ТЕОРЕТИЧЕСКАЯ И МАТЕМАТИЧЕСКАЯ ФИЗИКА

Защищённые квантовые каналы на основе многофотонной запутанности

А.В. Белинский,[1,*] А.П. Григорьева,[1] И.И. Джадан[1]

[1] *Московский государственный университет имени М. В. Ломоносова, физический факультет, кафедра математического моделирования и информатики*
Россия, 119991, Москва, Ленинские горы, д. 1, стр. 2

(Поступила в редакцию 09.12.2024; подписана в печать 14.01.2024)

Рассмотрены возможности передачи информации квантовыми каналами с многофотонной запутанностью.Составлены протоколы квантового распределения ключей и прямой передачи информации со строгим учётом времени отправки и получения сообщений, что помогает противодействовать широкому спектру атак.

PACS: 03.67.Dd УДК: 53.08

Ключевые слова: многофотонная запутанность, квантовые коммуникации, квантовое распределение ключей, квантовая криптография, квантовый хакинг, квантовая телепортация.

DOI: 10.55959/MSU0579-9392.80.2530102

ВВЕДЕНИЕ

Повышение защищённости каналов передачи информации предотвращает уязвимость к различным атакам [1–3]. Часто оказывается, что одного метода, даже такого надёжного, как физическая «неуязвимость» [4], недостаточно [5, 6]. В практически используемых системах применяются сразу нескольких методов [7], основанных на различных принципах, для надёжной защиты информации [8–11]. Так, в работе [12] показано, что даже весьма защищённые квантовые каналы квантовой телепортации могут иметь утечки информации при доступе к ним посторонних лиц, несмотря на запрет клонирования [13–15]. В других работах отмечается уязвимость ряда протоколов перед атаками перехвата-повторной отправки (intercept-resend), атакой со светоделителем (photon-number-splitting) и атакой посредника (man-in-the-middle) [16, 17]. Список возможных атак на квантовые каналы всё время растёт и в настоящее время включает широкий спектр вмешательств, таких как атака типа «квантовый троян», когерентные и некогерентные атаки, атака с ослеплением лавинных фотодетекторов, спектральная атака и атака на псевдослучайные числа [18]. Поэтому интересно проанализировать, предоставляет ли какие-либо дополнительные возможности защиты квантовый канал, организованный на основе многофотонных запутанных состояний [19, 20]. Такие каналы пока широко не используются и важно оценить их перспективы.

Принципы работы защищённого квантового канала на основе многофотонных запутанных состояний весьма схожи с принципами многофотонной квантовой телепортации [21]. Разница в том, что транслируемые квантовые состояния являются шаблонами и им приписываются двоичные значения. В связи с этим возникает ещё один вопрос: насколько оправданным может быть использование в линиях связи на основе многофотонной запутанности дополнительного классического канала, по которому, как и в случае квантовой телепортации, будет передаваться дополнительная информация?

1. ПРИГОТОВЛЕНИЕ МНОГОФОТОННЫХ ЗАПУТАННЫХ СОСТОЯНИЙ

В качестве источника многофотонной запутанности можно использовать модернизированную схему телепортационного эксперимента [21]. Она представлена на рисунке. Задействованы две запутанные по поляризации пары фотонов: один фотон пары 1–2 подаётся на один вход светоделителя, пары 3–4 — на другой. Их состояния синглетные, и это означает, что вид запутанности не зависит от выбора базиса отсчёта:

$$\begin{aligned} |\psi_{12}\rangle &= \frac{1}{\sqrt{2}}\left(|x_1 y_2\rangle - |y_1 x_2\rangle\right), \\ |\psi_{34}\rangle &= \frac{1}{\sqrt{2}}\left(|x_3 y_4\rangle - |y_3 x_4\rangle\right), \end{aligned} \tag{1}$$

где x_i и y_j обозначают горизонтальную и вертикальную поляризации соответствующих фотонов.

Искомое состояние получим путём постселекции, т.е. учёта только случаев одновременной регистрации всех четырёх фотонов в отдельности. Факторизованное состояние$|\Psi\rangle_{1234} = |\psi\rangle_{12} \otimes |\psi\rangle_{34}$ до светоделителя становится запутанным:

* E-mail: belinsky@inbox.ru

$$|\Psi'_{1234}\rangle = \frac{1}{2\sqrt{2}}\Big[(|y_1x_2^2x_3^2y_4\rangle + |y_1x_2^3x_3^3y_4\rangle) + (|x_1y_2^2y_3^2x_4\rangle + |x_1y_2^3y_3^3x_4\rangle) + \\ + \frac{1}{\sqrt{2}}(|y_1x_2^2y_3^2x_4\rangle + |y_1x_2^3y_3^3x_4\rangle) + \frac{1}{\sqrt{2}}(|y_1x_2^2y_3^3x_4\rangle - |y_1x_2^3y_3^2x_4\rangle) + \\ + \frac{1}{\sqrt{2}}(|x_1y_2^2x_3^2y_4\rangle + |x_1y_2^3x_3^3y_4\rangle) + \frac{1}{\sqrt{2}}(|x_1y_2^2x_3^3y_4\rangle - |x_1y_2^3x_3^2y_4\rangle)\Big]. \quad (2)$$

Здесь нижние индексы обозначают нумерацию каналов до светоделителя, а верхние — после.

В результате отсева компонент, связанных с уходом двух фотонов в одну моду, получим постселекционное состояние:

$$|\Psi''_{1234}\rangle = \frac{1}{2}\left(|y_1x^2y^3x_4\rangle + |x_1y^2x^3y_4\rangle - |x_1x^2y^3y_4\rangle - |y_1y^2x^3x_4\rangle\right). \quad (3)$$

В нашем случае постселекция означает отбор вариантов когда одновременно срабатывают все 4 детектора, то есть состояния с фотонами ϕ_2 и ϕ_3, имеющими одинаковую поляризацию и поэтому идущими в один канал, не рассматриваются в силу эффекта подавления взаимной корреляции [22]. Счётчик совпадений, устанавливаемый на приёмнике сигнала у Боба, отсечёт компоненты с y_2y_3 и x_2x_3. Таким образом, хотя поступающее на светоделитель состояние факторизовано, информативное состояние будет уже запутанным. И хотя эта запутанность не является максимальной в смысле ГХЦ [23], но и она может быть полезна.

Кодирование состояния $|\Psi''_{1234}\rangle$ производится устройствами PR, которые вращают плоскость поляризации. Ими могут быть вращатели Фарадея либо ячейки Поккельса.

2. ПРИНЦИПЫ КОДИРОВКИ

Поскольку в случае квантовой запутанности информация о системе содержится в виде условных значений измеряемых параметров, кодировка может быть осуществлена лишь на основании результатов двух измерений в разных каналах. Абсолютные значения поляризации остаются случайными и не могут нести какую-либо информацию. Такая особенность является и защитой от несанкционированного доступа: перехват одного канала даст лишь сплошной шум.

Установим следующую кодировку:

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{2}\left(|y_1x_2y_3x_4\rangle + |x_1y_2x_3y_4\rangle + |x_1x_2y_3y_4\rangle + |y_1y_2x_3x_4\rangle\right) \equiv 00,\\
|\psi_2\rangle &= \frac{1}{2}\left(|y_1x_2y_3y_4\rangle + |x_1y_2x_3x_4\rangle + |x_1x_2y_3x_4\rangle + |y_1y_2x_3y_4\rangle\right) \equiv 01,\\
|\psi_3\rangle &= \frac{1}{2}\left(|y_1y_2y_3y_4\rangle + |x_1x_2x_3x_4\rangle + |x_1y_2y_3x_4\rangle + |y_1x_2x_3y_4\rangle\right) \equiv 10,\\
|\psi_4\rangle &= \frac{1}{2}\left(|y_1y_2y_3x_4\rangle + |x_1x_2x_3y_4\rangle + |x_1y_2y_3y_4\rangle + |y_1x_2x_3x_4\rangle\right) \equiv 11.
\end{aligned} \quad (4)$$

Каждое последующее состояние получается из исходного ψ_1 вращением плоскости поляризации. Таким образом, для полученной 4-фотонной запутанности можно закодировать 2 бита информации, столько же, как и для двух пар в 2-фотонном канале. Для сравнения: при использовании 2-фотонной запутанности с аналогичным управлением вариантов состояний будет 2, и каждая отправка будет содержать 1 бит информации:

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}\left(|x_1y_2\rangle - |y_1x_2\rangle\right) \equiv 0,\\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}\left(|x_1x_2\rangle - |y_1y_2\rangle\right) \equiv 1.
\end{aligned} \quad (5)$$

В отличие от 2-фотонной запутанности [24] в 4-фотонном случае несанкционированный перехват даже двух каналов не позволяет прочесть сообщение, поскольку любая комбинация поляризаций двух фотонов может входить в разное сообщение в зависимости от результатов измерения оставшихся двух фотонов. Это существенно повышает конфиденциальность связи.

3. ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Чтобы Боб мог прочитать зашифрованное сообщение, Алисе нужно передать ему секретный ключ. Описанная схема позволяет делать это без всякой предварительной подготовки. Если ключ представляет собой сообщение длиной $2n$ бит, для его передачи Алисе необходимо отправить Бобу $2n$-битовых сообщений с общим числом $4n$ фотонов. При этом успех попытки S_i никак статистически не связан с успехом любой другой попытки S_j, то есть успешные события S_i и S_j не исключают друг друга, и для вероятно-

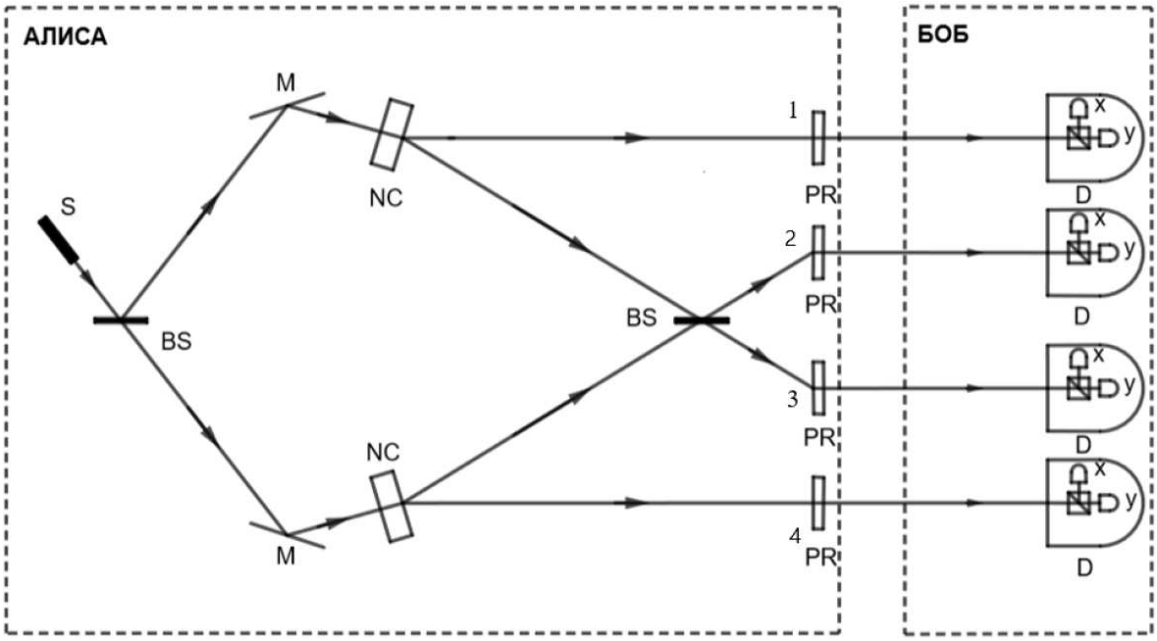

Рис. 1. Схема квантовой линии связи. Импульсный лазер Алисы (S) накачивает два идентичных нелинейных кристалла (NC), в которых рождаются запутанные по поляризации фотонные пары. Смешение происходит на светоделителе (BS). Кодировка сигнала осуществляется поляризационными фазовращателями (PR). Боб регистрирует четыре фотона четырьмя приемными устройствами (D) с измерением горизонтальной (x) и вертикальной (y) поляризации. M — зеркала

сти суммы этих событий верна формула Лагранжа: $P(S_i + S_j) = P(S_i) + P(S_j) - P(S_i, S_j)$, где $P(S_i, S_j)$ — вероятность совместного успеха двух разных попыток отправки. Учитывая статистическую независимость детектирования, верно также $P(S_i, S_j) = P(S_i)\,P(S_j)$.

Для большого числа однородных попыток отправки удобно переписать формулу сложения вероятностей с использованием отрицаний: $P(S_i + S_j) = 1 - P\left(\overline{S_i}, \overline{S_j}\right)$, где $P\left(\overline{S_i}, \overline{S_j}\right)$ — вероятность совместного неуспеха двух попыток отправки. Учитывая статистическую независимость отправок и их однородность, для k попыток отправки ключа из $2n$-битовых сообщений имеем вероятность успеха хотя бы одной попытки:

$$P\left(\sum_{i=1}^{k} S_i\right) = 1 - P^k\left(\overline{S}\right). \qquad (6)$$

$P(\overline{S})$ — вероятность неуспеха одной попытки отправки ключа.

Совокупная квантовая эффективность детекторов $0 < \eta < 1$ при детектировании необходимых для передачи шифроключа $2n$-битовых сообщений равна вероятности совместной регистрации $4n$ фотонов. Тогда $P\left(\overline{S}\right) = 1 - \eta$ — вероятность потери $4n$-фотонного сообщения в одной попытке, а $P^k\left(\overline{S}\right) = (1-\eta)^k$ — вероятность потери такого сообщения в k попытках. При этом вероятность передачи сообщения после k попыток равна $P^k(S) = 1 - P^k\left(\overline{S}\right)$. Таким образом, при росте числа k попыток S_i вероятность передать $4n$-фотонное сообщение равна $P^k(S) = 1 - (1-\eta)^k$.

Боб делает вывод, что шифроключ успешно передан, на основании того, что все 4 датчика фотонов одновременно сработали n раз подряд в течение короткого, заранее оговорённого промежутка времени Δt. Это означает, что потерь при передаче фотонов не было. После успешной передачи ключа Боб посылает Алисе открытое сообщение с указанием времени t_r прихода шифроключа. На основании знания t_r и при условии синхронизации часов Алисы и Боба, Алиса вычисляет время t_s отправки шифроключа и понимает, какой именно ключ успешно передан. Его будет использовать Боб в дальнейшем. Соответственно она шифрует своё классическое сообщение так, чтобы оно могло бы быть прочтено с использованием переданного ключа, и отправляет Бобу. Для своего ответа Алисе Боб повторяет все операции Алисы симметрично.

Пошаговое описание протокола передачи ключа от Алисы к Бобу следующее.

Протокол 1.

Шаг 1. Алиса готовит $2n$-битовый шифроключ, кодирует его соответственно таблице кодировки запутанных состояний и отправляет Бобу в виде $4n$-фотонных состояний, отмечая у себя время окончания отправки t_s.

Шаг 2. Боб, получив сообщение, отправляет по открытому классическому каналу Алисе время t_r его получения.

Шаг 3. Не получив ответ Боба в течение некоторого обусловленного времени, Алиса готовит другой шифроключ и делает следующую попытку отсылки. Попытки повторяются до тех пор, пока Али-

са не получит ответ Боба со временем t_r прихода сообщения.

Шаг 4. Сравнив время отправки сообщения и время прихода его Бобу и зная расстояние между излучателем и детектором, Алиса узнаёт, какой именно из отправленных ключей успешно получен Бобом, и этот ключ использует для шифрования классической информации.

Важно подчеркнуть, что, в отличие от ряда других протоколов квантового распределения ключей, например протокола $BB84$ [1], сообщение невозможно тайно перехватить путём установки фотоделителя, поскольку каждый вариант шифроключа передаётся лишь в одной попытке и, будучи перехваченным, в дальнейшем уже не используется. То есть даже в случае успешного перехвата злоумышленник (Ева) не сможет использовать его результат, поскольку сам факт перехвата делает перехваченную информацию нерелевантной. Такая особенность придаёт каналу устойчивость к атакам типа «перехват–пересылка» и «атака посредника». Всякая попытка подмены фотона со стороны Евы будет наталкиваться на необходимость точного соблюдения времени отправки оригинального фотона Алисой. Но на всякую подмену уйдёт время. Боб, получив партию из $4n$ фальшивых фотонов, ничего не заподозрит, но после отправки Алисе по классическому каналу значения времени t_r их прибытия последняя, рассчитав их фактическую задержку $t_r - t_s$ и увидев несоответствие с расчётной, поймёт, что канал перехвачен злоумышленником. Таким образом, точный контроль времени, являющийся главным средством против «атак посредника» [25], встроен в описанный протокол.

Основной недостаток протокола состоит в том, что он требует достаточно высокой квантовой эффективности η_0. Так, для передачи $2n$-битного шифроключа одним сообщением потребуется $4n$ фотонов порциями по 4 фотона, которые должны быть зарегистрированы приёмником без потерь. При этом вероятность успешной передачи $4n$-битного ключа с k-й попытки будет равна $P^k(S) = 1 - \left(1 - \eta_0^{4n}\right)^k$. Таким образом, эффективность канала существенно зависит от квантовой эффективности детекторов. Нетрудно посчитать, что для надёжной передачи по каналу 32-битового ключа понадобится около 10^{15} попыток при $\eta_0 = 0.6$, однако менее 10000 при $\eta_0 = 0.9$. Поскольку в настоящее время в шифровании нередко применяются ключи длиной 128–256 бит, а квантовая эффективность примерно 0.5, при отправке ключа одним сообщением потребуется слишком много попыток.

Однако данный протокол допускает возможность экспоненциально уменьшить необходимое для отправки число попыток, отправляя ключ по частям. В этом случае, к примеру, 256-битовый ключ может быть разбит максимально на 128 2-битовых фрагментов, каждый из которых отправляется последовательно. После каждой такой успешной отправки Боб посылает Алисе сообщение, в котором отмечает время t_r^m получения m-го фрагмента ключа, чтобы она могла по нему вычислить соответствующее время отправки t_s^m и после получения Бобом всех фрагментов понять, какие именно фрагменты ключа получил Боб. Соединяя последовательно фрагменты, Боб получает собственно секретный ключ. В этом случае также соблюдается принцип отсутствия потерь релевантной информации: на два зарегистрированных фотона всегда приходится один переданный бит. При $\eta_0 = 0.5$ вероятности $P^k(S)$ отправки 2-битового фрагмента ключа за k попыток будут:

$$P^1(S) = 1 - \left(1 - \eta_0^4\right) = 0.06,$$
$$P^{11}(S) = 1 - \left(1 - \eta_0^4\right)^{11} = 0.51,$$
$$P^{50}(S) = 1 - \left(1 - \eta_0^4\right)^{50} = 0.96.$$

Таким образом, современный уровень технологии детектирования фотонов вполне достаточен для реализации протокола на практике.

4. ПРОТОКОЛ ПЕРЕДАЧИ СООБЩЕНИЙ

Аналогичным образом запутанные состояния для двух или более пар запутанных фотонов можно использовать также для передачи защищённых сообщений. При использовании более двух каналов передачи фотонов прочтение сообщения даже с перехватом всех каналов невозможно без знания нумерации каналов. Таким образом, каналы на основе многофотонной запутанности предоставляет дополнительную возможность шифрования. Она может быть полезна в том случае, когда нельзя исключить утечку уже переданной информации. В этом случае физической защиты от перехвата, которая обеспечивается квантовым каналом, недостаточно. При наличии дополнительного шифроключа только персона, обладающая доступом к нему, сможет расшифровать уже полученное по квантовым каналам сообщение. Шифроключи могут передаваться по дополнительному классическому каналу. Это классическое сообщение можно также использовать и для контроля отправки квантового. Однако наиболее защищённым способом является квантовое распределение ключей, согласно протоколу 1. Такая возможность отсутствует в двухфотонном случае: для этого просто не хватает степеней свободы. Контроль статистики отправки и получения необходим, так как детекторы и каналы работают не идеально, и какая-то часть фотонов теряется. Отличить украденные фотоны от потерянных можно, сравнивая ожидаемую статистику с фактической. Заметное отклонение от ожидаемой статистики между числом классических и квантовых сообщений означает, что квантовое сообщение могло быть перехвачено и канал взломан.

В работе [12] показано, что телепортация в классической её форме [21] не даёт абсолютную физическую защиту от похищения квантового состояния.

Рождаются запутанные клоны, процесс утилизации которых необходимо контролировать, и это не противоречит теореме о запрете клонирования [13–15]. Но в случае использования многофотонного квантового канала нет необходимости контролировать утилизацию «холостых» фотонов: все запутанные клоны задействованы. Один фотон из четырёх может быть выделен как «опорный». Он может как передаваться Бобу, так и использоваться для измерения на месте и формирования классического сообщения, а остальные — передаются Бобу. Если бы передача осуществлялась по одному каналу, злоумышленник мог бы поставить светоделитель и незаметно украсть половину фотонов, не меняя статистику, однако пуск фотонов одновременно по четырём путям значительно затрудняет такую возможность. При такой схеме все фотоны учтены, и любое отклонение от ожидаемой статистики становится заметным.

Также стоит отметить, что большинство вариантов квантовых каналов используется в качестве средства квантового распределения ключей и в принципе не могут быть использованы для передачи непосредственно информации в зашифрованном виде. Лишь некоторые протоколы, например протокол Кэка [17], годятся и для непосредственной передачи зашифрованных сообщений. К таким каналам относится и предлагаемый канал на основе многофотонной запутанности. Базовый протокол передачи зашифрованных сообщений с использованием 4-фотонной запутанности и дополнительной классической криптозащитой строится так:

Протокол 2.

Шаг 1. Перед первой передачей Алиса и Боб формируют ключи, используя вышеописанный протокол квантового распределения ключей или обмениваясь информацией через отдельный классический канал, как, например, это описано в протоколе RSA [26]. Эти ключи используются в дальнейшем для дополнительной защиты канала, и их возможный взлом без взлома собственно квантового канала не приведёт злоумышленника к успеху.

Шаг 2. Алиса готовит запутанное 4-фотонное поляризационное состояние (3) и затем, используя вентили поляризационного вращения, переводит его в одно из состояний (4) в соответствии с выбранным заранее порядком нумерации четырёх каналов и отправляет Бобу.

Шаг 3. Параллельно Бобу по квантовому каналу с использованием протокола 1 либо по классическому каналу с использованием протоколов шифрования отправляется порядок нумерации каналов. При повторной n-й передаче порядок нумерации каналов определяется относительно порядка $n-1$-й передачи. Так что взломщик может надёжно расшифровать правильный порядок n-й передачи только если знает порядок предыдущей.

Шаг 4. Боб измеряет полученное 4-фотонное поляризационное состояние и, используя полученный ключ, восстанавливает порядок каналов. Сравнивая со списком интерпретаций (4), Боб восстанавливает смысл переданного 2-битного сообщения. Параллельно Боб отсылает время t_r регистрации сообщения Алисе.

Шаг 5. Алиса ждёт от Боба подтверждения получения с временем отправки. Если она его не получает, то отправляет то же самое сообщение повторно. Действие повторяется каждый оговорённый заранее промежуток времени до тех пор, пока Боб не получит сообщение и не подтвердит отправку.

Как и в случае протокола квантового распределения ключей, в протоколе передачи шифрованных сообщений применён контроль времени получения сообщения, который сводит к минимуму возможность хакерских атак с перехватом и последующей отсылкой фальшивых копий. Отличие протокола 2 в том, что в нём невозможно реализовать однократную попытку пересылки сообщения с последующей заменой одного сообщения новым, как в протоколе распределения ключей. Это объясняется необходимостью пересылки одного заранее подготовленного текста вместо случайным образом создаваемого ключа. Таким образом, учитывая неидеальность каналов и детекторов, повторные попытки отсылки одного и того же сообщения неизбежны, что приоткрывает некоторое окно для незамеченной кражи сообщений. Однако на помощь приходит дополнительная защита: шифроключ порядка каналов можно менять сколь угодно часто. Это придаёт каналу дополнительную устойчивость. Ведь поскольку для 4-х каналов число вариантов их нумерации равно $4! = 24$, при смене ключа каждый раз вероятность P_{theft} правильно прочесть украденное сообщение длиной $2k$ бит, даже при утечке результата измерения во всех 4-х квантовых каналах, будет экспоненциально уменьшаться с ростом длины передачи и будет равна $P_{theft} = \frac{1}{24^k}$, где k — число 4-фотонных отправок (2-битовых сообщений).

5. КОНТРОЛЬ ОТПРАВКИ ТИПА «ТЕЛЕПОРТАЦИЯ»

Отправитель сообщений может оставлять один фотон из четырёх себе в качестве «опорного», чтобы измерить его поляризацию самому, а остальные три фотона отправить адресату. В этом случае результат измерения направляется по классическому каналу для расшифровки уже переданного сообщения. При этом выясняется, что переданное состояние не зависит от временной последовательности измерительных коллапсов. В работе [12] рассмотрен похожий эффект «телепортации в прошлое», где также передаваемая по классическому каналу информация фактически играла роль шифроключа для правильной интерпретации телепортированного квантового состояния. Разберём это более подробно. Допустим, автор подготовил для пересылки состояние $\psi_2 = \frac{1}{2}(|y_1x_2y_3y_4\rangle + |x_1y_2x_3x_4\rangle + |x_1x_2y_3x_4\rangle + |y_1y_2x_3y_4\rangle) \equiv 01$ При использовании фотона ϕ_1 в качестве «опорного» он измеряется локально, а остальные три фотона отправляются

адресату. Если его поляризация оказалась вертикальной y_1, а адресат получит результат $x_2y_3y_4$, то до получения классического шифроключа адресат не будет знать точного сообщения. Чтобы адресат мог правильно расшифровать полученное сообщение, ему нужно знать

1. результат измерения первого фотона,

2. шифроключ последовательности каналов.

При этом не имеет значения, измерен ли «опорный» фотон до сигнальных или после, поэтому формально сообщение может быть отправлено «в прошлое», хотя, конечно, никакого физического воздействия на прошлое здесь не оказывается, а речь идёт, как и в случае «телепортации в прошлое» [12], о квантовых корреляциях запутанных состояний, которые не зависят от времени.

Измерение поляризации одного фотона из четырёх «на месте» с последующей отправкой результата по классическому каналу способно увеличить общую квантовую эффективность регистраций. При этом оно практически не компрометирует защиту канала, так как перехват результата регистрации в одном из четырёх каналов не ведёт к раскрытию всего сообщения.

ЗАКЛЮЧЕНИЕ. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Системы передачи информации на основе многофотонных запутанных состояний имеют, как представляется, хорошие перспективы использования. Они являются надёжными средствами связи, когда необходимо обеспечить максимальную защиту канала от взлома. Предлагаемый способ, построенный на использовании многофотонных запутанных состояний, отличается от более ранних тем, что позволяет запускать как протоколы квантового распределения ключей, так и непосредственной передачи зашифрованной информации. Имеется возможность контроля времени отправки-получения сообщений и дополнительные пути криптозащиты с использованием параллельного классического канала. Все эти меры в совокупности делают предлагаемый канал устойчивым к широкому спектру хакерских атак.

Исследование выполнено в рамках государственного задания МГУ имени М.В.Ломоносова.

[1] *Bennett C.H., Brassard G.* // Theoretical Computer Science. **560** (Part 1). 7 (2014).
[2] *Gisin N., Ribordy G., Tittel W., Zbinden H.* // Rev. Mod. Phys. **74**, N 1. 145 (2002).
[3] *Ekert A.* // Phys. Rev. Lett. **67**, N 6. 661 (1991).
[4] *Lo H.-K., Chau H.F.* // Science. **283**. 2050 (1999).
[5] *Bennett C.H.* et al. // Journal of Cryptology. **5**, N 1. 3 (1992).
[6] *Pirandola S.* // Communications Physics. **2**, N 1. 51 (2019).
[7] *Zhen-Qiu Z., Xiao-Hai Z.*et al. // Phys. Rev. Lett. **126**. 010503 (2021).
[8] *Pirandola S., Andersen U.L.* et al. // Advances in Optics and Photonics. **12**, N 4. 1012 (2020).
[9] *Erhard M., Krenn M., Zeilinger A.* // Nat. Rev. Phys. **2**. 365 (2020).
[10] *Vazirani U., Vidick T.* // Phys. Rev. Lett. **113**. 140501 (2014).
[11] *Merkle R.C.* // Communications of the ACM 21 (4). 294 (1978).
[12] *Белинский А.В., Григорьева А.П., Джадан И.И.* // Вестн. Моск. ун-та. Физ. Астрон. (2023). (*Belinsky A.V., Grigorieva A.P., Dzhadan I.I.* // Moscow Univ. Phys. Bull. **78**, N 5. (2023)).
[13] *Wootters W., Zurek W.* // Nature. **299**, N 5886, 802 (1982).
[14] *Peres A., Termo D.R.* // Rev. Mod. Phys.**76**, N 1. 93 (2004).
[15] *Dieks D.* // Phys. Lett. A. **92**, N 6. 271 (1982).
[16] *Chan K.W.C., El Rifai M., Verma P.* et al. // International Journal on Cryptography and Information Security (IJCIS). **5**, N 3/4. (2015).
[17] *Kak S.* Foundations of Physics Letters. **19**, N 3. (2005).
[18] *Белера Р.А., Деев Д.Д., Смирнов И.А.* и др. // Научное обозрение. Технические науки. № 4. 7 (2020).
[19] *Wang M., Wang X., Zhan T.* // Quantum Information Processing. **17**, N 2. 31 (2018).
[20] *Wengerowsky S., Joshi F. Steinlechner S.K.* et al. // Nature **564**. 225 (2018).
[21] *Bouwmeester D., Pan J.W., Mattle K.* et al. // Nature. **390**. 575 (1997).
[22] *Hong C.K., Ou Z.Y., Mandel L.* // Phys. Rev. Lett. **59**, N 18. 2044 (1987).
[23] *Greenberger D.M., Horne M.A., Zeilinger A.* // Dordrecht: Kluwer. p. 69 (1989).
[24] *Белинский А.В.* Квантовые измерения. М.: БИНОМ. Лаборатория знаний, 2008.
[25] *Aziz B., Hamilton G.* // Third International Conference on Emerging Security Information, Systems and Technologies: journal. P. 81 (2009).
[26] *Rivest R.L., Shamir A., Adleman L.A.* // Ideas That Created the Future. pp. 463-474 (1978).

Secure Quantum Channels Based on Multiphoton Entanglement

A.V. Belinsky[a], A.P. Grigorieva[b], I.I. Dzhadan[c]

Department of Mathematical Modeling and Informatics, Faculty of Physics, Lomonosov Moscow State University Moscow 119991, Russia

E-mail: [a] belinsky@inbox.ru, [b] arisa1511@mail.ru, [c] idzhadan@yandex.ru

The possibilities of transmitting information by quantum channels with multiphoton entanglement are considered. Protocols for quantum key distribution and direct information transmission with strict consideration of the time of sending and receiving messages are compiled, which helps to counteract a wide range of attacks.

PACS: 03.67.Dd.
Keywords: multiphoton entanglement, quantum communications, quantum key distribution, quantum cryptography, quantum hacking, quantumteleportation.
Received 09 December 2024.
English version: *Moscow University Physics Bulletin*. 2025. **80**, No. . Pp. .

Сведения об авторах

1. Белинский Александр Витальевич — доктор физ.-мат. наук, вед. науч. сотрудник; тел.: (495) 939-41-78, e-mail: belinsky@inbox.ru.
2. Григорьева Алиса Павловна — студентка; тел.: (495) 939-41-78, e-mail: arisa1511@mail.ru.
3. Джадан Игорь Иванович — физик; тел.: (495) 939-41-78, e-mail: idzhadan@yandex.