Протокол QKD на основе случайных группировок и измерений состояний Белла

Аннотация

Рассматривается четырехкубитный квантовый протокол распределения ключей [25], базирующийся 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 приводятся предпосылки появления рассматриваемого протокола. В главе 2 описываются основные идеи, а также алгоритм распределения ключа. После чего в главе 3 производится анализ стойкости протокола на примере атаки перехвата – повторной передачи и атаки троянского коня. Наконец, в приложении А представлены выкладки, демонстрирующие принцип группировки кубитов.

1 История и предпосылки создания

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 [1, 2]. Различные типы QKD также были экспериментально продемонстрированы на сегодняшний день [5, 22].

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 [4]. Авторами был описан способ распределения случайного секретного ключа между Алисой и Бобом.

Позднее Экерт предложил другой протокол QKD [11], названный E91, основанный на парадоксе Эйнштейна-Подольского-Розена [10]. После этого были теоретически предложены и экспериментально реализованы различные протоколы QKD, например, базирующиеся на однофотонных [20] и множественных состояниях [7]. 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 [10]. В качестве квантового канала состояние Белла было впервые предложено в [13] и подтверждено [12] как максимально запутанное состояние двухкубитной квантовой системы. Кроме того, по сравнению с другими мультикубитными аналогами (состояния W [9], GHZ [15] и кластерные состояния [6]), состояние Белла легче всего реализовать с помощью нелинейного процесса, описанного в [17].

В основополагающей работе [13] две стороны разделяют секретный ключ, сравнивая форму начального состояния Белла и результат измерения состояния Белла после квантовой передачи. Затем [28] повысил общую эффективность коммуникации до 100% по срав-

нению с достигнутыми 50% в [13]. В [27] представлен первый аутентифицированный полуквантовый протокол распределения ключей без использования аутентифицированных классических каналов, основанный на состояниях Белла.

Авторы [13] и [28] 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 [25] было предложено усовершенствование [28] 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 [25].

2 Протокол QKD на основе случайных группировок и измерений состояний Белла

2.1 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 [13, 28], благодаря которому протокол решает проблему ультракороткого времени когерентности квантовых состояний.

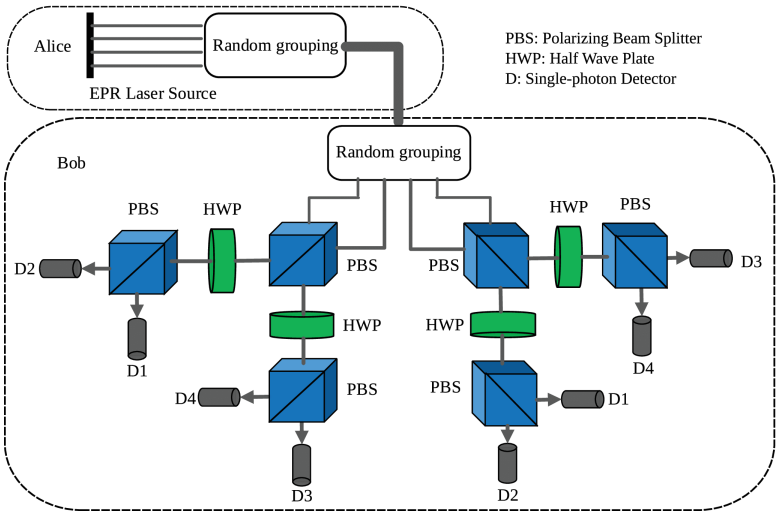

Рис. 1. Схема работы предлагаемого протокола QKD. Алиса подготавливает состояние из четырех кубитов и отправляет Бобу по квантовому каналу. Затем Боб группирует их случайным образом и измеряет эти кубиты в базисе состояний Белла.

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 (4)):

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

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

Из (1) 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 (1) представляет лишь одну из возможных комбинаций, подробный анализ всех состояний можно найти в [25, 18], 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. 1, где Алиса и Боб являются сертифицированными отправителем и приемником соответственно.

2.2 Алгоритм распределения ключей

- *Шаг 1. Подготовка состояний.* Алиса подготавливает одну из комбинаций четырёхкубитных состояний, например, представленную в уравнении (1). 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 [29]). 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.* [26, 29] 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 ${\mathcal{R}'}_B$.

2.3 Анализ доли ошибочных кубитов

Как уже оговаривалось, существует несколько различных способов группировок кубитов. Без ограничения общности будем считать, что группировка, приведённая в (1) 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 (1) выражается следующим образом (см. подробнее (5)):

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

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

Повторяя данные действия для всех возможных группировок, находим, что доля ошибочных кубитов $\varepsilon_0 = 0,0417$ [25]. Взаимная информация Алисы и Боба:

$$\mathcal{I}(A;B) = 1 - [-\varepsilon_0 \log_2 \varepsilon_0 - (1-\varepsilon_0)\log_2(1-\varepsilon_0)] = 0,7501 \text{ бит}. \tag{2}$$

3 Криптоанализ

3.1 Атака перехвата — повторной передачи

Одной из атак на QKD протоколы является атака перехвата — повторной передачи [8, 3, 21]. 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 [25] $\varepsilon = 0,1597$.

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 $n = 11$ ([25]), в то время как Алиса и Боб должны сравнить $n = 72$ в протоколе BB84 ([19]), чтобы достичь аналогичной вероятности.

Вычислим взаимную информацию между Алисой и Евой:

$$\mathcal{I}(A;E) = 1 - [-\varepsilon_e \log_2 \varepsilon_e - (1-\varepsilon_e)\log_2(1-\varepsilon_e)] = 0,3664 \text{ бит}. \tag{3}$$

Принимая во внимание (2) и (3), 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:

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

3.2 Атака троянского коня

Атака троянского коня [14, 16, 24], 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 [14], 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 [25].

При атаке троянского коня известно измерение [14, 23], 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:

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

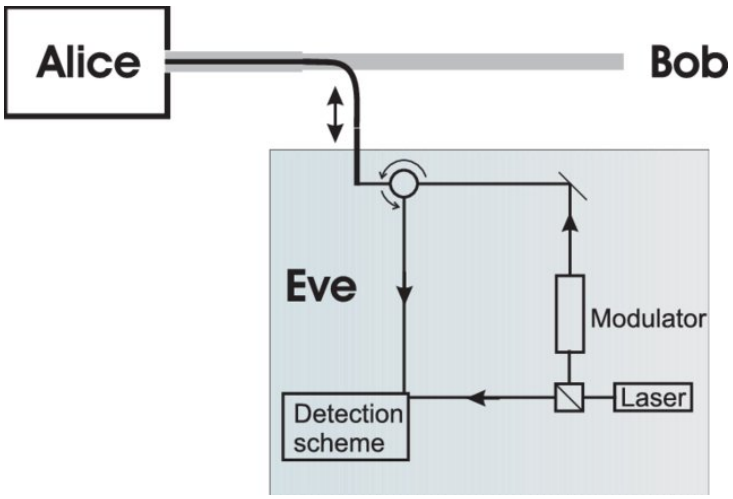

Рис. 2. Условная схема атаки троянского коня.

Согласно (2), полученному выражению и границам, представленным в [14], мы можем заключить [25], 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.

A Группировки состояний

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

$$
\begin{aligned}
|\mathcal{C}\rangle_{1234} &= |\phi^-\rangle_{12}\otimes|\phi^+\rangle_{34} = \frac{1}{2}\big(|00\rangle_{12}-|11\rangle_{12}\big)\otimes\big(|00\rangle_{34}+|11\rangle_{34}\big) = \\
&= \frac{1}{2}\big(|0000\rangle+|0011\rangle-|1100\rangle-|1111\rangle\big)_{1234} = \\
&= \frac{1}{2}\big(|0000\rangle+|0011\rangle-|1100\rangle-|1111\rangle\big)_{1234} = \\
&= \frac{1}{\sqrt{2}}\big(|00\rangle_{12}-|11\rangle_{12}\big)\cdot\frac{1}{\sqrt{2}}\big(|00\rangle_{34}+|11\rangle_{34}\big) = |\phi^-\rangle_{12}|\phi^+\rangle_{34}. \qquad (5)
\end{aligned}
$$

Список литературы

[1] *Quantum Key Distribution.* `https://en.wikipedia.org/wiki/Quantum_key_distribution`.

[2] *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`.

[3] 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.

[4] 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.

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

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

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

[8] 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.

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

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

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

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

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

[14] 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).

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

[16] 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.

[17] 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).

[18] 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.

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

[20] 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.

[21] 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.

[22] 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.

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

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

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

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

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

[28] 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.

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