КВАНТОВЫЕ УЗЛОВЫЕ КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ПЛАТЕЖЕЙ

В статье предложен вариант электронного протокола взаиморасчетов. Протокол квантовых платежей физически не допускает копирования не уполномоченными лицами. Взлом квантового протокола сложнее, чем классического.

Ключевые слова: платеж, квант, криптография, протокол, компьютер, полином Александера, перемещение Редемейстера, цепь.

QUANTUM BUNDLE CRYPTOGRAPHIC PAYMENT PROTOCOL

The paper deals with protocol for information-theoretically secure private-key quantum payment. Quantum payment is a cryptographic protocol in which a mint can produce a quantum state, no one else can copy the state, and anyone (with a quantum computer) can verify that the state came from the mint.

Keywords*:* quantum, payment, cryptographic, protocol, computer.

.

Безналичные платежи осуществляются с использованием протоколов разной степени защищенности. Методы защиты основаны на сложности воспроизводства купюр, монет или электронной подписи, сертификата. Квантовые протоколы[1-12] взаиморасчетов защищены физической невозможностью копирования, а следовательно — невозможности подделки. Защищенные платежи нуждаются в криптографическом протоколе, с помощью которого производитель может создать состояние, которое невозможно скопировать, и любой человек с помощью компьютера может удостовериться, что это состояние исходит от производителя. Рассмотрим конкретный протокол, базирующийся на суперпозициях диаграмм, кодирующих направленные цепи полиномов[2,3,5,7]. Протокол основан на узлах[13]. Безопасность схемы строится на том, что для двух отличных по внешнему виду, но эквивалентных состояний сложно найти реальный способ превращения одного в другое. Одна из главных проблем безопасности —

возможность физического копирования информации. Воспроизводя и пересылая такую информацию, агент обладает оригиналом. Особенность электронной коммерции — необходимость соединения с сервером для любой транзакции. Идея квантовых платежей базируется на теореме о невозможности клонирования квантового состояния[4]. Такие платежи избавляют от контакта с центральной базой данных, т.е. от авторизации, и одновременно решают проблему безопасности. Систему квантовых платежей сложнее взломать. Для использования квантового состояния требуется возможность его производства, проверки без повреждений и невозможность взлома. Схема квантовых платежей содержит собственно образец платежки и алгоритм проверки *M*. Обычно имеется серийный номер *p* (который присваивается производителем) с привязанным квантовым состоянием $|\$_p\rangle$ из *n* кубитов. Алгоритм проверки *M* принимает как данные квантовое состояние $|\phi\rangle$ и серийный номер *q*, а затем решает, является ли такая пара (*q*, $|\phi\rangle$) частью квантовых денег. Если получаемые данные говорят о том, что деньги подлинные, тогда проверка также возвращает состояние $|\phi\rangle$ не поврежденным. Таким образом, это состояние можно использовать снова. То есть существует алгоритм, производящий и состояние квантовых денег, и серийный номер *p*. Запуск алгоритма проверки *M* с вводом *p* и $|\$_p\rangle$ возвращает положительный результат и не повреждает $|\$_p\rangle$. Более того, любой, имеющий доступ к квантовому компьютеру, может запустить алгоритм проверки *M*. Если существует один кусок квантовых денег (*p*, $|\$_p\rangle$), то сложно сгенерировать квантовое состояние $|\psi\rangle$ для *2n* кубитов, такое, что каждая часть $|\psi\rangle$ (вместе с оригинальным серийным номером) пройдет алгоритм проверки. Что остановит злоумышленников от использования того же алгоритма для производства фальшивых состояний? Необходимость в аутентификации. Когда производитель выпускает деньги, он производит набор пар (*p*, $|\$_p\rangle$). В нашей схеме квантовых денег, производитель не создает серийные номера заранее. Их создание — абсолютно случайный процесс.

Можно получить новый набор пар, но с большой долей вероятности ни один из серийных номеров не будет соответствовать оригинальным серийным номерам, которые были созданы производителем. Простой способ убедиться в безопасности для производителя— публикация списка настоящих серийных номеров, а для бизнесменов — проверка по этому списку, является ли серийный номер проверяемых денег аутентичным. Альтернатива спискам — цифровая подпись серийного номера. Существуют протоколы цифровых подписей, которые позволяют любому, обладающему ключом, убедиться в том, что серийный номер был действительно создан конкретным производителем. Тем не менее, описание серийного номера можно легко скопировать. Здесь вступает в действие квантовая безопасность: знание серийного номера p не означает, что можно скопировать соответствующее квантовое состояние. Квантовые платежки с точки зрения конечного пользователя будут либо файлами на квантовом компьютере, либо другим материальным платежным средством с прикрепленным квантовым состоянием. До сих пор не до конца разрешен вопрос создания защищенных квантовых платежек, которые не требуют вмешательства производителя для использования. Можно выбрать обычный шифр для создания квантового состояния, привязанного к деньгам, и серийного номера. Нужно, чтобы скопировать квантовые деньги без знания этого шифра было очень тяжело. Одной из идей является схема, которая основана на состояниях. Сначала производитель выбирает случайное состояние из n кубитов. Затем строится набор проекций $|\psi_i\rangle\langle\psi_i|$ при $i \in \{1,...m\}$ так, чтобы это состояние являлось нулевым собственным вектором каждой проекции. Здесь m достаточно велико, чтобы состояние являлось единственным состоянием в общем нулевом собственном пространстве. Серийный номер, соответствующий состоянию – это цепочка битов, которая описывает каждую проекцию. Чтобы подтвердить состояние $|\phi\rangle$, измеряются все проекции $|\psi_i\rangle\langle\psi_i|$, и состояние подтверждается тогда и только тогда, когда все результаты равны 0. К сожалению, такая модель не является безопасной. Было доказано, что при

наличии образца квантового состояния и соответствующего серийного номера можно узнать шифр. Надежнее использовать механизм, основанный не на шифре, а на сложности создания суперпозиции. Эта идея разрабатывается. Ниже представлена схема квантовых денег, которая не основывается на квантовых предсказаниях и не требует связи с производителем для проверки подлинности. Производитель начинает с создания единообразной суперпозиции

$$|initial\rangle = \frac{1}{\sqrt{|B|}} \sum_{e \in B} |e\rangle|0\rangle \qquad (1)$$

где B – большое множество. Затем оно используется в некоторой функции f(e), принимая состояние, равное

$$\frac{1}{\sqrt{|B|}} \sum_{e \in B} |e\rangle|(\mathrm{f(e)}\rangle \qquad (2)$$

Наконец, производитель измеряет значение f. Если результатом измерения является v, то остаточное состояние равно

$$|\$_v\rangle|v\rangle = \frac{1}{\sqrt{N_v}} \sum_{e \in B} |e\rangle|v\rangle \qquad (3)$$

Таким образом, квантовые деньги представляют собой простой серийный номер v и квантовое состояние. Для проверки состояния нужно сначала измерить значение f в данном состоянии, чтобы удостовериться, что оно соответствует значению v. Затем нужно проверить, находится ли состояние в единообразной суперпозиции состояний с теми же значениями v для f. Непонятно, каким образом можно убедиться в единообразии суперпозиции, и в нашей схеме это будет одним из главных препятствий. Для работы такой схемы должны выполняться следующие требования:

- измерение функции f на двух незапутанных копиях исходного состояния должно давать различные значения с вероятностью, экспоненциально

близкой к 1; иначе взломщик может просто повторить действия производителя, и получить нужное ему состояние.

- для большинства значений v должно быть экспоненциальное количество исходных состояний e, таких, что $f(e) = v$. Более того, даже имея одно состояние $|e\rangle$ при $f(e) = v$, должно быть сложно создать единообразную суперпозицию для всех таких же состояний.

- проверяющий должен иметь возможность убедиться в том, что он располагает единообразной суперпозицией над состояниями с такими же значениями f. Чтобы воплотить в жизнь идею о квантовых платежах , используется теория узлов. Первоначально создаваемое состояние является единообразной суперпозицией над планарными решеточными диаграммами, которые являются представлениями ориентированных цепей (ориентированный узел – узел с предпочтительными направленностями в него, а ориентированная цепь представляет собой набор предположительно связанных ориентированных узлов). Измеряемая производителем функция f является полиномом Александра от ориентированной цепочки, представленной данной решеточной диаграммой. Наконец, процедура проверки основывается на перемещениях Редемейстера, которые не изменяют значение полинома (перемещения Редемейстера превращают узел в другой эквивалентный узел, а полиномы Александра для эквивалентных узлов равны). Кратко рассмотрим концепцию узлов и цепей, а также их представление с помощью диаграмм. Один узел может быть представлен разными диаграммами разными способами; перемещения Редемейстера представляют собой определенное количество локальных изменений в диаграмме, которые не изменяют сам узел или цепь. Мы рассмотрим, как вычислить полином Александра для данной диаграммы ориентированной цепи за полиномиальное время. Полином Александра является инвариантой цепи, то есть, если вычислить ее значение для диаграммы, которая представляет собой такую же ориентированную цепь, мы получим тот же полином. Наконец, мы рассмотрим планарные решеточные диаграммы и

перемещения, с помощью которых можно применять перемещения Редемейстера к решеточным диаграммам. Можно представить узел как трехмерную петлю, которая является отображением S^1 на R^3. Так как нарисовать узел в трех измерениях сложно, обычно он представляется проекцией 3D-объекта на двухмерную плоскость, где на каждом пересечении отмечено, какая ось проходит выше, а какая ниже. Такая диаграмма называется узловой диаграммой. Интересны примеры цепей, которые соответствуют одному или более сплетений (которые называют компонентами цепи). Ориентированной цепью называют цепь, каждая компонента которой имеет направление. Две цепи (или узла) равны, если один из них можно превратить в другой без прерывания связи. Если неориентированные цепи K_1 и K_2 равны, и они представлены схемами D_1 и D_2 соответствующим образом, то D_1 можно превратить в D_2 (и наоборот), используя перемещения Редемейстера[11]. Для ориентированных цепей можно нарисовать перемещения Редемейстера с такими же схемами, но с направлениями, проведенными по краям, которые должны согласоваться как до, так и после применения перемещений. В случае, если две схемы можно обратить в одну и ту же форму путем применения перемещений, то эти схемы соответствуют равным цепям. Расширяя это утверждение, получаем теорему.

Полином Александра – полином $\Delta(x)$, который можно вычислить из имеющейся схемы ориентированной цепи, и который будет инвариантен под действием перемещений Редемейстера. В этом разделе будет описан алгоритм вычисления полинома. Вычисление $\Delta(x)$ может быть проведено за полиномиальное время за число пересечений схемы.

Представим, что нам дана схема L. Если схема не соединена, применим перемещение Редемейстера для соединения. Пусть a – число пересечений схемы. Тогда кривая диаграммы разделяет двухмерную плоскость из $a+2$ разделов, включая один бесконечный (это следует из формулы Эйлера).

Следующий алгоритм используется для вычисления $\Delta(x)$:

1) Для каждого раздела $i \in \{1,\dots,a+2\}$ введем соответствующую a переменную

r_i.

2) Для каждого *a* пересечения запишем уравнение

$$xr_j - xr_k + r_l - r_m = 0 \qquad (4)$$

где $\{r_j, r_k, r_l, r_m\}$ – переменные, соотнесенные с разделами, смежными с пересечениями,

3) Запишем систему уравнений как матричное уравнение

$$M\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{m+2} \end{pmatrix} = 0 \qquad (5)$$

Матрица *M* имеет *a* строчек и *a+2* столбцов. В ней содержатся элементы множества $\{\pm 1, \pm x, 1+x, 1-x, -1+x, -1-x\}$.

4) Удалим 2 столбца матрицы *M*, которые соответствуют смежным разделам в схеме цепи. Таким образом, получим $a \times a$ матрицу M_0.

5) Детерминируем матрицу M_0, получим полином *x*. Разделим этот полином на множитель $\pm x^q$, чтобы сделать младший член положительной константой. Полученный полином будет полиномом Александра $\Delta(x)$ для данной цепи.

Когда мы говорим о полиноме Александра в данной работе, мы подразумеваем список коэффициентов, а не значение полинома, соотнесенное с каким-либо *x*. Уравнение $xr_j - xr_k + r_l - r_m = 0$ соотносится с каждым пересечением, в котором смежные разделы $\{r_j, r_k, r_l, r_m\}$ помечены соответствующим образом. Заметьте, что пометка смежных разделов зависит от того, какая ось находится сверху при пересечении. Удобно представлять узлы в виде планарных решеточных диаграмм. Планарная решеточная диаграмма – решетка $d \times d$, на которой мы отмечаем *d* X и *d* O. В каждой строчке и в каждом столбце должен быть один X и один O, но одновременное

нахождение X и O в одной клетке невозможно. Нарисуем горизонтальную прямую в каждой строке между O и X, и вертикальную прямую между X и O в каждом столбце. В месте пересечения горизонтальной и вертикальной прямых вертикальная прямая всегда находится над горизонтальной.

Узлы (либо цепи) в решеточной диаграмме имеют неявное направление: каждая вертикальная граница проходит от X до O, а каждая горизонтальная граница - от O до X. Планарная решеточная диаграмма G может быть детально раскрыта двумя несовместными перестановками $\pi_{X,}\pi_O \in S_d$, в случае чего X получат координаты $\{(i,\pi_X(i))\}$, а O – $\{(i,\pi_O(i))\}$ для $i \in \{1,...,d\}$. Две перестановки являются несовместными, если для всех $i\pi_X(i) \neq \pi_O(i)$. Таким образом, любые две несовместные перестановки $\pi_{X,}\pi_O \in S_d$ определяют планарную решеточную диаграмму $G=(\pi_X,\pi_O)$. Каждая цепь может быть представлена многими различными решеточными диаграммами.

Можно определить решеточные перемещения, которые имеют три типа перемещений (или трансформаций) на планарной решеточной диаграмме, которые, как перемещения Редемейстера для цепей, необходимы для образования всех планарных решеточных диаграмм одной направленной цепи. Первый тип перемещения – цикличная перестановка либо строк, либо столбцов. Можно представить это перемещение как перетаскивание двух маркеров в крайний правый столбец путем их перетягивания за страницу, и помещая их обратно вниз слева. Такие перемещения возможны всегда. Второй тип перемещения – перестановка двух смежных строк или столбцов. Оно возможно только в случае, если ни одна связь не порвется. Возможность такого перемещения зависит от положения маркеров в строках или столбцах.

Третий тип перемещения – добавление либо удаление одной строки и столбца (стабилизация или дестабилизация). Дестабилизация выбирает 3 маркера L-формы со сторонами длиной 1 и сжимает их в один. Таким образом, удаляется одна строка и один столбец. Обратное перемещение выбирает любой маркер, добавляет строку и столбец, смежные с этим

маркером, и заменяет этот маркер на 3 новых маркера. Любые X и O могут быть стабилизированы, а любые 3 маркера L-формы с единичной длиной – дестабилизированы, если только они не образуют «коробочку» (например, 2×2 с маркером во всех четырех положениях). Базисные векторы Гильбертова пространства – решеточные диаграммы $|G\rangle = |\pi_X, \pi_O\rangle$, где каждая решеточная диаграмма *G* представлена несовместными перестановками π_X, π_O. Измерение *d(G)* - число элементов в перестановках. Число несовместных пар перестановок *d* элементов равно *d!* числу перестановок, которые не имеют фиксированной запятой. Последнее значение называют числом расстройств на *d* элементов, и оно равно $\left[\frac{d!}{e}\right]$, где скобки показывают ближайшую целую функцию.

Чтобы создать квантовые деньги, производитель сначала выбирает параметр безопасности *D* и определяет ненормальное распределение

$$y(d) = \begin{cases} \dfrac{1}{d!\left[\dfrac{d!}{e}\right]} \exp\dfrac{-(d-\overline{D})^2}{2\overline{D}} & if\ 2 \le d \le 2D \\ 0 \end{cases} \qquad (6)$$

Определим целочисленную функцию

$$q(d) = \left\lceil \frac{y(d)}{y_{\min}} \right\rceil \qquad (7)$$

где $\lceil \cdot \rceil$ означает округление в большую сторону, а $y_{\min}$ – наименьшее значение *y(d)* при $d \in 2,...,2\overline{D}$ (необходимо распределение с целым значением). Затем производитель использует алгоритм для подготовки состояния (включая нормализацию)

$$\sum_{d=2}^{2\overline{D}} d!\sqrt{q(d)}|d\rangle \qquad (8)$$

Используя прямую единичную трансформацию, воздействуя на это состояние

и на дополнительную запись, производитель получает

$$\sum_{d=2}^{2\overline{D}} d!\sqrt{q(d)}\left|d\right\rangle\left(\frac{1}{d!}\sum_{\pi_X,\pi_0\in S_d}\left|\pi_X,\pi_0\right\rangle\right) \qquad (9)$$

и затем проверяет, являются ли 2 перестановки π_X,π_O несовместными (они являются несовместными с вероятностью, близкой к *1/e*). Если производитель получает несовместный результат измерения, он пересчитывает измерение *d* в первой записи для получения исходного состояния $\left|initial\right\rangle$ в последних двух записях, где

$$\left|initial\right\rangle = \frac{1}{\sqrt{N}}\sum_{\substack{grid\\diagrams\\G}}\sqrt{q(d(G))}\left|G\right\rangle \qquad (10)$$

а *N* – нормализующая константа. Если результат измерения не может быть определен, нужно начинать вычисления заново.

Распределение *q(d)* выбирают таким образом, что если нужно измерить *d(G)* на $\left|initial\right\rangle$, то тогда распределение результатов будет очень сильно приближенным к распределению Гаусса, что означает, что *D* ограничено границами интервала $\left[2,2\overline{D}\right]$. При увеличении *D*, недостающий вес в отклонении стремится к нулю.

Из состояния $\left|initial\right\rangle$, производитель вычисляет полином Александра *A(G)* для другой записи, и затем измеряет эту запись, получая полиномиальное *p*. Результирующее состояние -$\left|\$_p\right\rangle$, полная суперпозиция всех решеточных диаграмм (включая *2D* размерности) с полиномом Александра *p*

$$\left|\$_p\right\rangle = \frac{1}{\sqrt{N}}\sum_{G:A(G)=p}\sqrt{q(d(G))}\left|G\right\rangle \qquad (11)$$

где N отвечает за нормализацию. Квантовые деньги состоят из состояния $|\$_p\rangle$, и серийного номера, которым является полиномиальное p, представленное списком коэффициентов. Если полиномиальное p равно 0, то производитель должен начать создавать состояние заново. Проверка квантовых платежей возможна различными способами. Если вам передают квантовое состояние $|\phi\rangle$ и серийный номер, который соответствует полиномиальному числу p, и уверяют вас, что это подлинный квантовый платеж. Чтобы удостовериться в подлинности в этом случае, вы можете использовать следующий алгоритм проверки

0. удостоверьтесь, что $|\phi\rangle$ является суперпозицией базисных векторов, которые верно кодируют решеточные диаграммы. Если операция произведена успешно, перейдите к пункту 1,

1. вычислите полином Александра для состояния $|\phi\rangle$. Если результат измерения – p, перейдите к пункту 2. В противном случае закончите алгоритм,

2. измерьте проекции на решеточные диаграммы в области $\left[\frac{\overline{D}}{2};\frac{3\overline{D}}{2}\right]$. Если вы получите значение «+1», продолжите работу. В противном случае, закончите алгоритм. Для подлинных денег вы будете получать результат «+1» с высокой долей вероятности и не сильно повредите состоянию,

3. примените алгоритм проверки цепей Маркова, описанный в разделе 3.2.2. Если состояние пройдет проверку, то оно является подлинным.

Если платеж проходят шаги проверки 0 и 1, тогда $|\phi\rangle$ – суперпозиция решеточной диаграммы с верным полиномом Александра p. Шаги 2 и 3 подтвердят, что $|\phi\rangle$ является верной суперпозицией решеточной диаграммы. Такая процедура будет определять подлинные квантовые

состояния с высокой вероятностью, но, как упоминалось выше, будут и другие состояния, которые могут пройти проверку. Но такие состояния крайне тяжело создать. Возможен следующий алгоритм проверки цепей Маркова: 1) возьмем вводимое состояние $|\phi\rangle$, сделаем вторичную запись, которая содержит $i \in \{0,...,q_{\max}\}$, и создадим состояние

$$|\phi'\rangle = U(|\phi\rangle|0\rangle) \quad (12)$$

используя унитарность *U*, определенную выше;

2) присоединим вторичную запись, которая содержит $s = \{1,...,|S|\}$, и приведем эту запись в состояние $\sum_s \frac{1}{\sqrt{|S|}}|s\rangle$; таким образом, получим состояние

$$|\phi'\rangle\sum_s \frac{1}{\sqrt{|S|}}|s\rangle \quad (13)$$

в трех записях (в одной содержится решеточная диаграмма *G*, вторая содержит целые $i \in \{0,...,q_{\max}\}$, третья содержит целые $s = \{1,...,|S|\}$);

3) повторим *r = poly(D)* раз:

а) применим унитарность *V*, где

$$V = \sum_s P_s \otimes |s\rangle\langle s| \ , \quad (14)$$

данный оператор делает перестановку P_s первых двух записей, в зависимости от значений *s* в третьей записи;

б) вычислим проекцию

$$Q = I \otimes I \otimes \left(\sum_{s,s'} \frac{1}{S}|s\rangle\langle s'| \right) ; \quad (15)$$

4) если вы получили значение «1» для каждого из *r* повторений – платеж подлинный. В таком случае используйте U, а затем удалите первую и вторую записи. Конечное состояние первой записи – выходное состояние квантового платежа. В случае если значение «1» не было получено для каждой *r*-ой итерации – подлинность такого платежа сомнительна.

Для квантового состояния $|\$_p\rangle$ связанное состояние $|\$'_p\rangle\sum_s \frac{1}{\sqrt{|S|}}|S\rangle$, созданное на 1 и 2 шагах, не изменится от использования *V* в шаге 3а. Вычисление проекции *Q* для этого состояния в шаге 3б практически всегда дает +1. Таким образом, для подлинных квантовых платежей все результаты измерений равны +1, тогда квантовые платежи проходят проверку.

Теперь давайте проверим результат применения вышеописанного алгоритма к общему состоянию $|\phi\rangle$. Первый шаг алгоритма – создание $|\phi'\rangle = U(|\phi\rangle|0\rangle)$. Если единичная итерация в шаге 3 дает 1, то конечное состояние первых двух записей равно

$$\frac{\frac{1}{|S|}\sum_s P_s|\phi'\rangle}{\left\|\frac{1}{|S|}\sum_{s,t} P_s|\phi'\rangle\right\|} \tag{16}$$

Вероятность этого равна

$$\left\|\frac{1}{|S|}\sum_s P_s|\phi'\rangle\right\|^2 \tag{17}$$

Данная процедура повторяется *r* раз, а вероятность получения всех выходных единиц равна

$$\left\|\left(\frac{1}{|S|}\sum_s P_s\right)^r|\phi'\rangle\right\|^2 \tag{18}$$

В этом случае конечное состояние (в первых двух записях) равно

$$\frac{\left(\frac{1}{|S|}\sum_s P_s\right)^r|\phi'\rangle}{\left\|\left(\frac{1}{|S|}\sum_s P_s\right)^r|\phi'\rangle\right\|} \tag{19}$$

Чтобы было возможно предугадать, какие состояния пройдут хотя бы первую итерацию данной проверки с достаточно большой долей вероятности,

отметим, что состояние $\frac{1}{|S|}\sum_s P_s|\phi'\rangle$ может всего лишь быть достаточно близким к 1, если большинство условий было добавлено когерентно. Другими словами, большинство $P_s|\phi'\rangle$ должны быть практически идентичными (для подлинных платежей они и будут идентичными).

Так как $\frac{1}{|S|}\sum_s P_s = B$ – наша матрица Маркова, множество состояний, прошедшее все стадии проверки, напрямую зависит от смешиваемости цепей Маркова – эти состояния соответствуют собственным векторам *B* с собственными значениями, приближенными к 1. Рассмотрим безопасность квантовых платежей. Состояния квантовых платежей возможно создать, а также они проходят проверку подлинности с высокой вероятностью. Квантовые платежи тяжело подделать. Рассмотрим 4 типа атак.

Во-первых, взломщик может попытаться получить подлинное квантовое состояние $|\$_p\rangle$, чтобы узнать решеточную диаграмму с полиномом Александра *p*, и затем создать суперпозицию, содержащую такую же диаграмму, чтобы пройти проверку подлинности. Такое состояние будет суперпозицией для решеточных диаграмм, равных начальной диаграмме. Если бы взломщик смог сделать это, можно было бы использовать такой алгоритм взлома для определения равенства решеточных диаграмм (представляют ли две решеточных диаграммы одну и ту же связь). Но такого рода задача представляет собой проблему даже для квантовых компьютеров.

Во-вторых, существуют двумерные диаграммы *2D* (наибольшее решеточное измерение), в которых нет перемещений, которые могли бы понизить измерение (это следует из того, что каждая связь представлена наименьшим измерением решеточной диаграммы). Так как перемещения, повышающие значение измерения больше, чем на 2, запрещены, то начиная с одной из решеточных диаграмм с измерением *2D*, цепь Маркова будет смешивать небольшое множество диаграмм одного измерения. Единообразная суперпозиция этих множеств может пройти 3ий шаг проверки, однако 2ой

шаг создан для того, чтобы фильтровать такого рода суперпозиции. В-третьих, если цепь Маркова плохо смешается, то получатся собственные состояния матрицы *B* с собственными значениями, приближенно равными +1. Для таких собственных состояний могут быть созданы фальшивые квантовые деньги, которые пройдут проверку подлинности. Неизвестно, существуют ли такие состояния, и даже если существует, неясно, как их создать. Фактически, намного более простая задача, как, например, проверка равенства двух решеточных диаграмм, требующая супер полиномиального числа решеточных перемещений от одной к другой (либо доказательство того, что такие диаграммы не существуют), является очень трудновыполнимой.

В-четвертых, может попробовать использовать подлинное состояние $|\$_p\rangle$ и попытаться создать $|\$_p\rangle \otimes |\$_p\rangle$ (или какое-либо переплетенное состояние в двух записях, где каждая запись пройдет проверку подлинности). Такой атакой смогли взломать производственное состояние квантовых денег путем применения квантового восстановления. Тем не менее, в этом случае такая атака сработала, потому что производственное состояние содержало обычный шифр, который атакующий узнал, чтобы взломать состояние. В данной работе не содержатся какие-либо шифры, спрятанные в алгоритме проверки, и шпион не может использовать их в силу их отсутствия. Вышеперечисленные методы атаки – все способы, защиту от которых можно продумать. Любая реализация классических криптографических протоколов должна быть очень аккуратна, дабы избежать появления недостатков, допускающих уменьшение безопасности по сравнению с правильно используемым протоколом. Квантовые платежи безопаснее классических. Но это потребует еще более тщательной аппаратной реализации.

Список литературы

1. М.Нильсен, И.Чанг. Квантовые вычисления и квантовая информация. М.: Мир,

2006.

2. Farhi E., Gosset D., Hassidim A., Lutomirski A., Shor P. Quantum money from knots. *http://arxiv.org/pdf/1004.5127* (дата обращения 11.3.11)
3. Qin Li, Dongyang Long, Changji Wang Efficient Quantum Signature and Its Application in On-line Quantum Payment System http://arxiv.org/PS_cache/arxiv/pdf/0806/0806.0557v2.pdf (дата обращения 13.3.11)
4. Ezhov A.A. Role of interference and entanglement in quantum neural processing http://arxiv.org/ftp/quant-ph/papers/0112/0112082.pdf (дата обращения 13.3.11)
5. Lutomirski A. An online attack against Wiesner's quantum money http://arxiv.org/PS_cache/arxiv/pdf/1010/1010.0256v1.pdf (дата обращения 10.3.11)
6. Lutomirski A, Aaronson S, Farhi E, Gosset D, Hassidim A, Kelner J, Shor P. Breaking and making quantum money: toward a new quantum cryptographic protocol http://arxiv.org/PS_cache/arxiv/pdf/0912/0912.3825v1.pdf (дата обращения 11.3.11)
7. Farhi E, Gosset D, Hassidim A, Lutomirski A., Nagaj D., Shor P. Quantum state restoration and single-copy tomography http://arxiv.org/PS_cache/arxiv/pdf/0912/0912.3823v1.pdf (дата обращения 4.3.11) Mosca M., Stebila D. Quantum Coins http://arxiv.org/PS_cache/arxiv/pdf/0911/0911.1295v1.pdf (дата обращения 1.3.11)
8. Dieng L.M. Quantized interest rate at the money for american options. http://arxiv.org/ftp/arxiv/papers/0902/0902.4684.pdf (дата обращения 1.3.11)
9. Pitowsky I. Betting on the Outcomes of Measurements: A Bayesian Theory of Quantum Probability http://arxiv.org/PS_cache/quant-ph/pdf/0208/0208121v1.pdf (дата обращения 1.2.11)
10. Ilinski K.N., Stepanenko A.S. Electrodynamical model of quasi-efficient financial market. http://arxiv.org/PS_cache/cond-mat/pdf/9806/9806138v1.pdf(дата обращения 2.3.11)
11. Ilinski K.N. Physics of Finance http://arxiv.org/PS_cache/hep-th/pdf/9710/9710148v1.pdf(дата обращения 3.3.11)
12. Hoi-Kwong Lo Insecurity of Quantum Secure Computations http://arxiv.org/PS_cache/quant-ph/pdf/9611/9611031v2.pdf(дата обращения 3.3.11)
13. Мантуров В.О. Теория узлов. М. - Ижевск, 2005, с.326-341.