Схемы квантовых платежей.

Принцип неопределённости и теорема о запрете клонирования в квантовой механике сделали квантовые деньги одним из магистральных направлений исследований в рамках квантовой теории информации. Возможность создания цифровых денег, не подверженных подделке благодаря законам физики, представляется захватывающей идеей. Классические электронные деньги всесторонне исследованы, при этом степень их защиты постоянно повышается, но она принципиально ограничена тем, что обычные биты информации могут быть элементарно скопированы. Что касается квантовых денег, для предотвращения подделок рассчитывают использовать невозможность точного копирования квантовых состояний. Помимо невозможности подделывания, эффективная система кибернетических денег должна обладать и такими характеристиками, как возможность лёгкой верификации, анонимность, оборотистость и надёжность.

В рамках данной статьи опишем новый вид квантовых денег, называемый квантовыми монетами, где все монеты одного номинала представлены идентичными квантовыми состояниями. Формально определим, что понимается под исключением возможности подделки и опишем, как внедрить систему квантовых монет, используя операции чёрного ящика и слепое квантовое вычисление. А также охарактеризуем квантовые банкноты, которые затрагивают широкий перечень понятий, связанных с квантовыми деньгами. Каждая выпущенная банком монета должна представлять собой копию того же самого квантового состояния, т.е., монеты должны быть абсолютно идентичны. Кроме того, монетам обеспечивается локальный оборот, чтобы подтвердить их действенность и затем передать для дальнейшего обращения. Будет описано изготовление квантовых монет при помощи квантовых схем чёрного ящика и слепого квантового вычисления. Невозможность подделки в рамках нашей схемы обеспечивается сложным теоретическим допущением, касающимся ограниченности времени действия злоумышленника. Работа отличается от предыдущих концепций квантовых денег, которые называют квантовыми банкнотами: в системе квантовых банкнот банк выпускает особые талоны, являющиеся обычными, либо квантовыми парами, которые, в общем, различны. Классическая строка банкноты может при этом служить серийным номером или содержать переменную, используемую в процедуре верификации. Проект квантовых монет подразумевает использование в процессе верификации машины-оракула, работающей по принципу чёрного ящика, но пока ещё не ясно как именно это осуществить. Открытыми остаются и вопросы о способе дестабилизации

верификационной схемы, чтобы она действительно функционировала как чёрный ящик, и о самой модели дестабилизации квантовых схем, использующей вычислительные допущения. Опишем, как слепое квантовое вычисление можно применить в контексте верификации квантовых монет, а также отметим имеющиеся ограничения, в частности, необходимость наличия квантового канала связи в режиме реального времени. Снижение коммуникационных и вычислительных требований к слепой квантовой обработке данных представляет собой проблему, заслуживающую дальнейшего изучения.

Несмотря на то, что монеты по своей природе анонимны, если банк не допускает ошибок при их выпуске, до сих пор нет механизма, позволяющего пользователям системы удостовериться, что монеты действительно произведены корректно, что также остаётся нерешённым вопросом. Ниже вкратце обсудим образцы квантовых банкнот. Связанная с квантовыми банкнотами проблема состоит в нахождении автономно верифицируемой системы квантовых банкнот; это может потребовать использования понятия вычислительной надёжности. Представленная ниже часть работы организована следующим образом. Опишем и цели системы квантовых денег и проанализируем существующие системы в соответствии с этими целями. Далее представим два базовых типа квантовых денег, квантовые монеты и квантовые банкноты, а также опишем их точные характеристики безопасности. Коснемся внедрения квантовых монет в модель чёрного ящика и отметим имеющиеся ограничения степени защищённости монет от подделки. В конце обсудим внедрение квантовых монет с использованием слепого квантового вычисления.

Исследования

Электронные деньги. Электронные деньги тщательно исследованы в классических криптографических контекстах. Причём первые схемы были предложены [1-4]. Что касается классических проектов электронных денег, одной из первостепенных проблем оказывается проблема их многократного использования. Если можно легко сделать копии классических электронных купюр, то должен существовать метод, не позволяющий распознавание тех же знаков более одного раза. Схема работы в реальном времени, в которой каждый знак подтверждается банком в момент, когда этим знаком что-то оплачивают, мгновенно решает эту проблему, но онлайн верификация требует наличия интерактивного канала связи между продавцом и банком. Другим универсальным способом борьбы с многократным расходованием является внедрение некоторой идентифицирующей информации в сами денежные знаки; в этом случае, если знаком

пользуются однократно, транзакция остаётся анонимной, но если расходование отмечается более одного раза, банк может идентифицировать недобросовестного держателя знака посредством анализа множественных расходных операций. Более того, классические электронные деньги не являются оборотистыми, если не сделать возможным линейное возрастание размера обозначения в ряде операций [5].

Квантовые деньги. Квантовые деньги стали одним из первых практических применений квантовой теории информации, и были введены ещё в ранних работах [6,7]. В обеих схемах банк создаёт различающиеся квантовые знаки и соответствующие классические серийные номера. Знаки представляют собой кодировку случайной строки из случайно выбранного базиса, состоящего из двух не ортогональных исходных кубитов. Теорема о запрете клонирования исключает возможность точного копирования отдельных знаков. Тем не менее, знаки может верифицировать только банк. Верификация требует знания базиса, избранного для каждого знака и для классической строки, которые могут быть получены посредством измерений в соответствующих базах. Следовательно, между продавцом и банком должен существовать интерактивный квантовый канал. Эти знаки не являются оборотистыми и анонимными. Tokunaga, Okamoto и Imoto [8] предлагают схему анонимных квантовых денег с верификацией в режиме реального времени. В их системе пользователь получает от банка отдельный знак; знаки генерируются при помощи личных параметров и случайных величин, хранимых банком. Впоследствии пользователь с целью получения анонимности изменяет знак случайным унитарным преобразованием. При платеже держатель предъявляет знак продавцу, который передаёт его (посредством квантового канала) банку для верификации. Схема работает против злоумышленников, которые могут проверить только один знак, но оказывается неэффективной против тех, кому удаётся получить и проверить все квантовые знаки. Если использовать труды [9,10], вводится сложная теоретическая концепция запрета клонирования, позволяющая отстаивать невозможность подделки квантовых монет. Первые резуьтаты были представлены в [11-13]. Позднее Aaronson [14] расширил своё исследование и также включил в него представление о квантовых деньгах [14], выдвинув сходные концепции.

Безопасность

Обсудим свойства хорошей финансовой схемы.

1. Анонимность. Схема должна быть создана таким образом, чтобы третьей стороне было сложно проследить использование лексем и понять, кто и где применял их.
2. Невозможность подделки. При наличии лексем проверочного цикла, фальсификатору, занимающемуся подделкой документов, будет сложно создать

лексему, которая с не пренебрежимой вероятностью сможет пройти процедуру проверки.

3. Эффективная локальная проверка. Необходим эффективный и высокоточный механизм, способный верно определять без общения с банком верность или поддельность лексем.

4. Возможность передачи и повторного использования. Действующие маркеры лексемы не должны подвергаться каким-либо изменениям во время процедуры проверки, а, следовательно, могут быть переданы и использованы в последующих процедурах проверки.

Далее определим невозможность подделки в подробной таблице с разными видами денег.

Ниже приведена краткая сводка финансовых схем и их свойств, где отмечено , каким из обозначенных выше целей удовлетворяют существующие сегодня финансовые схемы. В столбце «тип» указано, являются ли маркеры лексем данного номинала идентичными («монеты») или отличающимися («банкнота»). Отметим, что, хотя гарантировать невозможность подделки в классических цифровых денежных схемах нельзя, можно отследить двукратное использование маркеров лексем и их возврат к нарушителям. Однако, такие схемы предоставляют анонимность и выявление двойных расходов в режиме offline только с условными допущениями. Описываемые финансовые схемы предполагают «частичную» анонимность. Кроме того, возможный размер суммы электронных денег для их последующей передачи должен постоянно увеличиваться в соответствии с количеством перечислений [15].

Схема	Тип	Аноним-ность	Невозмож-ность подделки	Эффективная локальная проверка	Возможность передачи/перевода
Физические деньги (монеты)	Монета	Да	Физическая	Да	Да
Физические деньги (банкноты)	Банкнота	Нет	Физическая	Да	Да
Обычные электронные деньги	Банкнота	Да	Выявление двойных расходов	Да	Кол-во денег, которые можно передать, постоянно растет
[6]	Квантовая банкнота	Нет	Да	Нет	Нет
[7]	Квантовая банкнота	Нет	Да	Нет	Нет
[8]	Квантовая банкнота	Да	Да	Нет	Нет
Черный ящик	Квантовая банкнота	Частично	Да	Да	Да
Слепые	Квантовая	Частично	Да	Нет	Да

квантовые вычисления	банкнота				

Табл. Краткая сводка финансовых схем и их свойств [4].

Типы квантовых денег.

Квантовые монеты

В одном из типов квантовых денег, квантовых монет, банк выпускает множество маркеров лексем определенного номинала, и все эти маркеры лексем являются (или, как минимум, должны являться) копиями одного и того же квантового состояния. Например, состояние монеты должно быть чистым $|\psi_5\rangle$, и банк производит множество копий $|\psi_5\rangle^{\approx 1000000}$, назначая по одной копии на каждую монету. Термин «квантовые монеты» используем потому, что «физические» монеты, которые используются в реальном обращении, имеют точно такие же свойства: между двумя монетами одного номинала не должно быть видимой разницы. Спецификация квантовой финансовой схемы состоит из спецификации соответствующего состояния и цикла проверки.

Определение Схемой квантовой монеты является *пара* $(V,|\psi\rangle)$, *где* $|\psi\rangle$*является чистым состоянием* n*-кубита в* 2^n*-мерном пространстве Гильберта* H^{2n}*, а V представляет собой квантовый цикл с* n*-кубитным входным регистром (обозначенный как "p"), плюс дополнительный служебный входной регистр, классический выходной бит и квантовый выходной* n*-кубитный регистр.*

Далее будет приведен базовый план работы схемы квантовых денег. Банк производит большое количество квантовых монет и хранит их. Клиент снимает монеты из банка через свой личный квантовый канал и также хранит их. Когда клиент хочет потратить монеты, он переводит их продавцу через квантовый канал. Для проверки монет продавец использует квантовый цикл. Эта процедура может включать классическую или квантовую связь (коммуникацию) с банком. В конце концов, продавец хранит эти монеты у себя до тех пор, когда не вернет их в банк или не использует в качестве сдачи другим клиентам.

Проверка

В большинстве ситуаций цикл проверки V работает на трех регистрах: 1-кубитный регистр считывания данных, n-кубитный входной регистр и произвольный m-кубитный служебный входной регистр. После применения V измеряется первый регистр, в результате выносится решение о том, действительным или поддельным является проверяемый маркер лексем. Если входящим элементом является действительная квантовая монета$|\psi\rangle$, тогда, после необходимых измерений и применения V, классический выход должен равняться 0, а частичный след от первого и третьего регистров должен оставить второй регистр в его изначальном состоянии$|\psi\rangle$. Диаграмма универсального цикла проверки схемы квантовых денег представлена в [12]. Нельзя представлять этот цикл публично полностью, так как в таком случае появится возможность глубокого анализа цикла и последующей подделки денежных средств. Ниже приводятся описания двух техник безопасного использования этого цикла. В ходе проверки черного ящика допускается проведение проверочного цикла и делается вывод о безопасности на основе сложных теоретических вычислений. Слепые квантовые вычисления позволяют одной из сторон выполнить операцию без сбора информации о других, уже выполненных операциях, а безопасность является теоретико-информационной. Таким образом, схема основана на вычислительных допущениях.

Невозможность подделки

Допустим, у человека, который собирается совершить подделку, имеются данные о цикле проверки V и большинство (или все) выпущенные банком маркеры лексем, например их k штук. Целью злоумышленника является создание изделий, которые с большой вероятностью пройдут более k проверок на подлинность. Поскольку цикл проверки предполагает состояние, принадлежащее к подпространству определенному$|\psi\rangle$, можно сказать, что этот процесс эквивалентен созданию состояния, имеющего достаточное частичное совпадение с состоянием$|\psi\rangle^{k+1}$.

Определение

Схема квантовых денег $(V,|\psi\rangle)$, где $|\psi\rangle$является n-кубитным состоянием, оказывается защищенной от подделок при заданном цикле проверки V и k копиях состояния $|\psi\rangle$, для любого $k\geq 0$, $k\in poly(n)$. Таким образом, злоумышленник, действующий во временном промежутке poly(n), не сможет добиться создания состояния p, так что $\langle\psi|¤k+1_\rho|\psi\rangle^{¤k+1}$является существенной (в n).[1]

Чтобы не позволить фальшивомонетчику сделать томографию квантового состояния [16] и точно определить состояние$|\psi\rangle$, банку не следует выпускать число монет, превышающее полиномиальное степени n.

С точки зрения теории не существует офлайн-схем квантовых денег, которые совершенно невозможно было бы взломать (то есть с $\langle\psi|¤k+1_\rho|\psi\rangle^{¤k+1}=0$ и при не действующем ограничении времени, как в определении). Если в руках фальшивомонетчика есть данные о проверочном цикле и неограниченные ресурсы для квантовых вычислений, он может последовательно генерировать тестовые состояния до тех пор, пока одно из них не окажется подходящим. После проверки это состояние станет действительным финансовым состоянием и, соответственно, сможет быть использовано в качестве финансового маркера лексем. Таким образом, должно внедрить вычислительные допущения, учитывающие деятельность фальшивомонетчика, и повысить предел объема работ, необходимых для взлома.

Без какой-либо дальнейшей детализации схемы квантовых денег и проверочного цикла невозможно предоставить больше информации о невозможности взлома данной схемы. Далее продемонстрируем невозможность взлома схемы квантовых денег с черным ящиком.

Анонимность**.**

В идеальном случае, все квантовые купюры определенного номинала произведены в одном квантовом состоянии$|\psi\rangle$. Однако банк может выпускать квантовые деньги с помощью разных квантовых состояний, каждое из которых проверяется в разных проверочных циклах. Несмотря на то, то что нет операций для клиентов, которые позволяют проверить анонимность системы, человек, контролирующий работу банка, имеет возможность регулярно просматривать все банковские операции и убедиться в выпуске идентичных маркеров лексем в виде купюр. Если все купюры на самом деле

[1]В терминологии [14], это единственный открытый ключ к квантовой монетной схеме с полнотой ошибок=0 и несущественной важности ошибки в n.

идентичны, проследить их использование совершенно невозможно. В случае запутанности квантового цикла возможно предоставление соответствующего цикла проверки в виде фиксированной открытой классической строки, которую затем смогут использовать индивидуальные предприниматели и торговые компании. В случае, если один цикл определен для всех продавцов, каждый из них, таким образом, получит соответствующие гарантии анонимности. Если для проверки необходим интерактивный протокол, в данном случае использование слепых квантовых вычислений, в целях увеличения гарантий анонимности продавцов возможно использование анонимной классической [30] и квантовой [31] коммуникации.

Квантовые банкноты

Поскольку все квантовые банкноты одного номинала имеют одно и то же квантовое состояние, к таким банкнотам приравниваются маркеры лексем, идентифицирующие квантовые «банкноты» одного номинала, но, возможно, разного квантового состояния. Также допустимо наличие классической информации, связанной с каждым из квантовых состояний. Таким образом, банк может выпустить целый ряд состояний $\{(s_{i,}|\psi_i\rangle): i \in \Gamma\}$, например, равных 50-рублевым банкнотам. Это относится к обычным банкнотам, каждая из которых имеет свой собственный серийный номер.

Приведет пример подхода, которым можно руководствоваться при создании квантовых банкнот. Допустим, a является элементом последовательности m некоторой группы G, a r является функцией, шифрующей элементы G. Допустим, существует возможность опубликовать цикл C, который выполняет (для любого группового элемента b и целого числа y∈{0,1…m-1}) отображение $|y\rangle|r(b)\rangle \rightarrow |y\rangle|r(ba^y)\rangle$, но для которого невозможно (помимо прочего) определить данный$|r(a^x)\rangle$. Необходимо принять во внимание, что классический квантовый дискретный логарифмический алгоритм для вычисления x потребует средства и возможности для вычисленияr(a^{zx+y}) для произвольных целых чисел z и y. Таким образом, генерация квантовых денег возможна только тогда, когда банк осуществляет оценку собственного значения (начиная с a состояния $|r(b)\rangle$),чтобы сгенерировать случайное собственное состояние операции, вызванной C, и форму

$$|\psi k\rangle = \sum_{x=0}^{m-1} e^{-2\pi ikx/m}|r(ba^x)\rangle$$

вместе с параметром собственного значения k. Затем банк публикует подлинный список действительных параметров k. Банкнота, таким образом, состоит из состояния$|\psi_k\rangle$ и классического значения k, которое можно проверить любым верификатором, осуществив оценку собственного значения банкноты и подтвердив, что параметров собственного состояния является именно k (и что k находится в подлинном списке действительных параметров). Существует множество вариаций приведенного выше подхода и много открытых вопросов, касающихся его. В данной статье обратимся к квантовым монетам.

Определение

Схемой квантовой банкноты является пара $(V, \{(s_i, |\psi_i\rangle) : i \in \Gamma\})$, где Γ является конечным множеством, а для каждого $i \in \Gamma$, s_i является обозначением множества S, $|\psi_1\rangle$ является n-кубитным чистым состоянием в 2^n-мерном пространстве Гильберта H^{2n}. Более того, V является квантовым циклом с квантовым входным регистром (обозначенным $|s\rangle$), квантовым входным n-кубитным регистром (обозначенным p), плюс дополнительный маркер лексем, идентифицирующих квантовые «банкноты», входного регистра, классический выходной бит и квантовый выходной регистр n кубитов.[2]

Верификация

Универсальный цикл схемы верификации квантовой банкноты приведен в [4].

$$(V, \{(s_i, |\psi_i\rangle) : i \in \Gamma\})$$

Использование классического обозначения s_i может варьироваться в соответствии со схемой. Например, в схемах Веснера [27] и Беннетта и др. [28] s_i является серийным номером, позволяющим эмитенту находить подробности верификации, в то время в схеме Токунги и др. [29] s_i фактически не используется; в их схемах s_i используется для отображения номинала купюры (например, 50 рублей), однако в нашей формулировке номинал фиксируется определенной схемой, так что обозначение в сущности является пустой строкой для всех $i \in \Gamma$. В схемах, обозначение s_i является нетривиальным и неизменяемым верификацией, оно, по сути, ограничивает их анонимность, так же это делает серийный номер, нанесённый на каждую банкноту.

В то время как все предыдущие схемы квантовых денег, рассмотренные ранее, классифицируются как схемы квантовых банкнот, основанные на упомянутой выше формуле, ни одна из них не имеет всех тех необходимых для безопасности свойств и характеристик. В частности, ни одна из предыдущих квантовых финансовых схем не поддается контролю в режиме офлайн: все они требуют проверки маркера лексем, идентифицирующего квантовые купюры, эмитентом посредством квантовой коммуникации – это требование, которые мы хотим исключить из списка необходимых для работы с квантовыми монетами. В остальной части данной работы хотелось бы обратиться к работе со схемами квантовых монет, а не банкнот.

Квантовые монеты и черный ящик

Первая реализация квантовых монет работает с моделью цикла черного ящика. Допустим, что цикл верификации, предоставляемый вниманию публики, является черным ящиком: «Всё, что какой-либо человек сможет вычислить с помощью этого цикла, он может вычислить и через режим входа-выхода программы [26, с.2]. С этим допущением представим схему, в которой монеты полностью защищены от подделки. Эта схема позволяет совершать передачу монет произвольное количество раз. Использование цикла с черным ящиком означает, что монеты можно проверить локально без какой либо – классической или квантовой – связи с банком.

---

[2] В терминологии [14], это открытый ключ квантовой финансовой схемы.

Отметим, что в настоящий момент неизвестно, можно ли использовать квантовый цикл как настоящий черный ящик. Что касается усложнения классических циклов[25], то здесь результаты неутешительны, однако по-прежнему существует несколько возможностей для этого: скажем, можно усложнить точечную функцию [24]. Однако по квантовым циклам никаких результатов нет. Еще одной классической техникой вычислений с помощью черного ящика является защищенное от внешнего воздействия оборудование, однако провести параллель с квантовыми вычислениями вновь не представляется возможным.

В данной конструкции черного ящика монета является случайно выбранным секретным состоянием, и во время цикла проверки происходит опознание именно этого состояния посредством использования модели оракула [23].

Допустим, $|\psi\rangle$является случайно выбранным чистым состоянием в соответствии с мерой Хаара из чистых состояний H^{2n}. Оракул верификации является $U_\psi = I - 2|\psi\rangle\langle\psi|$. Таким образом, поскольку это схема оракула черного ящика, доказательство невозможности подделки, представленное ранее, является действенным и в модели оракула черного ящика эта схема оказывается полностью защищенной от подделки.

На практике, однако, случайный выбор чистого состояния $|\psi\rangle$ в соответствии с мерой Хаара и с дополнительными ограничениями, которые должно будет вычислить по формуле $U_\psi = I - 2|\psi\rangle\langle\psi|$ и которые потребуют от нас производства большого числа их копий, оказывается проблематичным и совершенно неизвестно, как совершить этот выбор в течение полиномиального времени. Последние работы в этом направлении обращались к развитию приближенных квантовых t-моделей [22], в которых, грубо говоря, t копии состояния могут быть сконструированы таким образом, что тензорное состояние продукта оказывается очень близким к t копиям состояния, которое было случайно выбрано в соответствии с мерой Хаара. В [9 Теорема 8] предлагают технику для построения$|\psi\rangle$ копий псевдослучайного состояния, которые являются практически неотличимыми (то есть несущественно отличными) от t копий истинного случайного состояния в любых измерениях, допуская даже использование методики измерения для совершения полиномиального (n) количества запросов в адрес оракула U, который распознает состояние. Техника Ааронсона позволяет нам использовать псевдослучайные состояния вместо истинно случайных состояний с незначительным ущербом для безопасности.

Надо отметить, что выбор случайной двоичной строки со случайным кодированием в паре не ортогональных базисов – скажем, так называемых базисов “BB84” – не является достаточным для квантовых монет. Злоумышленник, имея небольшое количество квантовых монет, скажем, порядка O (logn), может измерить каждый кубит маркера лексем O (logn) в обоих базисах, и, вероятнее всего, обнаружит варианты базиса и, таким образом, случайную двоичную строку, позволив ей впоследствии создать произвольное количество поддельных монет.

Верификация

Допустим, U_ψ является оракулом, распознающим состояние $|\psi\rangle$ посредством транспонирования знака фазы состояния$|\psi\rangle$. То есть $U_\psi|\psi\rangle$=-$|\psi\rangle$ и $U_\psi|\phi\rangle$=$|\phi\rangle$ при всех $|\phi\rangle$

Ортогональны $|\psi\rangle$. Другими словами, $U_\psi = I - 2|\psi\rangle\langle\psi|$. Можно сконструировать проверочный цикл с оракулом U_ψ следующим образом. Вводит состояние |0› на регистре считывания данных, а затем подвергаем маркер лексемы, идентифицирующий квантовую «купюру», преобразованию Адамара. Затем используем маркер лексемы, идентифицирующий квантовую «купюру», в качестве управляющего бита контролируемого - U_ψ, направленного на состояние ввода р. Затем вновь повергаем маркер лексемы, идентифицирующий квантовую «купюру», преобразованию Адамара и измеряем ее, т.е. вычисляем. После выполнения измерений, т.е. вычислений в регистре маркер лексемы, идентифицирующий квантовую «купюру», результат будет равен$|1\rangle$, в то время как входное состояние рявляется $|\psi\rangle$и$|0\rangle$, в то время как входное состояние равняется $|\phi\rangle$для $\langle\phi|\psi\rangle$=0. Более того, состояние второго регистра остается неизменным, когда его ввод (входной сигнал) является$|\psi\rangle$.

Тот факт, что валидный маркер лексем остается неизменным в процессе верификации, обеспечивает простоту передачи квантовых монет. Когда человек расплачивается квантовой монетой в магазине, продавец, после проверки и подтверждения монеты, может хранить ее у себя до тех пор, пока не потребуется использовать ее в качестве сдачи другому покупателю. В течение этого времени продавец может отдать монеты в руки другому пользователю, который, после опциональной проверки монеты, может использовать ее в другой финансовой операции. Вообще, процесс верификации не только допускает простоту и надежность передачи монет, но и увеличивает их надежность. И, хотя с течением времени квантовое состояние может декогерировать, во время процесса верификации маркеров лексем по-прежнему может быть достаточно близким к ожидаемому состоянию$|\psi\rangle$, чтобы с наибольшей вероятностью пройти проверку. Если маркер лексем проходит верификацию, измерительный процесс вернет монету к ее изначальному состоянию$|\psi\rangle$.

Безопасность. Процедура верификации, описанная в предыдущем разделе, соответствует корректной квантовой финансовой схеме: валидные маркеры лексем всегда распознаются. Теперь поговорим о безопасности такой схемы. Чтобы избежать любой возможности взлома, нам необходимо, чтобы недействительные маркеры лексем опознавались как недействительные и, таким образом, подделка денег станет очень трудной задачей.

Невозможность взлома черного ящика

Для анализа возможности взлома схемы черного ящика, предположим, что цикл для единичного U_ψ является черным ящиком – таким образом, из процессов, протекающих внутри него, невозможно получить никакой информации. Соответственно, можно предположить, что U_ψявляется оракулом. Сделав это допущение, переходим к получению нижней границы числа запросов к оракулу, что необходимо для создания состояния с исключительно частичным совпадением p с $|\psi\rangle^{\text{¤}k+1}$, когда злоумышленник имеет только k монет. В следующем разделе докажем этот результат. Ааронсон дает следующую версию теоремы о запрете клонирования с точки зрения теории сложности, которая сочетает в себе нижнюю границу для квантового поиска с теоремой о запрете клонирования.

Теорема**.** Схема квантовых денег $(V,|\psi\rangle)$, где $|\psi\rangle$ является n кубитным состоянием, является черным ящиком, который невозможно взломать, при условии, что если оракул U_ψ распознал состояние $|\psi\rangle$ и k копий состояния$|\psi\rangle$ для любого k≥0, k∈poly(n), то злоумышленник не сможет, используя полиномиальное (n) количество запросов кU_ψ, воссоздать состояние p, так что $\langle\psi|¤k+1_\rho|\psi\rangle^{¤k+1}$пренебречь нельзя.[3]

Невозможность взлома означает, что злоумышленник может создать лишь (k+1) состояний регистра, имеющих частичное совпадение с $|\psi\rangle$. Согласно другой формулировке злоумышленнику необходимо воссоздать многорегистровое состояние так, чтобы только (k+1) из этих регистров, а не абсолютно каждый из них, имели частичное совпадение с $|\psi\rangle$. Эти формулировки абсолютно равнозначны. Злоумышленник имеет доступ к оракулу верификации и, для каждого из множества создаваемых им (оракулом) регистров он может применять оракул, отсеивая те, что не прошли проверку. Это требует дополнительных запросов в адрес оракула верификации. Однако их число укладывается в poly(n) запросов (так, в течение полиномиального времени злоумышленник может создать poly(n) регистров), и, тем не менее, остается в рамках указанных выше параметров безопасности.

Нет необходимости расширять эту формулировку до k+l копий $|\psi\rangle$. Злоумышленник, способный с большой вероятностью создать k+l копий$|\psi\rangle$, может, в частности, создать k+1 копий q $|\psi\rangle$. Другими словами, не существует большого риска, который принёс бы ожидаемые результаты. Формулировка исключает возможность создания очень большого числа монет с очень малой вероятностью, но с большим ожидаемым числом монет.

Теперь нашей целью является демонстрация того, что универсальная квантовая монетная схема, выполняемая с оракулом черного ящика и изображенная на рисунке 4, является полностью защищенной от взлома. Однако мы не можем использовать базовую теорему о запрете клонирования [19, 20] или результат приблизительного клонирования [21], потому у злоумышленника есть не только копии состояний$|\psi\rangle$, но и оракул U_ψ, который сообщит ему о том, была ли попытка клонирования успешной. Таким же образом мы не можем напрямую воздействовать нижней границейΩ($\sqrt{N}$)на квантовый поиск [32], поскольку в распоряжении злоумышленника находится не только оракул U_ψ, который распознает желаемое состояние, но и несколько копий этого состояния. Вероятнее всего, нам нужен гибрид двух результатов.

В [9] предлагают следующую сложно-теоретическую версию теории запрета на квантовое клонирование, которая сочетает нижний предел квантового поиска и теорему запрета на квантовое клонирование.

Теорема (Теорема 5, [9]). Допустим, $|\psi\rangle$является n-кубитным чистым состоянием. Допустим, мы имеем начальное состояние $|\psi\rangle^{¤k}$для некоторых k≥1 и для оракулаU_ψ, то есть $U_\psi|\psi\rangle$=-$|\psi\rangle$и $U_\psi|\phi\rangle$=$|\phi\rangle$ всякий раз, когда $\langle\phi|\psi\rangle$=0. Затем, чтобы добиться состояния p так, что

$$\langle\psi|k+1_\rho|\psi\rangle^{k+1} \geq p$$

[3]В терминологии [14], это единственный открытый ключ к квантовой монетной схеме с полнотой ошибок=0 и несущественной важности ошибки в n.

необходимы

$$\Omega\left(\frac{\sqrt{2^n p}}{k\log k}-k\right)$$

запросы к U_ψ

Примечание 2. В терминологии [14], это единственный личный ключ квантовой финансовой схемы с полнотой ошибок=0 и несущественной важности ошибки в n.

Это позволяет нам показать, что квантовая монетная схема в модели с оракулом черного ящика является неуязвимой для взлома.

Теорема Допустим, (V,|ψ⟩) является квантовой монетной схемой, где V, как на рис.4 U_ψ, является оракулом черного ящика, а |ψ⟩является n-кубитным чистым состоянием. Если выпущено не более поли (n) монет, (V,|ψ⟩)является защищенной от взлома черного ящика.

Доказательство: допустим обратное. В таком случае существует злоумышленник, который, получив k копий |ψ⟩ и используя q=po (n) запросов к(V,|ψ⟩), может добиться создания состояния p, так что $\langle\psi|¤k+1_\rho|\psi\rangle^{¤k+1}=p\in 1/\mathrm{poly}(n)$
Согласно теореме 4.2,

$$q=\Omega\left(\frac{\sqrt{2^n p}}{k\log k}\right)\Omega\left(\frac{\sqrt{2^n/\mathrm{poly}(n)}}{\mathrm{poly}(n)\log\mathrm{poly}(n)}-\mathrm{poly}(n)\right)=\Omega\left(\frac{\sqrt{2^n}}{\mathrm{poly}(n)}\right)(3)$$

запросы к U_ψ. Но злоумышленник может совершить только полиномиальное число q запросов кU_ψ,. Тогда получится результат, согласно которому q∈*poly*(n) и, следовательно, $\mathrm{poly}(n)=\Omega\left(\frac{\sqrt{2^n}}{\mathrm{poly}(n)}\right)$, что является противоречием. Таким образом, квантовая монетная схема является защищенной от взлома черного ящика.

Квантовые монеты и использование слепых квантовых вычислений.

Слепые квантовые вычисления позволяют одной стороне, Алисе, предоставить возможность другой стороне, Бобу, совершать вычисления от ее имени при том, что Боб не имеет данных о состоянии ввода и вывода, равно как и о проводимой операции.

Впервые слепые квантовые вычисления были использованы Чайлдсом[18] под названием «безопасные квантовые вычисления». Согласно базовой идее Алиса, которая имеет ограниченные вычислительные возможности (квантовая коммуникация, квантовая память, X- и Y-контролируемые квантовые вентили), может сделать так, чтобы Боб безопасно осуществил произвольные квантовые вычисления с квантовым входом и выходом. В протоколе Чайлдса Алиса и Боб должны осуществить большой объем квантовой коммуникации, которую, впрочем, можно заменить квантовой телепортацией (общая запутанность с измерением Белла и классической коммуникацией).

Броудбент, Фитцсиммонс и Кашефи[17] представили протокол слепых квантовых вычислений с квантовым входом и выходом и использованием квантовых вычислений, основанных на измерениях, которым требуется два цикла коммуникации – один в начале и один в конце. Слепые квантовые вычисления могут использоваться следующим образом для проверки квантовых монет. Продавец, играя роль Боба, вслепую проводит цикл

проверки для банка, который играет роль Алисы. Продавец получает монету в начале цикла и взаимодействует с банком, который помогает ему этот цикл пройти. В схеме [17] это требует главным образом классического взаимодействия, включающего цикл квантового взаимодействия в конце для коррекции конечного результата. В итоге конечный результат с информацией о приёме/отказе остается у продавца.

Хотя требования к квантовой коммуникации для верификации квантовых монет с использованием слепых квантовых вычислений не являются лучшим вариантом, чем простое телепортирование монеты в банк для проверки, требования к квантовым вычислениям для банка заметно ниже. Вместо обязанности осуществлять полный квантовый цикл верификации монеты для тысяч монет, проверяемых ежесекундно, имеется необходимость лишь в выполнении пятого пункта третьего протокола [17], который состоит (самое большее) из X- и Z-вентиля на кубит монеты.

Очевидно, было бы предпочтительнее еще сильнее снизить требования к квантовой коммуникации, например, оставив необходимость такой коммуникации только в начале протокола, а для его остальной части использовать классическую коммуникацию без использования общей запутанности для телепортации. Такой протокол будет интерактивным протоколом для запутывания квантового цикла, а проблема квантовой запутанности уже в течение долгого времени остается открытой.

Литература

1. D. Chaum, A. Fiat, M. Naor. Untraceable electronic cash (extended abstract). In Shafi Goldwasser, editor, *Advances in Cryptology – Proc. CRYPTO ’88*, *LNCS*, volume 403, pp. 319–327. Springer, 1988. DOI:10.1007/0-387-34799-2_25.
2. D. Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, **28**(10):1030–1044, October 1985. DOI:10.1145/4372.4373.
3. D. Chaum. Privacy protected payments: Unconditional payer and/or payee untraceability. In D. Chaum, I. Schaumuller-Bichl, editors, *Smartcard 2000*, pp. 69–93. North Holland, 1988.
4. M. Mosca, D. Stebila Quantum Coins http://arxiv.org/1/0/1/0/all/0/1
5. D. Chaum, T. Pryds Pedersen. Transferred cash grows in size. In Rainer A. Rueppel, editor, *Advances in Cryptology – Proc. EUROCRYPT ’92*, *LNCS*, volume 658, pp. 390–407. Springer-Verlag, 1992. DOI:10.1007/3-540-47555-9_32.
6. S. Wiesner. Conjugate coding. *ACM SIGACT News*, **15**(1):78–88, 1983. DOI:10.1145/1008908.1008920.
7. C. H. Bennett, G. Brassard, S. Breidbard, S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology – Proc. CRYPTO ’82*. Plenum Press, 1982.
8. Y. Tokunaga, T. Okamoto, and Nobuyuki Imoto. Anonymous quantum cash. In *ERATO Conference on Quantum Information Science (EQIS) 2003*, September 2003. URL http://www.qci.jst.go.jp/eqis03/program/papers/O09-Tokunaga.ps.gz
9. S. Aaronson, P. Christiano Quantum Money from Hidden Subspaces arXiv:1203.4740 [pdf, ps, other]
10. S. Aaronson. Ten semi-grand challenges for quantum computing theory, July 2005. http://www.scottaaronson.com/writings/qchallenge.html

11. M. Mosca, D. Stebila. Uncloneable quantum money. In *Canadian Quantum Information Students' Conference (CQISC) 2006*, Calgary, Alberta, August 2006. http://www.iqis.org/events/cqisc06/papers/Mon-1130-Stebila.pdf

12. M. Mosca, D. Stebila. A framework for quantum money. In *Quantum Information Processing (QIP) 2007*, Brisbane, Australia, January 2007.

13. D. Stebila. *Classical Authenticated Key Exchange and Quantum Cryptography*. http://www.douglas.stebila.ca/research/papers/ste09/

14. S. Aaronson. Quantum copy-protection and quantum money. http://www.scottaaronson.com/papers/noclone-ccc.pdf

15. D. Chaum, T. Pryds Pedersen. Transferred cash grows in size. http://link.springer.com/chapter/10.1007%2F3-540-47555-9_32

16. J. B. Altepeter, D. F. V. James, P. G. Kwiat. 4 qubit quantum state tomography. In Matteo Paris and Jaroslav ˇRehá ˇcek, editors, Quantum State Estimation, Lecture Notes in Physics, volume 649, pp. 113–145. Springer, 2004. DOI:10.1007/b98673.

17. A. Broadbent, J. Fitzsimons, E. Kashefi. Universal blind quantum computation. In Proc. 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2009. IEEE Press, 2009. EPRINT arXiv:0807.4154.

18. A. Childs. Secure assisted quantum computation. Quantum Information and Computation, 5(6):456–466, September 2005. EPRINT arXiv:quant-ph/0111046, URL http://www.rinton.net/xqic5/qic-5-6/456-466.pdf

19. W. K. Wootters,W. H. Zurek. A single quantum cannot be cloned. Nature, 299:802–803, October 1982. DOI:10.1038/299802a0.

20. D. Dieks. Communication by EPR devices. *Physics Letters A*, **92**(6):271–272, November 1982. DOI:10.1016/0375-9601(82)90084-6

21. D. Bruß, C. Macchiavello. Approximate quantum cloning. In D. Bruß and G. Leuchs, editors, *Lectures on Quantum Information*. Wiley-VCH, 2007. DOI:10.1002/9783527618637.

22. A. Ambainis, J. Emerson. Quantum t-designs: t-wise independence in the quantum world. In Proc. 22nd Ann. IEEE Conference on Computational Complexity (CCC) 2007, pp. 129–140. IEEE, June 2007. DOI:10.1109/CCC.2007.26. EPRINT arXiv:quant-ph/0701126.

23. M. Boyer, G. Brassard, P. Høyer, A. Tapp. Tight bounds on quantum searching. Fortschritte der Physik, 46(4–5):493–505, 1998. DOI:10.1002/(SICI)1521-3978(199806)46:4/5<493::AID-PROP493>3.0.CO;2-P. EPRINT arXiv:quant-ph/9605034.

24. H. Wee. On obfuscating point functions. In Proc. 37th Annual ACM Symposium on the Theory of Computing (STOC), pp. 523–532. ACM Press, 2005. DOI:10.1145/1060590.1060669. EPRINT http://eprint.iacr.org/2005/001.

25. B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *Advances in Cryptology– Proc. CRYPTO 2001*, *LNCS*, volume 2139, pp. 1–18. Springer, 2001. DOI:10.1007/3-540-44647-8_1.

26. B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, .K Yang. On the (im)possibility of obfuscating programs, 2001. EPRINT http://eprint.iacr.org/2001/069, URL http://www.wisdom.weizmann.ac.il/~oded/p_obfuscate.html.

*27. S. Wiesner. Conjugate coding. ACM SIGACT News, **15**(1):78–88, 1983. DOI:10.1145/1008908.1008920.*

28. C. H. Bennett, G/ Brassard, S. Breidbard, S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, Advances in Cryptology – Proc. CRYPTO '82. Plenum Press, 1982.

29. Y. Tokunaga, T. Okamoto, N. Imoto. Anonymous quantum cash. In ERATO Conference on Quantum Information Science (EQIS) 2003, September 2003. URL http://www.qci.jst.go.jp/eqis03/program/papers/O09-Tokunaga.ps.gz.

30. A. Broadbent, A. Tapp. Information-theoretic security without an honest majority. In Kurosawa [Kur07], pp. 410–426. DOI:10.1007/978-3-540-76900-2_25. EPRINT arXiv:0706.2010.

31. G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, A. Tapp. Anonymous quantum communication. In Kurosawa [Kur07], pp. 460–473. DOI:10.1007/978-3-540-76900-2_28. EPRINT arXiv:0706.2356.

*32. C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani. Strengths and weaknesses of quantum computing. SIAM Journal on Computing, **26**(5):1510–1523, 1997. DOI:10.1137/S0097539796300933. EPRINT arXiv:quant-ph/9701001.*