Январь 2021 г. *Том 191, № 1*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

МЕТОДИЧЕСКИЕ ЗАМЕТКИ

Стойкость метода обманных состояний в квантовой криптографии

А.С. Трушечкин, Е.О. Киктенко, Д.А. Кронберг, А.К. Федоров

Квантовая криптография или, более конкретно, квантовое распределение ключей (КРК) — активно развивающаяся квантовая технология. Секретность ключей, распределённых с помощью протоколов КРК, гарантируется фундаментальными законами квантовой механики. Рассматривается метод обманных состояний (от англ. "decoy state method", в другом переводе на русский язык — "метод состояний-ловушек") в КРК, направленный на устранение уязвимостей, связанных с использованием когерентных состояний света в протоколах КРК, теоретическая стойкость которых доказана в предположении кодирования информации в однофотонные состояния. Строго доказывается стойкость метода обманных состояний против всех возможных атак. Сравниваются две наиболее известные атаки на многофотонные посылки: атака расщеплением по числу фотонов и атака светоделителем. Обсуждается эквивалентность поляризационного и фазового кодирований.

Ключевые слова: квантовая криптография, квантовое распределение ключей, BB84, обманные состояния

PACS numbers: **03.67. – a**, 03.67.Dd, 03.67.Hk DOI: https://doi.org/10.3367/UFNr.2020.11.038882

Содержание

А.С. Трушечкин [1,2,†], **Е.О. Киктенко** [1,2,3,4], **Д.А. Кронберг** [1,3,4], **А.К. Федоров** [3,4,‡]

[1] Математический институт им. В.А. Стеклова РАН, ул. Губкина 8, 119991 Москва, Российская Федерация

[2] Национальный исследовательский технологический университет МИСиС, Центр компетенций Национальной технологической инициативы "Квантовые коммуникации", Ленинский просп. 4, 119049 Москва, Российская Федерация

[3] Российский квантовый центр, ул. Новая 100, 143025 Сколково, Московская обл., Российская Федерация

[4] Московский физико-технический институт (национальный исследовательский университет), Институтский пер. 9, 141701 Долгопрудный, Московская обл., Российская Федерация

E-mail: [†] trushechkin@mi-ras.ru, [‡] akf@rqc.ru

Статья поступила 23 марта 2020 г., после доработки 19 октября 2020 г.

1. Введение

Защита информации — одна из ключевых потребностей современного общества. В большинстве случаев информационная безопасность обеспечивается с использованием криптографических методов, например шифрования. Под шифрованием принято понимать преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст) с помощью определённого алгоритма [1]. При этом для шифрования легитимным сторонам коммуникаций нужен так называемый криптографический ключ — секретный параметр (как правило, двоичная строка определённой длины), который определяет выбор конкретного преобразования информации при шифровании. Задача распределения ключей является одной из важнейших в криптографии [1, 2]. Так, в [2] подчёркивается: "Ключи столь же ценны, что и все сообщения, зашифрованные ими. Для систем шифрования, известных всему миру, задача распределения ключей стоит весьма серьёзно".

Для распределения криптографических ключей используется несколько подходов. Во-первых, ключи могут быть доставлены доверенными курьерами. Основной недостаток данного метода — наличие человеческого фактора. Кроме того, ввиду возрастающего год от года объёма передаваемых данных физический перенос ключей становится всё более затруднительным. Альтернативным подходом является открытое распределение ключей, основанное на использовании так называемых односторонних функций, т.е. функций, которые легко вычисляются, но для которых трудно найти аргумент по заданному значению функции. В качестве примеров можно привести алгоритмы Диффи – Хеллмана и RSA (аббревиатура от фамилий Rivest, Shamir и Adleman)

(создан для шифрования сообщений, но на практике его часто применяют для распределения ключей), которые используют сложность решения задач дискретного логарифмирования и факторизации целых чисел соответственно. С помощью алгоритмов открытого распределения ключей, входящих в состав протокола HTTPS (HyperText Transfer Protocol Secure), защищается подавляющее большинство данных, передаваемых в интернете.

На сегодняшний день эффективные (полиномиальной сложности) классические алгоритмы решения задач факторизации и дискретного логарифмирования неизвестны, однако известен эффективный квантовый алгоритм Шора [3]. Следовательно, при появлении у злоумышленника квантового компьютера широко используемые алгоритмы распределения ключей перестанут обеспечивать информационную безопасность. Кроме того, невозможность существования эффективных классических алгоритмов для решения этих задач также не доказана и является лишь гипотезой. Сегодня квантовых компьютеров, способных реализовать квантовый алгоритм Шора для достаточно больших чисел, не существует, однако такие устройства могут появиться в обозримом будущем. Помимо того, развиваются альтернативные подходы к решению задачи факторизации, например, с помощью вариационных квантовых алгоритмов [4]. Таким образом, обеспечение конфиденциальности данных требует заблаговременного перехода на криптографические методы, которые были бы устойчивы к атакам с использованием квантового компьютера [5].

Одним из возможных решений для распределения ключей в "эпоху квантовых компьютеров" (в англоязычной литературе распространён термин "post-quantum era") является квантовое распределение ключей (КРК), предложенное Ч. Беннетом и Ж. Брассаром [6] в 1984 г., а также независимо А. Экертом [7] в 1991 г. В основе квантового распределения ключей лежит метод кодирования информации в квантовые состояния одиночных квантовых систем. Например, в наиболее распространённом протоколе КРК BB84 [6] используются состояния фотонов (например, поляризационные) в двух равноналонённых (mutually unbiased) базисах [8]. Идея использования равноналонённых базисов была введена С. Визнером в 1970-е годы (его статья [9] вышла позднее, в 1983 г.) в рамках концепции "квантовых денег". Фундаментальные запреты квантовой механики, такие как теорема о запрете клонирования квантового состояния и принцип неопределённости Гейзенберга, ограничивают возможность прочтения квантовой информации без внесения в неё изменений.

Первое полное математическое доказательство стойкости протокола BB84 в этом случае было получено Д. Майерсом [10, 11] в 1996 г. Далее последовали другие доказательства, например, в работах [12, 13]. Общая математическая теория квантового распределения ключей, основанная на теории информации и энтропийных характеристиках, построена Р. Реннером [14] и затем развита в последующих работах, среди которых выделим [15, 16]. Один из последних результатов в этом направлении — разработка техники "накопления энтропии" ("entropy accumulation") [17], которая позволяет переносить доказательство стойкости для случая так называемых коллективных атак (более простых для анализа) на случай атак общего вида (когерентных атак), сложных для непосредственного анализа [18, 19]. Для BB84 эта техника упрощает доказательство стойкости, а также позволяет доказывать стойкость к атакам общего вида в более общем случае, например в случае детекторов с несовпадающими эффективностями [20]. (Об операционном смысле параметра стойкости, используемого в квантовом распределении ключей, см. [21, 22].)

Однако в практических реализациях протоколов КРК закономерно возникают отличия от идеальных абстрактных протоколов [19, 23], оказывающие существенное влияние на криптографическую стойкость реализаций. Например, в протоколе BB84 предполагается кодирование информации в состояния одиночных фотонов. Однако генерация одиночных фотонов "по требованию" и с высокой скоростью является технически сложной задачей, в связи с чем вместо одиночных фотонов в КРК используются слабые когерентные импульсы [24]. Использование таких импульсов даёт возможность проведения атаки расщеплением по числу фотонов [25]: противник может невозмущающим образом измерить число фотонов в импульсе, отщепить себе по одному фотону от всех многофотонных состояний и заблокировать все однофотонные (т.е. надёжные) состояния или, по крайней мере, их часть. Это позволяет противнику узнать весь ключ или существенную его часть без внесения ошибок, что нарушает базовое свойство протокола о взаимосвязи уровня ошибок и количества перехваченной информации и, таким образом, делает реализацию протокола ненадёжной.

Уязвимость квантового распределения ключей к такой атаке может быть устранена с помощью метода обманных состояний ("decoy state method", в другом переводе на русский язык — "метода состояний-ловушек"), предложенного в серии работ [26 – 29]. Метод основан на том, что отправитель использует не одно фиксированное значение интенсивности для когерентных состояний, а каждый раз случайным образом выбирает интенсивность из известного (в том числе и противнику) конечного набора. Одна из этих интенсивностей (самая большая) является сигнальной и используется для генерации ключа, остальные — обманные — используются для оценки степени вмешательства противника в многофотонные импульсы.

Интенсивность, являющаяся просто параметром в распределении вероятностей (а именно в распределении Пуассона), — ненаблюдаемая величина, наблюдается только количество фотонов — реализация этой случайной величины. Поэтому противник не знает, какая интенсивность была использована в данной позиции, и осуществляет свои действия только исходя из наблюдаемого количества фотонов.

После окончания пересылки квантовых состояний отправитель объявляет и интенсивности каждой позиции. Затем легитимные стороны составляют статистику регистраций для каждой интенсивности по отдельности. Состояния с меньшими интенсивностями можно назвать обманными в том смысле, что для противника, в момент проведения атаки не знающего параметр интенсивности, они неотличимы от сигнальных, но после объявления интенсивностей они становятся как бы "помеченными", по которым можно составить отдельную статистику.

С математической точки зрения, статистика детектирования состояний с различными интенсивностями даёт легитимным сторонам дополнительные уравнения для

лучшей оценки неизвестных — количества позиций в просеянном ключе, полученных из однофотонных импульсов (т.е. таких, которые невозможно перехватить без внесения ошибок) и доли ошибок в них. В частности, блокировка противником всех однофотонных состояний приведёт к блокировке почти всех обманных состояний малой интенсивности.

На сегодняшний день протокол КРК BB84 с обманными состояниями подробно исследован теоретически [20, 26–33], многократно продемонстрирован экспериментально [23, 34], в том числе в отечественных системах [35], а также рассматривается в качестве кандидата на международный стандарт [36]. Тем не менее высказываются сомнения относительно его стойкости ко всем возможным атакам, а не только к атаке расщеплением по числу фотонов [37, 38]. Ввиду этого в настоящей статье мы не только излагаем метод обманных состояний, но и приводим формальное доказательство стойкости метода обманных состояний ко всем возможным атакам. Это обстоятельство обычно не объясняется в литературе, поскольку считается очевидным. Доказательство не будет ссылаться на атаку расщеплением по числу фотонов. Но атака расщеплением по числу фотонов, как будет показано, является оптимальной для противника, чем и объясняется то, что в литературе рассматривается противодействие только ей.

Отдельно мы сравним атаку расщеплением по числу фотонов с другой распространённой атакой — атакой светоделителем — и явно покажем меньшую эффективность последней. В то же время при реалистичных уровнях потерь, как будет показано, эти атаки дают похожие результаты.

Далее текст организован следующим образом. В разделе 2 приводится протокол BB84. В разделе 3 обсуждается проблематика, связанная с кодированием информации в этом протоколе в когерентные, а не в однофотонные состояния, рассматривается атака расщеплением по числу фотонов. Для того чтобы сформулировать дальнейшие результаты, касающиеся стойкости протокола, в разделе 4 вводятся понятия достижимой и предельно достижимой скоростей генерации секретного ключа, приводится известная формула Деветака–Винтера [39] для предельной скорости генерации секретного ключа. Раздел 5 посвящён сведению многофотонного случая к однофотонному, если отправляемые состояния являются статистическими смесями фоковских состояний (состояний с определённым числом фотонов). Теорема, приведённая в этом разделе, формально обосновывает использование метода обманных состояний, его стойкость ко всем возможным коллективным атакам. Здесь же обосновывается оптимальность атаки расщеплением по числу фотонов. Раздел 6 завершает этот анализ: эквивалентная формулировка протокола в терминах сцепленного состояния позволяет применить технику накопления энтропии и обосновать стойкость протокола ко всем возможным (а не только к коллективным) атакам. Раздел 7 посвящён изложению метода обманных состояний. В разделе 8 рассматривается другая атака — атака светоделителем, которая, в отличие от атаки расщеплением по числу фотонов, реализована экспериментально. В разделе 9 мы сравниваем атаки расщеплением по числу фотонов и атаку светоделителем и объясняем, почему последняя обладает меньшей эффективностью. Наконец, в разделе 10 мы отвечаем на высказанные сомнения [40] о применимости метода обманных состояний к ситуации фазового, а не поляризационного кодирования информации и показываем полную эквивалентность этих кодирований.

Стоит отметить, что область квантовой обработки информации уже становилась предметом нескольких обзоров в журнале *Успехи физических наук*. В частности, ряд вопросов квантовых вычислений рассмотрен в работах [41, 42], а ряд аспектов квантового распределения ключей — в статье [43]. Прогресс последних десятилетий в области разработки промышленных устройств для квантового распределения ключей перевёл исследования в этой области на следующий уровень, на котором на первый план вышел ряд важных практических аспектов реализации таких систем. В частности, одной из центральных задач данной области является анализ устойчивости к атакам протоколов квантового распределения ключей, что и представляет собой предмет настоящей статьи: основной результат состоит в строгом обосновании стойкости метода обманных состояний (состояний-ловушек) в квантовой криптографии.

2. Протокол BB84

В этом разделе мы опишем протокол BB84 [6] при предположении однофотонного источника на стороне отправителя. В каждом протоколе КРК можно выделить две основные стадии: передачу квантовых состояний и постобработку результатов измерений. Следуя [1], участников связи, желающих создать общий ключ, будем называть отправителем и получателем, подслушивающую сторону — противником. Отправителя и получателя вместе будем также называть легитимными сторонами.

На первой, "квантовой", стадии в протоколе BB84 используются четыре квантовых состояния, составляющих два ортогональных базиса: $z = \{|0\rangle_z, |1\rangle_z\}$ и $x = \{|0\rangle_x, |1\rangle_x\}$ — в двумерном гильбертовом пространстве $\mathbb{C}^2$. Квантовая система, соответствующая этому пространству, называется квантовым битом или кубитом. Символы 0 и 1 указывают, какой классический бит кодирует соответствующий базисный вектор. Элементы базисов выражаются через элементы другого базиса согласно соотношениям

$$|0\rangle_x = \frac{|0\rangle_z + |1\rangle_z}{\sqrt{2}}, \qquad |1\rangle_x = \frac{|0\rangle_z - |1\rangle_z}{\sqrt{2}}. \tag{1}$$

Если используется кодирование информации в поляризацию фотона, то векторы $|0\rangle_z$ и $|1\rangle_z$ могут соответствовать, например, горизонтальной и вертикальной поляризациям, $|0\rangle_x$ и $|1\rangle_x$ — двум диагональным поляризациям, повёрнутым относительно горизонтального направления на 45° и 135° соответственно. Мы будем предполагать поляризационное кодирование для удобства изложения, но фактически ограничение на способ кодирования информации не накладывается: формально $|0\rangle_z$, $|1\rangle_z$, $|0\rangle_x$ и $|1\rangle_x$ — векторы в гильбертовом пространстве и можно использовать любое кодирование, реализующее соотношения (1). В частности, эквивалентность поляризационного и фазового кодирования мы поясним в разделе 10.

Как видно из (1), при измерении кубита в базисе, отличном от базиса приготовления, результат является случайной величиной. В случае совпадения базисов при-

готовления и измерения состояния результат полностью коррелирует с приготовленным состоянием кубита (в идеальном случае, т.е. при отсутствии ошибок в канале и измерительном оборудовании).

Опишем теперь протокол BB84.

1. Отправитель случайным образом выбирает базис из множества $\{z, x\}$ и значение передаваемого бита информации: 1 или 0. Биты выбираются с равными вероятностями $1/2$.

2. Далее фотоны, приготовленные в соответствующих состояниях, передаются по квантовому каналу.

3. Получатель случайным образом выбирает базис измерения — z или x — для каждого кубита и проводит измерение состояния кубита в выбранном базисе. При совпадении базисов приготовления и измерения полученное значение бита совпадает (в идеале) с отправленным. При несовпадении базисов биты отправителя и получателя не коррелируют (т.е. с равными вероятностями могут совпадать или не совпадать) из-за равнонаклонённости базисов (1). Линия связи, как правило, содержит большие потери, поэтому не все позиции регистрируются получателем.

4. Перечисленные выше действия повторяются много раз, т.е. посылается большое число квантовых состояний. В результате легитимные стороны получают две битовые последовательности, $k_{\mathrm{A}}^{\mathrm{raw}}$ и $k_{\mathrm{B}}^{\mathrm{raw}}$, называемые *сырыми квантовыми ключами*.

Поскольку идеальную копию квантового состояния невозможно создать, а противник не знает базиса, в котором закодирован бит в данной позиции, противнику необходимо применять методы несовершенного копирования, которые вносят возмущение.

В исходной версии протокола базисы выбираются равновероятно. Позднее был предложен улучшенный вариант протокола, в котором один из базисов (например, базис z) выбирается чаще другого [44]. Это уменьшает число несовпадений базисов и, следовательно, долю отсеивающихся позиций, т.е. увеличивает скорость генерации ключа. Обозначим как p_z и $p_x = 1 - p_z$ вероятности выбора базисов. В пределе бесконечного числа посылок N можно положить $p_z \to 1$, $p_x \to 0$. Например, можно взять $p_x = O(1/\sqrt{N})$ — этого достаточно для точной статистической оценки параметров по наблюдениям в базисе x, поскольку статистические флуктуации будут иметь порядок $O(1/\sqrt{N})$. Тогда можно принять следующую модификацию протокола: для формирования ключа будут использоваться только позиции, в которых обе стороны применяли базис z. Биты, закодированные в базисе x, не участвуют в формировании секретного ключа, они будут нужны только для оценки степени вмешательства противника. Отметим, что вариант протокола, при котором базисы выбираются псевдослучайным образом на основе предварительно распределённой случайной последовательности, рассмотрен в работе [45].

На втором этапе легитимные стороны проводят классическую постобработку сырых ключей, используя общение по открытому аутентифицированному каналу [18, 46, 47]. Эта постобработка состоит из следующих шагов:

1. *Раскрытие информации*. Получатель объявляет номера позиций, в которых произошла регистрация сигнала. Отправитель и получатель объявляют использованные базисы во всех позициях. При использовании метода обманных состояний отправитель также объявляет тип каждой посылки (сигнальная или одна из обманных). Отправитель и получатель могут также объявить биты в позициях, которые не будут участвовать в формировании секретного ключа: в позициях, в которых стороны использовали базис x, в обманных посылках.

2. *Просеивание ключа*. Позиции, в которых была использована обманная интенсивность, не произошло регистрации или хотя бы одна из легитимных сторон использовала базис x, отсеиваются. Полученные в результате ключи, $k_{\mathrm{A}}^{\mathrm{sift}}$ и $k_{\mathrm{B}}^{\mathrm{sift}}$, называют *просеянными ключами*. В идеале они должны совпадать, но в результате естественного шума в канале или действий противника они не совпадают. Более того, противник может иметь частичную информацию о них.

3. *Исправление ошибок*. Один из просеянных ключей (например, отправителя) считается эталонным, отличия от него просеянного ключа другой стороны считаются ошибками. Для исправления ошибок можно использовать коды, устраняющие ошибки, или интерактивные процедуры исправления ошибок. Достаточно распространены коды с низкой плотностью проверки на чётность (Low-Density Parity-Check, LDPC). Часто данная процедура завершается *верификацией*: с помощью хеш-функций устанавливается идентичность просеянных ключей (см. [48]). В результате этого этапа у легитимных сторон с высокой вероятностью получаются идентичные *верифицированные ключи*, $k_{\mathrm{A}}^{\mathrm{ver}} = k_{\mathrm{B}}^{\mathrm{ver}}$. Эффективный метод исправления ошибок в протоколе BB84 на основе кодов с низкой плотностью проверки на чётность описан в работе [49] (см. также [50]).

4. *Оценка степени вмешательства противника* и принятие решения о создании ключа или отказе от него (прерывании протокола) на основе наблюдаемых данных. В основе квантовой криптографии лежит тот факт, что информацию, закодированную в неортогональные квантовые состояния, невозможно прочитать третьей стороне (которая не знает, в каком базисе закодирован бит ключа в данной позиции), не "испортив" эти состояния. Поэтому вмешательство противника приведёт к повышению доли ошибок у легитимных сторон, т.е. несовпадающих позиций в просеянных ключах. В данном варианте протокола, где в формировании ключа участвуют только биты, закодированные в базис z, для оценки степени вмешательства противника необходима только доля ошибок в базисе x. Если доля ошибок превышает определённый критический порог, то протокол прерывается. В противном случае стороны переходят к последнему шагу. Таким образом, в квантовой криптографии невозможно осуществить прослушивание, оставшись незамеченным.

5. *Усиление секретности*. Отправитель случайным образом выбирает так называемую хеш-функцию из некоторого семейства универсальных хеш-функций 2-го порядка и отправляет её получателю по открытому каналу. Затем оба вычисляют значение хеш-функции на своих (одинаковых) просеянных ключах. В результате они получают общий более короткий ключ (*конечный ключ*), $k_{\mathrm{A}}^{\mathrm{fin}} = k_{\mathrm{B}}^{\mathrm{fin}}$, но информация противника о нём пренебрежимо мала. При бесконечно большой длине просеянного ключа она может быть сделана сколь угодно малой. Чем больше информации имеет противник о просеянном ключе (в результате перехвата и раскрытия легитимными пользователями части информации при

исправлении ошибок), тем сильнее требуется сжать ключ в процедуре усиления секретности, т.е. тем короче конечный ключ и, соответственно, меньше скорость.

Как можно заметить, процедура постобработки требует сообщения сторон по классическому каналу. Предполагается, что противник может свободно слушать этот канал, но не может изменять передаваемые по нему сообщения и посылать свои. Это обеспечивается кодами аутентификации сообщений. В квантовой криптографии часто используюся теоретически стойкие коды Вегмана – Картера [51] (т.е. доказуемо стойкие без предположения о вычислительных мощностях противника). Они требуют наличия у легитимных сторон начального короткого секретного ключа. Достаточно иметь начальный общий секретный ключ для первого сеанса распределения ключей. Далее в каждом сеансе часть сгенерированного ключа сохраняется для использования в коде аутентификации сообщений в следующем сеансе и не используется в других целях. (О последних разработках в направлении сокращения объёма потребляемого ключа при аутентификации см. [52].)

Здесь мы предполагали, что отправитель посылает однофотонные состояния. Это соответствовало тому, что его гильбертово пространство — $\mathbb{C}^2$. В конце введения приведены ссылки, касающиеся истории доказательств стойкости протокола BB84 в данном случае.

3. Кодирование информации в слабые когерентные импульсы. Атака расщеплением по числу фотонов

Примем теперь во внимание, что на практике чаще всего информация кодируется не в истинные однофотонные состояния, а в слабые когерентные импульсы. Это означает, что гильбертово пространство отправителя — не $\mathbb{C}^2$, а $\mathscr{F}(\mathbb{C}^2)$ (бозонное пространство Фока над $\mathbb{C}^2$). Ортонормированный базис в этом пространстве составляют векторы $|\mathrm{vac}\rangle$ и $|j_0, j_1\rangle_z$, где $|\mathrm{vac}\rangle$ — вакуумный вектор,

$$|j_0, j_1\rangle_z = \frac{(a_{z0}^\dagger)^{j_0}(a_{z1}^\dagger)^{j_1}}{\sqrt{j_0! j_1!}}\,|\mathrm{vac}\rangle\,, \tag{2}$$

$j_0, j_1 \geqslant 0$ ($|0,0\rangle_z = |\mathrm{vac}\rangle$), $a_{z0}^\dagger$, $a_{z1}^\dagger$, a_{z0}, a_{z1} — операторы рождения и уничтожения фотона в состояниях $|0\rangle_z, |1\rangle_z \in \mathbb{C}^2$ соответственно. Другой ортонормированный базис составляют векторы $|\mathrm{vac}\rangle$ и $|j_0, j_1\rangle_x$, $j_0, j_1 \geqslant 0$, где

$$|j_0, j_1\rangle_x = \frac{(a_{x0}^\dagger)^{j_0}(a_{x1}^\dagger)^{j_1}}{\sqrt{j_0! j_1!}}\,|\mathrm{vac}\rangle\,, \tag{3}$$

$$a_{x0}^\dagger = \frac{a_{z0}^\dagger + a_{z1}^\dagger}{\sqrt{2}}\,, \qquad a_{x1}^\dagger = \frac{a_{z0}^\dagger - a_{z1}^\dagger}{\sqrt{2}} \tag{4}$$

— операторы рождения фотона в состояниях $|0\rangle_x, |1\rangle_x \in \mathbb{C}^2$ соответственно. В частности, векторы $|0\rangle_b, |1\rangle_b \in \mathbb{C}^2$ можно отождествить с векторами $|1,0\rangle_b, |0,1\rangle_b \in \mathscr{F}(\mathbb{C}^2)$ соответственно, $b \in \{z, x\}$.

Тогда отправляемые когерентные состояния имеют вид

$$|\alpha; u\rangle_b = \exp\left(-\frac{\mu}{2}\right)|\mathrm{vac}\rangle + \exp\left(-\frac{\mu}{2}\right)\sum_{j=1}^{\infty}\frac{\alpha^j}{\sqrt{j!}}\,|\psi_{ju}^b\rangle\,, \tag{5}$$

где $u \in \{0,1\}$, $b \in \{z, x\}$,

$$|\psi_{j0}^b\rangle = |j,0\rangle_b\,, \quad |\psi_{j1}^b\rangle = |0,j\rangle_b\,,$$

$b \in \{z, x\}$. Здесь $\alpha \in \mathbb{C}$ — параметр когерентного состояния, $\mu = |\alpha|^2$ — интенсивность импульса, $\alpha = \sqrt{\mu}\,\exp(\mathrm{i}\theta)$. Протокол требует, чтобы фаза когерентного состояния θ менялась случайным образом от посылки к посылке. Это обеспечивается либо режимом работы лазера (пассивная рандомизация), либо введением в оптическую схему отправителя дополнительного элемента, который подключён к генератору случайных чисел и рандомизирует фазу (активная рандомизация) (см. также замечание 1 в разделе 5). Тогда противник и получатель "видят" не чистое когерентное состояние, а смешанное — оператор плотности

$$\rho_{\mu u}^b = \frac{1}{2\pi}\int_0^{2\pi}\mathrm{d}\theta\,\big|\sqrt{\mu}\,\exp(\mathrm{i}\theta); u\big\rangle_b\big\langle\sqrt{\mu}\,\exp(\mathrm{i}\theta); u\big| =$$

$$= \exp(-\mu)|\mathrm{vac}\rangle\langle\mathrm{vac}| + \exp(-\mu)\sum_{j=1}^{\infty}\frac{\mu^j}{j!}\,|\psi_{ju}^b\rangle\langle\psi_{ju}^b|\,. \tag{6}$$

Здесь мы для простоты приняли, что базис b и бит u фиксированы, иначе необходимо усреднить и по ним. Данное смешанное состояние можно интерпретировать следующим образом: с вероятностью $\exp(-\mu)$ отправляется вакуумное состояние, с вероятностью $\exp(-\mu)\mu^j/j!$ — состояние с j фотонами в соответствующей поляризации. Таким образом, количество фотонов в посылке распределено по Пуассону с параметром (средним числом фотонов) μ. Обычно выбирают $\mu < 1$, поэтому такие импульсы называются слабыми когерентными.

Наличие в некоторых посылках более одного фотона даёт противнику возможность провести так называемую *атаку расщеплением по числу фотонов* [25]. Иногда под этим понимают атаку специального вида, но мы будем понимать целый класс атак, который сейчас опишем. Каждая атака этого класса начинается с того, что противник проводит измерение количества фотонов, т.е. измерение, которому соответствует вероятностная проекторнозначная мера $\{P_j\}_{j=0}^{\infty}$, где

$$P_j = \sum_{j_0+j_1=j}|j_0, j_1\rangle_z\,\langle j_0, j_1| = \sum_{j_0+j_1=j}|j_0, j_1\rangle_x\,\langle j_0, j_1|\,. \tag{7}$$

При исходе j состояние (6) переходит в $P_j\rho_{\mu u}^b P_j/\mathrm{Tr}\,(\rho_{\mu u}^b P_j)$. Такое измерение называется также неразрушающим, поскольку фотоны не уничтожаются и их поляризация не изменяется. На практике такое неразрушающее измерение на данный момент не реализовано, но в теории оно возможно, поскольку соответствующая вероятностная проекторнозначная мера существует. Если противник обнаруживает, что фотонов в посылке два или более ($j \geqslant 2$), то один фотон он отводит в свою квантовую память, остальные пересылает получателю. После объявления базисов по открытому каналу противник узнаёт, в каком базисе в данной позиции закодирован бит ключа. Он проводит измерение в этом базисе и узнаёт этот бит. При этом состояние тех фотонов, которые были пересланы получателю, не изменяется. Таким образом, нарушается базовый принцип квантовой криптографии, состоящий в том, что попытка прослушивания приводит к изменению состояний и возникновению (или повыше-

нию уровня) ошибок. Если посылка содержит один фотон, то противник по-прежнему может узнать закодированную в нём информацию только ценой изменения состояния и, соответственно, внесения ошибок. Поэтому противник может заблокировать все однофотонные состояния или их часть, т.е. остановить их передачу получателю, имитируя естественные потери в канале связи. Незаблокированные однофотонные состояния он может атаковать обычным образом (ценой внесения ошибок).

Блокировка противником некоторых посылок приводит к повышению уровня потерь, что может быть обнаружено легитимными сторонами. Поэтому предполагается, что противник может заменить линию связи и даже детекторы идеальными, т.е. без потерь, и затем заблокировать такое количество однофотонных посылок, которое позволит воспроизвести естественный уровень потерь. Чем выше уровень естественных потерь (который зависит прежде всего от длины линии связи (см. раздел 7)), тем больше однофотонных состояний противник может заблокировать. Если естественные потери в канале настолько велики, что противник может заблокировать все однофотонные состояния, то противник будет иметь полную информацию о ключе без внесения шума, так как все посылки, дошедшие до получателя, были при отправлении многофотонными. Таким образом, протокол квантового распределения ключей оказывается полностью скомпрометированным.

4. Скорость генерации секретного ключа

Под *скоростью генерации* конечного ключа будем понимать предел отношения длины конечного ключа к длине просеянного ключа при количестве посылок, стремящемся к бесконечности. Под *достижимой* скоростью генерации секретного ключа будем понимать скорость генерации ключа, при которой можно обеспечить требование бесконечно малого количества информации противника о конечном ключе (в указанном пределе). Как говорилось в разделе 2, для этого необходимо в достаточной мере сжать просеянный ключ в процедуре усиления секретности. Разумеется, если некоторая скорость является достижимой, то достижимыми являются и все меньшие скорости. *Предельно достижимой* (или просто *предельной*) скоростью генерации секретного ключа будем называть точную верхнюю грань множества достижимых скоростей. (Формальные определения см. в работе [39].)

Отметим, что иногда скорость генерации определяется как предел длины конечного ключа к числу посылок. Поскольку длина просеянного ключа пропорциональна числу посылок, эти определения совпадают с точностью до постоянного множителя.

Формулу предельной скорости генерации секретного ключа можно записать, воспользовавшись теоремой Деветака – Винтера [39] (см. также раздел 6). В её формулировке участвует трёхчастичное состояние отправителя, получателя и противника, которое имеет место после процедуры просеивания. Нашей ближайшей целью будет запись формулы этого состояния.

Введём регистр (формально — квантовую систему) $\overline{\mathrm{A}}$ размерностью 2, в который отправитель записывает своё значение бита. Подсистему, которой принадлежит отправляемое квантовое состояние (6), обозначим как A. Тогда совместное состояние $\overline{\mathrm{A}}$ и A при использовании базиса z имеет вид

$$\rho^{z}_{\overline{\mathrm{A}}\mathrm{A}} = \frac{1}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes \rho^{z}_{\mu u}\,, \tag{8}$$

где $\rho^{z}_{\mu u}$ даётся формулой (6).

Вследствие наличия естественного шума, естественных потерь в канале и/или действий противника состояние $\rho^{z}_{\mu u}$ подвергается воздействию некоторого квантового канала, т.е. линейного, вполне положительного, сохраняющего след отображения $\Upsilon_0\colon \mathfrak{T}(\mathscr{H}_{\mathrm{A}}) \to \mathfrak{T}(\mathscr{H}_{\mathrm{B}} \otimes \mathscr{H}_{\mathrm{E}})$, где $\mathscr{H}_{\mathrm{A}} = \mathscr{H}_{\mathrm{B}} = \mathscr{F}(\mathbb{C}^2)$ — гильбертовы пространства отправителя и получателя, $\mathscr{H}_{\mathrm{E}}$ — некоторое (неизвестное) гильбертово пространство противника, $\mathfrak{T}$ — пространство ядерных операторов в соответствующем гильбертовом пространстве.

Квантовые эффективности детекторов (вообще говоря, различные) и вероятности темновых срабатываний детекторов (аналогично) также можно включить в канал Υ_0: в первом случае состояние с фотонами с некоторой вероятностью переводится в состояние без фотонов, во втором — наоборот. Необходимо заметить, что включение этих эффектов делает Υ_0 зависимым от базиса. Преобразование состояния в линии связи не зависит от базиса, поскольку и противник не знает базиса в момент проведения атаки, и естественный шум и потери не зависят от базиса. Но дальнейшее преобразование состояния, связанное с измерением, уже оказывается зависимым от базиса, в котором это измерение проводится. Сейчас нас интересуют позиции, в которых обе стороны используют базис z, поскольку только такие позиции участвуют в формировании ключа. Измерению в базисе x будет соответствовать другое преобразование, но оно нам не потребуется.

После этого "идеальное" измерение (неединичные эффективности детекторов и темновой шум в них мы уже учли в Υ_0) соответствует вероятностной проекторнозначной мере $\{\bar{P}_{\varnothing}, \bar{P}_0, \bar{P}_1, \bar{P}_{01}\}$, где $\bar{P}_{\varnothing} = |\mathrm{vac}\rangle\langle\mathrm{vac}|$ соответствует несрабатыванию ни одного из детекторов, $\bar{P}_0 = \sum_{j=1}^{\infty} |j,0\rangle_z\langle j,0|$ и $\bar{P}_1 = \sum_{j=1}^{\infty} |0,j\rangle_z\langle 0,j|$ — срабатыванию одного детектора, $\bar{P}_{01} = \sum_{j,k=1}^{\infty} |j,k\rangle_z\langle j,k|$ — срабатыванию обоих детекторов.

Итак, вакуумная компонента состояния получателя не регистрируется. Потому соответствующие позиции отсеиваются и не участвуют в формировании ключа. Напомним, наша ближайшая цель состоит в записи формулы трёхчастичного состояния отправителя, получателя и противника, которое получается после процедуры просеивания. Обозначим

$$\Upsilon(\rho_{\mathrm{A}}) = \bigl[(I_{\mathrm{B}} - |\mathrm{vac}\rangle\langle\mathrm{vac}|) \otimes I_{\mathrm{E}}\bigr] \times \\ \times \Upsilon_0(\rho_{\mathrm{A}})\bigl[(I_{\mathrm{B}} - |\mathrm{vac}\rangle\langle\mathrm{vac}|) \otimes I_{\mathrm{E}}\bigr]$$

для любого $\rho_{\mathrm{A}} \in \mathfrak{T}(\mathscr{H}_{\mathrm{A}})$. Здесь I_{B} и I_{E} — тождественные операторы в пространствах $\mathscr{H}_{\mathrm{B}}$ и $\mathscr{H}_{\mathrm{E}}$ соответственно. Очевидно, что отображение Υ не сохраняет след, оно лишь не увеличивает его, $\operatorname{Tr}\Upsilon(\rho_{\mathrm{A}}) \leqslant \operatorname{Tr}\rho_{\mathrm{A}}$. Причина состоит в том, что Υ включает отсев части результатов, что уменьшает след.

Тогда искомая формула для трёхчастичного состояния отправителя, получателя и противника после про-

сеивания имеет вид

$$\rho_{\overline{\mathrm{A}}\mathrm{BE}} = (Q^{\mathrm{sz}})^{-1}(\mathrm{Id}_{\overline{\mathrm{A}}} \otimes \Upsilon)(\rho^{z}_{\overline{\mathrm{A}}\mathrm{A}}) = \frac{1}{2Q^{\mathrm{sz}}} \sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}} \langle u| \otimes \Upsilon(\rho^{z}_{\mu u}), \tag{9}$$

где

$$Q^{\mathrm{sz}} = \mathrm{Tr}\,(\mathrm{Id}_{\overline{\mathrm{A}}} \otimes \Upsilon)(\rho^{z}_{\overline{\mathrm{A}}\mathrm{A}})$$

— вероятность регистрации сигнального импульса (на что указывает верхний индекс s, впоследствии нам понадобятся и вероятности регистраций обманных импульсов), $\mathrm{Id}_{\overline{\mathrm{A}}}$ — тождественное квантовое преобразование операторов плотности в пространстве регистра $\overline{\mathrm{A}}$, т.е. $\mathbb{C}^2$.

По теореме Деветака – Винтера [39] предельная скорость генерации секретного ключа составит

$$R = H(\overline{\mathrm{A}}|\mathrm{E}) - H(\overline{\mathrm{A}}|\mathrm{B}), \tag{10}$$

где

$$\begin{aligned} H(\overline{\mathrm{A}}|\mathrm{B}) &= H(\rho_{\overline{\mathrm{A}}\mathrm{B}}) - H(\rho_{\mathrm{B}}), \\ H(\overline{\mathrm{A}}|\mathrm{E}) &= H(\rho_{\overline{\mathrm{A}}\mathrm{E}}) - H(\rho_{\mathrm{E}}) \end{aligned} \tag{11}$$

— квантовая условная энтропия. Мы здесь воспользовались следующим соглашением, касающимся обозначений состояния подсистем составной системы: если дано состояние составной системы $\rho_{\overline{\mathrm{A}}\mathrm{BE}}$, то $\rho_{\overline{\mathrm{A}}\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}\,\rho_{\overline{\mathrm{A}}\mathrm{BE}}$, $\rho_{\mathrm{B}} = \mathrm{Tr}_{\overline{\mathrm{A}}\mathrm{E}}\,\rho_{\overline{\mathrm{A}}\mathrm{BE}}$, $\rho_{\mathrm{E}} = \mathrm{Tr}_{\overline{\mathrm{A}}\mathrm{B}}\,\rho_{\overline{\mathrm{A}}\mathrm{BE}}$ и т.д. В свою очередь $H(\rho) = -\mathrm{Tr}\,(\rho \log \rho)$ — энтропия фон Неймана, $\log \equiv \log_2$. Поскольку состояние $\rho_{\overline{\mathrm{A}}\mathrm{BE}}$ — классически-квантовое (классическое по $\overline{\mathrm{A}}$ и квантовое по BE), оба члена в правой части (10) неотрицательны.

Первое слагаемое в правой части (10) характеризует *степень незнания*, или *нехватку информации* противника о бите ключа отправителя, второе слагаемое (без знака минус перед ним) — степень незнания (нехватку информации) получателя о том же бите. Обозначим через m минимальное количество информации, которое отправитель должен раскрыть о своём просеянном ключе, для того чтобы получатель смог исправить все ошибки и получить ключ, совпадающий с ключом отправителя. Если для этой цели используются коды, исправляющие ошибки, то m — длина синдрома. Но могут использоваться и итеративные процедуры исправления ошибок. Второе слагаемое в правой части (10) — это отношение m/n в пределе $n \to \infty$. Мы предполагаем, что используется оптимальный (по Шеннону) код исправления ошибок. В противном случае перед вторым слагаемым необходимо добавить множитель $f > 1$. Так, например, значение множителя $f = 1{,}22$ достижимо для современных кодов, исправляющих ошибки [49].

По неравенству Фано величину $H(\overline{\mathrm{A}}|\mathrm{B})$ можно оценить сверху через $h(E^{\mathrm{sz}})$, где

$$h(x) = -x \log x - (1-x) \log (1-x)$$

— двоичная энтропия, E^{sz} — доля ошибок в просеянных ключах. Верхние индексы s и z обозначают, что речь идёт о сигнальных состояниях и позициях, в которых обе стороны использовали базис z. Напомним, только такие позиции участвуют в формировании секретного ключа. Эта величина становится известной легитимным сторонам после исправления ошибок и верификации ключей: после верификации ключи с большой вероятностью совпадают, поэтому по количеству позиций, в которых произошли исправления, легитимные стороны узнают долю ошибок в просеянных ключах. Тогда для получения формулы достижимой скорости генерации секретного ключа легитимные стороны должны оценить первое слагаемое правой части (10), т.е. нехватку информации противника. Оценка первого слагаемого является ключевой в доказательстве стойкости любого протокола КРК.

5. Сведение многофотонного случая к однофотонному

Сведём задачу оценивания сверху $H(\overline{\mathrm{A}}|\mathrm{E})$ для состояния $\rho_{\overline{\mathrm{A}}\mathrm{BE}}$, включающего многофотонные посылки, к оценке квантовой условной энтропии для состояния, включающего только однофотонные посылки. Обозначим

$$\begin{aligned} \tilde{\rho}^{(0)}_{\overline{\mathrm{A}}\mathrm{A}} &= \frac{1}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes P_0\, \rho^{z}_{\mu u} P_0 = \\ &= \frac{\exp(-\mu)}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes |\mathrm{vac}\rangle\langle \mathrm{vac}|, \\ \tilde{\rho}^{(1)}_{\overline{\mathrm{A}}\mathrm{A}} &= \frac{1}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes P_1\, \rho^{z}_{\mu u} P_1 = \\ &= \frac{\mu \exp(-\mu)}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes |u\rangle_{z}\langle u|, \\ \rho^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{BE}} &= (Q^{\mathrm{sz}}_{(\geqslant 2)})^{-1}(\mathrm{Id}_{\overline{\mathrm{A}}} \otimes \Upsilon)(\tilde{\rho}^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{A}}), \\ Q^{\mathrm{sz}}_{j} &= \mathrm{Tr}\,(\mathrm{Id}_{\overline{\mathrm{A}}} \otimes \Upsilon)(\tilde{\rho}^{(j)}_{\overline{\mathrm{A}}\mathrm{A}}), \quad j = 0, 1, \end{aligned}$$

где P_j — проектор на j-фотонное подпространство в $\mathscr{F}(\mathbb{C}^2)$ (см. (7)), Q^{sz}_{j} — совместная вероятность того, что сигнальная посылка отправителя содержала j фотонов и была зарегистрирована получателем. Тогда доля j-фотонных посылок среди всех зарегистрированных получателем посылок, участвующих в формировании просеянного ключа, составит $Q^{\mathrm{sz}}_{j}/Q^{\mathrm{sz}}$.

Теорема. *Для любого линейного, вполне положительного, не увеличивающего след отображения* Υ *выполняется неравенство*

$$H(\overline{\mathrm{A}}|\mathrm{E}) \geqslant \frac{Q^{\mathrm{sz}}_{0}}{Q^{\mathrm{sz}}} + \frac{Q^{\mathrm{sz}}_{1}}{Q^{\mathrm{sz}}} H(\overline{\mathrm{A}}|\mathrm{E})_{(1)}, \tag{12}$$

где $H(\overline{\mathrm{A}}|\mathrm{E})$ *рассчитывается для состояния* $\rho_{\overline{\mathrm{A}}\mathrm{BE}}$, $H(\overline{\mathrm{A}}|\mathrm{E})_{(1)}$ *— для состояния* $\rho^{(1)}_{\overline{\mathrm{A}}\mathrm{BE}}$.

Доказательство. Квантовую условную энтропию можно выразить через квантовую относительную энтропию:

$$H(\overline{\mathrm{A}}|\mathrm{E}) = -D(\rho_{\overline{\mathrm{A}}\mathrm{E}} \| I_{\overline{\mathrm{A}}} \otimes \rho_{\mathrm{E}}).$$

Напомним, что квантовая относительная энтропия определяется как

$$D(\rho\|\sigma) = \mathrm{Tr}\,(\rho \log \rho) - \mathrm{Tr}\,(\rho \log \sigma)$$

и она совместно выпукла по своим двум аргументам [53, 54]:

$$\begin{aligned} D\big(p\rho_1 + (1-p)\rho_2 \,\big\|\, p\sigma_1 + (1-p)\sigma_2\big) \leqslant \\ \leqslant pD(\rho_1\|\sigma_1) + (1-p)D(\rho_2\|\sigma_2), \end{aligned}$$

для любых состояний $\rho_{1,2}$, $\sigma_{1,2}$ и $0 \leqslant p \leqslant 1$.

Тогда утверждение теоремы — это простое следствие того, что состояние $\rho^{z}_{\mu u}$ есть смесь состояний с определённым числом фотонов (6), линейности Υ и совместной выпуклости квантовой относительной энтропии. В самом деле,

$$\rho^{z}_{\mu u} = P_0\,\rho^{z}_{\mu u}P_0 + P_1\,\rho^{z}_{\mu u}P_1 + P_{\geqslant 2}\,\rho^{z}_{\mu u}P_{\geqslant 2}\,,$$

где $P_{\geqslant 2} = \sum_{j=2}^{\infty} P_j$. Поэтому ввиду линейности Υ

$$\rho_{\overline{\mathrm{A}}\mathrm{BE}} = (Q^{sz})^{-1}(\mathrm{Id}_{\overline{\mathrm{A}}}\otimes\Upsilon)(\rho_{\overline{\mathrm{A}}\mathrm{A}}) = \\ = \frac{Q_0^{sz}}{Q^{sz}}\,\rho^{(0)}_{\overline{\mathrm{A}}\mathrm{BE}} + \frac{Q_1^{sz}}{Q^{sz}}\,\rho^{(1)}_{\overline{\mathrm{A}}\mathrm{BE}} + \frac{Q_{\geqslant 2}^{sz}}{Q^{sz}}\,\rho^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{BE}}\,,$$

где

$$\rho^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{BE}} = (Q^{sz}_{\geqslant 2})^{-1}\,\mathrm{Tr}\,(\mathrm{Id}_{\overline{\mathrm{A}}}\otimes\Upsilon)(\tilde{\rho}^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{A}})\,,$$
$$Q^{sz}_{\geqslant 2} = \mathrm{Tr}\,(\mathrm{Id}_{\overline{\mathrm{A}}}\otimes\Upsilon)(\tilde{\rho}^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{A}})\,,$$
$$\tilde{\rho}^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{A}} = \frac{1}{2}\sum_{u=0}^{1}|u\rangle_{\overline{\mathrm{A}}}\langle u|\otimes P_{\geqslant 2}\,\rho^{z}_{\mu u}P_{\geqslant 2}\,.$$

Тогда вследствие совместной выпуклости квантовой относительной энтропии

$$H(\overline{\mathrm{A}}|\mathrm{E}) \geqslant \frac{Q_0^{sz}}{Q^{sz}}\,H(\overline{\mathrm{A}}|\mathrm{E})_{(0)} + \frac{Q_1^{sz}}{Q^{sz}}\,H(\overline{\mathrm{A}}|\mathrm{E})_{(1)} + \\ + \frac{Q_{\geqslant 2}^{sz}}{Q^{sz}}\,H(\overline{\mathrm{A}}|\mathrm{E})_{(\geqslant 2)} \geqslant \frac{Q_0^{sz}}{Q^{sz}} + \frac{Q_1^{sz}}{Q^{sz}}H(\overline{\mathrm{A}}|\mathrm{E})_{(1)}\,,$$

что и требовалось доказать. Здесь условные энтропии $H(\overline{\mathrm{A}}|\mathrm{E})_{(0)}$ и $H(\overline{\mathrm{A}}|\mathrm{E})_{(\geqslant 2)}$ рассчитываются для состояний $\rho^{(0)}_{\overline{\mathrm{A}}\mathrm{BE}}$ и $\rho^{(\geqslant 2)}_{\overline{\mathrm{A}}\mathrm{BE}}$ соответственно. Они неотрицательны, поскольку эти состояния — классически-квантовые. Также мы воспользовались тем, что $H(\overline{\mathrm{A}}|\mathrm{E})_{(0)} = H(\overline{\mathrm{A}}) = 1$, что следует из вида состояний $\tilde{\rho}^{(0)}_{\overline{\mathrm{A}}\mathrm{A}}$ и $\tilde{\rho}^{(0)}_{\overline{\mathrm{A}}\mathrm{BE}}$, неформально — вакуум не содержит никакой информации о посланном бите.

Теорема утверждает, что метод обманных состояний является универсальным, т.е. стойким к произвольным атакам (для произвольных отображений Υ), а не только к атаке расщеплением по числу фотонов. Точнее говоря, теорема утверждает универсальность нижней оценки (12), а метод обманных состояний позволяет оценить Q_0^{sz} и Q_1^{sz} снизу, а также получить оценки величин, входящих в оценку $H(\overline{\mathrm{A}}|\mathrm{E})_{(1)}$.

Оценка (12) становится точной при атаке расщеплением по числу фотонов, т.е. эта атака оптимальна. В самом деле, эта атака обеспечивает противнику знание всех битов, закодированных в многофотонных посылках, что и положено в основу этой оценки.

Всегда ли есть возможность провести атаку расщеплением по числу фотонов? Изымая фотон из многофотонной посылки, противник уменьшает вероятность её регистрации, т.е. повышает уровень потерь. Как говорилось выше, он может компенсировать это уменьшением уровня естественных потерь в канале связи или даже в оптической схеме приёмной стороны. Однако если естественные потери настолько малы, что даже их уменьшение до нуля не компенсирует потери, вносимые изъятием фотонов из многофотонных посылок, то противник не может провести атаку расщеплением по числу фотонов в полной мере. Поэтому оценка (12) перестаёт быть точной (но, разумеется, остаётся справедливой): $H(\overline{\mathrm{A}}|\mathrm{E})_{(\geqslant 2)} > 0$. Тем не менее при реалистичных потерях противник может провести атаку расщеплением по числу фотонов и оценка (12) точна.

Обратим теперь внимание на первое слагаемое в правой части (12). Оно связано с регистрацией вакуумных посылок. Регистрация вакуумной посылки может произойти из-за действий противника, который может послать получателю свой сигнал. Также это может произойти из-за темновых шумов в детекторах получателя. Однако если распределение ключей возможно, то доля темновых срабатываний в общем числе срабатываний (т.е. отношение Q_0^{sz}/Q^{sz}) невелика. Распределение ключей возможно только при относительно низкой доле ошибок. Хорошо известна теоретическая максимально допустимая доля ошибок для протокола BB84 — 11 % (при предположении, что доля ошибок одинакова для обоих базисов (см. ниже замечание 2)) [11, 12, 18]. На практике эта доля ещё меньше вследствие наличия многофотонных импульсов и необходимости учёта статистических флуктуаций. Поскольку темновое срабатывание является ошибочным с вероятностью $1/2$, это означает, что доля темновых отсчётов в общем числе срабатываний на стороне получателя не превышает 6 %. По этой причине вместо точной оценки (12) часто пользуются более грубой оценкой:

$$H(\overline{\mathrm{A}}|\mathrm{E}) \geqslant \frac{Q_1^{sz}}{Q^{sz}}\,H(\overline{\mathrm{A}}|\mathrm{E})_{(1)}\,. \tag{13}$$

Подчеркнём, что доля темновых срабатываний влияет на близость оценки (13) к точной оценке (12), но не на справедливость (13), которая непосредственно вытекает из (12) и положительности величин Q_0^{sz} и Q^{sz}. Это означает, что формула (13) позволяет генерировать секретный ключ при любом уровне темновых шумов, но с несколько меньшей скоростью, чем позволяет формула (12).

В дальнейшем в методе обманных состояний темновые срабатывания строго учитываются в величине Y_0 (см. формулы (22)–(24) в разделе 7). При реалистичных длинах линии связи и отсутствии перехвата, т.е. при "нормальном" функционировании системы, именно темновые срабатывания (а не ошибки, например, из-за неточной настройки оптической схемы) вносят основной вклад в долю ошибок.

Замечание 1. Требование фазовой рандомизации (6) здесь принципиально важно. Как упоминалось в разделе 3, оно может быть обеспечено двумя способами: на аппаратном уровне, когда лазер испускает импульс со случайной фазой, независимой от фаз предыдущих импульсов, или с помощью активной рандомизации, т.е. подключённого к генератору случайных чисел устройства, осуществляющего изменение фазы исходящих импульсов. В последнем случае рандомизация в соответствии с равномерным или другим непрерывным распределением невозможна, возможно лишь дискретное приближение, поэтому необходимо учитывать соответствующую поправку [55].

Формула скорости предельного ключа Деветака–Винтера (10) изначально была выведена для случая так называемой коллективной атаки. Напомним, что атаки

на протоколы квантовой криптографии разделяют (по возрастанию степени общности) на индивидуальные, коллективные и когерентные [18]. В коллективной атаке предполагается, что противник атакует посылаемые состояния одинаковым образом, так что после пересылки n импульсов образуется состояние $\rho_{\mathrm{ABE}}^{\otimes n}$ (см. (9)). Затем противник осуществляет коллективное (т.е. общего вида) измерение над своими частями.

В наиболее общем случае противник проводит над n импульсами произвольное квантовое преобразование, не обязательно являющееся тензорной степенью преобразования над одним импульсом. Такие атаки называются когерентными. В асимптотическом случае $n \to \infty$, которым мы ограничиваемся в этой статье, рассмотрение когерентных атак сводится к рассмотрению коллективных атак с помощью квантового представления де Финетти [14], поэтому формально использование формулы Деветака – Винтера не является ограничением. Но поправки, связанные с конечностью n, при использовании представления де Финетти оказываются достаточно велики при реалистичных n, поэтому на практике представлением де Финетти, как правило, не пользуются. Поясним, почему рассмотрение атаки расщеплением по числу фотонов не ограничивает общности и в случае когерентной атаки.

Для n посылок вместо состояния (8) имеем состояние

$$\rho_{\overline{\mathbf{A}}\mathbf{A}}^{z} = \frac{1}{2^n} \sum_{\mathbf{u} \in \{0,1\}^n} |\mathbf{u}\rangle_{\overline{\mathrm{A}}} \langle \mathbf{u}| \otimes \rho_{\mu\mathbf{u}}^{z}, \tag{14}$$

где $\mathbf{u} = u_1, \ldots, u_n$ — двоичная строка, $|\mathbf{u}\rangle = |u_1\rangle \otimes \ldots \otimes |u_n\rangle$,

$$\rho_{\mu\mathbf{u}}^{z} = \rho_{\mu u_1}^{z} \otimes \ldots \otimes \rho_{\mu u_n}^{z},$$

выделение жирным шрифтом регистров $(\overline{\mathbf{A}}, \mathbf{A})$ означает, что регистры — "векторные".

Поскольку

$$\rho_{\mu u}^{z} = \sum_{j=0}^{\infty} P_j \rho_{\mu u}^{z} P_j,$$

то

$$\rho_{\mu\mathbf{u}}^{z} = \sum_{j_1=0}^{\infty} \ldots \sum_{j_n=0}^{\infty} (P_{j_1} \rho_{\mu u_1}^{z} P_{j_1}) \otimes \ldots \otimes (P_{j_n} \rho_{\mu u_n}^{z} P_{j_n}). \tag{15}$$

Каждое слагаемое в правой части (15) представляет собой состояние (с точностью до нормировки) с определёнными количествами фотонов в каждой позиции. Поскольку преобразования квантовых состояний являются линейными (или аффинными) отображениями, любое преобразование состояния (15) является выпуклой суммой результатов преобразований состояний с определёнными количествами фотонов в каждой посылке. Поэтому рассмотрение только таких состояний не ограничивает общности. Измерения числа фотонов в каждой посылке, проводимые при атаке расщеплением по числу фотонов, не изменяют состояния (15) (поскольку оно уже имеет вид, диагональный относительно операторов $P_{j_1} \otimes \ldots \otimes P_{j_n}$), а просто позволяют противнику узнать число фотонов в каждой посылке. В этом смысле атака расщеплением по числу фотонов является оптимальной: если каждая посылка имеет определённое число фотонов и его можно узнать, не внося шум, то оптимально сделать это, т.е. провести измерения числа фотонов в каждой посылке.

Строгая оценка энтропии, характеризующей степень незнания противника, для состояния вида (15) с учётом конечного n выполнена в работе [56]. Целью настоящего рассмотрения было обоснование того, что рассмотрение состояний с определённым числом фотонов в каждой посылке не ограничивает общности.

6. Формулировка в терминах сцепленного состояния

С целью обобщения результата Деветака – Винтера для случая когерентных атак можно также использовать технику накопления энтропии ("entropy accumulation") [17]. Эта техника заключается в оценке сглаженной минэнтропии Реньи для состояния в $(\mathscr{H}_{\mathrm{A}} \otimes \mathscr{H}_{\mathrm{B}} \otimes \mathscr{H}_{\mathrm{E}})^{\otimes n}$ (которая необходима для оценки нехватки информации противника при когерентной атаке) через энтропию фон Неймана, которая стоит первым слагаемым в правой части формулы Деветака – Винтера (10). Таким образом, если удаётся применить эту технику, то формула Деветака – Винтера даёт предельно достижимую скорость генерации секретного ключа при когерентных атаках, т.е. атаках общего вида. Техника накопления энтропии позволяет также учесть эффекты, связанные с конечностью объёма статистической выборки (конечным числом n), что выходит за рамки настоящей статьи: напомним, мы работаем в пределе бесконечно больших n.

В работе [17] с помощью указанной техники обоснована формула Деветака – Винтера для протокола BB84 с однофотонным источником при атаках общего вида. Однако для этого используется эквивалентное представление протокола BB84 в терминах сцепленного состояния. Целью данного раздела является формулировка протокола BB84 с когерентными состояниями при рандомизированной фазе в терминах сцепленного состояния.

Напомним, через $\mathscr{H}_{\mathrm{A}}$ мы обозначили гильбертово пространство, соответствующее квантовому носителю информации: $\mathbb{C}^2$ в однофотонном случае и $\mathscr{F}(\mathbb{C}^2)$ в общем случае. Через $\overline{\mathrm{A}}$ мы обозначили двоичный регистр, в который отправитель записывает своё значение бита. Введём ещё одно гильбертово пространство, связанное с отправителем — $\mathcal{H}_{\widetilde{\mathrm{A}}}$. В протоколе BB84 отправитель посылает состояния $\rho_{\mu u}^{b} \in \mathfrak{T}(\mathscr{H}_{\mathrm{A}})$, $b \in \{z, x\}$, $u \in \{0, 1\}$, вида (6) с вероятностями $p_b/2$. Для задания протокола в терминах сцепленных состояний предполагается, что на стороне отправителя генерируется сцепленное состояние $\rho \in \mathfrak{T}(\mathscr{H}_{\widetilde{\mathrm{A}}} \otimes \mathscr{H}_{\mathrm{A}})$ составной системы $\mathscr{H}_{\widetilde{\mathrm{A}}} \otimes \mathscr{H}_{\mathrm{A}}$, в которой подсистему $\widetilde{\mathrm{A}}$ измеряет отправитель, а подсистема A, как и ранее, отправляется по линии связи получателю. Пусть наблюдаемая отправителя в подсистеме $\widetilde{\mathrm{A}}$ задаётся вероятностной проекторнозначной мерой $\Pi = \{\Pi_{ub}\}_{u \in \{0,1\}, b \in \{z,x\}}$ на пространстве $\mathscr{H}_{\widetilde{\mathrm{A}}}$. Потребуем выполнения следующих условий:

$$\mathrm{Tr}_{\widetilde{\mathrm{A}}} (\Pi_{ub} \rho \Pi_{ub}) = \frac{p_b}{2} \rho_{\mu u}^{b} \tag{16}$$

для всех u и b, где $\mathrm{Tr}_{\widetilde{\mathrm{A}}}$ — частичный след по пространству $\mathscr{H}_{\widetilde{\mathrm{A}}}$. Тогда отправитель может готовить состояния $\rho_{\mu u}^{b}$ с соответствующими вероятностями посредством измерения наблюдаемой Π в подсистеме $\widetilde{\mathrm{A}}$, так что мы получили математически эквивалентную схему протокола. Для его стойкости состояние ρ должно быть сцепленным, откуда и происходит название этой схемы протокола.

Если в действительности генерации сцепленного состояния и измерения одной из его подсистем отправителем не происходит, то система $\mathscr{H}_{\widetilde{\mathrm{A}}}$ и измерение в ней являются "фиктивными" — служат только для математически эквивалентной формулировки.

В однофотонном случае (тогда $\mathscr{H}_{\mathrm{A}} = \mathbb{C}^2$ и в состояниях $\rho^{b}_{\mu u}$ надо оставить только однофотонную компоненту) можно взять $\mathscr{H}_{\widetilde{\mathrm{A}}} = \mathbb{C}^2$, $\rho = |\Phi\rangle\langle\Phi|$, где

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle_z \otimes |1,0\rangle_z + |0,1\rangle_z \otimes |0,1\rangle_z\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|1,0\rangle_x \otimes |1,0\rangle_x + |0,1\rangle_x \otimes |0,1\rangle_x\right) \in \mathbb{C}^2 \otimes \mathbb{C}^2 \quad (17)$$

и $\Pi_{ub} = p_b|u\rangle_b\langle u|$. Стойкость такого протокола, основанного на сцепленном состоянии $|\Phi\rangle$, с помощью техники накопления энтропии доказана в статье [17]. В данном случае в результате измерения наблюдаемой Π в системе $\widetilde{\mathrm{A}}$ остаётся значение бита, посылаемого отправителем, поэтому регистр $\widetilde{\mathrm{A}}$ можно отождествить с $\overline{\mathrm{A}}$. Но в общем случае они не обязательно должны отождествляться.

Для того чтобы распространить результаты статьи [17] на многофотонный случай, необходимо предъявить схему протокола в терминах сцепленного состояния таким образом, чтобы в проекции на однофотонный случай и после нормирования снова получалось состояние (17) и наблюдаемая $\{p_b|u\rangle_b\langle u|\}$. Состояние (17) не удаётся непосредственно обобщить для многофотонного случая, поскольку

$$\frac{1}{\sqrt{2}}\left(|j,0\rangle_z \otimes |j,0\rangle_z + |0,j\rangle_z \otimes |0,j\rangle_z\right) \neq$$

$$\neq \frac{1}{\sqrt{2}}\left(|j,0\rangle_x \otimes |j,0\rangle_x + |0,j\rangle_x \otimes |0,j\rangle_x\right)$$

при $j \geqslant 2$.

Расширим поэтому пространство $\mathscr{H}_{\widetilde{\mathrm{A}}}$: пусть $\mathscr{H}_{\widetilde{\mathrm{A}}} = \mathbb{C}^2 \oplus \mathbb{C}^4$. В качестве базисов для пространства $\mathbb{C}^2$ попрежнему будем использовать $\{|0\rangle_z, |1\rangle_z\}$ и $\{|0\rangle_x, |1\rangle_x\}$: каждый элемент базиса маркирует бит отправителя. В качестве базиса для пространства $\mathbb{C}^4$ возьмём новые векторы $\{|0z\rangle, |1z\rangle, |0x\rangle, |1x\rangle\}$. Каждый вектор маркирует бит и базис (в $\mathbb{C}^2$), который использует отправитель. Эквивалентное представление протокола в терминах сцепленного состояния можно построить с помощью состояния

$$\rho = \mu \exp(-\mu)|\Phi\rangle\langle\Phi| + \sum_{u\in\{0,1\}}\sum_{b\in\{z,x\}} p_b \exp(-\mu)|ub\rangle\langle ub| \otimes$$

$$\otimes \left(|\mathrm{vac}\rangle\langle\mathrm{vac}| + \sum_{j=2}^{\infty}\frac{\mu^j}{j!}|\psi^{b}_{ju}\rangle\langle\psi^{b}_{ju}|\right) \quad (18)$$

и наблюдаемой Π, где $\Pi_{ub} = p_b|u\rangle_b\langle u| + |ub\rangle\langle ub|$. В проекции на однофотонную компоненту (см. (7)) состояние ρ после нормирования на единицу переходит в проектор на $|\Phi\rangle$, в формуле для Π_{ub} тогда остаётся существенным только первое слагаемое, что воспроизводит прежнюю наблюдаемую. В состоянии (18) сцепленность содержится только в однофотонной компоненте. Строить состояние, в котором сцепленность содержится и в многофотонных компонентах, нет необходимости, поскольку многофотонные посылки в любом случае считаются ненадёжными, т.е. нет смысла обеспечивать их надёжность.

Итак, сочетание доказанной в разделе 5 теоремы, которая сводит оценку нехватки информации противника в терминах энтропии фон Неймана к оценке соответствующей энтропии для состояний с однофотонными посылками, и оценки последней в работе [17] позволяет применить технику накопления энтропии для протокола BB84 с источником когерентных состояний и заключить, что формула Деветака – Винтера даёт предельно достижимую скорость генерации секретного ключа без предположений относительно класса атак противника.

7. Метод обманных состояний

Из формулы (13) следует, что задача получения достижимых скоростей генерации ключа (10) при произвольных коллективных атаках в пространстве $\mathscr{F}(\mathbb{C}^2)$ распадается на две подзадачи: оценка множителя Q_1^{sz}/Q^{sz}, т.е. доли позиций в просеянном ключе, полученных из однофотонных посылок, и оценка нехватки информации противника $H(\overline{\mathrm{A}}|\mathrm{E})_{(1)}$ об одном бите этой части ключа.

Хорошо известное [12, 13, 17] выражение для $H(\overline{\mathrm{A}}|\mathrm{E})_{(1)}$ имеет вид

$$H(\overline{\mathrm{A}}|\mathrm{E})_{(1)} = 1 - h(e_1^x)\,, \quad (19)$$

где e_1^x — вероятность битовой ошибки в однофотонной посылке при использовании обеими сторонами x-базиса. Поэтому выражение для достижимой скорости генерации секретного ключа принимает вид

$$R = \frac{Q_1^{sz}}{Q^{sz}}\left[1 - h(e_1^x)\right] - h(E^{sz})\,. \quad (20)$$

Замечание 2. Напомним, что в описываемом нами варианте протокола BB84 базис x выбирается редко. Но вероятность e_1^x оценивается только по тем немногочисленным позициям, в которых обе стороны выбрали базис x. С помощью формулы (20) прокомментируем пороговый уровень шума, при котором возможно распределение ключей, т.е. $R > 0$. Для простоты допустим, что все состояния — однофотонные, т.е. $Q_1^{sz} = Q^{sz}$. Если уровень ошибки не зависит от базиса, т.е. $e_1^x = E^{sz} = e$, то распределение ключей возможно при $1 - 2h(e) > 0$, т.е. при $e < e_{\mathrm{crit}} \approx 0{,}11$. Однако при теоретически возможной ситуации различных e_1^x и E^{sz} утверждение о критическом уровне ошибок 11 %, вообще говоря, перестаёт быть верным. Например, при $E^{sz} = 0$ критический уровень ошибок для e_1^x возрастает до 50 %. Аналогично при $e_1^x = 0$ критический уровень ошибок для E^{sz} также возрастает до 50 %.

Метод обманных состояний позволяет эффективно оценить множитель Q_1^{sz}/Q^{sz}, а также величину e_1^x. Он заключается в том, что в некоторых заранее не известных и выбираемых случайно позициях посылаются не "сигнальные" импульсы (т.е. используемые для формирования ключа) с интенсивностью μ (см. (5)), а "обманные", с меньшими интенсивностями. Позиции, в которых были использованы обманные импульсы, не участвуют затем в формировании ключа. После окончания пересылки квантовых состояний на этапе раскрытия информации отправитель объявляет интенсивности, которые были использованы в каждой посылке. На основании этой информации легитимные стороны вычисляют статистику регистраций посылок для каждой интенсивности, а затем сравнивают результаты для состояний с разными интенсивностями. Неформально говоря, идея метода состоит

в том, что при измерении числа фотонов противник не знает интенсивности, с которой была сгенерирована данная посылка, поэтому у него нет возможности поразному обращаться с сигнальными и обманными состояниями при том же количестве фотонов в посылке (которое, напротив, противник, как предполагается, знает). Если он блокирует все однофотонные компоненты, то это приведёт к блокировке почти всех обманных состояний с малой интенсивностью, что будет заметно на приёмной стороне. Формально это приведёт к нулевой скорости генерации ключа, что и соответствует обнаружению перехвата.

Наиболее распространён метод, использующий одно сигнальное и два обманных состояния, который мы и изложим. Будем использовать обозначения, схожие с обозначениями в [29, 32]. Также будем предполагать, что эффективности и вероятности темновых срабатываний детекторов совпадают. В противном случае формула (19) нуждается в корректировке (см. статью [20], в которой подробно рассмотрена адаптация метода обманных состояний для случая различных эффективностей детекторов). При совпадении эффективностей и вероятностей темновых срабатываний детекторов индекс z у величин Q_1^{sz} и Q^{sz} можно опустить: вероятности детектирования не зависят от базиса.

Пусть Y_i — вероятность того, что на приёмной стороне сработает один из детекторов, при условии, что на стороне отправителя посылка содержала i фотонов. Эта вероятность не зависит от интенсивности импульса (зависит только от числа фотонов в нём, т.е. от i), но может зависеть как от затухания в канале, так и от действий противника, который способен блокировать часть состояний или, наоборот, отправлять их на приёмную сторону без затухания. Отметим, что Y_0 отлична от нуля и равна вероятности темнового срабатывания одного из детекторов.

Q_i^v — вероятность того, что посылка содержит i фотонов и на приёмной стороне сработает один из детекторов, при условии, что отправитель использовал состояние типа $v \in \{s, d_1, d_2\}$ (сигнальное или одно из двух обманных). Обозначим интенсивность сигнального импульса $\mu_s = \mu$, интенсивности обманных импульсов — $\mu_{d_1} = v_1$, $\mu_{d_2} = v_2$, причём потребуем, чтобы

$$0 \leqslant v_2 < v_1\,, \quad v_1 + v_2 < \mu\,. \tag{21}$$

Поскольку вероятность того, что посылка содержит ровно i фотонов (при условии интенсивности импульса μ), равна $\exp(-\mu)\,\mu^i/i!$, то

$$Q_i^v = \exp(-\mu_v)\,\frac{\mu_v^i}{i!}\,Y_i\,. \tag{22}$$

Вероятность срабатывания детектора на приёмной стороне при передаче импульса типа v равна

$$Q^v = \sum_{i=0}^{\infty} Q_i^v = \sum_{i=0}^{\infty} \exp(-\mu_v)\,\frac{\mu_v^i}{i!}\,Y_i\,. \tag{23}$$

Величины Q^v становятся известными легитимным сторонам на этапе раскрытия информации (точнее, их оценки, но в пределе бесконечного числа посылок они совпадают с истинными значениями). По ним можно оценить неизвестную величину Y_1 и, соответственно, фигурирующую в (13) величину Q_1^s.

Для начала из цепочки неравенств

$$v_1 Q^{d_2} \exp v_2 - v_2 Q^{d_1} \exp v_1 = \\ = (v_1 - v_2)\,Y_0 - v_1 v_2 \sum_{i=2}^{\infty} (v_1^{i-1} - v_2^{i-1})\,\frac{Y_i}{i!} \leqslant (v_1 - v_2)\,Y_0$$

получаем нижнюю оценку для Y_0:

$$Y_0 \geqslant Y_0^L = \max\left\{\frac{v_1 Q^{d_2} \exp v_2 - v_2 Q^{d_1} \exp v_1}{v_1 - v_2},\, 0\right\}. \tag{24}$$

Это неравенство даёт оценку вероятности темнового срабатывания в одном из детекторов приёмной стороны, которая, как предполагается, заранее не известна легитимным пользователям и может находиться во власти противника.

Оценка для Y_1 получается из цепочки неравенств

$$Q^{d_1} \exp v_1 - Q^{d_2} \exp v_2 = (v_1 - v_2)\,Y_1 + \sum_{i=2}^{\infty} (v_1^i - v_2^i)\,\frac{Y_i}{i!} \leqslant$$

$$\leqslant (v_1 - v_2)\,Y_1 + \frac{v_1^2 - v_2^2}{\mu^2} \sum_{i=2}^{\infty} \frac{\mu^i}{i!}\,Y_i =$$

$$= (v_1 - v_2)\,Y_1 + \frac{v_1^2 - v_2^2}{\mu^2}\left(Q^s \exp\mu - Y_0 - Y_1\mu\right) \leqslant$$

$$\leqslant (v_1 - v_2)\,Y_1 + \frac{v_1^2 - v_2^2}{\mu^2}\left(Q^s \exp\mu - Y_0^L - Y_1\mu\right). \tag{25}$$

Первое неравенство этой цепочки использует условия (21), а также неравенство $a^i - b^i \leqslant a^2 - b^2$ при $0 < a + b < 1$ и $i > 2$. Отсюда

$$Y_1 \geqslant Y_1^L = \frac{\mu}{\mu(v_1 - v_2) - (v_1^2 - v_2^2)} \times \\ \times \left[Q^{d_1} \exp v_1 - Q^{d_2} \exp v_2 - \frac{v_1^2 - v_2^2}{\mu^2}\left(Q^s \exp\mu - Y_0^L\right)\right], \tag{26}$$

$$Q_1^s \geqslant Q_1^{sL} = \mu \exp(-\mu)\,Y_1^L\,. \tag{27}$$

Обозначим теперь через e_i^x вероятность битовой ошибки в i-фотонной посылке при использовании обеими сторонами базиса x и оценим вероятность e_1^x, фигурирующую в (19). Эта вероятность может включать в себя как несовершенство аппаратуры, так и действия противника, применяющего ту или иную атаку. Вероятность ошибки E^{vx} в импульсе типа v при использовании обеими сторонами базиса x определяется из

$$E^{vx} Q^v = \sum_{i=0}^{\infty} e_i^x\,Y_i\,\frac{\mu_v^i}{i!} \exp(-\mu)\,.$$

Тогда из неравенства

$$E^{d_1 x} Q^{d_1} \exp v_1 - E^{d_2 x} Q^{d_2} \exp v_2 = e_1^x (v_1 - v_2)\,Y_1 + \\ + \sum_{i=2}^{\infty} e_i^x (v_1^i - v_2^i)\,\frac{Y_i}{i!} \geqslant e_1^x (v_1 - v_2)\,Y_1 \geqslant e_1^x (v_1 - v_2)\,Y_1^L$$

следует верхняя оценка для e_1^x:

$$e_1^x \leqslant e_1^{xU} = \frac{E^{d_1 x} Q^{d_1} \exp v_1 - E^{d_2 x} Q^{d_2} \exp v_2}{(v_1 - v_2)\,Y_1^L}\,. \tag{28}$$

Подставляя полученные оценки в (13) и (19), получаем формулу для достижимой скорости генерации секретного ключа:

$$R = \frac{Q_1^{\mathrm{sL}}}{Q^{\mathrm{s}}}\left[1 - h(e_1^{x\mathrm{U}})\right] - h(E^{\mathrm{s}z}). \tag{29}$$

При отсутствии перехвата фактические значения всех величин, участвующих в определении скорости генерации секретного ключа, выражаются в виде (см. формулы (5)–(11) в [29])

$$Q^{\mathrm{s}} = p_{\mathrm{d}} + 1 - \exp\left[-\eta\mu T(L)\right], \tag{30}$$

$$Y_1 = p_{\mathrm{d}} + \eta T(L), \tag{31}$$

$$Q_1^{\mathrm{s}} = \left[p_{\mathrm{d}} + \eta T(L)\right]\mu\exp(-\mu), \tag{32}$$

$$E^{\mathrm{s}z} = \frac{p_{\mathrm{d}}}{2}, \tag{33}$$

$$e_1^{x} = \frac{p_{\mathrm{d}}}{2Y_1}, \tag{34}$$

где p_{d} — вероятность темнового срабатывания хотя бы одного из детекторов, $T(L) = 10^{-\delta L/10}$ — коэффициент прохождения в линии связи длиной L, δ — удельный коэффициент потерь, η — квантовая эффективность каждого однофотонного детектора. Будем предполагать, что ошибки возникают только из-за темнового шума, а оптическая часть настроена идеально.

Можно рассмотреть зависимость длины ключа от длины линии связи при реалистичных параметрах на приёмной стороне: интенсивности сигнального и обманных состояний $\mu = 0{,}5$, $\nu_1 = 0{,}01$, $\nu_2 = 0{,}001$, $p_{\mathrm{d}} = 10^{-6}$, $\eta = 0{,}1$, $\delta = 0{,}2$ дБ км$^{-1}$. На рисунке представлен график R, вычисленный по формулам (20) и (29), в зависимости от длины линии связи. В обоих случаях наблюдаемая статистика приёма $Q^{\mu}, Q^{\nu_1}, Q^{\nu_2}, E^{\mu}, E^{\nu_1}$ и E^{ν_2} вычисляется по формулам (30) и (33), т.е. для случая отсутствия подслушивания.

В статье [29] показано, что при $\nu_1, \nu_2 \to 0$ и отсутствии перехвата (или при таком перехвате, который не меняет статистику регистраций) оценки $Q_1^{\mu,\mathrm{L}}$ и e_1^{U} становятся точными, т.е. стремятся к фактическим значениям Q_1^{μ} и e_1, которые задаются формулами (32) и (34). Так что в асимптотическом случае скорость генерации секретного ключа определяется (20), где Q^{μ}, Q_1^{μ} и e_1 определяются формулами (30)–(34).

Замечание 3. Важно отметить, что оценки (26)–(28) не предполагают, что известны коэффициент прохождения линии $T(L)$, вероятность темнового шума p_{d}, эффективность детекторов η и другие параметры оптической и детектирующей схемы приёмной стороны. При выводе указанных оценок не предполагается и постоянство этих коэффициентов в различных посылках. То есть фактически метод обманных состояний обеспечивает стойкость даже тогда, когда противник может изменять эти параметры, что подробно объясняется, например, в статье [20]. Таким образом, будем считать, что противник может уменьшать естественные потери и естественные ошибки в канале связи и даже в детекторах, вплоть до создания линии связи и детекторов без потерь и без ошибок. Это даёт ему определённую свободу в создании желаемой статистики регистрации состояний с разной интенсивностью на приёмной стороне.

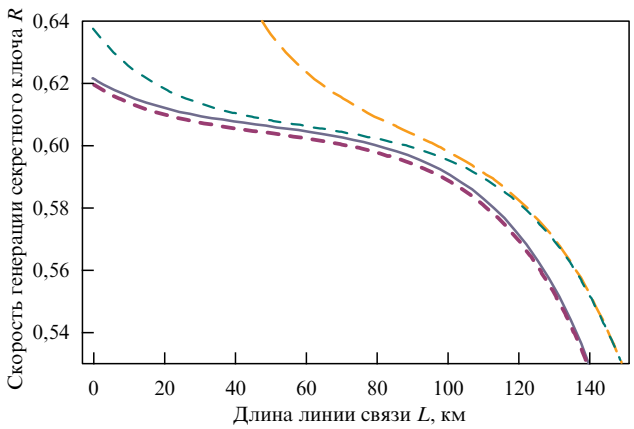

Рисунок. (В цвете онлайн.) Скорость генерации секретного ключа в зависимости от длины линии связи. Сплошная синяя кривая: расчёт для атаки расщеплением по числу фотонов с когерентной атакой на однофотонные состояния по формуле (20). Сиреневая штриховая кривая: расчёт для той же атаки по формуле (29), в которой, вообще говоря, неизвестные фактические значения Q_1^{μ} и e_1 заменены их оценками снизу и сверху соответственно (формулы (27) и (28) с формулами (30) и (33) для значений наблюдаемой статистики регистраций). Зелёная штриховая кривая: расчёт для атаки светоделителем (формула (37) с $t = \eta T(L)$), оранжевая штриховая кривая: расчёт для атаки светоделителем, при которой противник не меняет эффективности детекторов на приёмной стороне (формула (37) с $t = T(L)$). Интенсивности сигнального и обманных состояний $\mu = 0{,}5$, $\nu_1 = 0{,}01$, $\nu_2 = 0{,}001$, вероятность темновых шумов на строб $p_{\mathrm{d}} = 10^{-6}$, квантовая эффективность каждого однофотонного детектора $\eta = 0{,}1$, удельный коэффициент потерь в линии связи $\delta = 0{,}2$ дБ км$^{-1}$.

8. Атака светоделителем

Как отмечено в разделе 5, при практических уровнях потерь в канале оценки (12) и, следовательно, (20) становятся точными при осуществлении противником атаки расщеплением по числу фотонов. Однако пока данная атака не реализована на практике. Сравним с ней более простую атаку светоделителем, которая также часто рассматривается в квантовой криптографии [18, 57–59].

Простая атака светоделителем заключается в том, что противник с помощью светоделителя отводит себе ту часть сигнала (когерентного состояния), которая поглощается в канале в результате естественных потерь. Оставшуюся часть сигнала он передаёт получателю по идеальному каналу, т.е. каналу без потерь. В результате эта атака не меняет статистику регистраций состояний получателя, которая имеет место в естественных условиях (при отсутствии противника).

С формальной точки зрения речь идёт об изометрии $V_{\mathrm{BS}}\colon \mathscr{F}(\mathbb{C}^2) \to \mathscr{F}(\mathbb{C}^2) \otimes \mathscr{F}(\mathbb{C}^2)$, для определения которой достаточно задать её действие на всевозможные когерентные состояния (5):

$$V_{\mathrm{BS}}|\alpha, u\rangle_b = \left|\sqrt{t}\,\alpha, u\right\rangle_b \otimes \left|\sqrt{1-t}\,\alpha, u\right\rangle_b, \tag{35}$$

где t и $1-t$ — показатели пропускания и преломления соответственно. Первое пространство в тензорном произведении, в которое отображает V_{BS}, интерпретируется как пространство получателя, второе — пространство

противника. Композиция отображения

$$\rho^z_{\mu u} \mapsto V_{\mathrm{BS}}\, \rho^z_{\mu u} V^\dagger_{\mathrm{BS}}\,, \tag{36}$$

описывающего перехват, с отображением, описывающим измерение на стороне получателя, даёт канал Υ_0 (см. раздел 5), соответствующий данной атаке. В любом случае, поскольку после отображения (36) состояние противника уже не претерпевает изменений, отображения (36) достаточно для того, чтобы задать состояние $\rho_{\overline{\mathrm{A}}\mathrm{E}}$ и, следовательно, определить энтропию $H(\overline{\mathrm{A}}|\mathrm{E})$ в (10):

$$\begin{aligned}
\rho_{\overline{\mathrm{A}}\mathrm{E}} &= \frac{1}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes \mathrm{Tr}_{\mathrm{B}}\left(V_{\mathrm{BS}}\, \rho^z_{\mu u} V^\dagger_{\mathrm{BS}}\right) = \\
&= \frac{\exp\left(-\mu_{\mathrm{E}}\right)}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes \\
&\otimes \left[|\mathrm{vac}\rangle\langle\mathrm{vac}| + \sum_{j=1}^{\infty} \frac{\mu_{\mathrm{E}}^j}{j!}\, |\psi^z_{j\mu_{\mathrm{E}}}\rangle_{\mathrm{E}}\langle\psi^z_{j\mu_{\mathrm{E}}}|\right] = \\
&= \frac{\exp\left(-\mu_{\mathrm{E}}\right)}{2}\, I_{\overline{\mathrm{A}}} \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}| + \frac{\exp\left(-\mu_{\mathrm{E}}\right)}{2}\sum_{u=0}^{1} |u\rangle_{\overline{\mathrm{A}}}\langle u| \otimes \\
&\otimes \sum_{j=1}^{\infty} \frac{\mu_{\mathrm{E}}^j}{j!}\, |\psi^z_{j\mu_{\mathrm{E}}}\rangle_{\mathrm{E}}\langle\psi^z_{j\mu_{\mathrm{E}}}|\,,
\end{aligned}$$

где $\mu_{\mathrm{E}} = (1-t)\mu$, $u \in \{0,1\}$. Отсюда видим, что противник имеет нулевую информацию о бите ключа (соответственно, нехватка информации равна единице), если у него реализовалась вакуумная компонента, что имеет место с вероятностью $\exp\left(-\mu_{\mathrm{E}}\right)$. В противном случае он обладает полной информацией о бите ключа. Поскольку состояние (35) имеет вид тензорного произведения, реализация вакуумной компоненты у противника не зависит от события, заключающегося в регистрации фотона на стороне получателя. Поэтому вероятность вакуумной компоненты при условии срабатывания одного из детекторов получателя равна безусловной вероятности этого события. Следовательно, $H(\overline{\mathrm{A}}|\mathrm{E}) = \exp\left[-(1-t)\mu\right]$ и

$$R_{\mathrm{BS}} = \exp\left[-(1-t)\mu\right] - h(E^{\mathrm{sz}})\,. \tag{37}$$

При отсутствии перехвата фактический показатель пропускания всей оптической системы (линии связи и детекторов) равен $\eta T(L)$. Если предположить, что доля сигнала, поглощающаяся в канале и на детекторах, целиком уходит к противнику, то следует установить $t = \eta T(L)$. Обычно это объясняется следующим образом: мы предполагаем, что противник может заменить линию связи и детекторы идеальными (т.е. без потерь) и благодаря этому отводить себе долю сигнала $1 - \eta T(L)$, воспроизводя естественный уровень потерь. Если мы предположим, что противник может заменить линию связи идеальной, но не имеет власти над эффективностью детекторов η, то можно положить $t = T(L)$, что уменьшает информацию противника о ключе и позволяет легитимным сторонам при этом предположении о противнике генерировать ключ с большей скоростью.

В обзоре [18] обсуждается реалистичность предположения о способности противника заменить канал бесшумным. Отмечается, что все существующие решения имеют фундаментальные ограничения на минимальный коэффициент потерь. Имеются гипотетические решения, теоретически способные обеспечить канал без потерь, но в обзоре [18] делается заключение, что они нереалистичны в любом обозримом будущем. Однако в квантовой криптографии часто предполагаются нереалистично большие возможности противника, для того чтобы решить вопрос о надёжном распределении ключей фундаментально. Так, например, даже если противник не может создать линию связи без потерь, он может создать линию связи с меньшими потерями. На эффективность детекторов он также способен влиять в некоторых пределах. Для того чтобы не обсуждать вопросы, какими могут быть эти пределы, можно сделать наиболее слабое предположение о полном контроле противника над коэффициентом пропускания линии и эффективностями детекторов. Но, напомним, здесь мы рассматриваем случай одинаковых эффективностей детекторов, т.е. предполагаем, что противник может поменять эффективности всех детекторов только на одинаковую величину.

На рисунке приведены графики R_{BS} для $t = \eta T(L)$ и $t = T(L)$. Сравнивая их с расчётными достижимыми скоростями (20) и (29), заключаем, что R_{BS} выше расчётных достижимых скоростей. Этого и следовало ожидать, поскольку атака светоделителем — частный вид атаки, тогда как формулы (20) и (29) выведены для общего случая. Ввиду важности атаки светоделителем в разделе 9 мы рассмотрим, почему атака светоделителем оказывается менее эффективной, чем атака расщеплением по числу фотонов.

Сравнивая графики R_{BS} для $t = \eta T(L)$ и $t = T(L)$, мы видим, что на малых длинах, когда основной вклад в потери дают детекторы, включение для противника возможности отведения большей доли сигнала за счёт повышения эффективности детекторов сильно снижает достижимую скорость генерации ключа и сближает её с достижимой скоростью генерации для атаки расщеплением по числу фотонов. На длинах линии связи от 50 км основной вклад в потери дают уже не детекторы, а линия связи, поэтому кривые для этих двух случаев сближаются и на длинах от 120 км практически совпадают.

Отметим, что в недавних работах [60–63] рассмотрены обобщения атаки светоделителем для протоколов B92, COW (Coherent One Way) и DPS (Differential Phase Shift), когда противник способен менять интенсивность состояний и дальнейшие его действия над передаваемым состоянием зависят от того, удалось ли ему извлечь информацию из части состояния, отведённой светоделителем.

9. Сравнение атак расщеплением по числу фотонов и светоделителем

Атаки светоделением и расщеплением по числу фотонов очень важны в квантовой криптографии, поэтому в данном разделе рассмотрим, почему первая атака менее эффективна, чем вторая. Для этого сначала докажем неравенство

$$R < R_{\mathrm{BS}}\,, \tag{38}$$

где R рассчитывается по формуле (20), а R_{BS} — по формуле (37) для $t = \eta T(L)$ (т.е. при наиболее слабом

предположении о противнике). Если неравенство (38) заменить нестрогим, то оно следует непосредственно из формулы (20), поскольку последняя выведена для произвольной атаки. Докажем строгое неравенство, т.е. что атака светоделителем всегда неоптимальна. Напомним также, что атака расщеплением по числу фотонов оптимальна, т.е. скорость генерации ключа (20) является предельно достижимой.

Докажем (38) для случая $\mu \leqslant 1$. Случай $\mu > 1$ также может быть разобран, но на практике $\mu \leqslant 1$, так что для краткости ограничимся рассмотрением только этого случая. Также мы предполагаем, что величина $\eta T(L)$ строго положительна (иначе невозможны не только распределение ключей, но и любая связь). Напомним также, что $\eta T(L) \leqslant 1$.

Поскольку слагаемое $h(E^{sz})$ в обеих формулах, (20) и (29), одинаково, доказательство (38) сводится к доказательству неравенства

$$\frac{Q_1^\mu}{Q^\mu}\left[1 - h(e_1^x)\right] < \exp\left[-(1-t)\mu\right]. \tag{39}$$

Докажем более сильное неравенство:

$$\frac{Q_1^\mu}{Q^\mu} < \exp\left[-(1-t)\mu\right]. \tag{40}$$

Воспользовавшись (30)–(32), для левой части имеем

$$\frac{Q_1^\mu}{Q^\mu} = \frac{\mu \exp(-\mu)(p_d + t)}{p_d + 1 - \exp(-\mu t)}. \tag{41}$$

Рассмотрим дробь

$$\frac{p_d + t}{p_d + 1 - \exp(-\mu t)}. \tag{42}$$

Ввиду неравенства $1 - \exp(-x) < x$ при $x > 0$ и, следовательно, $1 - \exp(-\mu t) < \mu t \leqslant t$ заключаем, что дробь убывает с увеличением p_d, так что

$$\frac{\mu \exp(-\mu)(p_d + t)}{p_d + 1 - \exp(-\mu t)} \leqslant \frac{\mu t \exp(-\mu)}{1 - \exp(-\mu t)}. \tag{43}$$

Итак, необходимо доказать неравенство

$$\frac{\mu t \exp(-\mu)}{1 - \exp(-\mu t)} < \exp\left[-\mu(1-t)\right], \tag{44}$$

или

$$\frac{\mu t}{\exp(\mu t) - 1} < 1. \tag{45}$$

Очевидно, что это неравенство следует из $\exp x - 1 > x$ при $x > 0$. Неравенство (40) и, следовательно, неравенство (38) доказаны.

Проанализируем теперь причины, по которым неравенство (38) является строгим, т.е. атака светоделителем неоптимальна. Во-первых, в процессе доказательства (38) мы воспользовались неравенством $h(e_1^x) > 0$ при $e_1^x > 0$. Это означает, что в атаке светоделителем не осуществляется атака на однофотонные посылки ценой внесения шума, присущая атаке расщеплением по числу фотонов. Это первая причина неоптимальности атаки светоделителем.

Во-вторых, неравенство (40) возникает из-за следующего эффекта. Поскольку отправляемое состояние — смесь фоковских, можно говорить об определённом числе фотонов в посылке, даже если эта наблюдаемая в действительности никем не измеряется. Можно представить себе ещё одного участника, который до действий противника измеряет число фотонов в посылке (не изменяя состояния) и затем наблюдает за действиями противника, обладая знанием о числе фотонов. Тогда он будет наблюдать, что при атаке расщеплением по числу фотонов противник с достоверностью узнаёт информацию, закодированную в многофотонных посылках, тогда как при атаке светоделителем с некоторой вероятностью он может пропустить все фотоны к получателю, не оставляя себе ни одного фотона, или, наоборот, забирает себе все фотоны, не пропуская ни одного к получателю, в результате чего получатель не зарегистрирует посылку (если не произойдёт темновое срабатывание) и эта позиция не войдёт в просеянный ключ. В последнем случае снижается доля многофотонных (ненадёжных) посылок в просеянном ключе. Напротив, в атаке расщеплением по числу фотонов блокируются только однофотонные посылки. Вероятностная обработка многофотонных посылок в атаке светоделителем вместо оптимальной детерминированной обработки в атаке расщеплением по числу фотонов является причиной неравенства (40). Более того, если после измерения числа фотонов противник применит вероятностную обработку многофотонных посылок, то он может воспроизвести (промоделировать) атаку светоделителем.

В [37] отмечается, что в атаке светоделителем противник отводит себе почти все квантовые состояния. Однако в формировании ключа участвуют только те позиции, в которых одновременно и противник, и получатель регистрируют получение фотона, поэтому отведение противником почти всех квантовых состояний приводит к потерям, но не обязательно приводит к большому знанию противника о просеянном ключе.

Из рисунка, приведённого в разделе 7, мы видим, что при рассмотренных параметрах и длине линии связи до приблизительно 140 км возможности этих двух атак практически совпадают: достижимая скорость генерации секретного ключа при атаке светоделителем лишь ненамного превышает достижимую скорость генерации при атаке расщеплением по числу фотонов. На длинах линии связи свыше 140 км преимущества атаки расщеплением по числу фотонов становятся существенными и кривые расходятся. На длине приблизительно 200 км достижимая скорость при атаке расщеплением по числу фотонов убывает до нуля, тогда как при атаке светоделителем генерация секретного ключа ещё возможна.

Из приведённых выше рассуждений можно ещё раз (см. конец раздела 5) легко вывести оптимальность атаки расщеплением по числу фотонов. Если можно измерить число фотонов, не портя состояние, то оптимально это сделать. Далее следует осуществить действия, оптимальные при заданном известном числе фотонов. Очевидно, что если посылка многофотонная, то оптимально изъять из неё один фотон (можно больше, но полную информацию о бите ключа даёт и один фотон). Если посылка однофотонная, то оптимально осуществить оптималь-

ную атаку для однофотонных посылок ценой внесения шума. Вследствие того что отправляемое состояние — смесь фоковских, а любое квантовое преобразование линейно, любую возможную атаку можно промоделировать, измерив число фотонов и применив ту или иную вероятностную обработку посылки в зависимости от числа фотонов в ней. Теорема, приведённая в разделе 5, фактически представляет собой формализацию этих рассуждений.

В заключение этого раздела упомянем также про атаку посредством различения состояний с определённым исходом (unambiguous state discrimination attack, USD-attack). Применительно к протоколу BB84 она рассмотрена в работе [58], в которой также подчёркивается, что в случае когерентных состояний с рандомизированной фазой атака расщеплением по числу фотонов (без атаки на однофотонные посылки) является оптимальным различением состояний с определённым исходом.

10. Поляризационное и фазовое кодирование

Некоторыми исследователями высказываются сомнения, насколько метод обманных состояний применим к случаю не поляризационного, а фазового кодирования, которое также широко используется [40]. Чтобы разрешить эти сомнения, в данном разделе мы покажем, что два указанных способа кодирования полностью эквивалентны, поэтому метод обманных состояний применим к фазовому кодированию, так же как и к поляризационному.

Отметим, что предшествующее изложение никак не опиралось на то, какой вид кодирования используется, хотя мы и ссылались на поляризационное кодирование для примера.

При поляризационном кодировании операторы рождения $a_{z0}^\dagger$, $a_{z1}^\dagger$, $a_{x0}^\dagger$ и $a_{x1}^\dagger$ в (2)–(4) могут быть, например, операторами рождения фотона соответственно с горизонтальной, вертикальной, диагональной и антидиагональной поляризациями: $a_{\mathrm{H}}^\dagger$, $a_{\mathrm{V}}^\dagger$, $a_{\mathrm{D}}^\dagger$ и $a_{\mathrm{A}}^\dagger$ соответственно. Отправляемые состояния тогда можно представить в виде

$$\begin{aligned}
|\alpha,0\rangle_z &= |\alpha\rangle_{z0}|0\rangle_{z1} \equiv |\alpha\rangle_{\mathrm{H}}|0\rangle_{\mathrm{V}}\,,\\
|\alpha,1\rangle_z &= |0\rangle_{z0}|\alpha\rangle_{z1} \equiv |0\rangle_{\mathrm{H}}|\alpha\rangle_{\mathrm{V}}\,,\\
|\alpha,0\rangle_x &= |\alpha\rangle_{x0}|0\rangle_{x1} \equiv |\alpha\rangle_{\mathrm{D}}|0\rangle_{\mathrm{A}} = \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{H}}\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{V}}\,,\\
|\alpha,1\rangle_x &= |0\rangle_{x0}|\alpha\rangle_{x1} \equiv |0\rangle_{\mathrm{D}}|\alpha\rangle_{\mathrm{A}} = \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{H}}\left|-\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{V}}\,,
\end{aligned} \tag{46}$$

где $|\alpha\rangle = \exp(-\mu/2)\sum_{j=1}^{\infty}(\alpha^j/\sqrt{j!})|j\rangle$ и $|j\rangle$, $j = 0,1,\ldots$ — когерентное состояние и состояние с определённым числом фотонов в соответствующей моде, $\alpha \in \mathbb{C}$, $\mu = |\alpha|^2$.

Однако при фазовом кодировании используются состояния вида [18, 40]

$$\left|(-1)^u\,\frac{\exp(\mathrm{i}\varphi_b)\alpha}{\sqrt{2}}\right\rangle_1\left|\frac{\alpha}{\sqrt{2}}\right\rangle_2, \tag{47}$$

где $u \in \{0,1\}$ — кодируемый бит, $b \in \{z,x\}$ — базис, $\varphi_z = 0$, $\varphi_x = \pi/2$, моды 1 и 2 — два временны́х окна. То есть каждый сигнал состоит из двух импульсов с согласованными фазами. Фаза в каждой паре импульсов выбирается случайным образом, т.е. противник и получатель "видят" состояние вида

$$\frac{1}{2\pi}\int_0^{2\pi}\mathrm{d}\theta\left(\left|(-1)^u\exp\left[\mathrm{i}(\varphi_b+\theta)\right]\sqrt{\frac{\mu}{2}}\right\rangle_1\left|\exp(\mathrm{i}\theta)\sqrt{\frac{\mu}{2}}\right\rangle_2\right)\times$$
$$\times\left(\left\langle\exp(\mathrm{i}\theta)\sqrt{\frac{\mu}{2}}\right|_2\left\langle(-1)^u\exp\left[\mathrm{i}(\varphi_b+\theta)\right]\sqrt{\frac{\mu}{2}}\right|_1\right). \tag{48}$$

Интерференционная схема на стороне получателя устроена так, что важна только разность фаз в двух окнах.

Покажем, как состояния поляризационного кодирования также могут быть эквивалентно представлены в виде (47). Рассмотрим операторы рождения фотонов с правой и левой круговой поляризациями:

$$\begin{aligned}
a_{\mathrm{R}}^\dagger &= \frac{a_{\mathrm{H}}^\dagger - \mathrm{i}a_{\mathrm{V}}^\dagger}{\sqrt{2}}\,,\\
a_{\mathrm{L}}^\dagger &= \frac{a_{\mathrm{H}}^\dagger + \mathrm{i}a_{\mathrm{V}}^\dagger}{\sqrt{2}}\,.
\end{aligned} \tag{49}$$

Тогда состояния (46) можно записать в виде

$$\begin{aligned}
|\alpha,0\rangle_z &= \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{R}}\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{L}}\,,\\
|\alpha,1\rangle_z &= \left|\frac{\mathrm{i}\alpha}{\sqrt{2}}\right\rangle_{\mathrm{R}}\left|-\frac{\mathrm{i}\alpha}{\sqrt{2}}\right\rangle_{\mathrm{L}}\,,\\
|\alpha,0\rangle_x &= \left|\frac{(1+\mathrm{i})\alpha}{2}\right\rangle_{\mathrm{R}}\left|\frac{(1-\mathrm{i})\alpha}{2}\right\rangle_{\mathrm{L}}\,,\\
|\alpha,1\rangle_x &= \left|\frac{(1-\mathrm{i})\alpha}{2}\right\rangle_{\mathrm{R}}\left|\frac{(1+\mathrm{i})\alpha}{2}\right\rangle_{\mathrm{L}}\,.
\end{aligned} \tag{50}$$

Первое состояние совпадает с состоянием (47) при $u = 0$, $b = z$, второе состояние совпадает с соответствующим состоянием (47) при сдвиге обеих фаз на $\pi/2$ (т.е. замены $\alpha \to \exp(\mathrm{i}\pi/2)\alpha$), третье — при сдвиге фаз на $\pi/4$ и, наконец, четвёртое — при сдвиге фаз на $-\pi/4$. Ввиду фазовой рандомизации (6) и (48) эти сдвиги фаз не имеют значения. Выполнив обратные сдвиги фаз в (47) и применив преобразование, обратное (49) (с другим наименованием мод, поскольку они теперь не соответствуют поляризациям), мы получим состояния (6).

Таким образом, поляризационное и фазовое кодирования математически полностью эквивалентны: они представляют собой различные разложения по модам одних и тех же состояний. Именно поэтому можно заключить, что теорема (см. раздел 5) и оценки (27) и (28) не зависят от выбранного способа кодирования: к состояниям вида (6) могут быть приведены состояния как поляризационного, так и фазового кодирования.

Это подтверждают и результаты работы [40], в которой для случая фазового кодирования получены те же самые оценки по методу обманных состояний, что и для поляризационного кодирования. Но следует отметить, что эквивалентность имеет место тогда, когда *суммарная* интенсивность импульсов в двух окнах в (47) совпадает с интенсивностью сигнала при поляризационном кодировании (46), $\mu = |\alpha|^2$. Интенсивность импульса в каждом окне должна быть, соответственно, в два раза меньше. С учётом этого замечания оценки, выведенные в работе [40], полностью совпадают с хорошо известными оценками, выведенными в работе [29].

Важно, что преобразование (49) сохраняет количество фотонов:

$$a_{\mathrm{H}}^{\dagger}a_{\mathrm{H}} + a_{\mathrm{V}}^{\dagger}a_{\mathrm{V}} = a_{\mathrm{D}}^{\dagger}a_{\mathrm{D}} + a_{\mathrm{A}}^{\dagger}a_{\mathrm{A}} = a_{\mathrm{R}}^{\dagger}a_{\mathrm{R}} + a_{\mathrm{L}}^{\dagger}a_{\mathrm{L}}\,.$$

Это означает, что оценки, связанные с числом однофотонных импульсов или ошибок в них, полученные для одного разложения состояния по модам, верны и для другого.

Пользуясь описанными преобразованиями, можно, например, атаку расщеплением по числу фотонов, сформулированную для поляризационного кодирования, переформулировать для фазового кодирования. Конечно, математическая эквивалентность двух способов кодирования не означает одинаковую технологическую сложность осуществления атаки расщеплением по числу фотонов в том и другом случае. Однако при расчёте длины ключа мы не интересуемся технологической сложностью тех или иных операций противника, поскольку предполагаем, что противник может осуществлять любые преобразования, разрешённые математическим аппаратом.

11. Заключение

Выше мы рассказали о методе обманных состояний в квантовой криптографии, попытавшись уделить особое внимание вопросам, обычно не разъясняемым в научной литературе. Первый из них — формальное доказательство того, что стойкость протокола с источником когерентных состояний и рандомизированной фазой сводится к стойкости соответствующего протокола с однофотонным источником. Это строго обосновывает стойкость протокола с обманными состояниями ко всевозможным атакам, а не только к атаке расщеплением по числу фотонов.

Упор на атаку расщеплением по числу фотонов в литературе связан с тем, что такая атака оптимальна. Однако доказательство стойкости метода обманных состояний не опирается на этот факт. В частности, мы сравнили атаку расщеплением по числу фотонов с атакой светоделителем, аналитически и численно показали меньшую эффективность последней.

Другой вопрос, затронутый в статье, — это эквивалентность поляризационного и фазового кодирования с точки зрения стойкости квантовой криптографии с обманными состояниями. Несмотря на то что технологически два указанных способа кодирования информации и, значит, атаки на соответствующие реализации существенно различаются, математически они полностью эквивалентны. При анализе стойкости мы предполагаем, что противник может осуществлять любые преобразования, разрешённые математическим аппаратом, поэтому аргумент о математической эквивалентности достаточен для обоснования равной теоретической стойкости протоколов, использующих эти два вида кодирования.

Таким образом, во многочисленных теоретических работах, посвящённых протоколу BB84 с обманными состояниями, а также в экспериментальных реализациях этого протокола, включая реализацию, описанную в работе [35], оценка длины секретного ключа является оправданной и строго доказанной.

Также отметим, что в работе [33] приводится один из методов вычисления оценок по методу обманных состояний с учётом статистических флуктуаций, а в работе [20] — обобщение формул оценок по методу обманных состояний для случая, когда эффективности двух детекторов различны.

Благодарности. Исследование в разделах 3–6 (основной результат — теорема в разделе 5) выполнено в рамках государственного задания Математического института им. В.А. Стеклова РАН. Исследование в разделах 7–9 (основные результаты — неравенство (38)) и 10 (доказательство эквивалентности поляризационного и фазового кодирований и график на рисунке в разделе 7) выполнено за счёт гранта Российского научного фонда (проект № 17-71-20146).

Список литературы

1. Алферов А П и др. *Основы криптографии* 2-е изд. (М.: Гелиос АРВ, 2002)
2. Schneier B *Applied Cryptography*: *Protocols, Algorithms, and Source Code in C* 2nd ed. (New York: Wiley, 1996)
3. Shor P W *SIAM J. Comput.* **26** 1484 (1997)
4. Anschuetz E et al., in *Quantum Technology and Optimization Problems. QTOP 2019* (Lecture Notes in Computer Science, Vol. 11413, Eds S Feld, C Linnhoff-Popien) (Cham: Springer, 2019) p. 74
5. Mosca M *IEEE Secur. Priv.* **16** (5) 38 (2018)
6. Bennet C H, Brassard G, in *Proc. of the IEEE Intern. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (New York: IEEE, 1984) p. 175
7. Ekert A K *Phys. Rev. Lett.* **67** 661 (1991)
8. Холево А С *Математические основы квантовой информатики* (Лекционные курсы НОЦ, Вып. 30) (М.: МИАН, 2018) с. 3
9. Wiesner S *ACM SIGACT News* **15** (1) 78 (1983)
10. Mayers D, in *Advances in Cryptology — CRYPTO 96. CRYPTO 1996* (Lecture Notes in Computer Science, Vol. 1109, Ed. N Koblitz) (Berlin: Springer, 1996) p. 343; quant-ph/9606003
11. Mayers D *J. ACM* **48** 351 (2001)
12. Shor P W, Preskill J *Phys. Rev. Lett.* **85** 441 (2000)
13. Koashi M *New J. Phys.* **11** 045018 (2009)
14. Renner R "Security of quantum key distribution", Ph.D. Thesis (Zürich: ETH, 2005); quant-ph/0512258
15. Tomamichel M et al. *Nat. Commun.* **3** 634 (2012)
16. Tomamichel M, Leverrier A *Quantum* **1** 14 (2017)
17. Dupuis F, Fawzi O, Renner R *Commun. Math. Phys.* **379** 867 (2020)
18. Gisin N et al. *Rev. Mod. Phys.* **74** 145 (2002)
19. Scarani V et al. *Rev. Mod. Phys.* **81** 1301 (2009)
20. Bochkov M K, Trushechkin A S *Phys. Rev. A* **99** 032308 (2019)
21. Portmann C, Renner R, arXiv:1409.3525
22. Трушечкин А С *Квантовая электроника* **50** 426 (2020); Trushechkin A S *Quantum Electron.* **50** 426 (2020)
23. Diamanti E et al. *npj Quantum Inf.* **2** 16025 (2016)
24. Huttner B et al. *Phys. Rev. A* **51** 1863 (1995)
25. Brassard G et al. *Phys. Rev. Lett.* **85** 1330 (2000)
26. Hwang W-Y *Phys. Rev. Lett.* **91** 057901 (2003)
27. Lo H-K, Ma X, Chen K *Phys. Rev. Lett.* **94** 230504 (2005)
28. Wang X-B *Phys. Rev. Lett.* **94** 230503 (2005)
29. Ma X et al. *Phys. Rev. A* **72** 012326 (2005)
30. Curty M et al. *Nat. Commun.* **5** 3732 (2014)
31. Lim C C W et al. *Phys. Rev. A* **89** 022307 (2014)
32. Zhang Z et al. *Phys. Rev. A* **95** 012333 (2017)
33. Trushechkin A S, Kiktenko E O, Fedorov A K *Phys. Rev. A* **96** 022316 (2017)
34. Lo H-K, Curty M, Tamaki K *Nat. Photon.* **8** 595 (2014)
35. Duplinskiy A V et al. *J. Russ. Laser Res.* **39** 113 (2018)
36. Chen K, Ma J, Shi H, Talk, ISO/IEC JTC1 SC27 WG3 SP Proposal, Security Requirements, Test and Evaluation Methods for the Decoy State BB84 Quantum Key Distribution (QKD), Berlin, Germany, 10/31/2017; ISO/IEC JTC 1/SC 27/WG 3 N 1537, 30th ISO/IEC JTC1/SC27 Working Group Meeting, H Shi, J Ma, G Pradel

Wuhan, China, April 2018 30th Security Requirements, Test and Evaluation Methods for Quantum Key Distribution
37. Молотков С Н, Кравцов К С, Рыжкин М И *ЖЭТФ* **155** 636 (2019); Molotkov S N, Kravtsov K S, Ryzhkin M I *J. Exp. Theor. Phys.* **128** 544 (2019)
38. Молотков С Н, Кравцов К С, Рыжкин М И *ЖЭТФ* **156** 379 (2019); Molotkov S N, Kravtsov K S, Ryzhkin M I *J. Exp. Theor. Phys.* **129** 319 (2019)
39. Devetak I, Winter A *Proc. R. Soc. Lond. A* **461** 207 (2005)
40. Kulik S P, Molotkov S N *Laser Phys. Lett.* **14** 125205 (2017)
41. Килин С Я *УФН* **169** 507 (1999); Kilin S Ya *Phys. Usp.* **42** 435 (1999)
42. Валиев К А *УФН* **175** 3 (2005); Valiev K A *Phys. Usp.* **48** 1 (2005)
43. Молотков С Н *УФН* **176** 777 (2006); Molotkov S N *Phys. Usp.* **49** 750 (2006)
44. Lo H-K, Chau H F, Ardehali M *J. Cryptology* **18** 133 (2005)
45. Trushechkin A S et al. *Phys. Rev. A* **97** 012311 (2018)
46. Fung C-H F, Ma X, Chau H F *Phys. Rev. A* **81** 012318 (2010)
47. Kiktenko E, Trushechkin A, Kurochkin Yu, Fedorov A *J. Phys. Conf. Ser.* **741** 012081 (2016)
48. Fedorov A K, Kiktenko E O, Trushechkin A S *Lobachevskii J. Math.* **39** 992 (2018)
49. Kiktenko E O et al. *Phys. Rev. Appl.* **8** 044017 (2017)
50. Kronberg D A *Матем. вопр. криптогр.* **8** (2) 77 (2017)
51. Wegman M N, Carter J L *J. Comput. Syst. Sci.* **22** 265 (1981)
52. Kiktenko E O et al. *IEEE Trans. Inform. Theory* **66** 6354 (2020)
53. Lieb E H *Adv. Math.* **11** 267 (1973)
54. Холево А С *Квантовые системы, каналы, информация* (М.: Изд-во МЦНМО, 2010); Пер. на англ. яз.: Holevo A S *Quantum Systems, Channels, Information*: a Mathematical Introduction (Berlin: De Gruyter, 2012)
55. Cao Z et al. *New J. Phys.* **17** 053014 (2015)
56. Lim C C W et al. *Phys. Rev. A* **89** 022307 (2014)
57. Bennett C H et al. *J. Cryptology* **5** 3 (1992)
58. Dušek M, Jahma M, Lütkenhaus N *Phys. Rev. A* **62** 022306 (2000)
59. Félix S et al. *J. Mod. Opt.* **48** 2009 (2001)
60. Кронберг Д А, Курочкин Ю В *Квантовая электроника* **48** 843 (2018); Kronberg D A, Kurochkin Yu V *Quantum Electron.* **48** 843 (2018)
61. Кронберг Д А, Киктенко Е О, Федоров А К, Курочкин Ю В *Квантовая электроника* **47** 163 (2017); Kronberg D A, Kiktenko E O, Fedorov A K, Kurochkin Yu V *Quantum Electron.* **47** 163 (2017)
62. Avanesov A S, Kronberg D A, Pechen A N *P-Adic Num. Ultrametr. Anal. Appl.* **10** 222 (2018)
63. Kronberg D A, Nikolaeva A S, Kurochkin Y V, Fedorov A K *Phys. Rev. A* **101** 032334 (2020)

Security of the decoy state method for quantum key distribution

A.S. Trushechkin [(1,2,†)], **E.O. Kiktenko** [(1,2,3,4)], **D.A. Kronberg** [(1,3,4)], **A.K. Fedorov** [(3,4,‡)]
[(1)] *Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russian Federation*
[(2)] *National University of Science and Technology MISIS, Competence Center of the Quantum Communications National Technology Initiative, Leninskii prosp. 4, 119049 Moscow, Russian Federation*
[(3)] *International Center for Quantum Optics and Quantum Technologies* (*Russian Quantum Center*), *ul. Novaya 100, 143025 Skolkovo, Moscow region, Russian Federation*
[(4)] *Moscow Institute of Physics and Technology* (*National Research University*), *Institutskii per. 9, 141701 Dolgoprudny, Moscow region, Russian Federation*
E-mail: [(†)] *trushechkin@mi-ras.ru*, [(‡)] *akf@rqc.ru*

Quantum cryptography or, more precisely, quantum key distribution (QKD), is one of the advanced areas in the field of quantum technologies. The confidentiality of keys distributed with the use of QKD protocols is guaranteed by the fundamental laws of quantum mechanics. This paper is devoted to the decoy state method, a countermeasure against vulnerabilities caused by the use of coherent states of light for QKD protocols whose security is proved under the assumption of single-photon states. We give a formal security proof of the decoy state method against all possible attacks. We compare two widely known attacks on multiphoton pulses: photon-number splitting and beam splitting. Finally, we discuss the equivalence of polarization and phase coding.

Keywords: quantum cryptography, quantum key distribution, BB84, decoy states

PACS numbers: **03.67.–a**, 03.67.Dd, 03.67.Hk

Bibliography — 63 references

Received 23 March 2020, revised 19 October 2020

Uspekhi Fizicheskikh Nauk **191** (1) 93–109 (2021)

Physics–Uspekhi **64** (1) (2021)

DOI: https://doi.org/10.3367/UFNr.2020.11.038882

DOI: https://doi.org/10.3367/UFNe.2020.11.038882