передает получившийся набор кубит Бобу, и Боб производит измерение каждого из них в случайном базисе.

Боб и Алиса по классическому каналу связи выясняют, для каких кубитов выбранный ими базис совпал, остальные отбрасывают.

Значения, полученные в результате измерения не отброшенных кубитов, у Алисы и Боба должны совпадать. Несовпадение хотя бы одного кубита будет указывать либо на то, что в канале связи есть помехи, либо на то, что канал прослушивается. Для выявления несовпадающих кубитов среди измеренных часть из них раскрывается и сравнивается. Таким образом, предполагая канал связи помехоустойчивым, увеличения количества переданных и раскрытых кубитов делает вероятность канала быть прослушиваемым экспоненциально маленькой. В случае несовпадения хотя бы одного значения делается вывод, что канал прослушивается. Данный метод целиком основан на квантово-вычислительной теореме о невозможности клонирования [7].

**Сетевая топология**

Главной целью объединения нескольких ЭВМ в общую сеть является распределение и совместное использование ресурсов [8]. Естественной кажется идея объединить в одну сеть и КВМ с тем же умыслом. Также понятным кажется использование построения пакетов сообщений, добавляя к кубитам сообщения служебные кубиты. Таким образом, коммутации каналов будет предпочтена коммутация пакетов [9], что в дальнейшем облегчит переход к многоранговым сетям.

В качестве физической, а также логической топологии была выбрана топология типа «Звезда» [9]. «Звезда» есть такая одноранговая сеть, когда все устройства (в данном случае, КВМ) подключаются к одному маршрутизатору в центре.

Помимо вполне классических достоинств и недостатков, в рамках работы с КВМ будут интересны непосредственно три аспекта:

1) Потребность в связи устройств одновременно и по квантовому и по классическому каналу связи легко разрешается за счет одного многофункционального маршрутизатора в центре «звезды».

2) Возможную необходимость раздачи ЭПР-пар разным КВМ также будет удобно полностью делегировать маршрутизатору.

3) Понятность схемы адресации с идеей однотипного горизонтального и вертикального масштабирования.

Таким образом, данная топология является не только оправданной, но и предпочтительной.

**Схема маршрутизации и адресации**

В рамках данной работы помимо обычной цели маршрутизации как поиска маршрута для некоторого пакета предполагается также использование такой схемы, которая обеспечит некоторый уровень защиты информации об адресате и получателе пакета.

Естественно, что для маршрутизатора-КВМ в качестве математической задачи адресации будет выбрана та, что эффективно решена для КВМ и не решена для ЭВМ, что обеспечит защиту от перехвата пакетов классическими ЭВМ. В качестве такой задачи будет служить Задача, соответствующая Алгоритму Гровера.

На первом этапе выбирается некоторая булева функция $f$ от $n$ переменных $x_i$ такая, что $f(\bar{x}_i) = 1$ только для одного набора $\bar{x}_i$. Порты маршрутизатора кодируются некоторыми двоичными числами $S$ длины $n$.

Предположим, что клиент $k$ отправляет клиенту $p$ некоторое сообщение из нескольких кубитов $|a_j>$. Для этого он дополняет сообщение номером порта получателя $b_i$, состоящему из $n$ двоичных чисел, как $|b_i> \otimes |a_j>$, где под тензорным произведением подразумевается зацепление пакета кубитов $|a_j>$ с пакетом кубитов $|b_i>$ в чистом состоянии. Физически это может означать и зацепление каждого кубита $|a_j>$, и каждого запутанного набора из $|a_j>$, и что-то другое в зависимости от протокола передачи кубитов и способа формирования пакета. В данном случае, пакет $|a_j>$ формируется как тензорное произведение незацепленных кубитов, а в качестве протокола связи на физическом уровне выбран, например, оптоволоконный канал связи.

Маршрутизатор, получая пакет $|b_i> \otimes |a_j>$, проводит измерение первых $n$ бит, получая набор $b_i$, после чего с помощью алгоритма Гровера решает задачу нахождения набора битов, соответствующих решению $f(x_i \oplus b_i) = 1$, тем самым получая $S$ – код порта, на который необходимо отправить оставшийся пакет $|a_j>$.

**Особенности схемы маршрутизации**

В рамках изучения данной схемы можно выделить то, что все коды портов должны быть определены заранее и согласованы с заранее выбранными адресами, что делает систему менее гибкой. С другой стороны, определив функцию *f* на маршрутизаторе и количество $l$ подключенных к нему устройств, можно делегировать ему генерацию пар $(b_i^l, S^l)$ и выдачу каждому КВМ полного набора $b_i^l$. Тем самым предполагая, что злоумышленник завладеет адресами с одной из КВМ и узнает адреса всех устройств с идеей в последствие «нарушить» канал связи на физическом уровне между нежелательными ему устройствами, он не сможет определить соответствие между адресами и кодами портов, даже имея в своем распоряжении КВМ, за неимением функции *f*.

Сам маршрутизатор не хранит решения задач маршрутизации в готовом виде, поэтому их невозможно выкрасть обычным способом. Стоит также сказать, что дополнительные затраты на решение задач на маршрутизации каждого пакета сглаживаются тем, что задача решается Алгоритмом Гровера. Более того, при правильной организации вентилей на физическом уровне такой способ маршрутизации будет работать быстрее, чем обычный поиск порта по номеру, каким бы странным это не казалось.

Слабым местом данной системы является функция *f*, зная которую злоумышленник может без труда находить коды портов по адресам, поэтому главным местом для защиты должна быть защита функции на физическом (в виде «оракула») уровне, а также противодействие «coffee-break» атаке.

Отметим также возможную масштабируемость такой схемы – соединяя маршрутизаторы между собой и используя таблицы маршрутизации, где вместо

номеров портов будут записаны коды портов, возможно обеспечить маршрутизацию на нескольких уровнях сети. Для адресации в таком случае потребуется либо добавлять дополнительные служебные кубиты до отправки, либо добавлять их на каждом роутере, что, в принципе, не является затруднительным.

**Возможные направления исследования**

1) Исследовать возможность замены протоколов на другие протоколы соответствующего уровня, например, использовать BB92 для генерации ключей вместо BB84.

2) Для физического уровня возможно провести качественное и количественное сравнение метода распределения ЭПР-пар с идеей квантовой телепортации и передачи кубитов по квантовому каналу, например, оптоволокну.

3) Исследовать алгоритм раздачи ЭПР-пар, а также большего числа спутанных кубитов, для многоранговых сетей.

4) Провести сравнительный анализ различных сетевых топологий и их возможностей для объединения КВМ для распределения ресурсов.

5) Исследовать возможность построения маршрутизации на основе других быстро разрешимых для КВМ задач.

**Заключение**

Представляет большой интерес дальнейшее исследование методов коммуникации между КВМ. В данной работе описаны метод квантовой телепортации, Алгоритм Гровера, протокол квантового распределения ключей BB84. Предложена схема маршрутизации для сетевой топологии квантовых устройств типа «Звезда». Описан принцип работы, а также особенности данной схемы. Рассмотрены возможные подходы к развитию идеи пакетной коммутации кубитов и предложены направления для дальнейшего изучения.

## СПИСОК ЛИТЕРАТУРЫ

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ. – М.: Мир, 2006. – 824 с.

2. Ключарев П.Г. Основы квантовых вычислений и квантовой криптографии // Вестник МГТУ им. Н.Э. Баумана. – 2006. – № 2 (63). – С. 36-46. Сер. “Приборостроение”.

3. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. – 1997. – Pp. 1484-1509.

4. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. – М.: МЦНМО–ЧеРо, 1999. – 192 с.

5. Холево А.С. Введение в квантовую теорию информации. – М.: МЦНМО, 2002. – 128 с.

6. Ян С.Й. Криптоанализ RSA. – М.-Ижевск: НИЦ «Регулярная и хаотическая динамика». – Ижевск: Ижевский институт компьютерных исследований, 2011. – 312 с.

7. Rieffel E., Polak W. Основы квантовых вычислений // Квантовые компьютеры и квантовые вычисления. – 2000. – № 1 (1). – С. 4-57.

8. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – СПб.: Питер, 2020. – 1008 с.

9. Таненбаум Э., Уэзеролл Д. Компьютерные сети, 5-е изд. – СПб.: Питер, 2012. – 960 с.