Протокол QKD на основе случайных группировок и измерений состояний Белла

Аннотация

В работе содержится описание четырёхкубитного квантового протокола распределения ключей, представленного в [39]. Произведён сравнительный анализ с имеющимися аналогами. Приводятся дополнительные теоретические выкладки и сведения для обеспечения лучшего понимания материала.

Рассматриваемый протокол базируется на измерении пар состояний Белла. Кубиты объединяются в единый блок, передаваемый от отправителя к получателю в каждом сообщении. Шифрование осуществляется путем случайной группировки четырех отдельных кубитов в две новые пары; аналогичный механизм также является одним из способов обнаружить подслушивающее устройство в квантовом канале. Незамедлительно после приёма блока кубитов приемник случайным образом разбивает четыре кубита на пары и проверяет их при помощи измерений состояний Белла. Из сравнения информации о группировке этих четырех кубитов обе стороны соединения могут обнаружить нелегального пользователя в канале. В рассматриваемом протоколе приемник обрабатывает блок кубитов мгновенно во время получения, что является эффективным способом преодоления ультракороткого времени когерентности квантовых состояний.

Дальнейшее изложение построено следующим образом: в главе 1 приводится краткая теоретическая справка с пояснением используемой терминологии. Затем в 2 содержатся предпосылки появления рассматриваемого протокола. В главе 3 описываются основные идеи, а также алгоритм распределения ключа. После чего в главе 4 производится анализ стойкости протокола на примере атаки перехвата – повторной передачи и атаки троянского коня. В 5 представлены варианты практического применения протоколов квантового распределения ключей и рассматриваемого протокола в частности. Наконец, в приложении А представлены выкладки, демонстрирующие принцип группировки кубитов.

1 Теоретическое введение

1.1 Кубиты [6]

Рассмотрим некоторую двухуровневую квантовую систему, примерами которой могут быть спин фермиона с $s = \frac{1}{2}$ или состояние поляризация электромагнитного поля (фотона) [22]. Формально такая система описывается Гильбертовым пространством двух квантовых состояний $\mathcal{H}_2$. Обозначим ортонормированный базис такого пространства $\{|0\rangle, |1\rangle\}$ или сокращенно $\{|i\rangle\}$, $i = 1, 2$, $\langle i|j\rangle = \delta_{ij}$. В соответствии с принципом суперпозиции наиболее общее нормированное состояние в $\mathcal{H}_2$ может быть представлено в виде:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \quad \langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1, \tag{1}$$

где a и b — комплексные числа. Состояние (1) в теории квантовых вычислений называется кубитом (англ.: qubit, quantum bit). Проектируя состояние кубита на ортонормированный базис $\{|i\rangle\}, i = 1, 2$, получим

$$\langle 0|\psi\rangle = a, \quad \langle 1|\psi\rangle = b,$$

где $|a|^2$ — вероятность обнаружить в состоянии $|\psi\rangle$ состояние $|0\rangle$, а $|b|^2$ — вероятность обнаружить в состоянии $|\psi\rangle$ состояние $|1\rangle$. Общая фаза кубита, в соответствии с постулатами квантовой теории, физического смыла не имеет, значит, состояния $|\psi\rangle$ и $e^{i\alpha}\,|\psi\rangle$ тождественны:

$$|\psi\rangle \equiv e^{i\alpha}\,|\psi\rangle\,, \quad \alpha \in \mathbb{R}. \tag{2}$$

После проектирования на ортонормированный базис состояние кубита $|\psi\rangle$ коллапсирует, то есть переходит в состояние $|0\rangle$ ($|\psi\rangle \to |0\rangle$) или в состояние $|1\rangle$ ($|\psi\rangle \to |1\rangle$).

В квантовой теории информации кубит определяется как единица квантовой информации, аналогично тому, как бит (0 или 1) определяется как единица классической теории информации.

Однако в отличие от бита в классической теории, информация которого может быть измерена без разрушения состояния, кубит при считывании переходит в одно из двух своих базисных состояний $|0\rangle$ или $|1\rangle$.

Понятие кубита имеет геометрическую интерпретацию в воображаемом пространстве состояний. Два комплексных числа a и b в (1) содержат 4 действительных параметра. В силу условия нормировки независимыми являются три из них. С учетом свойств квантовых состояний (2) достаточно два действительных параметра для описания кубита. Таким образом, если представить выражение (1) в виде:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{3}$$

то действительные параметры θ и ϕ определяют точку на сфере. Вектор, соединяющий начало координат этого воображаемого пространства с точкой на сфере, задает геометрическую интерпретацию вектора состояния $|\psi\rangle$ или кубита. Геометрическое место точек конца такого вектора образуют сферу единичного радиуса [10].

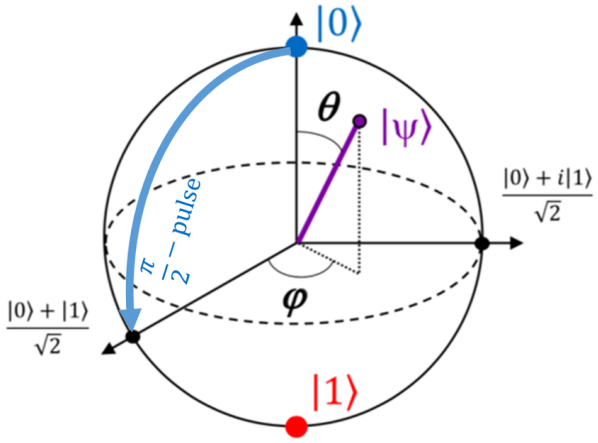

Рис. 1. Сфера Блоха как геометрическая интерпретация кубита.

Эта сфера также называется сферой Блоха [1]. Как видно из рис. 1 при $\phi = 0$ и $\theta = 0$ вектор $|\psi\rangle$ задаёт состояние $|0\rangle$. При $\theta = \pi$ — вектор задаёт состояние $|1\rangle$. При такой интерпретации ортогональными являются векторы противоположного направления. При этом согласно постулатам квантовой механики считать из кубита можно только эти два состояния: $|0\rangle$ или $|1\rangle$, то есть две единицы классической информации.

1.2 Квантовая запутанность [6, 14]

Важной отличительной чертой кубитов от классических битов является то, что несколько объединённых кубитов могут демонстрировать квантовую запутанность. Квантовая запутанность — это нелокальное свойство двух или более кубитов, которое позволяет набору кубитов выражать более сложную взаимосвязь, чем это возможно в классических системах [14]. Как нетрудно догадаться, самая простая система для отображения квантовой запутанности — это система двух кубитов. Рассмотрим, например, два запутанных кубита в состоянии Белла $|\phi^+\rangle$, которые будут упомянуты в дальнейшем:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

В этом состоянии, называемом равновероятной суперпозицией, при измерении мы получим состояния $|00\rangle$ или $|11\rangle$ с равными вероятностями $|1/\sqrt{2}|^2 = 1/2$. Другими словами, невозможно определить, находится первый кубит в отдельности в состоянии $|0\rangle$ или $|1\rangle$, что также верно и для второго кубита.

Представьте себе, что эти два запутанных кубита разделены, один достался Алисе, а другой — Бобу. Алиса измеряет свой кубит, получая с равной вероятностью либо $|0\rangle$, либо $|1\rangle$, т.е. теперь она может определить, в каком из состояний находится её кубит. Из-за наличия квантовой запутанности кубитов Боб должен теперь получить точно такие же измерения, как и Алиса. Например, если она получила $|0\rangle$, Боб должен получить то же самое, поскольку $|00\rangle$ — единственное состояние, в котором кубит Алисы находится в состоянии $|0\rangle$. Другими словами, что бы ни измеряли Алиса или Боб, информация об одном из запутанных кубитов улучшает наши знания о другом.

Явление квантовая запутанности также позволяет одновременно изменять сразу несколько состояний отдельных кубитов, в отличие от классических битов, которые могут изменять только одно значение за раз. В настоящее время, предполагается, что квантовая запутанность — это некоторый ресурс, который является уникальным для квантовых систем. Запутанность — необходимый компонент любых квантовых вычислений, которые не могут быть эффективно выполнены на классическом компьютере. Она также является основой алгоритмов сверхплотного кодирования, квантовой телепортации и квантовой криптографии.

2 История и предпосылки создания

Одним из подходов квантовой криптографии является квантовое распределение ключей. Квантовое распределение ключей (англ.: Quantum Key Distribution, QKD) — метод передачи ключа, который использует квантовые явления для гарантии безопасной связи. Этот метод позволяет двум сторонам, соединенным по открытому классическому каналу связи, создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифрования сообщений, передаваемых по классическому каналу [4, 8]. Различные типы QKD также были экспериментально продемонстрированы на сегодняшний день [12, 34].

В настоящее время предложено много работ по данной тематике. Самый первый протокол QKD был предложен Беннеттом и Брассаром в 1984 году. Данный протокол получил название BB84 и базировался на использовании двух взаимно несмещенных состояний поляризации фотонов [11]. Авторами был описан способ распределения случайного секретного ключа между Алисой и Бобом.

Позднее Экерт предложил другой протокол QKD [20], названный E91, основанный на парадоксе Эйнштейна-Подольского-Розена [19]. После этого были теоретически предложены и экспериментально реализованы различные протоколы QKD, например, базирующиеся на однофотонных [32] и множественных состояниях [15]. В этих работах для переноса информации широко используются фотоны, поскольку ими легко манипулировать и они передают информацию со скоростью света.

Новый виток в развитии QKD связан с использованием состояний Белла [19]. В качестве квантового канала состояние Белла было впервые предложено в [24] и подтверждено [21] как максимально запутанное состояние двухкубитной квантовой системы. Кроме того, по сравнению с другими мультикубитными аналогами (состояния W [18], GHZ [26] и кластерные состояния [13]), состояние Белла легче всего реализовать с помощью нелинейного процесса, описанного в [29].

В основополагающей работе [24] две стороны разделяют секретный ключ, сравнивая форму начального состояния Белла и результат измерения состояния Белла после квантовой передачи. Затем [42] повысил общую эффективность коммуникации до 100% по сравнению с достигнутыми 50% в [24]. В [41] представлен первый аутентифицированный полуквантовый протокол распределения ключей без использования аутентифицированных классических каналов, основанный на состояниях Белла.

Авторы [24] и [42] предложили два протокола QKD, которые используют состояния Белла, распределенные между отправителем и получателем. В этих протоколах две пары состояний Белла разделены между двумя сертифицированными сторонами связи. Отправитель и получатель хранят по два кубита, запутанные друг с другом. После одновременного измерения состояний Белла с двух сторон реализуется квантовая запутанность уже между четырьмя кубитами.

В недавней работе [39] было предложено усовершенствование [42] для предотвращения подслушивания с более низким коэффициентом ошибок при подтверждении сообщений, а также с более быстрым обнаружением битов ключа, основанных на четырехкубитном состоянии, которое состоит из двух пар состояний Белла. Дальнейшая речь пойдёт о протоколе, представленном в [39].

3 Протокол QKD на основе случайных группировок и измерений состояний Белла

3.1 Основные идеи

Рассматриваемый протокол предполагает использование четырёхкубитных конфигураций, состоящих из двух пар состояний Белла. Каждый раз передатчик (Алиса) подготавливает группу, состоящую из четырёх кубитов, для незамедлительной отправки приёмнику (Бобу). Боб производит измерение квантового состояния сразу же после получения всей партии кубитов. Это односторонний процесс, что является важным нововведением по сравнению с двусторонними протоколами, в которых квантовое состояние должно сохраняться до завершения передачи [24, 42], благодаря которому протокол решает проблему ультракороткого времени когерентности квантовых состояний.

Если приводить более формальное описание, то можно обозначить четыре кубита двух состояний Белла как P_1, P_2, P_3 и P_4. Условимся, что квантовая запутанность имеет место между P_1 и P_2, а также между P_3 и P_4. После измерения состояний Белла с обеих сторон запутанными оказываются P_1 и P_3, P_2 и P_4 соответственно. Базисные функции состояний Белла выражаются следующим образом:

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle \pm |11\rangle\,\big), \quad |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(\,|01\rangle \pm |10\rangle\,\big).$$

Например, если начальными состояниями Белла были $|\phi^-\rangle$ и $|\phi^+\rangle$, то общее запутанное состояние из четырёх кубитов запишется следующим образом (см. подробнее (7)):

$$\begin{aligned} |\mathcal{C}\rangle_{1234} &= |\phi^-\rangle_{12} \otimes |\phi^+\rangle_{34} = \\ &= \frac{1}{2}\big(\,|\phi^+\rangle_{13}\,|\phi^-\rangle_{24} + |\phi^-\rangle_{13}\,|\phi^+\rangle_{24} + |\psi^+\rangle_{13}\,|\psi^-\rangle_{24} + |\psi^-\rangle_{13}\,|\psi^+\rangle_{24}\,\big), \end{aligned} \tag{4}$$

где индексы 1, 2, 3 и 4 обозначают номер связанного кубита, а $\otimes$ обозначает операцию тензорного произведения.

Из (4) можно сделать вывод, что общее состояние становится суперпозицией четырех состояний, это означает, что мы можем получить четыре различных результата при измерении комбинаций состояний Белла. Также обратим внимание, что уравнение (4) представляет лишь одну из возможных комбинаций, подробный анализ всех состояний можно

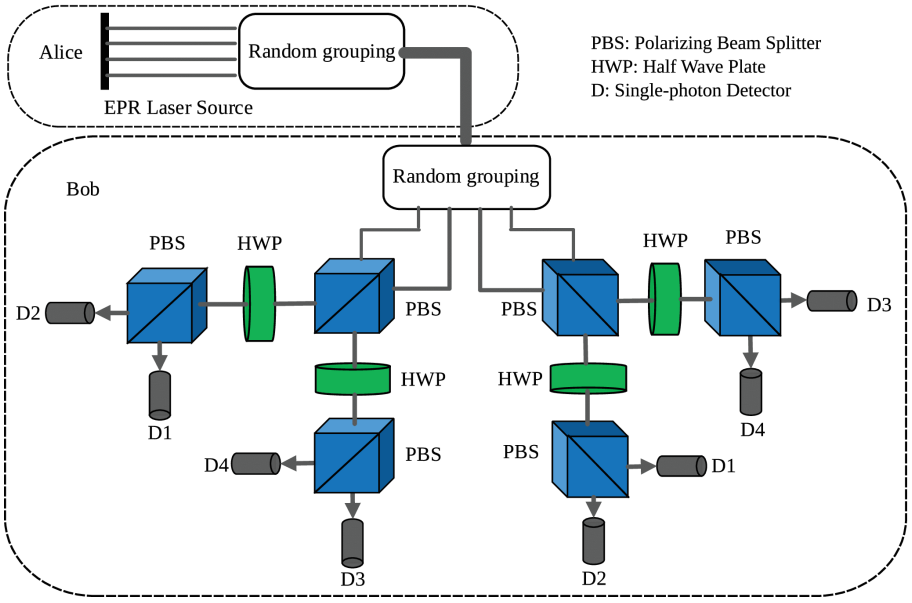

Рис. 2. Схема работы предлагаемого протокола QKD. Алиса подготавливает состояние из четырех кубитов и отправляет Бобу по квантовому каналу. Затем Боб группирует их случайным образом и измеряет эти кубиты в базисе состояний Белла.

найти в [39, 30], а также в А. Вкратце, существует несколько форм случайной группировки этих четырех кубитов, из которых только одна группировка будет определена как правильная. Это основной метод шифрования информации во время коммуникации. Предлагаемый протокол показан на рис. 2, где Алиса и Боб являются сертифицированными отправителем и приемником соответственно.

3.2 Алгоритм распределения ключей

- *Шаг 1. Подготовка состояний.* Алиса подготавливает одну из комбинаций четырёхкубитных состояний, например, представленную в уравнении (4). Такая комбинация состоит из четырёх кубитов P_γ, где $\gamma \in \{1, 2, 3, 4\}$. Каждой паре состояний Белла ставятся в соответствие два информационных бита ключа. Алиса запоминает текущую случайную группировку и пару состояний Белла, которая участвует в передаче.

- *Шаг 2. Передача кубитов.* Алиса случайным образом перемешивает эти четыре кубита и отправляет их Бобу по квантовому каналу.

- *Шаг 3. Измерение состояний Белла.* Боб принимает отправленные ему кубиты и случайным образом разбивает их на две части. После чего он выполняет измерение состояний Белла на этих двух частях и отправляет информацию о группировке и полученные результаты измерений Алисе по классическому каналу.

- *Шаг 4. Сравнение результатов.* Алиса принимает результаты Боба и сравнивает их с сохранённой информацией о P_γ. Если Алиса увидит совпадение, она объявит по классическому каналу *True* и весь процесс коммуникации может перейти к шагу 5 или вернуться на шаг 1 для следующей итерации. Если же совпадения не случится, она объявит *False*, после чего оба участника отбросят данные текущей итерации и процесс коммуникации начнётся сначала с шага 1 или оборвётся.

- *Шаг 5. Формирование согласованных ключей.* После нескольких итераций последовательностей шагов с 1 по 4 Алиса и Боб получают двоичную последовательность, которая представляет собой некоторый необработанный ключ $\mathcal{R}$ (также называемый

сырым [43]). Под $\mathcal{R}_A$ и $\mathcal{R}_B$ будем понимать необработанные ключи Алисы и Боба соответственно. Алиса случайным образом выбирает части $\mathcal{R}_A$ и собирает из них свой согласованный ключ $\mathcal{C}_A$, после чего объявляет позиции выбранных частей по классическому каналу. Затем Боб согласно этим позициям выбирает свой согласованный ключ $\mathcal{C}_B$ из ключа $\mathcal{R}_B$.

- *Шаг 6. Усиление конфиденциальности.* [40, 43] Из полученного набора битов $\mathcal{C}_B$ Боб выбирает некоторые в качестве битов чётности $\mathcal{D}_B$ и объявляет $\mathcal{D}_B$ вместе с их соответствующими позициями. Аналогичным образом Алиса выбирает свой набор $\mathcal{D}_A$ и сравнивает его с полученным $\mathcal{D}_B$. Если процент битовых ошибок в таком сравнении меньше некоторого наперёд заданного порога, то соединение может считаться безопасным и процесс коммуникации может перейти к следующему шагу 7; если нет, то необходимо вернуться на шаг 1 или же окончательно оборвать связь.

- *Шаг 7. Формирование окончательных ключей.* На последнем шаге окончательно выбираются ключи $\mathcal{R}'_A$ и $\mathcal{R}'_B$, которые будут использоваться для шифрования в дальнейшем процессе коммуникации по классическому каналу. Теоретически, в идеальном случае должно получиться $\mathcal{R}'_A = \mathcal{R}'_B$, где $\mathcal{R}'_A$ — это необработанный ключ $\mathcal{R}_A$ исключая биты $\mathcal{C}_A$, аналогичное верно для $\mathcal{R}'_B$.

3.3 Анализ доли ошибочных кубитов

Как уже оговаривалось, существует несколько различных способов группировок кубитов. Без ограничения общности будем считать, что группировка, приведённая в (4) является правильной, а остальные — неправильными. Учитывая, что каждая из m группировок получается равновероятно, вероятность правильной группировки для Боба равна $\frac{1}{m}$. Измеряя состояния Белла, в каждом из случаев Боб может получить любую из перечисленных комбинаций состояний Белла: $\{|\phi^+\rangle, |\phi^-\rangle\}$, $\{|\phi^-\rangle, |\phi^+\rangle\}$, $\{|\psi^+\rangle, |\psi^-\rangle\}$ и $\{|\psi^-\rangle, |\psi^+\rangle\}$. Отметим, что если Боб выберет правильную группировку, то он может получить верную комбинацию состояния Белла с вероятностью 1. Если в канале нет подслушивающего устройства, то вероятность ошибки ε_0 может быть получена из анализа совпадений пары состояний Белла для каждой группировки.

Пусть Боб случайным образом получил неправильную группировку кубитов, например $\{(P_1, P_2), (P_3, P_4)\}$. Тогда состояние (4) выражается следующим образом (см. подробнее (8)):

$$|\mathcal{C}\rangle_{1234} = \frac{1}{2}\big(\,|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\,\big)_{1234} = \big(\,|\phi^-\rangle_{12}\,|\phi^+\rangle_{34}\,\big).$$

В этом случае при измерении из всех возможных комбинаций состояний Белла он может получить только $|\phi^-\rangle_{12}\,|\phi^+\rangle_{34}$. Сравнивая с (4), заключаем, что Боб получит правильную группировку состояний с вероятностью $\frac{1}{4}$.

Повторяя данные действия для всех возможных группировок, находим, что доля ошибочных кубитов $\varepsilon_0 = 0,0417$ [39]. Взаимная информация Алисы и Боба:

$$\mathcal{I}(A;B) = 1 - [-\varepsilon_0 \log_2 \varepsilon_0 - (1-\varepsilon_0)\log_2(1-\varepsilon_0)] = 0,7501 \text{ бит}. \tag{5}$$

4 Криптоанализ

4.1 Атака перехвата — повторной передачи

Одной из атак на QKD протоколы является атака перехвата — повторной передачи [16, 9, 33]. Суть атаки заключается в измерении злоумышленником (Евой) непосредственно квантового состояния носителя (например, фотона) и последующей повторной посылке нового

фотона в состоянии, полученном в результате измерения. Поскольку злоумышленник не пропускает квантовые состояния отправителя, а фактически генерирует новые и отправляет их получателю, то данная атака также называется непрозрачной.

В рассматриваемом протоколе Ева может взаимодействовать с полученным сообщением и повторно послать Бобу новое состояние из четырех кубитов, чтобы он продолжал получать сообщения. Тогда Ева играет ту же роль, что и Боб в процессе коммуникации. Злоумышленник аналогично Бобу может разбить состояние из четырех кубитов на две части и измерить состояния Белла каждой из них.

После шага 2 распределения ключа четыре кубита, отправленные Алисой, будут передаваться по квантовому каналу связи. Предположим, что Ева перехватывает эти четыре кубита и обрабатывает их так же, как и Боб. Затем Ева пересылает свои четыре обновлённых кубита Бобу.

Перебирая все возможные случаи группировок кубитов Евой и Бобом, можно получить полную вероятность того, что Боб получит неверный результат при измерении состояний Белла. Данная вероятность также называется долей ошибочных кубитов ε_e. Согласно [39] $\varepsilon = 0,1597$.

Найдём число битов двоичной случайной последовательности n, которые нужно сравнить Алисе и Бобу, чтобы обнаружить Еву с вероятностью $p_d = 1 - 10^{-9}$:

$$p_d = 1 - \varepsilon_e^n.$$

Минимальное значение $n = 11$ ([39]), в то время как Алиса и Боб должны сравнить $n = 72$ в протоколе BB84 ([31]), чтобы достичь аналогичной вероятности.

Вычислим взаимную информацию между Алисой и Евой:

$$\mathcal{I}(A;E) = 1 - [-\varepsilon_e \log_2 \varepsilon_e - (1-\varepsilon_e)\log_2(1-\varepsilon_e)] = 0,3664 \text{ бит}. \tag{6}$$

Принимая во внимание (5) и (6), заключаем, что $\mathcal{I}(A;B) > \mathcal{I}(A;E)$, то есть связь безопасна. Более того, $\mathcal{I}(A;B)$ в рассматриваемом протоколе больше чем $\mathcal{I}'(A;B) = 0,1887$ бит в протоколе BB84. Теоретическое значение секретности ключа:

$$\mathcal{R} = \mathcal{I}(A;B) - \mathcal{I}(A;E) = 0,7501 - 0,3664 = 0,3837 > 0.$$

4.2 Атака троянского коня

Атака троянского коня [25, 28, 37], подразумевает, что система QKD может быть взломана Евой путем отправки яркого света в квантовый канал и анализа обратного отражения. Ева использует вспомогательный источник, модулирует его и анализирует обратно рассеянный сигнал с помощью детектора. Как правило [25], схема обнаружения истинного сигнала основана на особенностях вспомогательного источника, например, на его фазе. Еве необходимо удалить часть истинного сигнала, и затем компенсировать введенные потери с помощью улучшения квантового канала. Следовательно, Еве нужно подготовить канал, который имеет меньшее затухание, чем изначальный квантовый канал. Если это выполнено, Ева может измерить перехваченное состояние с помощью квантовой памяти [39].

При атаке троянского коня известно измерение [25, 35], которое максимизирует собственную информацию Евы, т.е. информационный выигрыш:

$$\mathcal{I}_{Eve}^{T}(|\alpha|^2) = 1 - h(p),$$

где $p = \frac{1}{2}\left(\sqrt{1 - |\langle \alpha, 0|0, \alpha\rangle|^2}\right) \approx \frac{1+\sqrt{2}|\alpha|}{2}$, $h(p) = -p\log_2(p) - (1-p)\log_2(p)$, $|\alpha|^2$ обозначает номер фотона Евы.

Раскладывая выражение для собственной информации Евы в ряд Тейлора, получим:

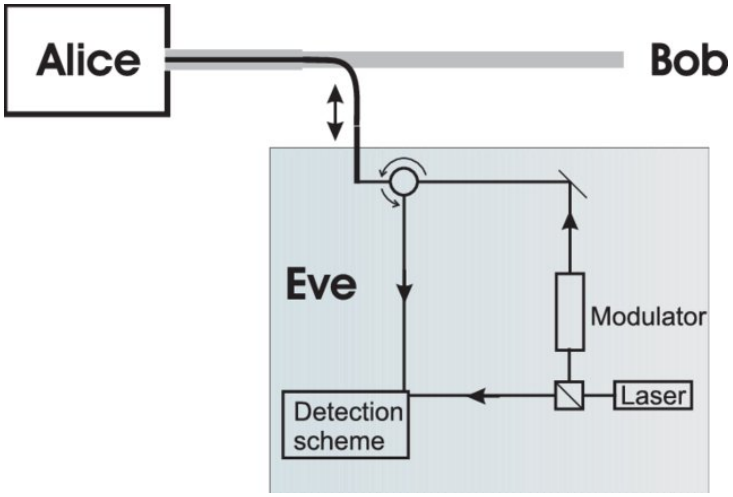

Рис. 3. Условная схема атаки троянского коня.

$$\mathcal{I}^T_{Eve}(|\alpha|^2) \approx 1 + \Big(\frac{1+\sqrt{2}|\alpha|}{2}\Big)\log_2\Big(\frac{1+\sqrt{2}|\alpha|}{2}\Big) + \Big(\frac{1-\sqrt{2}|\alpha|}{2}\Big)\log_2\Big(\frac{1-\sqrt{2}|\alpha]|}{2}\Big) =$$
$$= 1 - 1 + \frac{(\sqrt{2}|\alpha|)^2}{\log 4} + \frac{(\sqrt{2}|\alpha|)^4}{6\log 4} + \mathcal{O}(|\alpha|^6) = \frac{|\alpha|^2}{\log 2} + \mathcal{O}(|\alpha|^4).$$

Согласно (5), полученному выражению и границам, представленным в [25], мы можем заключить [39], что $\max\limits_{|\alpha|^2}\{\mathcal{I}^T_{Eve}(|\alpha|^2)\} < \mathcal{I}(A;B)$. Следовательно, атака троянского коня может быть предотвращена в рассматриваемом протоколе.

5 Практическое применение

Подводя итоги, ещё раз отметим, что рассмотренный протокол является перспективным усовершенствованием используемых в текущий момент квантовых протоколов [39, 24].

Приведём некоторые примеры практического использования QKD протоколов. Лос-Аламосская Национальная Лаборатория (англ.: Los Alamos National Laboratory) в 2007 году продемонстрировала использование квантового распределения ключей по оптоволокну длиной более 140 км с использованием протокола BB84 [27, 38]. Примечательно, что этого расстояния достаточно для почти всех участков современных волоконно-оптических сетей. Имеет смысл отметить достижение физиков из Института квантовых вычислений и Университета Ватерлоо, которые в 2017 впервые продемонстрировали функционирование квантового протокола распределения ключей от наземного передатчика к движущемуся самолету [36].

Также в настоящее время множество компаний предлагают коммерческие системы распределения квантовых ключей: ID Quantique [2], MagiQ Technologies Inc. [3], Quintessence Labs [5] и другие. В 2004 году в был осуществлен первый в мире банковский перевод с использованием квантового распределения ключей [7]. Технология квантового шифрования, предоставленная швейцарской компанией Id Quantique, использовалась в швейцарском штате Женева для передачи результатов голосования в столицу на национальных выборах, состоявшихся 21 октября 2007 года [23]. В 2013 году Мемориальный институт Баттеля (англ.: Battelle Memorial Institute) установил систему QKD, созданную ID Quantique, между их главным кампусом и их производственным предприятием в соседнем городе [17].

Авторы рассматриваемого протокола обещают в скором времени представить практическую демонстрацию [39].

A Группировки состояний

$$
\begin{aligned}
|\mathcal{C}\rangle_{1234} &= |\phi^-\rangle_{12} \otimes |\phi^+\rangle_{34} = \frac{1}{2}\big(\,|00\rangle_{12} - |11\rangle_{12}\,\big) \otimes \big(\,|00\rangle_{34} + |11\rangle_{34}\,\big) = \\
&= \frac{1}{2}\big(\,|0000\rangle + |0011\rangle - |1100\rangle - |1111\rangle\,\big)_{1234} = \\
&= \frac{1}{4}\big(2\,|0000\rangle + 2\,|0011\rangle - 2\,|1100\rangle - 2\,|1111\rangle\,\big)_{1234} = \\
&= \frac{1}{4}\big(\big[\,|0000\rangle - |0101\rangle + |1010\rangle - |1111\rangle\,\big] + \big[\,|0000\rangle + |0101\rangle - |1010\rangle - |1111\rangle\,\big] + \\
&+ \big[\,|0011\rangle - |0110\rangle + |1001\rangle - |1100\rangle\,\big] + \big[\,|0011\rangle + |0110\rangle - |1001\rangle - |1100\rangle\,\big]\big)_{1234} = \\
&= \frac{1}{4}\big([|00\rangle_{13}|00\rangle_{24} - |00\rangle_{13}|11\rangle_{24} + |11\rangle_{13}|00\rangle_{24} - |11\rangle_{13}|11\rangle_{24}] + \\
&+ [|00\rangle_{13}|00\rangle_{24} + |00\rangle_{13}|11\rangle_{24} - |11\rangle_{13}|00\rangle_{24} - |11\rangle_{13}|11\rangle_{24}] + \\
&+ [|01\rangle_{13}|01\rangle_{24} - |01\rangle_{13}|10\rangle_{24} + |10\rangle_{13}|01\rangle_{24} - |10\rangle_{13}|10\rangle_{24}] + \\
&+ [|01\rangle_{13}|01\rangle_{24} + |01\rangle_{13}|10\rangle_{24} - |10\rangle_{13}|01\rangle_{24} - |10\rangle_{13}|10\rangle_{24}]\big) = \\
&= \frac{1}{2}\big(|\phi^+\rangle_{13}|\phi^-\rangle_{24} + |\phi^-\rangle_{13}|\phi^+\rangle_{24} + |\psi^+\rangle_{13}|\psi^-\rangle_{24} + |\psi^-\rangle_{13}|\psi^+\rangle_{24}\big).
\end{aligned}
\tag{7}
$$

$$
\begin{aligned}
|\mathcal{C}\rangle_{1234} &= |\phi^-\rangle_{12} \otimes |\phi^+\rangle_{34} = \frac{1}{2}\big(\,|00\rangle_{12} - |11\rangle_{12}\,\big) \otimes \big(\,|00\rangle_{34} + |11\rangle_{34}\,\big) = \\
&= \frac{1}{2}\big(\,|0000\rangle + |0011\rangle - |1100\rangle - |1111\rangle\,\big)_{1234} = \\
&= \frac{1}{2}\big(\,|0000\rangle + |0011\rangle - |1100\rangle - |1111\rangle\,\big)_{1234} = \\
&= \frac{1}{\sqrt{2}}\big(|00\rangle_{12} - |11\rangle_{12}\big) \cdot \frac{1}{\sqrt{2}}\big(|00\rangle_{34} + |11\rangle_{34}\big) = |\phi^-\rangle_{12}|\phi^+\rangle_{34}.
\end{aligned}
\tag{8}
$$

Список литературы

[1] *Bloch sphere*. https://en.wikipedia.org/wiki/Bloch_sphere.

[2] *ID Quantique*. https://www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution.

[3] *MagiQ Technologies Inc.* https://www.magiqtech.com/solutions/network-security/.

[4] *QKD*. https://en.wikipedia.org/wiki/Quantum_key_distribution.

[5] *Quintessence Labs*. https://www.quintessencelabs.com/quantum-cybersecurity/.

[6] *Quantum Computation and Quantum Information*. Cambridge University Press, USA, 2000.

[7] World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photons. Press conference and demonstration of the ground-breaking experiment, Vienna City Hall. 2004.

[8] *Public debate on the Security of Quantum Key Distribution at the conference Hot Topics in Physical Informatics*, Nov 2013. http://www.ece.tamu.edu/~noise/HotPI_2013/HotPI_2013.html.

[9] Azuma, H., and Ban, M. The intercept/resend attack and the collective attack on the quantum key distribution protocol based on the pre- and post-selection effect, 2020.

[10] Beckers, A., Tajalli, A., and Sallese, J.-M. A Review on Quantum Computing: Qubits, Cryogenic Electronics and Cryogenic MOSFET Physics.

[11] Bennett C. H., B. G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of International Conference on Computers, Systems Signal Processing* (December 1984), p. 175.

[12] Breguet, J., Muller, A., and Gisin, N. Quantum Cryptography with Polarized Photons in Optical Fibres. *Journal of Modern Optics 41*, 12 (1994), 2405–2412.

[13] Briegel, H. J., and Raussendorf, R. Persistent Entanglement in Arrays of Interacting Particles. *Physical Review Letters 86*, 5 (Jan 2001), 910–913.

[14] Bub, J. Quantum Entanglement and Information. In *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed., summer 2020 ed. Metaphysics Research Lab, Stanford University, 2020.

[15] Chen, D., and Zhang, P. Four-state quantum key distribution exploiting maximum mutual information measurement strategy. *Quantum Inf Process 15* (2016), 881–891.

[16] Curty, M., and Lütkenhaus, N. Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses. *Phys. Rev. A 71* (Jun 2005), 062301.

[17] Dillow, C. *Unbreakable encryption comes to the U.S.* `https://web.archive.org/web/20131014104149/http://tech.fortune.cnn.com/2013/10/14/quantum-key/`.

[18] Dür, W., Vidal, G., and Cirac, J. I. Three qubits can be entangled in two inequivalent ways. *Physical Review A 62*, 6 (Nov 2000).

[19] Einstein, A., Podolsky, B., and Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev. 47* (May 1935), 777–780.

[20] Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett. 67* (Aug 1991), 661–663.

[21] Enríquez, M., Wintrowicz, I., and Życzkowski, K. Maximally Entangled Multipartite States: A Brief Survey. *Journal of Physics: Conference Series 698* (mar 2016), 012003.

[22] Feynman, R. P., Leighton, R. B., and Sands, M. *The Feynman lectures on physics; New millennium ed.* Basic Books, New York, NY, 2010. Originally published 1963-1965.

[23] Frank, J. Swiss Call New Vote Encryption System Unbreakable.

[24] Gao, G. Quantum key distribution by comparing Bell states. *Optics Communications 281*, 4 (2008), 876 – 879.

[25] Gisin, N., Fasel, S., Kraus, B., Zbinden, H., and Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review. A 73* (02 2006).

[26] Greenberger, D. M., Horne, M. A., and Zeilinger, A. Going Beyond Bell's Theorem, 2007.

[27] Hiskett, P. A., Rosenberg, D., Peterson, C. G., Hughes, R. J., Nam, S., Lita, A. E., Miller, A. J., and Nordholt, J. E. Long-distance quantum key distribution in optical fibre. *New Journal of Physics 8*, 9 (Sep 2006), 193–193.

[28] Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C., and Leuchs, G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New Journal of Physics 16*, 12 (dec 2014), 123030.

[29] Kim, Y.-H., Kulik, S. P., and Shih, Y. Bell-state preparation using pulsed nondegenerate two-photon entanglement. *Physical Review A 63*, 6 (May 2001).

[30] Li, C., Song, H.-S., Zhou, L., and Wu, C.-F. A random quantum key distribution achieved by using Bell states. *Journal of Optics B: Quantum and Semiclassical Optics 5*, 2 (Feb 2003), 155–157.

[31] Li J., Li N., L. L. One Step Quantum Key Distribution Based on EPR Entanglement. *Sci Rep 6* (2016).

[32] Liang, W.-Y., Li, M., Yin, Z.-Q., Chen, W., Wang, S., An, X.-B., Guo, G.-C., and Han, Z.-F. A simple implementation of quantum key distribution based on single-photon Bell state measurement, 2015.

[33] Mogos, G. Intercept-resend attack on quantum key distribution protocols with two, three and four-state systems: Comparative analysis. In *2015 2nd International Conference on Information Science and Security (ICISS)* (2015), pp. 1–4.

[34] Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., and Gisin, N. "Plug and play" systems for quantum cryptography. *Applied Physics Letters 70*, 7 (Feb 1997), 793–795.

[35] Peres, A. Quantum Theory: Concepts and Methods. *Kluwer Academic Publishers* (1993).

[36] Pugh, C. J., Kaiser, S., Bourgoin, J.-P., Jin, J., Sultana, N., Agne, S., Anisimova, E., Makarov, V., Choi, E., Higgins, B. L., and et al. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology 2*, 2 (Jun 2017), 024009.

[37] Sajeed, Minshull, Jain, and Makarov. Invisible Trojan-horse attack. *Scientific Reports* (2017).

[38] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A., and Weinfurter, H. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett. 98* (Jan 2007), 010504.

[39] Song, D., and Chen, D. Quantum Key Distribution Based on Random Grouping Bell State Measurement. *IEEE Communications Letters 24*, 7 (2020), 1496–1499.

[40] Watanabe, Y. Privacy amplification for quantum key distribution. *Journal of Physics A: Mathematical and Theoretical 40*, 3 (dec 2006), F99–F104.

[41] Yu K., Yang C., L. C. Authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf Process 13*, 5 (2014), 1457–1465.

[42] Yuan, H., Song, J., fang Han, L., Hou, K., and hua Shi, S. Improving the total efficiency of quantum key distribution by comparing Bell states. *Optics Communications 281*, 18 (2008), 4803 – 4806.

[43] Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. *Квантовая криптография.* Макс Пресс., 2011. Печатается по решению издательского отдела факультета ВМК МГУ.