07

О криптографической стойкости протокола квантового распределения ключа на основе векторных оптических вихрей

© Д.Д. Решетников, Э.Р. Зинатуллин, Е.Н. Башмакова, А.В. Баева, Е.А. Вашукевич

Санкт-Петербургский государственный университет,
Санкт-Петербург, Россия

e-mail: d.reshetnikov@spbu.ru

Поступила в редакцию 12.11.2025 г.
В окончательной редакции 12.11.2025 г.
Принята к публикации 10.12.2025 г.

Исследована криптографическая стойкость протокола квантового распределения ключей, использующего векторные оптические вихри с аксиально-симметричным пространственным профилем поляризации. Представлен теоретический анализ стойкости протокола против двух типов атак: атаки „прием-перепосыл“ и некогерентной симметричной атаки. Особое внимание уделено анализу потенциального преимущества злоумышленника (Евы) при использовании квантовых систем с пространством состояний более высокой размерности (куквартов). Проведенный анализ показал, что для данного протокола критический уровень квантовых ошибок составляет 25% для обеих рассмотренных атак. Показано, что использование Евой куквартных стратегий не снижает этот порог и не дает ей дополнительного преимущества по сравнению с атаками в кубитном пространстве.

Ключевые слова: квантовое распределение ключей, квантовая криптография, векторные оптические вихри, криптографическая стойкость.

DOI: 10.61011/OS.2026.02.62690.8777-25

1. Введение

Квантовое распределение ключей (КРК) представляет собой криптографическую технологию, которая позволяет двум легитимным пользователям (Алисе и Бобу) сгенерировать общий секретный ключ, безопасность которого гарантируется фундаментальными законами квантовой механики. В отличие от классических криптосистем, стойкость которых основывается на вычислительной сложности определенных математических задач, безопасность КРК является безусловной и не зависит от вычислительных мощностей злоумышленника (Евы) [1].

Самый первый протокол КРК BB84 [2] основан на использовании двух сопряженных базисов для кодирования классической информации с помощью квантовых состояний одиночных фотонов. Это делает невозможным однозначное различение состояний Евой в силу теоремы о запрете клонирования. Однако ключевым препятствием к широкому применению данного протокола стало отсутствие истинно однофотонных источников. Позже были созданы протоколы, адаптированные для использования ослабленных когерентных состояний вместо однофотонных. Наиболее известным является протокол SARG04 [3], который устойчив к атаке с разделением числа фотонов (PNS — атака), а также протоколы на основе decoy-state метода [4,5]. Широкое распространение получили протоколы на основе непрерывных переменных (CV-QKD), в которых информация кодируется в квадратурах когерентных состояний света, а детектирование осуществляется с помощью гомодинного измерения [6].

Теоретическое обоснование безопасности является краеугольным камнем систем и протоколов КРК. Подход к доказательству безопасности можно разделить на два основных направления. Первое направление, восходящее к работе Майера [7], использует методы квантовой теории информации. Этот подход позволяет вычислить скорость выработки секретного ключа на основе взаимной информации Шеннона между квантовыми подсистемами легитимных пользователей и злоумышленника [8]. Этот подход является фундаментальным, однако основывается на асимптотических приближениях теории информации и не учитывает таких аспектов, как конечная длина ключа или возможное многократное его применение.

Второе направление, известное как метод композиционной безопасности (composable security), было формализовано в работах Р. Реннера и др. [9,10]. Оно основывается на парадигме универсальной безопасности, которая гарантирует стойкость протокола не только в изоляции, но и при его использовании совместно с другими криптографическими системами. Этот метод позволяет учитывать конечное число передаваемых квантовых состояний, что критически важно для практических реализаций КРК.

Несмотря на доказанную теоретическую стойкость, практические реализации протоколов КРК уязвимы для атак на аппаратное обеспечение. Класс таких атак получил название „атак на побочные каналы“ (side-channel attacks). Наиболее известными примерами являются атаки с ослеплением однофотонных детекторов, когда злоумышленник с помощью яркой засветки переводит детекторы в линейный режим работы, что позволяет ему

полностью контролировать их срабатывание [11]. Также критической уязвимости подвержены аттенюаторы лазерных источников, которые могут быть переведены злоумышленником в режим многофотонной генерации. Это мгновенно открывает возможность PNS-атаки, снижая эффективность decoy-state метода [12–14].

Важную роль в практической реализации играют системы КРК в свободном пространстве. Помимо решения вышеперечисленных проблем, для кодирования бит сырого ключа необходимо использовать степени свободы квантовой системы, которые были бы устойчивы как к влиянию атмосферной турбулентности (случайным флуктуациям показателя преломления), так и к спонтанным поворотам плоскости поляризации. Особенности поляризационного кодирования проявляются также и в так называемой проблеме прицеливания. В свободном пространстве относительная ориентация приемно-передающих модулей может произвольно изменяться из-за механических вибраций, температурных дрейфов и атмосферной турбулентности, что приводит к непредсказуемым вращениям плоскости поляризации фотонов и, как следствие, к росту уровня квантовых ошибок (QBER) и полному нарушению работы протокола [1,15]. Для решения этой проблемы в литературе предложен ряд подходов, включающих использование активных систем слежения с обратной связью, основанных на измерении векторов Стокса опорного сигнала [16], либо применение пассивных методов, таких как оптические компенсаторы на основе жидких кристаллов [17].

Альтернативным и более фундаментальным решением является переход к протоколам, нечувствительным к глобальному вращению плоскости поляризации. В работе [18] был предложен протокол на основе квантовых состояний света с аксиально-симметричным распределением поляризации, обладающий рядом преимуществ. Во-первых, такой способ кодирования не требует предварительного согласования плоскостей поляризации приемно-передающей аппаратуры (как, например, в случае традиционного протокола BB84 на основе базисов линейных поляризаций). Во-вторых, хорошо разработанный теоретически и экспериментально аппарат восстановления волнового фронта таких пучков позволяет их эффективно использовать в условиях атмосферной оптической турбулентности (проблема „последней мили“) [19]. Важной особенностью предложенного протокола является также возможность быстрой генерации квантовых состояний, кодирующих информацию. Это является критическим аспектом протоколов, использующих состояния пространственных мод, так как распространенные и широко применяемые методы генерации состояний при помощи пространственных модуляторов света (SLM) оказываются сильно ограничены для применения в реальных технических реализациях систем КРК в силу сравнительно небольшой скорости работы модулятора [20]. Мы предложили интерференционную схему как для генерации, так и для детектирования квантовых кодовых состояний, что позволяет их генерировать со скоростью работы фазового модулятора [21]. Работа посвящена оценке криптографической стойкости протокола против ключевых и наиболее распространенных типов атак на протокол: атаки прием-перепосыл и некогерентной атаки с симметричными измерениями.

2. Протокол квантового распределения ключей на основе аксиально-симметричных векторных пучков

Перед тем, как переходить к процедуре оценки криптографической стойкости, приведем описание протокола КРК на основе аксиально-симметричных поляризационных пучков и отметим его ключевые особенности [18–22]. В основе протокола лежат 4 базисных состояния ($|\Phi_{11}\rangle$ — радиально-поляризованный (РП) пучок, $|\Phi_{12}\rangle$ — аксиально-поляризованный (АП) пучок, $|\Phi_{21}\rangle$ — правоскрученный поляризационный (ПСП) пучок, $|\Phi_{22}\rangle$ — левоскрученный поляризационный (ЛСП) пучок), на основе которых кодируются биты секретного ключа:

$$|\Phi_{11}\rangle = |\mathbf{D_R}|LG_{0,1}|\rangle,\ |\Phi_{12}\rangle = |\mathbf{D_A}|LG_{0,1}|\rangle, \tag{1}$$

$$|\Phi_{21}\rangle = |\mathbf{D_{RR}}|LG_{0,1}|\rangle,\ |\Phi_{22}\rangle = |\mathbf{D_{LR}}|LG_{0,1}|\rangle, \tag{2}$$

где $\mathbf{D_i}$ — векторы Джонса, указанные на рис. 1, $|LG_{0,1}|$ — модуль функции Лагерра-Гаусса [23].

Пара ортогональных состояний $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$, как и пара $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$, образует базис гильбертова пространства размерности 2, причем базисы являются сопряженными. В рамках описываемого протокола генерация аксиально-симметричных поляризационных состояний осуществляется путем сложения оптических пучков с орбитальным угловым моментом (топологическим зарядом) ± 1 и циркулярными поляризациями в схеме интерферометра Маха-Цендера (рис. 2, *a*). При этом разложение базисных состояний выглядит следующим образом:

$$|\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle + |L\rangle \otimes |-1\rangle) = \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} + \begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right), \tag{3}$$

$$|\Phi_{12}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle - |L\rangle \otimes |-1\rangle) = \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} - \begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right), \tag{4}$$

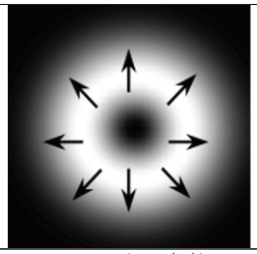
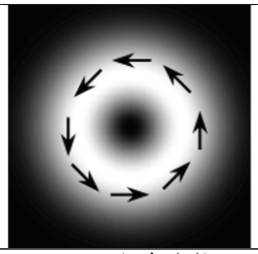
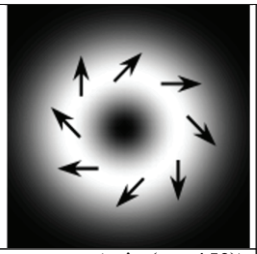
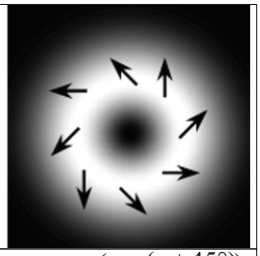
Beam structure				
Jones vector	$\mathbf{D_{RP}}=\begin{pmatrix}\cos(\varphi)\\ \sin(\varphi)\end{pmatrix}$	$\mathbf{D_{AP}}=\begin{pmatrix}-\sin(\varphi)\\ \cos(\varphi)\end{pmatrix}$	$\mathbf{D_{LRP}}=\begin{pmatrix}-\sin(\varphi+45^\circ)\\ \cos(\varphi+45^\circ)\end{pmatrix}$	$\mathbf{D_{RRP}}=\begin{pmatrix}\cos(\varphi+45^\circ)\\ \sin(\varphi+45^\circ)\end{pmatrix}$

Рис. 1. Базисные моды, используемые в протоколе квантового распределения ключа и соответствующие им векторы Джонса.

$$|\Phi_{21}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle + i|L\rangle \otimes |-1\rangle)$$
$$= \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} + i\begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right), \quad (5)$$

$$|\Phi_{22}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle - i|L\rangle \otimes |-1\rangle)$$
$$= \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} - i\begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right). \quad (6)$$

Здесь кет-векторы $|R\rangle$ и $|L\rangle$ обозначают поляризационные моды с право- и левоциркулярными поляризациями соответственно. Кет-векторы $|\pm 1\rangle$ отвечают за орбитальный угловой момент оптического вихря, при этом знак плюс отвечает вращению фазы по часовой стрелке, а минус — против часовой стрелки.

На рис. 2, *a* представлена упрощенная схема генерации оптических вихрей с требуемыми поляризационными состояниями и топологическим зарядом в схеме модифицированного интерферометра Маха-Цендера с уголковыми отражателями.

На выходе схемы формируется состояние

$$|\Phi_{\text{out}}\rangle = 1/\sqrt{2}(|R, +1\rangle + e^{iP}|L, -1\rangle). \quad (7)$$

Отправитель (Алиса) может кодировать значения бит ключа в базисе $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ или в базисе $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$. Для этого она выбирает нужное значение фазы P при помощи фазового модулятора PM $(0, \pi$ для первого базиса и $\pi/2$, $-\pi/2$ для сопряженного) между состояниями $|R, +1\rangle$ и $|L, -1\rangle$ и складывает их в выходном интерферометре Маха-Цендера.

Схема детектирования оптических вихрей показана на рис. 2, *b*. Получатель (Боб) использует аналогичный интерферометр Маха-Цендера для декомпозиции азимутально-симметричных поляризационных состояний, после чего посредством статичных оптических элементов (фазовых голограмм ОАМ ± 1) преобразует их в состояния с нулевым топологическим зарядом и линейной поляризацией. Выбор Бобом дополнительной фазы PM 2 определяет базис детектирования: фаза 0 отвечает детектированию в базисе $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$, фаза $\pi/2$ —детектированию в базисе $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$. Наконец, Боб смешивает пучки на обыкновенном светоделителе BS и проводит измерения в обоих выходных каналах при помощи однофотонных детекторов. При измерении в базисе $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ срабатывание детектора SPD 1 будет означать, что разность фаз между пучками равна 0, а значит, Алиса отправляла состояние $|\Phi_{11}\rangle$. В свою очередь, срабатывание детектора SPD 2 свидетельствует о наличии разности фаз π и отправке состояния $|\Phi_{12}\rangle$. При этом, если измерять такие состояния в сопряженном базисе, детекторы будут срабатывать равновероятно. Процедуры просеивания ключа и усиления секретности осуществляются аналогично протоколу BB84.

По окончании процедуры просеивания Алиса и Боб раскрывают часть секретного ключа для сравнения с целью определения попыток вторгнуться в квантовый канал распределения ключа. По результатам сравнения они делают вывод о наличии подслушивания третьим лицом (Евой). При оценке криптографической стойкости протокола мы ограничимся случаем симметричных атак. В этом случае результаты действий Евы будут статистически неотличимы от физического шума в квантовом канале, а факт наличия или отсутствия Евы в канале связи Алиса и Боб будут делать на основе сравнения уровня ошибок QBER с некоторым критическим уровнем ошибок. В следующем разделе мы определим критический уровень ошибок для двух типов атак: прием-перепосыл и коллективной атаки с симметричными измерениями.

3. Атака прием-перепосыл

Простейшей стратегией подслушивания является атака прием-перепосыл. В рамках этой атаки Ева перехватывает каждое состояние, которое Алиса посылает Бобу. После проводит над ним измерение и отправляет Бобу состояние, являющееся копией измеренного. Оценим количество информации, к которой имеет доступ Ева. В общем случае информация Шеннона определяется следующим образом:

$$I_{\text{Eve}} = \log_2 d + \sum_{i=1}^{d} p_i \log_2 p_i, \quad (8)$$

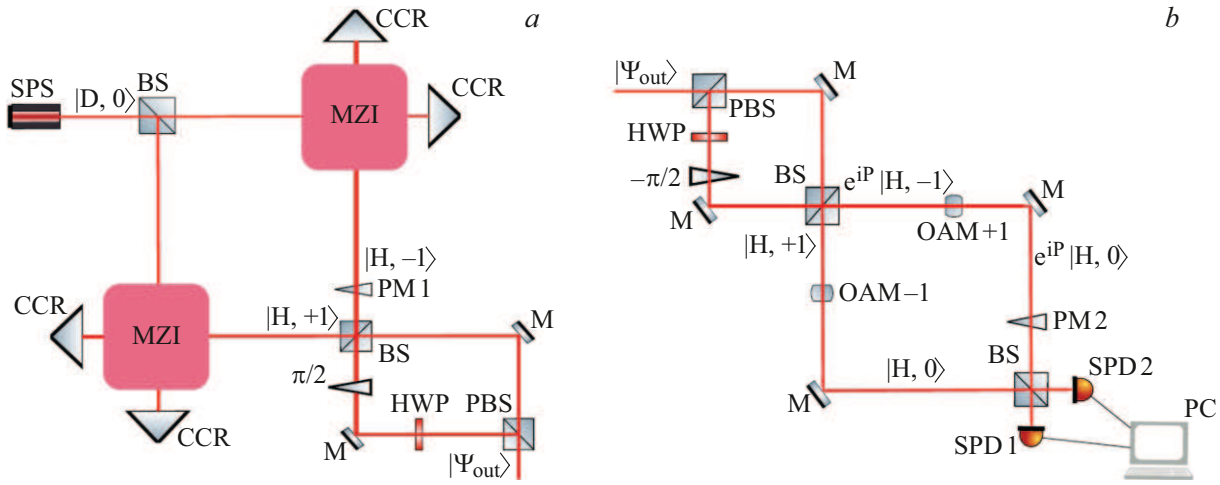


Рис. 2. Упрощенная схема генерации (a) и схема детектирования (b) базисных состояний протокола квантового распределения ключа. SPS — источник одиночных фотонов, BS — светоделительный куб, PBS — поляризационный светоделительный куб, MZI — интерферометр Маха-Цендера, CCR — уголковый отражатель, HWP — $\lambda/2$-пластинка, $\pm\pi/2$ — фазовая пластинка, PM — управляемый фазовый модулятор, M — зеркало, OAM ±1 — фазовые голограммы, изменяющие значение орбитального углового момента пучка, SPD — детектор одиночных фотонов.

где p_i — вероятности различных исходов измерений, а d — размерность используемого пространства состояний.

Перед тем, как перейти к оценке доступной Еве информации, отметим одну важную особенность протокола. Используемые базисные состояния могут быть описаны в пространстве более высокой размерности, а именно — в пространстве куквартов, с логическим базисом вида

$$\begin{aligned}|1\rangle &= |H\rangle \otimes |+1\rangle,\\ |2\rangle &= |H\rangle \otimes |-1\rangle,\\ |3\rangle &= |V\rangle \otimes |+1\rangle,\\ |4\rangle &= |V\rangle \otimes |-1\rangle,\end{aligned} \tag{9}$$

где кет-векторы $|H\rangle, |V\rangle$ описывают состояния фотона с горизонтальной и вертикальной поляризацией соответственно, а кет-векторы $|+1\rangle, |-1\rangle$ — состояния фотона с топологическим зарядом, равным ±1. В данном базисе кодовые состояния Алисы записываются следующим образом:

$$\begin{aligned}|\Phi_{11}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle + |L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle + |2\rangle + i|3\rangle - i|4\rangle\right),\end{aligned} \tag{10}$$

$$\begin{aligned}|\Phi_{12}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle - |L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle - |2\rangle + i|3\rangle + i|4\rangle\right),\end{aligned} \tag{11}$$

$$\begin{aligned}|\Phi_{21}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle + i|L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle + i|2\rangle + i|3\rangle + |4\rangle\right).\end{aligned} \tag{12}$$

$$\begin{aligned}|\Phi_{22}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle - i|L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle - i|2\rangle + i|3\rangle - |4\rangle\right).\end{aligned} \tag{13}$$

Подобное представление базисных состояний предоставляет Еве потенциальную возможность строить свои атаки из пространства более высокой размерности, поэтому в дальнейшем рассмотрении мы будем рассматривать 2 типа атак: с использованием Евой состояний из пространства кубитов и состояний из пространства куквартов.

3.1. Атака прием-перепосыл в пространстве кубитов

Для начала оценим количество информации Евы при атаке в кубитном пространстве ($d = 2$):

• Пусть Ева правильно угадывает базис, т.е. ее базис измерения совпадает с тем, который использовала Алиса для кодирования состояния. Распределение вероятностей измерения различных состояний имеет вид $p_i = \{1; 0\}$, т.е. Ева всегда при измерении будет получать состояние, отправленное Алисой. Тогда энтропия Шеннона равна

$$H_{\text{success}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -(1\log_2 1 + 0\log_2 0) = 0\,\text{бит}. \tag{14}$$

• Пусть Ева неправильно угадывает базис, т.е. ее базис не совпадает с базисом, который использовала

для кодирования Алиса. Распределение вероятностей измерения различных состояний имеет вид $p_i = \{\frac{1}{2}; \frac{1}{2}\}$, т. е. Ева при измерении будет получать состояние, отправленное Алисой, лишь с вероятностью 50%. Тогда энтропия Шеннона равна

$$H_{\text{failure}} = -\sum_{i=1}^{d} p_i \log_2 p_i$$

$$= -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}\right) = 1\,\text{бит}. \qquad (15)$$

• Поскольку в данной атаке Ева выбирает один из двух базисов ($\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ или $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$) случайным образом, усредненная информация Евы равна

$$I_{\text{Eve}} = \log_2 d - \frac{1}{2}H_{\text{success}} - \frac{1}{2}H_{\text{failure}} = \frac{1}{2}\,\text{бит}, \qquad (16)$$

и Ева имеет доступ к половине передаваемой информации. Суммарная ошибка равна произведению вероятностей ошибок детектирования Евы и Боба и составляет

$$P_{\text{sum}} = P_{\text{Eve}}P_{\text{Bob}} = \frac{1}{2}\frac{1}{2} = \frac{1}{4}. \qquad (17)$$

Данные результаты полностью аналогичны оценке для протокола BB84 на линейных поляризациях [25].

3.2. Атака прием-перепосыл в пространстве куквартов

Теперь оценим доступную Еве информацию в случае атаки с использованием куквартного базиса для измерений ($d = 4$). Поскольку распределение вероятностей измерения различных состояний напрямую зависит от коэффициентов разложения состояний Алисы по состояниям в базисах детектирования, необходимо построить все возможные проекторы состояний, чтобы оценить оптимальную стратегию Евы. В пространстве куквартов существует 5 различных взаимно-несмещенных базисов (mutually unbiased bases — MUB), которые может использовать Ева [24]. При этом оценка „правильности“ угаданного базиса становится нетривиальной задачей. В Приложении A рассчитаны все проекции состояний, используемых для кодирования Алисой на состояния, составляющие взаимно-несмещенные базисы куквартного пространства измерений Евы. Наибольшее количество информации Еве принесут измерения в тех базисах, которые дают наименьшую неопределенность, т. е. наибольшую возможность различения состояний. Основной интерес с точки зрения максимизации вероятностей представляют измерения в базисах IV и V:

$$|\langle\Phi_{11}|\Psi_{\text{IV},1}\rangle|^2 = 1, \quad |\langle\Phi_{11}|\Psi_{\text{V},1}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\text{IV},2}\rangle|^2 = 0, \quad |\langle\Phi_{11}|\Psi_{\text{V},2}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\text{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{11}|\Psi_{\text{V},3}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\text{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{11}|\Psi_{\text{V},4}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},1}\rangle|^2 = 0, \quad |\langle\Phi_{12}|\Psi_{\text{V},1}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},2}\rangle|^2 = 1, \quad |\langle\Phi_{12}|\Psi_{\text{V},2}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{12}|\Psi_{\text{V},3}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{12}|\Psi_{\text{V},4}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},1}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{21}|\Psi_{\text{V},1}\rangle|^2 = 0;$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},2}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{21}|\Psi_{\text{V},2}\rangle|^2 = 0;$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{21}|\Psi_{\text{V},3}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{21}|\Psi_{\text{V},4}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\text{IV},1}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{22}|\Psi_{\text{V},1}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\text{IV},2}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{22}|\Psi_{\text{V},2}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\text{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{22}|\Psi_{\text{V},3}\rangle|^2 = 0;$$

$$|\langle\Phi_{22}|\Psi_{\text{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{22}|\Psi_{\text{V},4}\rangle|^2 = 0. \qquad (18)$$

Здесь индекс состояния $|\Psi_{i,j}\rangle$ $i \in \{\text{I, II, III, IV, V}\}$ обозначает MUB, индекс $j \in \{1, 2, 3, 4\}$ — порядковый номер базисного вектора в этом MUB. Полная информация о коэффициентах разложения представлена в Приложении A.

Для точного различения состояний из базиса $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ Еве необходимо производить измерения в IV MUB. При этом, если Ева попытается измерить состояния из базиса $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$, она получит равновероятные проекции на состояния $|\Psi_{\text{IV},1}\rangle$ и $|\Psi_{\text{IV},2}\rangle$. Для различения этих состояний ей придется произвести измерения в базисе II или V (с этой точки зрения они равноправны). Допустим, Ева будет использовать базис V. В таком случае при детектировании состояний $|\Psi_{\text{V},3}\rangle$ или $|\Psi_{\text{V},4}\rangle$ она делает вывод, что Алиса отправляла состояние $|\Phi_{21}\rangle$, а при детектировании состояний $|\Psi_{\text{V},1}\rangle$ или $|\Psi_{\text{V},2}\rangle$ — что Алиса отправляла состояние $|\Phi_{22}\rangle$ (разумеется, при условии, что Ева угадала базис кодирования). Оценим количество доступной Еве информации при описанном подходе к атаке:

• Пусть Ева правильно угадывает базис, т. е. проводит измерения в наиболее подходящем из доступных MUB для отправленного состояния Алисы. Рассмотрим случай использования Евой базиса IV. В данном базисе Ева может однозначно идентифицировать состояния $|\Phi_{11}\rangle$ и $|\Phi_{12}\rangle$. Распределение вероятностей измерения различных

состояний имеет вид $p_i = \{1;0;0;0\}$, т.е. Ева всегда при измерении будет получать состояние, отправленное Алисой. Тогда энтропия Шеннона равна

$$H_{\text{success}_{\text{IV}}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -(1\log_2 1 + 0\log_2 0 + 0\log_2 0 + 0\log_2 0) = 0 \text{ бит}. \quad (19)$$

В случае использования Евой базиса V Ева не различает однозначно состояния $|\Phi_{12}\rangle$ и $|\Phi_{22}\rangle$, однако с вероятностью $1/2$ получает в результате измерения состояния $|\Psi_{\text{V},1}\rangle$ и $|\Psi_{\text{V},2}\rangle$ или $|\Psi_{\text{V},3}\rangle$ и $|\Psi_{\text{V},4}\rangle$ для состояний Алисы $|\Phi_{21}\rangle$ и $|\Phi_{22}\rangle$ соответственно. Распределение вероятностей измерения различных состояний имеет вид $p_i = \{\frac{1}{2};\frac{1}{2};0;0\}$. Тогда энтропия Шеннона равна

$$H_{\text{success}_{\text{V}}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -\Big(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2} + 0\log_2 0 + 0\log_2 0\Big) = 1 \text{ бит}. \quad (20)$$

• Пусть Ева неправильно угадывает базис, т.е. проводит измерения в неподходящем для состояния Алисы MUB. Рассмотрим случай использования Евой базиса IV. При попытке измерить в этом базисе состояния $|\Phi_{21}\rangle$ и $|\Phi_{22}\rangle$ Ева с равными вероятностями будет детектировать состояния $|\Psi_{\text{V},1}\rangle$ и $|\Psi_{\text{V},2}\rangle$. Распределение вероятностей измерения различных состояний имеет вид $p_i = \{\frac{1}{2};\frac{1}{2};0;0\}$. Тогда энтропия Шеннона равна

$$H_{\text{failure}_{\text{IV}}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -\Big(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2} + 0\log_2 0 + 0\log_2 0\Big) = 1 \text{ бит}. \quad (21)$$

В случае использования Евой базиса V при измерении состояний $|\Phi_{11}\rangle$ и $|\Phi_{12}\rangle$ она с равной вероятностью будет детектировать любое из базисных состояний. Распределение вероятностей измерения различных состояний имеет вид $p_i = \{\frac{1}{4};\frac{1}{4};\frac{1}{4};\frac{1}{4}\}$. Тогда энтропия Шеннона равна

$$H_{\text{failure}_{\text{V}}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -\Big(\frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4}\Big) = 2 \text{ бита}. \quad (22)$$

• Поскольку в данной атаке Ева выбирает базис случайным образом (IV или V), усредненная информация, доступная Еве, равна

$$I_{\text{Eve}} = \log_2 d - \frac{1}{2}H_{\text{success}} - \frac{1}{2}H_{\text{failure}} = 2 - \frac{1}{2}\Big(\frac{1}{2}0 + \frac{1}{2}1\Big) - \frac{1}{2}\Big(\frac{1}{2}1 + \frac{1}{2}2\Big) = 1 \text{ бит}, \quad (23)$$

и Ева вновь имеет доступ к половине передаваемой информации. Вероятность суммарной ошибки равна произведению вероятностей ошибок Евы и Боба и составляет

$$P_{\text{sum}} = P_{\text{Eve}}P_{\text{Bob}} = \frac{1}{2}\frac{1}{2} = \frac{1}{4}. \quad (24)$$

Таким образом, использование Евой пространства состояний более высокой размерности не дает ей преимущества при проведении атаки прием-перепосыл, а критический уровень ошибок составляет 25%. Полученные результаты аналогичны атаке прием-перепосыл на классический протокол BB84, причем Ева также имеет доступ к половине передаваемой информации [25].

4. Некогерентная атака с симметричными измерениями

В ряде работ [26,27] была предложена оптимальная для Евы стратегия, при которой она получает максимальное значение информации при минимальном вносимом возмущении. Ева действует следующим образом: она перехватывает состояния Алисы, перепутывает их со своей вспомогательной системой и отправляет Бобу исходное перехваченное, но теперь уже возмущенное состояние Алисы. После этого Ева сохраняет состояние вспомогательной системы в квантовой памяти и дожидается этапа публичного оглашения базисов, после чего производит измерения. Количество информации, которое теперь получает Ева, определяется величиной воздействия на состояния Алисы, а также способом измерения состояний вспомогательной системы. Чем сильнее воздействие, тем больше информации получает Ева, но при этом увеличивается и возмущение, вносимое ею в квантовый канал связи.

Данная атака в пространстве кубитов была подробно рассмотрена в работе [27]. На основе фундаментальных энтропийных соотношений было показано, что критический уровень ошибок при вмешательстве Евы в канал связи составляет

$$D_c = \frac{1}{2} - \frac{1}{4}\sqrt{2} \approx 0.146 \quad (25)$$

или 14.6 %. Далее мы рассмотрим стратегию Евы при использовании ею базисных состояний пространства более высокой размерности ($d = 4$) и сравним получившийся результат с критической ошибкой в случае атаки с использованием гильбертова пространства размерности 2.

В общем случае стратегия Евы в пространстве куквартов выглядит следующим образом:

$$U|0\rangle \otimes |E\rangle = \sqrt{D-1}|0\rangle \otimes |E_{00}\rangle + \sqrt{D/3}|1\rangle \otimes |E_{01}\rangle + \sqrt{D/3}|2\rangle \otimes |E_{02}\rangle + \sqrt{D/3}|3\rangle \otimes |E_{03}\rangle,$$

$$U|1\rangle \otimes |E\rangle = \sqrt{D/3}|0\rangle \otimes |E_{10}\rangle + \sqrt{D-1}|1\rangle \otimes |E_{11}\rangle + \sqrt{D/3}|2\rangle \otimes |E_{12}\rangle + \sqrt{D/3}|3\rangle \otimes |E_{13}\rangle,$$

$$U|2\rangle \otimes |E\rangle = \sqrt{D/3}|0\rangle \otimes |E_{20}\rangle + \sqrt{D/3}|1\rangle \otimes |E_{21}\rangle + \sqrt{D-1}|2\rangle \otimes |E_{22}\rangle + \sqrt{D/3}|3\rangle \otimes |E_{23}\rangle,$$
$$U|3\rangle \otimes |E\rangle = \sqrt{D/3}|0\rangle \otimes |E_{30}\rangle + \sqrt{D/3}|1\rangle \otimes |E_{31}\rangle + \sqrt{D/3}|2\rangle \otimes |E_{32}\rangle + \sqrt{D-1}|3\rangle \otimes |E_{33}\rangle, \quad (26)$$

где $|i\rangle$, $i \in \{0, 1, 2, 3\}$ — векторы состояния логического базиса пространства куквартов, $|E\rangle$ и $|E_{00}\rangle$, $|E_{01}\rangle, \ldots$ — нормированные векторы вспомогательного состояния Евы до и после взаимодействия соответственно, D — величина возмущения, вносимого Евой в канал связи, U — унитарное перепутывающее преобразование. В силу унитарности оператора U состояния Евы должны удовлетворять свойству ортогональности:

$$\langle E| \otimes \langle i|U^{\dagger}U|j\rangle \otimes |E\rangle = 0, \, i, \, j \in \{0, 1, 2, 3\}. \quad (27)$$

В ходе атаки Ева стремится максимизировать доступную ей информацию о квантовой системе Алисы, при этом внося как можно меньшее возмущение. Фактически Ева выбирает свои вспомогательные состояния так, чтобы решить данную задачу оптимизации. Взаимодействие Евы с произвольным состоянием Алисы приводит к возмущению состояния, полученного Бобом $D_{(k)}$, которое можно найти, как

$$D_{(k)} = 1 - \langle k|\rho^{(k)}_{B,\mathrm{Out}}|k\rangle, \quad (28)$$

где $\langle k| \in \{|\Phi_{11}\rangle, |\Phi_{12}\rangle, |\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ — одно из возможных состояний Алисы, а $\rho^{(k)}_{B,\mathrm{Out}}$ — редуцированная матрица плотности состояния, отправленного Бобу после воздействия Евы. Ее можно вычислить следующим образом:

$$\rho^{(k)}_{B,\mathrm{Out}} = \mathrm{Tr}_E[U|k\rangle \otimes |E\rangle\langle E| \otimes \langle k|U^{\dagger}]. \quad (29)$$

Величина вносимого возмущения зависит от выбора вспомогательных состояний Евы и последующей процедуры их измерения. Таким образом, необходимо получить явную взаимосвязь между возмущением D и скалярными произведениями вспомогательных состояний. Поскольку мы рассматриваем случай симметричной атаки, все возмущения $D_{(k)}$ должны быть равны между собой:

$$1 - \langle k|\mathrm{Tr}_E[U|k\rangle \otimes |E\rangle\langle E| \otimes \langle k|U^{\dagger}]|k\rangle = D,$$
$$k \in \{\Phi_{11}, \Phi_{12}, \Phi_{21}, \Phi_{22}\}. \quad (30)$$

Действие оператора U на состояния Алисы вычисляется на основе уравнений (26). Поэтому решая систему (30) вместе с условиями ортогональности (27), мы получаем выражения, связывающие величину возмущения со скалярными произведениями вспомогательных состояний Евы $|E_{ij}\rangle$. В силу симметрии задачи ненулевыми оказываются следующие скалярные произведения:

$$\langle E_{ii}|E_{jj}\rangle = s, \quad \text{где} \quad i \neq j, \quad (31)$$

$$\langle E_{ij}|E_{hk}\rangle = w, \quad \text{где} \quad j \neq i, \quad (h = j \ \text{ и } k = i) \ \text{ или } \ (h \neq k \neq i \neq j), \quad (32)$$

а величина возмущения связана с ними как

$$s = \frac{1 - wD}{1 - D} + \frac{4}{3}\frac{D}{D-1}. \quad (33)$$

Важно отметить, что полученная взаимосвязь (33) аналогична полученной в работе [26] для случая двух базисов кодирования в пространстве куквартов.

Теперь найдем как с выбором вспомогательных состояний Евы связана взаимная информация подсистем Алиса-Ева. Для этого рассмотрим возможные ситуации. В первом случае Боб верно определяет состояние Алисы с вероятностью $1 - D$, Ева при этом также верно определяет это состояние с некоторой вероятностью $p_1(s, w, D)$. Явный вид зависимости вероятности от параметров задачи достаточно громоздкий и мы ограничимся здесь ссылкой на работу [26], в которой похожая теория изложена более полно. Во втором случае Боб при измерении получает отличное от отправленного Алисой состояние с вероятностью D. Ева при этом верно определит отправленное состояние с вероятностью $p_2(s, w, D)$. Тогда взаимная информация подсистем Алиса-Ева I_{AE} равна

$$I_{AE}(s, w, D) = (1 - D)I_4(p_1) + DI_4(p_2), \quad (34)$$

где информация Шеннона $I_4(x)$ в пространстве куквартов равна

$$I_4(x) = 1 + x\log_4(x) + (1 - x)\log_4\left(\frac{1 - x}{3}\right). \quad (35)$$

Ева стремится получить максимальную информацию о системе Алисы, а значит, подбирает вспомогательные состояния оптимальным образом. Взаимная информация подсистем Алиса-Ева $I_{AE}(s, w, D)$ достигает максимального значения при

$$w = 1 - \frac{4}{3}D. \quad (36)$$

Условия (33), (36) определяют выбор Евой вспомогательных состояний, а вероятности $p_1(s, w, D)$ и $p_2(s, w, D)$ теперь зависят только от величины возмущения D и имеют следующий вид:

$$p_1(D) = \frac{2D^2 - D - 2\sqrt{3}\sqrt{-(D-1)^3 D} - 1}{4(D-1)}, \quad (37)$$

$$p_2(D) = \frac{1}{4}\left(2D + 2\sqrt{3}\sqrt{-(D-1)D} + 1\right). \quad (38)$$

Наконец, мы можем определить критический уровень ошибки в случае некогерентной симметричной атаки Евы. Критическим порогом ошибки является такое значение возмущения D_c, при котором сравниваются взаимные информации подсистем Алиса-Ева $I_{AE}(D)$ и

Алиса-Боб $I_{AB,4}(D)$. Последняя в пространстве куквартов находится следующим образом:

$$I_{AB,4}(D) = 1 + (1-D)\log_4(1-D) + D\log_4\frac{D}{3}. \quad (39)$$

Решая уравнение

$$I_{AE}(D_c) = I_{AB,4}(D_c), \quad (40)$$

находим, что критический уровень ошибки для некогерентной симметричной атаки составляет $D_c = 0.25$ (25 %). Сравнивая данный результат с выражением (25), отметим, что использование Евой куквартного пространства состояний не дало ей преимущества при некогерентной атаке. Таким образом, оптимальной стратегией действий Евы в случае некогерентной атаки будет симметричная атака из пространства кубитов. В таком случае при одинаковой величине доступной информации Ева будет вносить меньшее возмущение в канал связи.

5. Заключение

Мы продемонстрировали устойчивость протокола на основе аксиально-симметричных поляризационных вихрей к двум самым распространенным типам атак: прием-перепосыл и некогерентная атака с симметричными измерениями. При этом была учтена особенность протокола, связанная с тем, что кодовые состояния Алисы могут быть описаны как в кубитном, так и куквартном гильбертовом пространствах. Было строго показано, что использование Евой атак из пространства состояний более высокой размерности не дает преимущества в смысле уменьшения критической ошибки. При этом мы не рассматривали когерентную атаку с коллективными измерениями, когда Ева взаимодействует одновременно со всеми квантовыми системами Алисы. Данный тип атаки является оптимальным, так как приводит к наименьшей критической ошибке (11 % для протокола BB84). Однако когерентную атаку сложнее всего осуществить на практике. Кроме того, в работах [28,29] было показано, что данный тип атак в пространстве произвольной размерности сводится к фундаментальным энтропийным соотношениям вне зависимости от используемых Алисой кодовых состояний. Критическая ошибка при этом также растет с увеличением размерности пространства.

Анализируя стойкость протокола против атак на техническую составляющую систем КРК, можно отметить, что в рамках рассматриваемого протокола и методов генерации и детектирования базисных состояний актуальными являются атаки, связанные с зондированием излучения и вмешательством в работу фазового и амплитудного модуляторов на стороне Алисы, а также аналогичное воздействие на фазовый модулятор и детекторы одиночных фотонов на стороне Боба. Однако в работах [30,31] показано, что для систем с фазовыми методами генерации базисных состояний атаки с ослеплением лавинных детекторов и атака типа Detectors Mismatch оказываются неэффективными.

Наш дальнейший интерес в изучении протоколов КРК сосредоточен в области высокоразмерных протоколов, использующих для кодирования информации не бинарную логику, поскольку рассматриваемые векторные состояния с аксиально-симметричным состоянием поляризации имеют естественное описание в логическом пространстве размерности 4. Однако расширение протокола на куквартный случай требует анализа методов генерации и детектирования такого излучения, а также детального изучения вопросов криптостойкости высокоразмерных протоколов КРК.

Финансирование работы

Работа была выполнена при поддержке гранта АО „РЖД“ (договор № 5950981 от 17.12.2024).

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Приложение А. Проекторы кодовых состояний Алисы на состояния MUB в пространстве куквартов

В пространстве куквартов с логическим базисом вида $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ существуют 5 взаимно-несмещенных MUB. Если подготовить квантовую систему в собственном состоянии одного из MUB, прогнозируется, что все результаты измерения относительно любого другого MUB произойдут с равной вероятностью $1/d$. Здесь d — размерность гильбертова пространства, в котором описывается квантовая система. В гильбертовом пространстве размерности 4, этот набор базисов выглядит, как показано в таблице.

Коэффициенты разложения кодовых состояний $|\Phi_{11}\rangle, |\Phi_{12}\rangle, |\Phi_{21}\rangle, |\Phi_{22}\rangle$ по логическим состояниям MUB вычисляются как модуль квадрата проектора:

$$|\langle\Phi_{11}||0\rangle|^2 = \left|\left(\frac{1}{2}(|1\rangle + |2\rangle + i|3\rangle - i|4\rangle)\right)|0\rangle\right|^2$$

$$= \frac{1}{4}\left|\langle 0|0\rangle + \langle 1|0\rangle + \langle 2|0\rangle + \langle 3|0\rangle\right|^2 = \frac{1}{4}, \quad (A1)$$

в силу ортогональности состояний $\langle i|j\rangle = 0$, $i \neq j$, $i, j \in \{0, 1, 2, 3\}$. Аналогичным образом вычисляются и все остальные коэффициенты разложения. Индекс состояния $|\Psi_{i,j}\rangle$ $i \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{V}\}$ обозначает MUB, индекс $j \in \{1, 2, 3, 4\}$ — порядковый номер базисного вектора в этом MUB:

$$|\langle\Phi_{11}|\Psi_{\mathrm{I},1}\rangle|^2 = \frac{1}{4}, |\langle\Phi_{11}|\Psi_{\mathrm{II},1}\rangle|^2 = \frac{1}{4}, |\langle\Phi_{11}|\Psi_{\mathrm{III},1}\rangle|^2 = \frac{1}{4},$$

Логические базисные состояния MUB в пространстве куквартов

Номер базиса	Базисные состояния
I	$\|0\rangle$ $\|1\rangle$ $\|2\rangle$ $\|3\rangle$
II	$\frac{1}{2}(\|0\rangle + \|1\rangle + \|2\rangle + \|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle + \|2\rangle - \|3\rangle)$ $\frac{1}{2}(\|0\rangle + \|1\rangle - \|2\rangle - \|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle - \|2\rangle + \|3\rangle)$
III	$\frac{1}{2}(\|0\rangle + i\|1\rangle + i\|2\rangle - \|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle + i\|2\rangle + \|3\rangle)$ $\frac{1}{2}(\|0\rangle + i\|1\rangle - i\|2\rangle + \|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle - i\|2\rangle - \|3\rangle)$
IV	$\frac{1}{2}(\|0\rangle + \|1\rangle + i\|2\rangle - i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle + i\|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle + \|1\rangle - i\|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle - i\|2\rangle - i\|3\rangle)$
V	$\frac{1}{2}(\|0\rangle + i\|1\rangle + \|2\rangle - i\|3\rangle)$ $\frac{1}{2}(\|0\rangle + i\|1\rangle - \|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle + \|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle - \|2\rangle - i\|3\rangle)$

$$|\langle\Phi_{11}|\Psi_{\mathrm{IV},1}\rangle|^2 = 1,\ |\langle\Phi_{11}|\Psi_{\mathrm{V},1}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\mathrm{I},2}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{11}|\Psi_{\mathrm{II},2}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{11}|\Psi_{\mathrm{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{11}|\Psi_{\mathrm{IV},2}\rangle|^2 = 0,\ |\langle\Phi_{11}|\Psi_{\mathrm{V},2}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\mathrm{I},3}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{11}|\Psi_{\mathrm{II},3}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{11}|\Psi_{\mathrm{III},3}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{11}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0,\ |\langle\Phi_{11}|\Psi_{\mathrm{V},3}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\mathrm{I},4}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{11}|\Psi_{\mathrm{II},4}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{11}|\Psi_{\mathrm{III},4}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{11}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0,\ |\langle\Phi_{11}|\Psi_{\mathrm{V},4}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{I},1}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{II},1}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{III},1}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},1}\rangle|^2 = 0,\ |\langle\Phi_{12}|\Psi_{\mathrm{V},1}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{I},2}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{II},2}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},2}\rangle|^2 = 1,\ |\langle\Phi_{12}|\Psi_{\mathrm{V},2}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{I},3}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{II},3}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{III},3}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0,\ |\langle\Phi_{12}|\Psi_{\mathrm{V},3}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{I},4}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{II},4}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{12}|\Psi_{\mathrm{III},4}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0,\ |\langle\Phi_{12}|\Psi_{\mathrm{V},4}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{I},1}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{21}|\Psi_{\mathrm{II},1}\rangle|^2 = 0,\ |\langle\Phi_{21}|\Psi_{\mathrm{III},1}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},1}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{21}|\Psi_{\mathrm{V},1}\rangle|^2 = 0;$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{I},2}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{21}|\Psi_{\mathrm{II},2}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{21}|\Psi_{\mathrm{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},2}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{21}|\Psi_{\mathrm{V},2}\rangle|^2 = 0;$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{I},3}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{21}|\Psi_{\mathrm{II},3}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{21}|\Psi_{\mathrm{III},3}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0,\ |\langle\Phi_{21}|\Psi_{\mathrm{V},3}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{I},4}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{21}|\Psi_{\mathrm{II},4}\rangle|^2 = 0,\ |\langle\Phi_{21}|\Psi_{\mathrm{III},4}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0,\ |\langle\Phi_{21}|\Psi_{\mathrm{V},4}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{I},1}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{22}|\Psi_{\mathrm{II},1}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{22}|\Psi_{\mathrm{III},1}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},1}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{22}|\Psi_{\mathrm{V},1}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{I},2}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{22}|\Psi_{\mathrm{II},2}\rangle|^2 = 0,\ |\langle\Phi_{22}|\Psi_{\mathrm{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},2}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{22}|\Psi_{\mathrm{V},2}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{I},3}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{22}|\Psi_{\mathrm{II},3}\rangle|^2 = 0,\ |\langle\Phi_{22}|\Psi_{\mathrm{III},3}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0,\ |\langle\Phi_{22}|\Psi_{\mathrm{V},3}\rangle|^2 = 0;$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{I},4}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{22}|\Psi_{\mathrm{II},4}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{22}|\Psi_{\mathrm{III},4}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0,\ |\langle\Phi_{22}|\Psi_{\mathrm{V},4}\rangle|^2 = 0. \qquad \text{(A2)}$$

Измерения в MUB I и III являются наименее информативными для Евы, поскольку каждое из кодовых состояний Алисы имеет одинаковые проекции на векторы этих MUB. Также отметим, что не существует базиса, в котором коэффициенты разложения всех состояний Алисы были бы равны 1. Это значит, что ни один из 5 MUB в пространстве куквартов не позволяет Еве однозначно определить произвольное кодовое состояние Алисы. Для различения состояний Алисы из базиса $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ с точки зрения максимизации информации Еве выгоднее использовать IV MUB, для различения состояний Алисы из базиса $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ — II или V MUB. В данном случае II и V MUB оказываются эквивалентны, поскольку существуют ненулевые проекции кодовых состояний Алисы $|\Phi_{21}\rangle$ и $|\Phi_{22}\rangle$ на две непересекающиеся пары базисных векторов. А значит, при детектировании любого вектора из пары Ева точно будет знать, какое кодовое состояние Алисы из базиса

$\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ она измерила. Поэтому при анализе атаки прием-перепосыл в основной части работы мы используем только один базис — V MUB.

Также отметим, что проекции состояний Алисы из базиса $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ на векторы IV MUB имеют аналогичную величину $\frac{1}{2}$, однако ненулевые проекции существуют только на те базисные векторы, что и у состояний $|\Phi_{11}\rangle$, $|\Phi_{12}\rangle$, что усложняет Еве задачу максимизации информации о состоянии Алисы при измерении.

Список литературы

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Rev. Mod. Phys., **74** (1), 145 (2002). DOI: 10.1103/RevModPhys.74.145

[2] C.H. Bennett, G. Brassard. Theoretical Computer Science, **560** (1), 7 (2014). DOI: 10.1016/j.tcs.2014.05.025

[3] V. Scarani, A. Ac'ın, G. Ribordy, N. Gisin. Physical Review Letters, **92** (5), 057901 (2004). DOI: 10.1103/PhysRevLett.92.057901

[4] S.P. Kulik, S.N. Molotkov. Laser Phys. Lett., **14**, 125205 (2017). DOI: 10.1088/1612-202X/aa8ecc

[5] K.S. Kravtsov, S.N. Molotkov. Phys. Rev. A, **100**, 042329 (2019). DOI: 10.1103/PhysRevA.100.042329

[6] F. Grosshans, P. Grangier. Physical Review Letters, **88** (5), 057902 (2002). DOI: PhysRevLett.88.057902

[7] D. Mayers. Journal of the ACM (JACM), **48** (3), 351 (2001). DOI: 10.1145/382780.382781

[8] P.W. Shor, J. Preskill. Physical Review Letters, **85** (2), 441 (2000). DOI: 10.1103/PhysRevLett.85.441

[9] R. Renner. *Security of quantum key distribution*. Doctoral dissertation (Swiss Federal Institute Of Technology, Zurich, 2005). URL: https://arxiv.org/pdf/quant-ph/0512258

[10] R. Renner, R. König. In: *Theory of Cryptography. TCC 2005*, ed. by. J. Kilian. Lecture Notes in Computer Science (Springer, Berlin, Heidelberg, 2005), vol. 3378. DOI: 10.1007/978-3-540-30576-7_22

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov. Nature Photonics, **4** (10), 686 (2010). DOI: 10.1038/nphoton.2010.214

[12] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders. Physical Review Letters, **85** (6), 1330 (2000). DOI: 10.1103/PhysRevLett.85.1330

[13] I. Sushchev, K. Bugai, S. Molotkov, D. Bulavkin, A. Sidelnikova, D. Melkonian, V. Vakhrusheva, R. Lokhmatov, D. Dvoretskiy. DOI: 10.48550/arXiv.2507.15446

[14] С.Н. Молоткова, К.С. Кравцов, М.И. Рыжкин. Журнал Экспериментальной и Теоретической Физики (ЖЭТФ), **155** (4), 636 (2018). DOI: 10.1134/S0044451019040060

[15] M. Gellert, D. Sulimov, B. Nasedkin, R. Goncharov, I. Filipov, P. Morozova, F. Goncharov, D. Yashin, V. Chistiakov, E. Samsonov, V. Egorov, B. Pervushin, I. Adam. Journal of Optical Technology, **90** (2), 55 (2023). DOI: 10.1364/JOT.90.000055

[16] S. Lorenz, N. Korolkova, G. Leuchs. Appl. Phys. B, **79**, 273 (2004). DOI: 10.1007/s00340-004-1574-7

[17] A. Jimenez-Girela, D. Merino-Pérez, A. Campos-Jara, Negrín, J. Socas, Parejo, P. Garcia, A. Álvarez-Herrero. Phys. Rev. Applied, **23** (6), 064070 (2025). DOI: 10.1103/8plr-m6n8

[18] D.D. Reshetnikov, A.L. Sokolov, E.A. Vashukevich, V.M. Petrov, T.Yu. Golubeva. Radiophys Quantum El., **67**, 51 (2024). DOI: 10.1007/s11141-025-10352-z

[19] J.S. Sidhu, T. Brougham, D. McArthur, R.G. Pousa, D.K.L. Oi. Commun Phys., **6**, 210 (2023). DOI: 10.1038/s42005-023-01299-6

[20] S. Turtaev, I.T. Leite, K.J. Mitchell, M.J. Padgett, D.B. Phillips, T. Cizmá. Opt. Express, **25**, 29874 (2017). DOI: 10.1364/OE.25.029874

[21] I.-C. Benea-Chelmus, S. Mason, M.L. Meretska, D.L. Elder, D. Kazakov, A. Shams-Ansari, L.R. Dalton, F. Capasso. Nat Commun., **13**, 3170 (2022). DOI: 10.1038/s41467-022-30451-z

[22] Д.Д. Решетников, А.А. Рыжая, М.Е. Павелина, Е.А. Вашукевич, А.А. Севрюгин, А.Л. Соколов, В.Ю. Венедиктов, В.М. Петров. Оптический журнал, **92** (3), 58 (2025). DOI: 10.17586/1023-5086-2025-92-03-58-67

[23] L. Allen, M.W. Beijersbergen, R.J.C. Spreeuw, J.P. Woerdman. Phys. Rev. A, **45**, 8185 (1992). DOI: 10.1103/PhysRevA.45.8185

[24] E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, F. Sciarrino. Phys. Rev. A., **81**, 052317 (2010). DOI: 10.1103/PhysRevA.81.052317

[25] S.P. Kulik, A.P. Shurupov. Atoms, Molecules, Optics, **104**, 736 (2007). DOI: 10.1134/S106377610705007X

[26] F. Caruso, H. Bechmann-Pasquinucci, C. Macchiavello. Phys. Rev. A, **72**, 032340 (2005). DOI: 10.1103/PhysRevA.72.032340

[27] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, A. Peres. Phys. Rev. A, **56**, 1163 (1997). DOI: 10.1103/PhysRevA.56.1163

[28] S. Pirandola. International Journal of Quantum Information, **6**, 765 (2008). DOI: 10.1142/S0219749908004080

[29] L. Sheridan, V. Scarani. Phys. Rev. A, **82**, 030301 (2011). DOI: 10.1103/PhysRevA.82.030301

[30] K.A. Balygin, A.N. Klimov, I.B. Bobrov, K.S. Kravtsov, S.P. Kulik, S.N. Molotkov. Laser Physics Letters, **15** (9), 095203 (2018). DOI: 0.1088/1612-202X/aad1c9

[31] W.-Y. Hwang. Physical Review Letters, **91** (5), 057901 (2003). DOI: 10.1103/PhysRevLett.91.057901