КВАНТОВЫЕ СЕТИ: РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ ЧЕРЕЗ НЕДОВЕРЕННЫЕ УЗЛЫ

Кулик С.П.[1], Молотков С.Н.[2]

DOI: 10.21681/2311-3456-2025-3-90-98

Цель исследования: *анализ секретности квантового распределения ключей через недоверенные узлы в квантовых сетях.*

Метод исследования: *использование энтропийных соотношений неопределенностей.*

Результат(ы) исследования: *приведено доказательство секретности квантового распределения ключей через недоверенные узлы в квантовых сетях. Использование энтропийных соотношений неопределенностей позволяет получить точное решение для длины секретного ключа в однофотонном случае. Сделано сравнение с точным решением для протокола BB84 и явно показана принципиальная разница в логической структуре доказательств секретности ключей в этих протоколах, что, на наш взгляд, является важным для развития систем квантовой криптографии.*

Научная новизна: *приведено доказательство секретности квантового распределения ключей через недоверенные узлы в квантовых сетях.*

Ключевые слова: *квантовая криптография, фотоны, недоверенные узлы, энтропийные соотношения неопределенности.*

1. Введение

При построении волоконных систем квантовой криптографии важной задачей является увеличение дальности распределения секретных ключей. Неоднофотонность источника квантовых состояний и потери в линии связи приводят к тому, что длина линии связи оказывается ограниченной до величины, для которой гарантируется секретность распределяемых ключей. На сегодняшний день обсуждается несколько способов решения проблемы увеличения дальности:

1) использование квантовых повторителей;
2) распределение ключей по цепочке через промежуточные доверенные узлы;
3) передача ключей с использованием промежуточных недоверенных узлов;
4) использование специального протокола Measurement-Device-Independent (MDI-QKD) [1].

Первый способ требует пока отсутствующей долговременной квантовой памяти, поэтому практически не реализован.

Второй способ технически самый простой, но самый слабый с криптографической точки зрения, поскольку секретные ключи доступны на промежуточном доверенном узле, через который по цепочке происходит распределение секретных ключей. Использование доверенных узлов требует полной, в криптографическом смысле (технической и физической), защиты промежуточного узла; той же степени серьезности, как и защиты передающей и приемной станций.

В способе MDI-QKD промежуточные узлы выполняют измерения квантовых состояний, но не имеют доступа к самому ключу. Это позволяет снизить риск утечки информации через недоверенные узлы. Его преимущество – высокая безопасность и устойчивость к атакам на измерительные устройства. Однако существенным ограничением является сложная аппаратная реализация.

Третий способ привлекателен, поскольку не требует полной криптографической защиты промежуточного узла связи из-за того, что секретные ключи не возникают на данном узле. По этой причине такие промежуточные узлы называются недоверенными. Злоумышленник может видеть и знать всю работу аппаратуры на узле, но при этом не будет знать секретного ключа, который будет распределен между двумя легитимными пользователями через недоверенный узел. Такая удивительная, на первый взгляд, ситуация, кажется невозможной, тем не менее, может быть реализована с использованием квантовой криптографии.

Данная идея была сформулирована, по-видимому, впервые в работе [2], и основана на интерференции квантовых состояний от двух пространственно разделенных источников.

Идея квантового распределения ключей на основе квантового компаратора использует следующее свойство когерентных состояний – излучения лазера. При «сбивке» двух когерентных состояний $|\alpha\rangle$ и $|\beta\rangle$ на входах симметричного светоделителя,

1 Кулик Сергей Павлович, доктор физико-математических наук, профессор, Центр квантовых технологий, МГУ имени М.В. Ломоносова, Москва, Россия. E mail: sergei.kulik@physics.msu.ru

2 Молотков Сергей Николаевич, доктор физико-математических наук, профессор, Институт физики твердого тела имени Ю.А. Осипьяна РАН, г. Черноголовка Московской области, Россия. E-mail: molotkov@issp.ac.ru

на двух выходах светоделителя возникают состояния $\left|\frac{(\alpha+\beta)}{\sqrt{2}}\right\rangle$ и $\left|\frac{(\alpha-\beta)}{\sqrt{2}}\right\rangle$ (Рис. 1). Входные состояния «складываются» на одном выходе и «вычитаются» на другом выходе светоделителя – фактически сравниваются (именно с этим в работе [2] было связано название – квантовый компаратор). Иначе говоря, если фаза и амплитуда входных состояний одинаковы $\alpha = \beta = e^{i\varphi}|\alpha|$, то срабатывает детектор L (рис.1). Если фазы противоположны $\alpha = -\beta = e^{i\varphi}|\alpha|$, то срабатывает детектор R.

На такой идее может быть реализовано квантовое распределение ключей через недоверенные узлы, что потенциально может увеличить дальность распределения ключей в два раза. Отсчеты детектора публично известны Алисе, Бобу и злоумышленнику на узле, который знает работу всей аппаратуры[3].

В работе приведено точное доказательство секретности для квантового распределения ключей с недоверенным узлом.

2. Общая идея распределения ключей через недоверенные узлы

Протокол распределения ключей выглядит следующим образом. Алиса случайно и равновероятно посылает сильно ослабленные когерентные состояния, которые получаются ослаблением лазерного излучения, $0 \longrightarrow |\alpha\rangle_A$ или $1 \longrightarrow |-\alpha\rangle_A$. Аналогично, Боб посылает $0 \longrightarrow |\alpha\rangle_B$ или $1 \longrightarrow |-\alpha\rangle_B$.

Отсчеты детекторов на недоверенном узле публично известны. Алиса и Боб, зная отсчет детекторов, L или R, и зная бит, который они посылали, могут синхронизовать свои биты – получить общий одинаковый бит ключа (рис. 1). Причем, зная только отсчеты детекторов на недоверенном узле, узнать ключ невозможно.

Данный метод распределения ключей рассматривается как перспективная технология квантовой криптографии – квантового распределения секретных ключей [3].

Разумеется, техническая реализация метода достаточно сложна, поскольку требует реализации устойчивой интерференции квантовых состояний из двух пространственно разделенных лазеров. Принципиальная возможность интерференции состояний из разных источников в лабораторных условиях была продемонстрирована еще в 1967 г. в работе [4]. Перенос таких экспериментов на реальные волоконные линии связи, когда участники разделены линией в несколько сотен километров до недоверенного узла, представляет собой задачу с принципиально другим уровнем сложности по сравнению с лабораторными экспериментами. Важно отметить, что никаких принципиальных физических запретов на реализацию таких систем нет.

3 Разумеется, злоумышленник может вывести из строя саму аппаратуру, при этом ключи не будут распределены. Важно, что нарушитель может знать работу всей аппаратуры, но не будет знать секретных ключей.

Для распределения ключей достаточно посылать пакеты когерентных состояний, локализованные в одном временном окне (рис. 1). Однако, как будет видно ниже, для доказательства секретности удобнее использовать пару состояний, локализованных в двух временных окнах вида

$$|\alpha\rangle_{1A} \otimes |e^{i\varphi_A}\rangle_{2A}, |\alpha\rangle_{1B} \otimes |e^{i\varphi_B}\rangle_{2B}, \quad (1)$$

где фазы состояний

$$\text{базис} + \begin{cases} \varphi_A = 0,\pi \\ \varphi_B = 0,\pi \end{cases}, \text{базис} \times \begin{cases} \varphi_A = \frac{\pi}{2}, \frac{3\pi}{2} \\ \varphi_B = \frac{\pi}{2} \end{cases}. \quad (2)$$

Нижние индексы отвечают за временные окна, в которых локализованы пакеты когерентных состояний. Состояния, локализованные в первом временном окне, никакой информации о бите ключа не несут, т.к. информация содержится в фазе когерентного состояния, локализованного во втором временном окне. Поскольку подслушиватель знает работу аппаратуры на недоверенном узле, длину линии от Алисы и Боба до недоверенного узла, то считается, что он знает и фазу самого когерентного состояния – знает

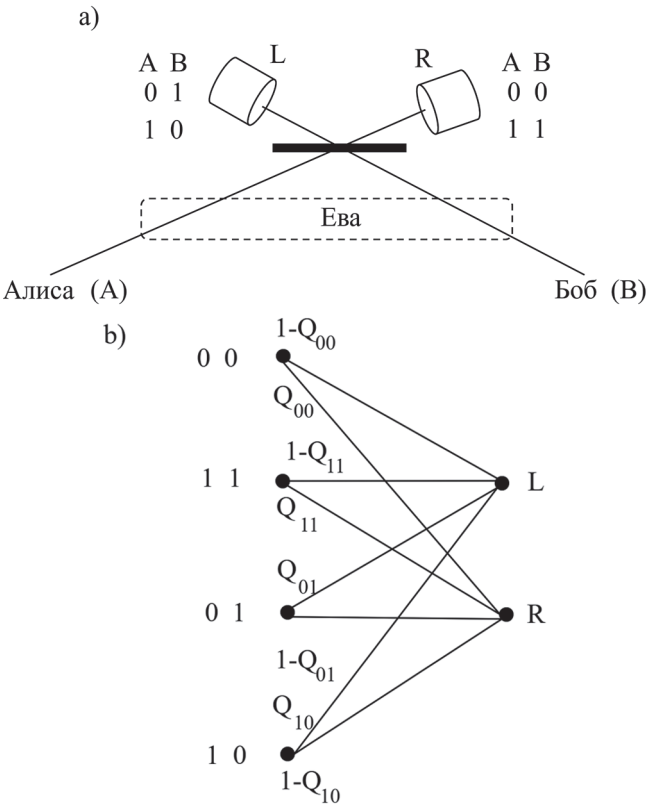

Рис. 1. a) Схематическое изображение квантового распределения ключей через недоверенный узел, и атака подслушивателя на два квантовых канала связи.

b) Структура классического канала (Алиса, Боб) – недоверенный узел. Показаны входной и выходной алфавит, а также переходные вероятности, описывающие канал связи.

комплексный параметр α, но не знает случайные в каждой посылке фазы φ_A и φ_B, несущие информацию о битах ключа.

Сбивка состояний на светоделителе приводит к состояниям на двух выходах, которые регистрируются детекторами L и R. Состояния на выходах светоделителя имеют вид

$$\text{Детектор } R\ |\frac{\alpha(e^{i\varphi_A}-e^{i\varphi_A})}{\sqrt{2}}\rangle_2 = |\sqrt{2}\bar{\alpha}\ \sin(\frac{\Delta\varphi}{2})\rangle_2,$$
$$\text{Детектор L}\ |\frac{\alpha(e^{i\varphi_A}+e^{i\varphi_A})}{\sqrt{2}}\rangle_2 = |\sqrt{2}\bar{\alpha}\ \cos(\frac{\Delta\varphi}{2})\rangle_2, \quad (3)$$

где

$$\Delta\varphi = \varphi_A - \varphi_B,\ \ .\bar{\alpha} = e^{i(\frac{\varphi_A+\varphi_B}{2})}. \quad (4)$$

Вероятность детектирования состояний детекторами L и R пропорциональна

$$Pr\{R,\Delta\varphi,\eta,l\} \propto 2\mu\sin^2(\frac{\Delta\varphi}{2})\eta_R\ T(l),$$
$$Pr\{L,\Delta\varphi,\eta,l\} \propto 2\mu\cos^2(\frac{\Delta\varphi}{2})\eta_L\ T(l), \quad (5)$$

где $T(l)$ – пропускание линии связи, l – длина линии связи, $\eta_{L,R}$ – квантовые эффективности детекторов.

В реальной ситуации в качестве информационных состояний используются сильно ослабленные когерентные состояния, которые имеют пуассоновскую статистику по числу фотонов. Т.е., кроме однофотонной компоненты, когерентные состояния содержат многофотонные составляющие фоковских состояний.

Первая задача состоит в получении доказательства секретности для однофотонных информационных состояний, поскольку секретный ключ формируется из однофотонной компоненты когерентных состояний.

Информация из многофотонных компонент, консервативно в пользу подслушивателя, считается полностью известной подслушивателю. Доля однофотонной компоненты на втором этапе доказательства секретности ключей может быть оценена, например, с использованием т.н. Decoy State метода [5].

Насколько нам известно, доказательство секретности ключей даже в однофотонном случае для квантового распределения ключей с недоверенным узлом не получено. Например, в работе [3], приводится длина секретного ключа для однофотонной компоненты, которая приведена без всякого вывода и, по сути, взята из работ, относящихся к протоколу BB84 [6]. Хотя сразу видно, что ситуация физически принципиально другая по сравнению с ситуацией, когда ключи распределяются непосредственно между Алисой и Бобом, поэтому и логика анализа секретности ключей также принципиально другая. Как будет видно ниже, длина секретного ключа будет зависеть от четырех параметров (ошибки в двух каналах связи Алиса – недоверенный узел, и Боб – недоверенный узел). Этот факт вносит принципиальное различие в анализ секретности, выполненный для протокола BB84 [6].

Ниже будет приведено точное доказательство секретности для квантового распределения ключей с недоверенным узлом. Под точным решением понимается решение, которое основано на фундаментальных энтропийных соотношениях неопределенностей, использование которых позволяет оценить верхнюю границу утечки информации к подслушивателю по наблюдаемому уровню ошибок при детектировании состояний детекторами L и R. Энтропийные соотношения, возникающие в данной задаче, по логике и структуре принципиально отличаются от соответствующих энтропийных соотношений при доказательстве секретности протокола BB84. Будет также проведено сравнение с доказательством секретности для протокола BB84, и явно показана принципиальная разница в логике и структуре доказательства, а также результатах по оценке длины секретного ключа.

3. Однофотонный случай, двойное запутанное квантовое состояние

При доказательстве секретности стандартного протокола BB84 используется сведение протокола, к так называемой, ЭПР-версии (запутанное состояние Эйнштейна-Подольского-Розена) [7–9].

Необходимость сведения протокола к ЭПР-версии связана с дальнейшим использованием энтропийных соотношений неопределенностей. Такое сведение является формальным математическим приемом. ЭПР-версия протокола эквивалентна исходной версии – приготовление, посыл состояний. ЭПР-пара нужна для использования энтропийных соотношений неопределенностей, поскольку в них фигурирует матрица плотности Алиса-Боб-Ева, которая происходит в разных базисах из одного и того же исходного состояния.

ЭПР-версия протокола выглядит следующим образом. Алиса генерирует ЭПР-пару, свою подсистему оставляет себе, а подсистему Боба отправляет на приемную станцию. Измерение Алисы над своей подсистемой в одном из базисов переводит ЭПР-пару в одно из базисных состояний для Алисы и Боба. Подсистема Боба подвержена атакам подслушивателя в канале связи.

При распределении с недоверенным узлом Алиса и Боб независимо посылают состояния, отвечающие 0 и 1. Посылки, где базисы Алисы и Боба не совпадали, отбрасываются. В каждом базисе возможны 4 комбинации состояний Алисы и Боба в канале связи, которые доступны для подслушивателя: (00), (11), (01), (10), отсчеты детекторов также известны.

Ниже протокол будет сведен к ЭПР-версии, при этом приходится использовать две независимые

ЭПР-пары. Уже на данном этапе возникает существенное отличие от доказательства секретности для протокола BB84.

Введем вспомогательные состояния Алисы (индекс $\bar{A}$) и Боба (индекс $\bar{B}$). Это состояния, которые остаются как эталонные на передающих станциях Алисы и Боба. Состояния, которые посылаются Алисой и Бобом в линию связи, имеют индексы A и B. Представления ЭПР-пары $\bar{A}A$) для канала (Алиса–недоверенный узел) в разных базисах имеет вид

$$|\Phi\rangle_{\bar{A}A} = \frac{1}{\sqrt{2}}\left(|\bar{0}^{+}\rangle_{\bar{A}} \otimes |\bar{0}^{+}\rangle_{A} + |\bar{1}^{+}\rangle_{\bar{A}} \otimes |\bar{1}^{+}\rangle_{A}\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|\bar{0}^{\times}\rangle_{\bar{A}} \otimes |\bar{0}^{\times}\rangle_{A} + |\bar{1}^{\times}\rangle_{\bar{A}} \otimes |\bar{1}^{\times}\rangle_{A}\right). \quad (6)$$

Аналогично для ЭПР-пары $\bar{B}B$) для канала (Боб – недоверенный узел) имеем

$$|\Phi\rangle_{\bar{B}B} = \frac{1}{\sqrt{2}}\left(|\bar{0}^{+}\rangle_{\bar{B}} \otimes |\bar{0}^{+}\rangle_{B} + |\bar{1}^{+}\rangle_{\bar{B}} \otimes |\bar{1}^{+}\rangle_{B}\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|\bar{0}^{\times}\rangle_{\bar{B}} \otimes |\bar{0}^{\times}\rangle_{B} + |\bar{1}^{\times}\rangle_{\bar{B}} \otimes |\bar{1}^{\times}\rangle_{B}\right). \quad (7)$$

Соответственно, двойная ЭПР-пара имеет вид

$$|\Phi\rangle_{\bar{A}\bar{B}AB} = |\Phi\rangle_{\bar{A}A} \otimes |\Phi\rangle_{\bar{B}B}. \quad (8)$$

Выбор состояния, которое посылается в каждый канал связи, осуществляется при помощи измерения в выбранном базисе над вспомогательными подсистемами $\bar{A}$ и $\bar{B}$. Измерения даются разложениями единицы

$$I_{\bar{A}} = |\bar{0}^{+}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{0}^{+}| + |\bar{1}^{+}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{1}^{+}| = |\bar{0}^{\times}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{0}^{\times}| + |\bar{1}^{\times}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{1}^{\times}|. \quad (9)$$

Аналогично для подсистемы $\bar{B}$

$$I_{\bar{B}} = |\bar{0}^{+}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{0}^{+}| + |\bar{1}^{+}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{1}^{+}| = |\bar{0}^{\times}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{0}^{\times}| + |\bar{1}^{\times}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{1}^{\times}|. \quad (10)$$

Измерение над двумя вспомогательными подсистемами для двух каналов дается разложением единицы

$$I_{\bar{A}\bar{B}} = I_{\bar{A}} \otimes I_{\bar{B}}. \quad (11)$$

4. Атака подслушивателя на квантовые состояния

После измерений подсистемы A и B переходят в одно из четырех состояний, которые подвержены атаке подслушивателя. Атака подслушивателя описывается супероператором T_{EAB}, явный вид которого, не потребуется. После атаки подслушивателя состояния в линиях связи даются следующими матрицами плотности в двух линиях связи

$$\rho_{ABE}(00) = T_{EAB}(|0^{+}0^{+}\rangle_{AB_{AB}}\langle 0^{+}0^{+}|),$$
$$\rho_{ABE}(01) = T_{EAB}(|0^{+}1^{+}\rangle_{AB_{AB}}\langle 0^{+}1^{+}|), \quad (12)$$
$$\rho_{ABE}(10) = T_{EAB}(|1^{+}0^{+}\rangle_{AB_{AB}}\langle 1^{+}0^{+}|),$$
$$\rho_{ABE}(11) = T_{EAB}(|1^{+}1^{+}\rangle_{AB_{AB}}\langle 1^{+}1^{+}|), \quad (13)$$

Для полной матрицы плотности в базисе + получаем

$$\rho_{\bar{A}\bar{B}AB} = (T_{EAB}(I_{\bar{A}\bar{B}}|\Phi\rangle_{\bar{A}\bar{B}AB_{\bar{A}\bar{B}AB}}\Phi|I_{\bar{A}\bar{B}}))=$$
$$= \frac{1}{4}\left(|\bar{0}^{+}\bar{0}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{0}^{+}\bar{0}^{+}| \otimes \rho_{ABE}(00) + \right.$$
$$+ |\bar{0}^{+}\bar{1}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{0}^{+}\bar{1}^{+}| \otimes \rho_{ABE}(01) +$$
$$+ |\bar{1}^{+}\bar{0}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{1}^{+}\bar{0}^{+}| \otimes \rho_{ABE}(10) +$$
$$\left. + |\bar{1}^{+}\bar{1}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{1}^{+}\bar{1}^{+}| \otimes \rho_{ABE}(11)\right), \quad (14)$$

В дальнейшем удобно ввести более компактные обозначения, заменив подсистемы $\bar{A}\bar{B}$ на случайную переменную X, которая имеет 4 значения. Для матрицы плотности в базисе + имеем

$$\rho_{X^{+}(AB)E} = \frac{1}{4}\sum_{x^{+}\in X^{+}}|x^{+}\rangle_{X_X}\langle x^{+}| \otimes \rho^{x^{+}}_{(AB)E}, \quad (15)$$

где

$$X^{+} = \{0^{+}0^{+},0^{+}1^{+},1^{+}0^{+},1^{+}1^{+}\}. \quad (16)$$

Аналогично в базисе ×

$$\rho_{X^{\times}(AB)E} = \frac{1}{4}\sum_{x^{\times}\in X^{\times}}|x^{\times}\rangle_{X_X}\langle x^{\times}| \otimes \rho^{x^{\times}}_{(AB)E}, \quad (17)$$

где значения случайной переменной X принадлежат алфавиту

$$X^{+} = \{0^{\times}0^{\times},0^{\times}1^{\times},1^{\times}0^{\times},1^{\times}1^{\times}\}. \quad (18)$$

5. Измерения на недоверенном узле

Рассмотрим измерения над состояниями в (15), поступающими из линий связи, на недоверенном узле. Преобразование состояний после измерений на недоверенном узле удобно описывать при помощи операторов Крауса, которые проектируют информационные состояния из обоих каналов. Поскольку результат детектирования известен, то удобно ввести формальные состояния $|L\rangle$ и $|R\rangle$, которые «привязаны» к отсчетам детекторов. В базисе + имеем

$$K^{+}_{(00),L} = |0^{+}0^{+}\rangle_{(AB)_Y}\langle L|,\ K_{(00),L} = |L\rangle_{Y_{(AB)}}\langle 0^{+}0^{+}|, \quad (19)$$
$$K^{+}_{(11),L} = |1^{+}1^{+}\rangle_{(AB)_Y}\langle L|,\ K_{(11),L} = |L\rangle_{Y_{(AB)}}\langle 1^{+}1^{+}|L|, \quad (20)$$
$$K^{+}_{(01),R} = |0^{+}1^{+}\rangle_{(AB)_Y}\langle R|,\ K_{(01),R} = |R\rangle_{Y_{(AB)}}\langle 0^{+}1^{+}|, \quad (21)$$
$$K^{+}_{(10),R} = |1^{+}0^{+}\rangle_{(AB)_Y}\langle R|,\ K_{(10),R} = |R\rangle_{Y_{(AB)}}\langle 1^{+}0^{+}|. \quad (22)$$

Аналогично предыдущему, операторы Крауса в базисе × имеют вид

$$K^{+}_{(00),L} = |0^{\times}0^{\times}\rangle_{(AB)_Y}\langle L|,\ K_{(00),L} = |L\rangle_{Y_{(AB)}}\langle 0^{\times}0^{\times}|, \quad (23)$$
$$K^{+}_{(11),L} = |1^{\times}1^{\times}\rangle_{(AB)_Y}\langle L|,\ K_{(11),L} = |L\rangle_{Y_{(AB)}}\langle 1^{\times}1^{\times}|, \quad (24)$$
$$K^{+}_{(01),R} = |0^{\times}1^{\times}\rangle_{(AB)_Y}\langle R|,\ K_{(01),R} = |R\rangle_{Y_{(AB)}}\langle 0^{\times}1^{\times}|, \quad (25)$$
$$K^{+}_{(10),R} = |1^{\times}0^{\times}\rangle_{(AB)_Y}\langle R|,\ K_{(10),R} = |R\rangle_{Y_{(AB)}}\langle 1^{\times}0^{\times}|, \quad (26)$$

где состояния $|R\rangle_Y$ и $|L\rangle_Y$ описывают отсчеты в одном из детекторов.

Результат измерений описывается случайной переменной Y, значения которой (y) принадлежат выходному алфавиту – отсчету в L или R детекторе,

$$y \in Y = \{L,R\}. \quad (27)$$

После измерений отсчета детектора на недове-

ренном узде, матрица плотности всех участников протокола Алиса-Боб-Ева в базисе + принимает вид

$$\rho_{X^+YE} = \frac{1}{4}\sum_{x^+\in X^+}\sum_{y\in Y}|x^+\rangle_{X_X}\langle x^+| \otimes |y\rangle_{Y_Y}\langle y| \otimes \rho_E^{x^+y}, \quad (28)$$

где

$$\rho_E^{x^+y} = \sum_{i=0,1}\sum_{j=0,1} K_{(ij),y}\, \rho^{x^+}_{(AB)E}\, K^+_{(ij),y}. \quad (29)$$

Аналогично для матрицы плотности в базисе × находим

$$\rho_{X^\times YE} = \frac{1}{4}\sum_{x^\times\in X^\times}\sum_{y\in Y}|x^\times\rangle_{X_X}\langle x^\times| \otimes |y\rangle_{Y_Y}\langle y| \otimes \rho_E^{x^\times y}, \quad (30)$$

где

$$\rho_E^{x^\times y} = \sum_{i=0,1}\sum_{j=0,1} K_{(ij),y}\, \rho^{x^\times}_{(AB)E}\, K^+_{(ij),y}. \quad (31)$$

Перейдем теперь к энтропийным соотношениям неопределенностей, в которых фигурируют матрицы плотности (15, 28, 30) и которые позволяют получить фундаментальную верхнюю границу утечки информации к подслушивателю.

6. Энтропийные соотношения неопределенностей

Для стандартного протокола BB84 энтропийные соотношения неопределенностей представляют собой «закон сохранения суммы двух условных энтропий – информаций Алиса-Евы и Алиса-Боб» (см. детали в [8, 10]). Данные соотношения позволяют найти верхнюю границу нехватки информации Евы относительно информационной строки Алисы через нехватку информации Боба относительно информационной строки Алисы. Нехватка информации Боба, классическая условная энтропия Шеннона Алиса-Боб, после измерений Боба оценивается через открытый классический канал связи по наблюдаемому числу ошибок.

В рассматриваемом случае энтропийные соотношения неопределенностей представляют собой закон сохранения суммы двух условных энтропий – $H(X^\times|E)$ условная энтропия между случайной величиной $X^\times$, находящейся у Алисы и Боба (см. (15, 17)) и Евой, и условной энтропией $H(X^+|Y)$ между X^+ (Алиса-Боб в сопряженном базисе) и Y – недоверенным узлом.

В асимптотическом пределе энтропийные соотношения неопределенностей [7,8] принимают вид

$$H(X^\times|E) + H(X^+|Y) \geq -\log|c|^2 = 2,$$
$$|c|^2 = \max_{i,j,i',j'=0,1} |_{\bar{A}\bar{B}}\langle i^+ j^+|i'^\times\, j'^\times\rangle_{\bar{A}\bar{B}}|^2 = \frac{1}{4}, \quad (32)$$

где

$$H(X^\times|E) = H(\rho_{X^\times E}) - H(\rho_E),\ H(X^+|Y) = H(\rho_{X^+Y}) - H(\rho_Y). \quad (33)$$

Частичная матрица плотности подслушивателя ρ_E в (33) относится к базису +. Матрица плотности (Алиса, Боб) – недоверенный узел $\rho_{X^+Y} = Tr_E\{\rho_{X^+YE}\}$ выражается через наблюдаемые параметры классического канала (Алиса, Боб) – недоверенный узел. Структура канала изображена на рис. 1. Для матрицы плотности находим

$$\rho_{X^+Y} =$$
$$= \frac{1}{4}|0^+0^+\rangle_{X_X}\langle 0^+0^+| \otimes \{(1-Q_{00})|L\rangle_{Y_Y}\langle L| + Q_{00}\,|R\rangle_{Y_Y}\langle R|\} +$$
$$+ \frac{1}{4}|0^+1^+\rangle_{X_X}\langle 0^+1^+| \otimes \{(1-Q_{01})|R\rangle_{Y_Y}\langle R| + Q_{01}|L\rangle_{Y_Y}\langle L|\} +$$
$$+ \frac{1}{4}|1^+0^+\rangle_{X_X}\langle 1^+0^+| \otimes \{(1-Q_{10})|R\rangle_{Y_Y}\langle R| + Q_{10}|L\rangle_{Y_Y}\langle L|\} +$$
$$+ \frac{1}{4}|1^+1^+\rangle_{X_X}\langle 1^+1^+| \otimes \{(1-Q_{11})|L\rangle_{Y_Y}\langle L| + Q_{10}|R\rangle_{Y_Y}\langle R|\}. \quad (34)$$

Переходные вероятности Q_{ij}, задающие классический канал связи (рис. 1) относятся к базису +, индекс базиса + для краткости опускаем. Для однофотонной компоненты для дальнейшего удобно обозначить так

$$P_{X|Y}(y|X=(ij)) = Q_{ij}, \quad (35)$$

где $y = L,R$. Например, $P_{X|Y}(L|X=(00))$ – условная вероятность того, что Алиса и Боб послали (00), и сработал детектор L, и т.д. Индекс базиса для краткости опускаем.

С учетом (33, 34) (см. также рис.) для условной энтропии находим

$$H(\rho_{X^+Y}) = 2 + \frac{1}{4}\sum_{i,j=0,1} h(Q_{ij}). \quad (36)$$

где $h(x) = -x\log(x) - (1-x)\log(1-x)$ – бинарная энтропийная функция Шеннона.

В симметричном случае, когда $Q_{ij} = Q$, получаем

$$H(\rho_{X^+Y}) = 2 + h(Q). \quad (37)$$

Далее для частичной матрицы плотности, описывающей состояния на недоверенном узле, с учетом (34), находим

$$\rho_Y = Tr_{X^+}\{\rho_{X^+Y}\} =$$
$$= \frac{1}{4}\{[2 - Q_{00} - Q_{11} + Q_{01} + Q_{10}]|L\rangle_{Y_Y}\langle L| +$$
$$+ [2 - Q_{01} - Q_{10} + Q_{00} + Q_{11}]|R\rangle_{Y_Y}\langle R|\}. \quad (38)$$

$$H(\rho_Y) = 1 - \bar{h}(q), \quad (39)$$

$$\bar{h}(q) = -(1-q)\log(1-q) - (1+q)\log(1+q),$$
$$q = \frac{1}{2}(Q_{00} + Q_{11} - Q_{01} - Q_{10}). \quad (40)$$

В итоге для условной энтропии находим с учетом (37) и (39)

$$H(X^+|Y) = 1 + \frac{1}{4}\sum_{i,j=0,1} h(Q_{ij}) - \bar{h}(q). \quad (41)$$

В симметричном случае ф-ла (41) принимает простой вид

$$H(X^+|Y) = 1 + h(q). \quad (42)$$

Интерпретация (42) имеет простой смысл. Канал на рис. 2 имеет четыре равновероятных состояний на входе (00), (11), (01), (10) и два состояния на выходе L и R. Уловная энтропия $H(X^+|Y)$ выхода

относительно входа имеет смысл нехватки информации выхода относительно входа, точнее говоря, нехватка информации в битах о входе при условии, что известен выход. На входе в канал поступает два бита информации – (00), (11), (01), (10). Если нет ошибок $Q = 0$, то знание того, какой детектор сработал L или R дает один бит информации. Условная энтропия при этом $H(X^+|Y) = 1$, т.е. не хватает одного бита, чтобы полностью знать информацию – два бита на входе в канал. Если подслушиватель вторгается в оба канала от Алисы и Боба к недоверенному узлу и получает информацию о передаваемых состояниях, то при этом возмущает их, что приводит к ошибкам в отсчетах детекторов.

7. Сравнение с точным решением для протокола BB84

В протоколе BB84 при доказательстве секретности используется одна ЭПР-пара Алиса-Боб

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0^+\rangle_A \otimes |\bar{0}^+\rangle_B + |1^+\rangle_A \otimes |1^+\rangle_B\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|0^\times\rangle_A \otimes |0^\times\rangle_B + |1^\times\rangle_A \otimes |1^\times\rangle_B\right). \quad (43)$$

В асимптотическом пределе вместо (32, 33) возникают следующие энтропийные соотношения неопределенностей

$$H(X^\times|E) + H(X^+|Y) \geq -\log|c|^2 = 1,$$

$$|c|^2 = \max_{i,j,=0,1}|A\langle i + |j^\times\rangle A|^2 = \frac{1}{2}. \quad (43)$$

Соответственно, матрица плотности в базисе +, вместо (34), принимает вид

$$\rho_{X^+Y} = \frac{1}{2}|0^+\rangle_{X_X}\langle 0^+| \otimes \{(1 - Q_0)|0\rangle_{Y_Y}\langle 0| + Q_0|1\rangle_{Y_Y}\langle 1|\} +$$

$$+ \frac{1}{2}|1^+\rangle_{X_X}\langle 1^+| \otimes \{(1 - Q_1)|1^+\rangle_{Y_Y}\langle 1^+| + Q_1|0^+\rangle_{Y_Y}\langle 0^+|\}. \quad (45)$$

С учетом (45) , находим

$$H(\rho_{X^+Y}) = 1 + \frac{1}{2}\left(h(Q_0) + h(Q_1)\right). \quad (44)$$

В симметричном случае, когда $Q_0 = Q_1 = Q$, получаем

$$H(\rho_{X^+Y}) = 1 + h(Q). \quad (45)$$

Далее для частичной матрицы плотности Боба, с учетом (45), находим

$$\rho Y = Tr_{X^+}\{\rho_{X^+Y}\} = \frac{1}{2}\{|0^+\rangle_{Y_Y}\langle 0^+| + |1^+\rangle_{Y_Y}\langle 1^+|\}. \quad (46)$$

$$H(\rho_Y) = 1. \quad (47)$$

Напомним, что матрица плотности ρ_Y в ф-лах выше относится к базису +.

В итоге для условной энтропии, с учетом (46) и (49), получаем

$$H(X^+|Y) = \frac{1}{2}\left(h(Q_0) + h(Q_1)\right). \quad (48)$$

В симметричном случае ф-ла (50) принимает простой вид

$$H(X^+|Y) = h(Q), \quad (49)$$

которая дает нехватку информации выхода дискретного классического бинарного канала связи относительно входа [10]. В общем случае канал несимметричен.

8. Утечка информации при коррекции ошибок

После передачи квантовых состояний и измерений – отсчетов L и R детекторами, Алиса и Боб связаны бинарным (не обязательно симметричным) классическим каналом связи. Ситуация поясняется на рис. 2. Поскольку цель Алисы и Боба – получить идентичную битовую последовательность, то необходимо «привязаться», пусть для определенности, Бобу к битовой строке Алисы.

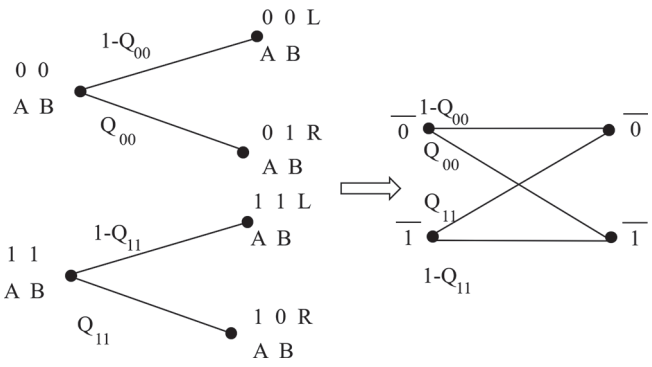

Рис. 2. Пояснения к процедуре коррекции ошибок Алисой и Бобом. Привязка происходит к биту Алисы (левая половина рис.). Правая половина – структура бинарного классического канала связи, в котором происходит коррекция ошибок – общего бита $\bar{0}$ или $\bar{1}$. Показаны также переходные вероятности бинарного канала связи в котором происходит коррекция ошибок.

Пусть привязка общих бит ($\bar{0}$, $\bar{1}$) идет к битам Алисы (см. рис. 2). Алиса всегда считает общим битом тот бит, который она послала. Алиса послала 0, тогда отсчет детектора L считает общим битом $\bar{0}$. Послала 1 – отсчет детектора L считает общим бит $\bar{1}$.

Далее Алиса послала 0 – отсчет детектора R считает общим бит $\bar{0}$, послала 1 – отсчет детектора R считает общим бит $\bar{1}$.

Пусть Алиса и Боб посылали 0 и 0 (уже в совпадающем базисе.) Пусть произошел отсчет в детекторе L – правильный отсчет. Тогда Алиса и Боб будут иметь одинаковый бит. Вероятность такого события есть $1 - Q_{00}$.

Если произошел отсчет в детекторе R, то Алиса будет считать общим битом свой бит 0 – привязка идет к ее битам, а Боб будет считать общим битом 1, что будет ошибкой. Вероятность такого события есть Q_{00}.

Аналогично, если Алиса посылала 1 и Боб посылал 1. Вероятность правильного отсчета есть $1 - Q_{11}$ – совпадение бита Алисы и Боба. Соответственно, вероятность ошибки есть Q_{11}.

Аналогично проводятся рассуждения, когда Алиса и Боб посылали противоположные значения бит.

С учетом сказанного, приходим к задаче исправления ошибок в бинарном классическом канале связи, точнее в двух независимых каналах связи с переходными вероятностями $\{1-Q_{00}, Q_{00}, 1-Q_{11}, Q_{11}\}$ и $\{1-Q_{01}, Q_{01}, 1-Q_{10}, Q_{10}\}$.

Далее, пусть передана и зарегистрирована серия длины n в асимптотическом пределе длинных последовательностей, в $\frac{1}{4}n$ посылок посылались состояния (00), $\frac{1}{4}n$ – (11), $\frac{1}{4}n$ – (01), $\frac{1}{4}n$ – (10). Утечка информации leak на одну посылку, которая требуется для исправления ошибок во всей последовательности в асимптотическом пределе

$$n\cdot leak = n[\frac{1}{2}\frac{(h(Q_{00})+h(Q_{11}))}{2}+\frac{1}{2}\frac{(h(Q_{01})+h(Q_{10}))}{2}. \quad (50)$$

Соответственно, в симметричном случае получаем

$$n\cdot leak = n[\frac{1}{2}\frac{(h(Q)+h(Q))}{2}+\frac{1}{2}\frac{(h(Q)+h(Q))}{2}. \quad (51)$$

Для сравнения, в протоколе BB84 ситуация между Алисой и Бобом после передачи и измерения квантовых состояний описывается одним классическим бинарным (в общем случае несимметричным) каналом связи, поэтому утечка информации при коррекции ошибок в асимптотическом пределе есть

$$n\cdot leak = n\frac{(h(Q_0)+h(Q_1))}{2}. \quad (52)$$

Для бинарного симметричного классического канала связи имеем

$$n\cdot leak = nh(Q). \quad (53)$$

Теперь можем перейти к вычислению длины секретного ключа.

9. Оценка длины секретного ключа

Для оценки длины секретного ключа (l) в пределе асимптотически длинных последовательностей ($n\longrightarrow\infty$) имеет место (см. детали в [7–9])

$$l=\lim_{n\to\infty}\frac{ln}{n}=H(X^{\times}|E)-leak, \quad (54)$$

здесь $leak$ – количество бит в пересчете на одну зарегистрированную посылку n, расходуемых на коррекцию ошибок. Ф-ла (56) имеет простую интерпретацию. Неформально, условная энтропия $H(X^{\times}|E)$ есть нехватка информации подслушивателя на одну посылку, которой не хватает до полного знания значения случайной переменной $X^{\times}$ при условии, что подслушиватель имеет в своем распоряжении квантовую систему E. Условная энтропия $H(X^{\times}|E)$ содержит в себе всю информацию об атаках подслушивателя. Энтропийные соотношения неопределенностей (32) позволяют найти фундаментальную нижнюю границу $H(X^{\times}|E)$ в базисе ×, не перебирая различные атаки, а получить оценку этой границы через наблюдаемые параметры классического канала (Алиса, Боб) – (детекторы L,R) в сопряженном базисе +.

Выражая $H(X^{\times}|E)$ через энтропийные соотношения неопределенностей (32), с учетом (41), получаем

$$H(X^{\times}|E)\geq 2-H(X^{+}|Y)=$$
$$=2-(1+\frac{1}{2}\sum_{i,j=0,1}h(Q_{ij})-\bar{h}(q)), \quad (55)$$

и

$$l=(X^{\times}|E)-leak=2-H(X^{+}|Y)-leak=$$
$$=1-(\frac{1}{2}\sum_{i,j=0,1}h(Q_{ij})-\bar{h}(q)). \quad (56)$$

В случае симметричного канала связи, когда $Q_{ij}=Q$ из (58), получаем

$$l=1-2h(Q), \quad (57)$$

Для сравнения приведем оценку длины секретного ключа для протокола BB84, с учетом (50,54) и (56), получаем

$$l=1-(h(Q_0)+h(Q_1)), \quad (58)$$

соответственно, в симметричном случае $Q_0=Q_1=Q$ находим

$$l=1-2h(Q). \quad (59)$$

В симметричном случае критическая ошибка Q, до которой можно распределять секретные ключи в протоколе распределения ключей через недоверенные узлы, такая же как в симметричном случае в протоколе BB84, и дается корнем уравнений (59) и (61), и оказывается равной $Q\approx 11\ \%$.

10. Заключение

На сегодняшний день передачу данных между узлами квантовой сети выполняют так называемые доверенные промежуточные узлы связи. При этом владелец сети контролирует все оборудование, которое генерирует, передает и принимает фотоны – носители информации. Такое решение проблемы позволяет исключить подключение к ним злоумышленников – за счет архитектуры сети. Однако такое построение систем связи не позволяет подключать большое число абонентов к инфраструктуре.

Для масштабирования квантовых коммуникаций предстоит создать технологию «недоверенных промежуточных узлов связи», то есть разработать такие устройства и системы, которые обеспечивали бы необходимый уровень безопасности, требуемую пропускную способность и гарантировали надежность коммуникаций. В теории это возможно, остается найти технологическое решение.

В данной работе обсуждается реализация квантового распределения ключей на основе квантового компаратора при помощи когерентных состояний, локализованных в определенных временных окнах.

Показано, что, хотя критическая ошибка в симметричном случае для протоколов совпадает, протоколы структурно совершенно различны. В общем несимметричном случае оценка для длины секретного ключа оказывается разной. Более того, в протоколе с недоверенным узлом длина секретного ключа в каждом базисе определяется в общем случае четырьмя параметрами $Q_{ij}(i,j = 0,1)$. В протоколе BB84 длина секретного ключа в каждом базисе в общем случае зависит от двух параметров Q_0 и Q_1. В обоих протоколах различные ошибки – переходные вероятности в классических каналах связи могут быть связаны как с разными характеристиками детекторов, так и неточностью приготовления информационных состояний. Важно, что в обоих протоколах в формулу для длины секретного ключа входят только наблюдаемые параметры. При этом характеристики детекторов – квантовые эффективности, темновые шумы, которые разумеется влияют на ошибки – сами явно не входят в формулу для длины секретного ключа.

Интерпретируем полученные результаты. Для удобства будем рассматривать симметричный случай. В протоколе BB84, как следует из энтропийных соотношений неопределенностей (44), нехватка информации подслушивателя $H(X|E) \geq 1 - h(Q)$, первое слагаемое 1 в правой части неравенства говорит о том, что без вторжения в линию связи, подслушиватель не знает 1 бит информации. Вторжение в линию связи приводит к ошибкам на приемной стороне. Чем больше ошибка Q, тем больше информации подслушиватель может получить. За это отвечает второе слагаемое в неравенстве (44). Таким образом, полная нехватка информации подслушивателя, которую он получает из квантового канала связи, производя при этом ошибку Q на приемной стороне, есть $1 - h(Q)$. Для исправления ошибок Q легитимные пользователи должны передать через открытый классический канал связи не менее $h(Q)$ бит информации в пересчете на одну посылку. Данная дополнительная информация доступна подслушивателю. При передаче квантовых состояний каждая посылка несет один бит секретной информации. Подслушиватель получает $h(Q)$ бит из квантового канала, и еще $h(Q)$ бит из классического канала при коррекции ошибок. В итоге полная нехватка информации подслушивателя, которая и является секретным ключом, есть $1 - h(Q) - h(Q)$ (см. ф-лу (61)).

В протоколе с недоверенным узлом в квантовый канал поступает пара квантовых состояний от Алисы и Боба, которые несут два бита секретной информации. Если подслушиватель не вторгается в квантовые каналы, а имеет доступ только к детекторам, то после отсчета одного из двух детекторов подслушиватель получает один бит информации. Как следует из энтропийных соотношений неопределенностей (32), нехватка информации подслушивателя есть $H(X|E) \geq 2 - (1 + h(Q)) = 1 - h(Q)$. Данное неравенство можно интерпретировать следующим образом. Исходная нехватка информации подслушивателя до отсчетов детекторов и без вторжения в каналы связи составляет два бита. Отсчет одного из детекторов уменьшает нехватку на один бит, слагаемое 1 в $(1 + h(Q))$ выше. Слагаемое $h(Q)$ отвечает за уменьшение нехватки информации за счет вторжения в каналы связи, что приводит к ошибке Q в отсчетах детекторов. Исправление ошибок требует публичного раскрытия не менее $leak = h(Q)$ бит информации при коррекции ошибок, что также уменьшает нехватку информации подслушивателя. В итоге полная нехватка информации подслушивателя (уже после коррекции ошибок) есть

$$H(X|E) - leak \geq 2 - (1 + h(Q)) - h(Q) = 1 - 2h(Q).$$

В заключение еще раз отметим, что, хотя формулы для длины секретного ключа в обоих протоколах и совпадают в симметричном случае, структурно и логически протоколы принципиально разные. В общем несимметричном случае длина секретного ключа оказывается разной.

Выше был рассмотрен случай однофотонных состояний, учет многофотонных компонент можно произвести, используя, например, Decoy State метод [5]. Изложение результатов такого анализа требует отдельного рассмотрения.

Выражаем благодарность В. Л. Елисееву, А. В. Уривскому, сотрудникам ИнфоТекс и СФБ Лаборатории за интерес к работе, обсужденние, сотрудничество и поддержку.

Исследования выполнены в рамках государственного задания МГУ имени М. В. Ломоносова.

Литература

1. Lo, H.-K., Curty, M., & Qi, B. Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503 (2012).
2. Молотков С. Н. Квантовая криптография на когерентных состояниях на основе квантового компаратора // Письма в Журнал экспериментальной и теоретической физики, 66, 736 (1997).

3 M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters, Nature, 557, 400 (2018).
4. R. L. Pfleegor, L. Mandel, Interference of Independent Photon Beams, Phys. Rev., 159, 1084 (1967).
5. Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen, Decoy States Quantum Key Distribution, Phys. Rev. Lett., 94, 230504 (2005).
6. C. H. Bennett and G.Brassard, Quantum cryptography: Public key distribution and coin tossing, In Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process., pages 175–179, Bangalore, India (1984).
7. R. Renner, Security of Quantum Key Distribution, PhD thesis, ETH Zürich, arXiv:0512258 (2005).
8. M. Tomamichel, R. Renner, Uncertainty Relation for Smooth Entropies, Phys. Rev. Lett., 106, 110506 (2011).
9. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, R. Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv:1103.4130 v2 (2011); Nature Communications, 3, 1 (2012).
10. T. M. Cover, J. A. Thomas. Elements of Information Theory. Wiley, (1991).

QUANTUM NETWORKS: KEY DISTRIBUTION VIA UNTRUSTED NODES

Kulik S. P.[4], Molotkov S. N.[5]

Keywords: *quantum cryptography, photons, untrusted nodes, entropy uncertainty relations.*

The aim of the research *is to analyze the secrecy of quantum key distribution through untrusted nodes in quantum networks.*

Research method: *the use of entropy uncertainty relations.*

Result(s) of the study: *the secrecy of quantum key distribution through untrusted nodes in quantum networks is proved. The use of entropy uncertainty relations makes it possible to obtain an accurate solution for the length of the secret key in the single-photon case. A comparison with the exact solution for the BB84 protocol is made and the fundamental difference in the logical structure of proof of the secrecy of keys in these protocols is clearly shown, which, in our opinion, is important for the development of quantum cryptography systems.*

Scientific novelty: *the article proves the secrecy of quantum key distribution through untrusted nodes in quantum networks.*

References

1. Lo, H.-K., Curty, M., & Qi, B. Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503 (2012).
2. S. N.Molotkov, Quantum cryptography on coherent states based on a quantum comparator, Letters to the Journal of Experimental and Theoretical Physics, 66, 736 (1997).
3 M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters, Nature, 557, 400 (2018).
4. R. L. Pfleegor, L. Mandel, Interference of Independent Photon Beams, Phys. Rev., 159, 1084 (1967).
5. Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen, Decoy States Quantum Key Distribution, Phys. Rev. Lett., 94, 230504 (2005).
6. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process., pages 175–179, Bangalore, India (1984).
7. R. Renner, Security of Quantum Key Distribution, PhD thesis, ETH Zürich, arXiv:0512258 (2005).
8. M. Tomamichel, R. Renner, Uncertainty Relation for Smooth Entropies, Phys. Rev. Lett., 106, 110506 (2011).
9. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, R. Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv:1103.4130 v2 (2011); Nature Communications, 3, 1 (2012).
10. T. M. Cover, J. A. Thomas. Elements of Information Theory. Wiley, (1991).

4 Sergey P. Kulik, Doctor of Physics and Mathematics. Doctor of Science, Professor, Center for Quantum Technologies, Lomonosov Moscow State University, Moscow, Russia. E-mail: sergei.kulik@physics.msu.ru
5 Sergey N. Molotkov, Doctor of Physics and Mathematics. Doctor of Medicine, Professor, Institute of Solid State Physics named after Y. A. Osipyan of the Russian Academy of Sciences, Chernogolovka, Moscow. Region, Russia. E-mail: molotkov@issp.ac.ru