Письма в ЖЭТФ, том 121, вып. 12, с. 976 – 986

Обобщение атаки разделением по числу фотонов и ее эффективность при применении к протоколу квантовой криптографии на боковых частотах

Д. А. Кронберг[1)]

Математический институт им. В. А. Стеклова РАН, 119991 Москва, Россия

Поступила в редакцию 21 апреля 2025 г.
После переработки 6 мая 2025 г.
Принята к публикации 9 мая 2025 г.

Протоколы квантовой криптографии на когерентных состояниях представляют интерес из-за простоты практической реализации. Но доказательство стойкости против всех атак для таких протоколов может быть непростым из-за затухания в линии связи, которое может быть использовано перехватчиком. В этой работе строится атака на протокол квантовой криптографии на боковых частотах, которая обобщает атаку разделением по числу фотонов. Анализируется эффективность атаки, в том числе в условиях отсутствия у перехватчика квантовой памяти.

DOI: 10.31857/S0370274X25060193, EDN: OTJLEV

1. Введение. Квантовая криптография [1] позволяет распределять секретные ключи между удаленными пользователями. Важное преимущество квантовой криптографии – возможность строгого математического доказательства стойкости [2–5], что обеспечивает секретность распределяемых ключей.

Однако доказательство стойкости является сложным элементом квантового распределения ключей (КРК), и для ряда протоколов исследования продолжаются и в отсутствие доказательства стойкости против всех возможных атак. Напомним, что доказательства стойкости для первого известного протокола КРК BB84 появились на много лет позже самого протокола и экспериментов по его практической реализации. В связи с этим распространена ситуация, когда разработчики протокола КРК обосновывают его стойкость против ряда наиболее известных атак, высказывая тем самым предположение, что новые атаки не демонстрируют существенно большей эффективности.

Для практического применения КРК необходима стойкость в практических условиях. Так, генерация однофотонных импульсов на практике затруднена, и вместо них используются ослабленные когерентные состояния. Также неизбежно затухание в линиях связи при передаче ключа на большие расстояния. Важной атакой в условиях затухания является атака разделением по числу фотонов [6], которая в случае протокола BB84 при его реализации на когерентных состояниях приводит к уязвимости, т.е. к полной информации перехватчика о ключе при относительно небольшой длине линии связи.

Оригинальное определение атаки разделением по числу фотонов было дано на языке физических действий и включало в себя неразрушающее измерение числа фотонов в сигнальном импульсе, а также операцию отведения одного или нескольких фотонов в квантовую память перехватчика. Для протокола КРК на боковых частотах [7, 8] было показано, что измерение числа фотонов в одной моде уничтожает информацию о фазе [9], а измерение числа фотонов в двух модах, сохраняющее относительную фазу этих двух мод, уменьшает различимость состояний [8], поскольку протокол использует большое количество частотных мод.

В этой работе строится атака на протокол КРК на боковых частотах, которую можно рассматривать как обобщение атаки разделением по числу фотонов: она использует не отведение фотона из исходного пучка, а отображение исходного состояния на новое, содержащее состояния перехватчика с определенным количеством фотонов, удобные для последующего получения информации о ключе. Такая обобщенная атака уже не включает в себя неразрушающее измерение количества фотонов, и ad hoc методы защиты от атаки разделением по числу фотонов оказываются против нее неэффективными.

Показывается, что для практически используемых параметров протокола (8 состояний оптической мощности 0.025 фотона на импульс) на боковых ча-

1)e-mail: dmitry.kronberg@gmail.com

стотах уже на 20 км демонстрируется уязвимость: информация перехватчика оказывается больше, чем величина Холево [10] исходных состояний внутри каждого базиса, которая использовалась как верхняя оценка информации перехватчика. При длине линии связи 81 км перехватчику уже становится известен весь ключ, в то время как при использовании атаки безошибочным различением состояний критическая длина составляет 324 км. Также строится модификация атаки, не требующая наличия квантовой памяти у перехватчика, и показывается, что в этих условиях протокол демонстрирует уязвимость начиная с длины линии связи в 50 км.

При построении атаки предполагается работа оборудования легитимных пользователей в точном соответствии с теоретической моделью, и не используются методы "квантового хакинга" [11], позволяющие получать информацию за счет несовершенства оборудования легитимных пользователей.

Работа организована следующим образом. В разделе 2 приводятся краткие сведения о протоколе, из которых наибольшее значение имеют скалярные произведения отправляемых состояний. Раздел 3 посвящен основному атакующему преобразованию перехватчика, которое в случае успеха отображает сигналы на состояния, удобные для получения информации о ключе. В разделе 4 оценивается эффективность построенной атаки и приводится график зависимости информации перехватчика от длины линии связи. В разделе 5 рассматривается эффективность атаки при отсутствии квантовой памяти у перехватчика. Затем обсуждаются результаты.

2. Протокол квантовой криптографии на боковых частотах. В этом разделе будут даны краткие сведения о протоколе квантового распределения ключей на боковых частотах, достаточные для построения атакующей стратегии. Подробности физической реализации протокола даются в соответствующих работах [7, 8].

Протокол квантового распределения ключей на боковых частотах использует когерентные состояния, распределенные по $2S+1$ частотным модам, и кодирование происходит в набор относительных фаз, который зависит от основной фазы φ_i. Состояния протокола записываются как

$$|\psi_{\mu_A}(\varphi_i)\rangle = \bigotimes_{j=-S}^{S} |\alpha_j(\varphi_i)\rangle_j = \bigotimes_{j=-S}^{S} |\alpha_0 d_{0j}^S(\beta) e^{-i\varphi_i j}\rangle_j, \tag{1}$$

где оптическая мощность $\mu_A = \frac{|\alpha_0|^2 m^2}{2}$, m – индекс модуляции, $d_{0j}^S(\beta)$ – d-функция Вигнера.

Их скалярные произведения асимптотически при количестве частотных мод $S \to \infty$ равны

$$\langle\psi_{\mu_A}(\varphi_1)|\psi_{\mu_A}(\varphi_2)\rangle = e^{-\mu_A(1-\cos(\varphi_1-\varphi_2))}, \tag{2}$$

и в дальнейшем будет использоваться именно эта формула. Скалярные произведения состояний важны для построения атак, поскольку именно они определяют вероятность успеха того или иного постселективного преобразования [12, 13], используемого перехватчиком.

Конфигурация состояний схожа с конфигурацией протокола [14, 15] на геометрически однородных когерентных состояниях $|\alpha e^{i\varphi_i}\rangle$, поскольку фазы φ_i также образуют симметричный набор, принимая значения $\{2\pi i/N\}_{i=0}^{N-1}$. Но важное отличие заключается в том, что скалярные произведения (2) состояний протокола на боковых частотах являются неотрицательными вещественными числами и равны модулям скалярных произведений соответствующих симметричных когерентных состояний:

$$|\langle\sqrt{\mu_A}e^{i\varphi_1}|\sqrt{\mu_A}e^{i\varphi_2}\rangle| = e^{-\mu_A(1-\cos(\varphi_1-\varphi_2))} =$$

$$= \langle\psi_{\mu_A}(\varphi_1)|\psi_{\mu_A}(\varphi_2)\rangle.$$

Как и для протокола на геометрически однородных когерентных состояниях, N состояний разделены на $N/2$ пар (базисов). Такое разделение можно, вообще говоря, сделать по-разному (см. [15]), в этой работе будет рассматриваться разделение, предложенное в работах [7, 8], при котором фазовый сдвиг между состояниями каждого базиса равен π.

При распределении ключа передающая сторона (Алиса) случайным образом выбирает один из базисов, а также битовое значение (0, 1), и посылает соответствующий сигнал $|\psi(\varphi_i)\rangle$.

На стороне приемника (Боба) происходит выбор одного из N значений фазы φ_k и повторная модуляция, которая аналогична интерференции. Если базис приготовления и измерения совпадают (в противном случае посылки отбрасываются при последующем общении легитимных пользователей), то математически такое измерение можно описать измерением в ортонормированном базисе $\{|\psi_{\mu_A}(\varphi_k)\rangle,\ |\psi_{\mu_A}^{\perp}(\varphi_k)\rangle\}$. В этом случае сигнал, соответствующий $|\psi_{\mu_A}^{\perp}(\varphi_k)\rangle$, в отсутствие помех означает, что было приготовлено состояние $|\psi_{\mu_A}(\varphi_k+\pi)\rangle$, т.е. этот результат соответствует успешному безошибочному различению состояний пары Алисы $\{|\psi_{\mu_A}(\varphi_k)\rangle, |\psi_{\mu_A}(\varphi_k+\pi)\rangle\}$. Если Боб выбрал фазу $\varphi_k+\pi$, то, аналогично, элемент $|\psi_{\mu_A}^{\perp}(\varphi_k+\pi)\rangle$ измерения отвечает за безошибочное детектирование сигнала $|\psi_{\mu_A}(\varphi_k)\rangle$.

Это приводит к вероятности детектирования сигнала при совпадении базисов, равной с учетом затухания

$$P_{\text{det}} = \frac{1}{2}\left(1 - |\langle\psi_{\mu_A\eta}(\varphi_k)|\psi_{\mu_A\eta}(\varphi_k+\pi)\rangle|^2\right) = \\ = \frac{1}{2}(1 - e^{4\mu_A\eta}) \approx 2\mu_A\eta, \quad (3)$$

где η – показатель пропускания с учетом затухания в канале, оптической схеме и детекторах Боба. Коэффициент $1/2$ отвечает выбору фазы между φ_k и $\varphi_k+\pi$, а выражение в скобках – вероятность исхода в случае подходящего выбора фазы, что соответствует выражению из работы [16] для безошибочного различения двух состояний без дополнительной оптимизации [17].

После передачи и измерения состояний происходит согласование базисов, и посылки с не совпавшими базисами отбрасываются, в результате чего остается только доля $2/N$ от исходных посылок. После этого, как и для многих других протоколов квантовой криптографии, легитимные пользователи оценивают вероятность битовой ошибки, исправляют ошибки с помощью методов коррекции ошибок, и проводят усиление секретности: согласованное сжатие ключа, после которого информация перехватчика об итоговом ключе становится ничтожно малой.

Важной частью работ по протоколу является обоснование его криптографической стойкости. Для протокола на боковых частотах оно проведено для ряда известных атак. Для атак перехватчика с попыткой измерить состояние применяется граница Холево [10], ограничивающая информацию перехватчика величиной Холево исходных состояний внутри каждого базиса. Против атаки безошибочным различением состояний проводится оценка вероятности успеха этой операции, и накладывается требование, что вероятность детектирования исходных состояний должна быть не меньше этой вероятности. Следовательно, протокол применим на длинах линии связи, для которых это требование выполняется. Так, для оптической мощности $\mu_A = 0.025$ (см. (2)) и количества состояний 8 (эти данные впоследствии будут использоваться как характерные для практической реализации протокола[2)]), критическая длина составляет 324.9 км, что выше расстояний, на которых протокол применяется на практике.

Против атаки разделением по числу фотонов [6] приводится следующая аргументация. Атака разделением по числу фотонов использует неразрушающее измерение количества фотонов и отведение одного фотона в квантовую память перехватчика. Поскольку используются состояния с большим числом S частотных мод (см. (1)), показывается, что измерение количества фотонов в одной моде ведет к потере информации о фазе, следовательно, перехватчик не сможет извлечь информацию о ключе [9]. При измерении же в двух модах [8] информация о ключе уменьшается по сравнению с исходной, и оказывается небольшой, следовательно, атака не является эффективной.

Таким образом, можно сказать, что ad hoc методом защиты от атаки разделением по числу фотонов является использование большого количества частотных мод, что делает неэффективными операции проекции на одну или две моды, используемые в оригинальном описании атаки разделением по числу фотонов.

3. Преобразование перехватчика. В дальнейшем мы будем концентрироваться именно на атаке разделением по числу фотонов и строить ее существенное обобщение, которое, как будет показано, значительно эффективнее исходной версии. Обобщение заключается в том, что перехватчику достается не фотон из исходного пучка, а новый фотон, который дает много информации о ключе, когда раскрывается информация о базисе. Отобразить исходное состояние на этот фотон можно и без измерения числа фотонов в пучке.

Ключевую роль в принципиальной возможности и вероятности успеха того или иного преобразования квантовых состояний играют скалярные произведения состояний на входе или на выходе, в то время как физические характеристики, такие как количество фотонов или способ кодирования (фазовое или поляризационное), второстепенны, и влияют на вероятность успеха только опосредованно, через скалярные произведения. Поэтому в дальнейшем будем брать за основу набор скалярных произведений (2). Нам требуется построить преобразование

$$|\psi_{\mu_A}(\varphi_i)\rangle_A \to |\psi_i\rangle_B \otimes |\varepsilon_i\rangle_E, \quad (4)$$

которое в случае успеха переводит исходные состояния Алисы $|\psi(\varphi_i)\rangle_A$ в состояния Боба $|\psi_i\rangle_B$ и перехватчика (Евы) $|\varepsilon_i\rangle_E$, хорошо сбалансированное с точки зрения двух пожеланий:

- большая информация перехватчика о ключе, что означает хорошую различимость состояний Евы в каждом базисе;
- применимость атаки при небольших длинах линии связи, что означает большую вероятность

[2)] Автор выражает благодарность А. В. Козубову за предоставление данных о характерных параметрах протокола.

успеха преобразования и состояния Боба, ведущие к срабатыванию детектора.

Эти пожелания сложно реализовать одновременно. Одним экстремальным случаем является операция безошибочного различения состояний, при которой перехватчик знает всю информацию, но которая имеет очень малую вероятность успеха. Второй важный частный случай – атака светоделителем [7, 18] для канала с затуханием, которая реализуется с единичной вероятностью, но информация перехватчика в ней относительно невелика и принципиально ограничена величиной Холево исходных состояний каждого базиса в силу самой детерминированности операции, поскольку величина Холево монотонна относительно детерминированных квантовых каналов.

3.1. Полная информация перехватчика. Рассмотрим сначала концептуально более простой случай извлечения полной информации перехватчиком. Для протокола на боковых частотах предлагается преобразование, которое в случае успеха преобразует состояния следующим образом:

$$|\psi_{\mu_A}(\varphi_i)\rangle_A \to |\psi_{\mu_B}(\varphi_i)\rangle_B \otimes |\varepsilon(\varphi_i)\rangle_E^{\otimes 2}, \tag{5}$$

где $|\psi_{\mu_B}(\varphi_i)\rangle_B$ – состояния Боба, отличающиеся от состояний Алисы другой интенсивностью, а $|\varepsilon(\varphi_i)\rangle_E$ – состояния Евы, которые имеют вид

$$|\varepsilon(\varphi_i)\rangle_E = \cos\frac{\varphi_i}{2}|0\rangle + \sin\frac{\varphi_i}{2}|1\rangle, \tag{6}$$

т.е. Ева получает два идентичных фотона среди множества симметричных состояний в плоскости XZ сферы Блоха.

Принимающая сторона после применения атаки получает либо вакуумные состояния (в случае неудачи преобразования, что эквивалентно блокировке импульса), либо состояния, которые отличаются от исходных лишь интенсивностью, что не приводит к ошибкам, так как когерентные состояния преобразуются в оптоволокне самоподобным образом. Таким образом, вместо ожидаемого состояния $|\psi_{\mu'_A}(\varphi_i)\rangle_A$ интенсивности

$$\mu'_A = \mu_A 10^{-\frac{\delta l}{10}} \tag{7}$$

Боб получает смешанное состояние

$$p_{\text{succ}}|\psi_{\mu_B}(\varphi_i)\rangle_B\langle\psi_{\mu_B}(\varphi_i)| + (1-p_{\text{succ}})|0\rangle\langle 0|,$$

но его измерительная аппаратура не способна заметить между ними принципиальных отличий, так как фиксируется только факт срабатывания детектора, а измерения интенсивности состояний не происходит.

Скалярные произведения состояний перехватчика (6) равны

$$_E\langle\varepsilon(\varphi_i)|\varepsilon(\varphi_j)\rangle_E = \cos\left(\frac{\varphi_j-\varphi_i}{2}\right),$$

и они оказываются взаимно ортогональными для фазового сдвига π внутри базиса, который и предлагается разработчиками [7, 8]. Следовательно, перехватчик может получить полную информацию, сделав измерение после того, как легитимные пользователи раскроют базисы каждой посылки по открытому каналу. Следует отметить, что для других значений фазового сдвига внутри базиса предлагаемая атака становится менее эффективной и нуждается в дальнейшей модификации.

Вероятность успеха преобразования зависит от скалярных произведений состояний на входе и на выходе, а не от деталей их физической реализации. Эту вероятность удобно вычислять, пользуясь матрицами Грама состояний входа G_{in} и выхода G_{out}, которые, напомним, состоят из скалярных произведений соответствующих векторов, т.е.

$$G_{\text{in}} = \{_A\langle\psi_{\mu_A}(\varphi_i)|\psi_{\mu_A}(\varphi_j)\rangle_A\}_{i,j},$$

$$G_{\text{out}} = \{_B\langle\psi_{\mu_B}(\varphi_i)|\psi_{\mu_B}(\varphi_j)\rangle_B \cdot {}_E\langle\varepsilon(\varphi_i)|\varepsilon(\varphi_j)\rangle_E^2\}_{i,j} =$$

$$= G_B \circ G_E,$$

где $G_B \circ G_E$ – поэлементное (Адамарово) произведение матриц Боба и Евы соответственно.

Вероятность успеха p_{succ} отображения (5) не меньше [12, 13] максимума, при котором

$$G_{\text{in}} - p_{\text{succ}} G_{\text{out}} \geq 0, \tag{8}$$

что дает возможность несложным образом численно вычислить вероятность успеха для различных входных и выходных интенсивностей μ_A и μ_B. Состояния Евы фиксированы и не зависят от интенсивности.

Интуиция выбора в (5) состояний перехватчика вида (6) связана с оригинальной атакой разделением по числу фотонов, примененной к протоколам с симметричными когерентными состояниями. Когерентные состояния вида $|\alpha e^{i\theta}\rangle \otimes |\alpha e^{i(\varphi+\theta)}\rangle$ после общей фазовой рандомизации (соответствующей случайному выбору θ) распадаются в смесь состояний с определенным количеством фотонов (см. [19]), и можно неразрушающим образом измерить количество фотонов, после чего при должном их количестве отвести один фотон в состоянии $\frac{1}{\sqrt{2}}(|1\rangle\otimes|0\rangle + e^{i\varphi}|0\rangle\otimes|1\rangle)$ в квантовую память перехватчика, что и происходит в оригинальном сценарии атаки разделением по числу фотонов. Но можно заметить, что само по себе отображение

$$|\alpha e^{i\theta}\rangle \otimes |\alpha e^{i(\varphi_i+\theta)}\rangle \to \frac{1}{\sqrt{2}}(|1\rangle\otimes|0\rangle + e^{i\varphi_i}|0\rangle\otimes|1\rangle) \quad (9)$$

не обязательно требует фазовой рандомизации исходных состояний, и имеет вероятность успеха $1 - e^{-2|\alpha|^2}$, не зависящую от набора фаз $\{\varphi_i\}$. Примером физической реализации такого отображения как раз является усреднение по общей фазе θ, неразрушающее измерение числа фотонов и в случае их ненулевого количества (что и происходит с вероятностью $1 - e^{-2|\alpha|^2}$) отбор одного фотона. Однако именно такая реализация не является единственно возможной, и принципиальная возможность той или иной операции определяется лишь скалярными произведениями состояний на входе и выходе. Так, операция

$$|\alpha e^{i\varphi_i}\rangle \to \frac{1}{\sqrt{2}}\left(|1\rangle|0\rangle + e^{i\varphi_i}|0\rangle|1\rangle\right)\otimes|\alpha e^{i\varphi_i}\rangle \quad (10)$$

также возможна (при этом вероятность успеха будет зависеть от набора фаз $\{\varphi_i\}$), хотя она уже не сводится к неразрушающему измерению числа фотонов, и исходное состояние $|\alpha e^{i\varphi_i}\rangle$ сохраняется, что может, на первый взгляд, показаться физически контринтуитивным. Этот пример уже приводился в схожем контексте в работе [20]. Поэтому важно отметить разницу между отображением состояния на фотон и физической операцией по отведению фотона от пучка, которая является частным случаем такого отображения.

Преобразование (5) основано на преобразовании (10) и адаптировано под конфигурацию (2), в частности, в (5) использованы два фотона в плоскости XZ для вещественных положительных скалярных произведений, что позволяет увеличить вероятность успеха.

Предложенное преобразование ведет к эффективной атаке из-за того, что это преобразование не предполагает получения лишней информации, что позволяет экономить такой ресурс, как вероятность успеха. В частности, перехватчику не требуется на момент атаки знать посланное состояние, поскольку информацию о базисе он получит в дальнейшем. Поэтому построенное преобразование имеет значительно более высокую вероятность успеха, чем операция безошибочного различения состояний. Так, для $N = 8$ состояний интенсивности $\mu_A = 0.1$, если принять выходную интенсивность $\mu_B = 0.05$ (вдвое меньшая выходная интенсивность – типичное значение, реально оптимальное значение подбирается для максимизации эффективности атаки на данной длине линии связи и может быть несколько другим), то вероятность успеха отображения (5) превосходит вероятность успеха безошибочного различения состояний примерно в 48 тысяч раз. А при $\mu_A = 0.025$, $\mu_B = 0.0125$ соотношение вероятностей успеха превосходит 3 миллиона. Таким образом, операция безошибочного различения всех состояний является очень "дорогой" в смысле вероятности успеха, и отказ от этой операции позволяет построить атаку намного более высокой эффективности, которая по-прежнему дает перехватчику полную информацию о ключе.

3.2. Неполная информация перехватчика. Можно рассмотреть более общий случай, когда состояния Евы в каждом базисе неортогональны. Такой подход позволяет увеличить вероятность успеха p_{succ} преобразования перехватчика, что означает применимость атаки на более широком диапазоне длин линии связи. Рассмотрим вместо (5) преобразование

$$|\psi_{\mu_A}(\varphi_i)\rangle_A \to |\psi_{\mu_B}(\varphi_i)\rangle_B \otimes |\varepsilon(\varphi_i)\rangle_E, \quad (11)$$

с состояниями Евы вида

$$|\varepsilon(\varphi_i)\rangle_E = |\varepsilon(\varphi_i)^{(1)}\rangle_E \otimes |\varepsilon(\varphi_i)^{(2)}\rangle_E, \quad (12)$$

где

$$|\varepsilon(\varphi_i)^{(1)}\rangle_E = \cos\frac{\eta}{2}|0\rangle + e^{i\varphi_i}\sin\frac{\eta}{2}|1\rangle,$$
$$|\varepsilon(\varphi_i)^{(2)}\rangle_E = \cos\frac{\eta}{2}|0\rangle + e^{-i\varphi_i}\sin\frac{\eta}{2}|1\rangle,$$

тогда скалярные произведения состояний Евы равны

$$\begin{aligned} {}_E\langle\varepsilon_i|\varepsilon_j\rangle_E &= {}_E\langle\varepsilon_i^{(1)}|\varepsilon_j^{(1)}\rangle_E \cdot {}_E\langle\varepsilon_i^{(2)}|\varepsilon_j^{(2)}\rangle_E = \\ &= (\cos^2\frac{\eta}{2} + \sin^2\frac{\eta}{2}e^{-i\Delta_{ij}})(\cos^2\frac{\eta}{2} + \sin^2\frac{\eta}{2}e^{i\Delta_{ij}}) = \end{aligned} \quad (13)$$

$$= 1 - \frac{\sin^2\eta}{2}\left(1 - \cos\Delta_{ij}\right), \quad (14)$$

где $\Delta_{ij} = \varphi_j - \varphi_i$. Немного отличающиеся (в знаке фазы) состояния первого и второго фотона используются для того, чтобы сделать общее скалярное произведение вещественным.

При $\eta = 0$ состояния Евы совпадают, и она не получает информации, а при $\eta = \frac{\pi}{2}$ соответствующие состояния лежат в плоскости XY сферы Блоха, и ортогональны для фазового сдвига π внутри базиса, что эквивалентно преобразованию (5).

Информация Евы дается величиной Холево ее состояний фиксированного базиса, и она при фазовом сдвиге π между состояниями внутри базиса равна

$$I_{AE} = \chi_E = h_2\left(\frac{\sin^2\eta}{2}\right), \quad (15)$$

где $h_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ – бинарная энтропия.

На рисунке 1 показан график зависимости вероятности успеха от угла η между состояниями Евы, также показана величина Холево для исходных состояний одного базиса (пунктирной линией) и для состояний Евы (штриховой линией). Видно, что уже при небольших значениях угла Ева получает больше информации, чем величина Холево исходных состояний, которая является верхней оценкой информации Евы при атаках без постселективных преобразований.

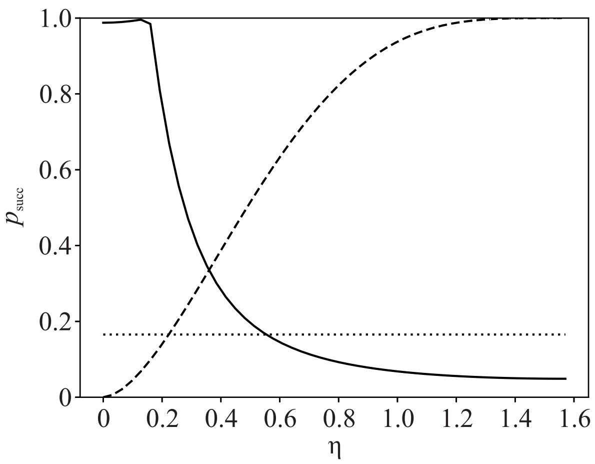

Рис. 1. Сплошной линией показан график зависимости вероятности успеха преобразования (11) от параметра атаки η, а штриховой линией – информация перехватчика (15). Пунктирной линией показана величина Холево исходных состояний Алисы внутри базиса. Исходная интенсивность $\mu_A = 0.025$, число состояний $N = 8$

Таким образом, построено эффективное преобразование, с одной стороны, имеющее высокую вероятность успеха (особенно по сравнению с операцией безошибочного различения состояний), и при этом дающее большую информацию перехватчику, которая для большого диапазона значений параметра η превосходит величину Холево исходных состояний.

4. Эффективность атаки. Теперь рассчитаем эффективность атаки на основе построенного преобразования для произвольной длины линии связи. Для каждого фиксированного значения длины линии связи есть ожидаемая вероятность срабатывания детектора (3) с учетом ослабленной интенсивности (7), и требуется, чтобы вероятность срабатывания детектора в условиях атаки для состояний $\{|\psi_{\mu_B}(\varphi_i)\rangle_B\}_i$, получаемых принимающей стороной, была не меньше, что ведет к требованию

$$p_{\rm succ} P_{\rm det}(\mu_B) = P_{\rm det}\left(\mu_A 10^{-\frac{\delta l}{10}}\right). \qquad (16)$$

В частности, это означает, что для небольших длин линии связи Ева не должна выставлять параметры преобразования так, чтобы вероятность успеха была слишком малой, а также она не может посылать Бобу состояния слишком малой интенсивности μ_B.

Таким образом, Еве требуется с учетом ограничения (16) найти параметры атаки (угол η и интенсивность $\mu_B \geq 0$ состояний на принимающей стороне), дающие ей наибольшую информацию, т.е. наибольшее значение угла η.

Для фиксированного значения η несложно численно найти наилучшее значение μ_B, дающее наибольшую вероятность детектирования. В самом деле, при нулевой интенсивности $\mu_B = 0$ вероятность детектирования также нулевая, а при слишком высоких значениях вероятность успеха становится очень малой, так как большая интенсивность выходных состояний фактически означает, что перехватчик проводит безошибочное различение состояний, а это преобразование имеет очень низкую вероятность успеха для практически важных значениях параметров протокола. Поэтому оптимальное значение $\mu_B^{\rm opt}$ обычно меньше исходной интенсивности μ_A.

Следовательно, задача сводится к поиску максимально возможного значения η для данного расстояния l между легитимными пользователями. Если такое значение η достигает $\pi/2$, то для данной длины линии связи протокол теряет стойкость, поскольку перехватчик получает полную информацию. Минимальная длина линии связи, на которой это происходит, является критической длиной линии связи для данного значения исходной интенсивности μ_A.

На рисунке 2 показан график зависимости критической длины линии связи, начиная с которой Ева знает всю информацию, от исходной интенсивности μ_A. Так, для $\mu_A = 0.025$ критическая длина линии связи составляет 80.77 км, для $\mu_A = 0.1$ – это 52.51 км, а для $\mu_A = 0.2$ это 39.64 км.

На рисунке 3 сплошной линией показано, как информация перехватчика зависит от длины линии связи для исходной интенсивности $\mu_A = 0.025$, для тех значений длины линии связи, которые меньше критической величины. Пунктирной линией показа величина Холево исходных состояний Алисы внутри базиса, и видно, что оценка информации перехватчика через величину Холево перестает выполняться уже на расстоянии около 20 км, что говорит об эффективности построенной атаки.

5. Модификация атаки при отсутствии квантовой памяти. Традиционно в квантовой криптографии не рассматриваются какие-либо огра-

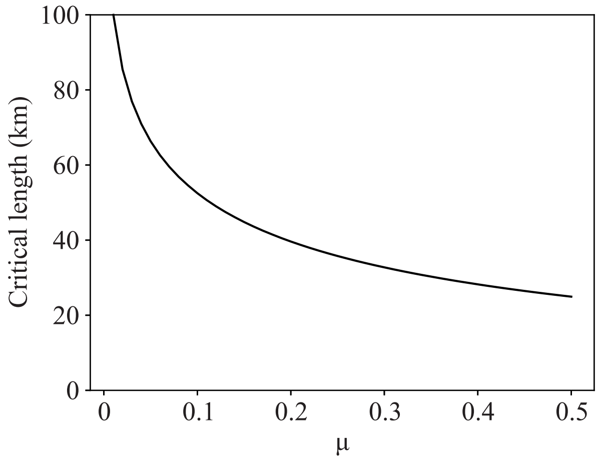

Рис. 2. График зависимости критической длины линии связи, начиная с которой перехватчик знает весь ключ, от исходной интенсивности μ_A. Число состояний $N = 8$

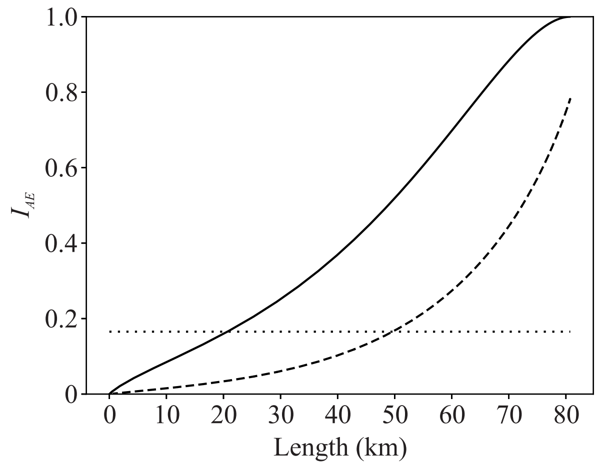

Рис. 3. Сплошной линией показан график зависимости величины Холево состояний перехватчика от длины линии связи при исходной интенсивности $\mu_A = 0.025$. Пунктирной линией показана величина Холево исходных состояний Алисы (в обоих случаях имеются в виду состояния, соответствующие одному базису). Штриховой линией показан график для информации перехватчика (20) при измерении в отсутствие квантовой памяти. Число состояний $N = 8$

ничения на технические возможности перехватчика. Но возможен подход, при котором технологический уровень перехватчика предполагается ограниченным, и важным частным случаем является вполне разумное предположение о том, что перехватчик не может хранить состояния в квантовой памяти сколь угодно долго. Это предположение имеет смысл в том числе потому, что даже если произойдет существенный прогресс в разработке квантовой памяти, то распределенные до этого квантовые ключи не потеряют стойкости, поскольку были распределены в условиях отсутствия квантовой памяти. Это выгодно отличает предположение об отсутствии квантовой памяти от вычислительных предположений классической криптографии: если эти предположения окажутся неверными (например, перехватчик научится быстро факторизовывать большие числа), схемы классической криптографии теряют стойкость, и уже распределенные ключи могут перестать быть секретными.

Для квантовой криптографии отсутствие квантовой памяти у перехватчика означает необходимость измерять состояния сразу после их получения, без возможности дождаться объявления базисов. В то же время перехватчик может воспользоваться информацией, которая раскрывается при объявлении базисов. Также перехватчик лишен возможности измерять состояния коллективным образом, извлекая из них всю информацию, доступную по границе Холево: даже если перехватчик может совершать коллективные измерения, граница Холево достигается только при знании кодовых слов (см. [21], а также [22] для примера применения этого факта в квантовой криптографии), и легитимные стороны могут задержать их объявление [1]. Поэтому фактически перехватчик ограничен эффективностью индивидуальных измерений.

Опишем измерения перехватчика над его состояниями (12), а также посчитаем соответствующую информацию перехватчика.

Может показаться, что если Еве следует узнать бит ключа, то Ева стоит перед задачей различения смешанных состояний $\{\rho_0, \rho_1\}$, соответствующих значениям бита 0 и 1 (т.е. ρ_0 является смесью 4 состояний, соответствующих биту 0 при 4 возможных базисах, а ρ_1 – смесью остальных 4 состояний, соответствующих биту 1). Но эффективнее рассмотреть измерение, которое учитывает, что в распоряжении Евы два фотона, и она измеряет разные наблюдаемые для них, а впоследствии использует информацию о базисах, раскрываемую легитимными сторонами.

Рассмотрим случай $N = 8$ состояний, разбитых на 4 базиса с фазовым сдвигом π внутри базиса. На рисунке 4 показана плоскость XY сферы Блоха и проекции состояний одного фотона Евы на эту плоскость. Базисы b состояний $|\varepsilon_k^{(b)}\rangle$ обозначены верхним индексом в скобках, а значения ключа k – нижним индексом (соответствие с индексом i в (12) очевидно из картинки). Штриховой линией показаны предлагаемые базисы измерения для каждого фотона, которые лежат в плоскости XY и задаются выражениями

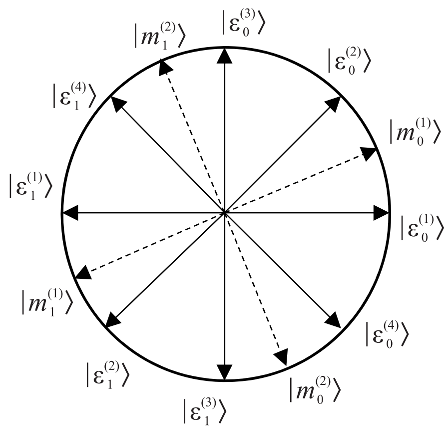

Рис. 4. Однофотонные состояния перехватчика при $N = 8$, показаны состояния $|\varepsilon(\varphi_i)^{(1)}\rangle_E$ из (12) в проекции на ось XY с явным указанием базисов (верхний индекс, в скобках) и битов ключа (нижний индекс). Также штриховой линией показаны два измерения в отсутствие квантовой памяти: в базисе (1) и в базисе (2)

$$\begin{aligned}
|m_0^{(1)}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{8}}|1\rangle\right),\\
|m_1^{(1)}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{9\pi}{8}}|1\rangle\right),\\
|m_0^{(2)}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{5\pi}{8}}|1\rangle\right),\\
|m_1^{(2)}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{13\pi}{8}}|1\rangle\right).
\end{aligned} \tag{17}$$

Из рисунка 4 можно видеть, что базис измерения $\{|m_0^{(1)}\rangle, |m_1^{(1)}\rangle\}$ хорошо подходит для различения состояний первого (1) и второго (2) базисов, в то время как базис измерения $\{|m_0^{(2)}\rangle, |m_1^{(2)}\rangle\}$ подходит для различения состояний третьего (3) и четвертого (4) базисов. Можно явно посчитать вероятности исходов для измерения состояний базиса (1) в базисе $\{|m_0^{(1)}\rangle, |m_1^{(1)}\rangle\}$:

$$\begin{aligned}
p_0 &= |\langle m_0^{(1)}|\varepsilon_0^{(1)}\rangle|^2 = |\langle m_1^{(1)}|\varepsilon_1^{(1)}\rangle|^2 =\\
&= \left|\frac{1}{\sqrt{2}}\left(\cos\frac{\eta}{2} + e^{i\frac{\pi}{8}}\sin\frac{\eta}{2}\right)\right|^2,\\
p_1 &= |\langle m_1^{(1)}|\varepsilon_0^{(1)}\rangle|^2 = |\langle m_0^{(1)}|\varepsilon_1^{(1)}\rangle|^2 =\\
&= 1 - \left|\frac{1}{\sqrt{2}}\left(\cos\frac{\eta}{2} + e^{i\frac{\pi}{8}}\sin\frac{\eta}{2}\right)\right|^2,
\end{aligned} \tag{18}$$

и симметричным образом для измерения состояний базиса (2), вероятности будут равны либо p_0, либо p_1. Такие же вероятности будут для исходов, соответствующих измерению $\{|m_0^{(2)}\rangle, |m_1^{(2)}\rangle\}$ и базисам (3) и (4). Отметим, что на рис. 4 показаны базисы для измерения элементов первого фотона из двух в (12), а для второго фотона в базисе измерения фаза в показателе экспоненты должна быть изменена на противоположную, поскольку в (12) у него тоже противоположная фаза, что приведет в точности к тем же вероятностям исходов.

Также отметим, что формально измерение в базисе $\{|m_0^{(2)}\rangle, |m_1^{(2)}\rangle\}$ не дает информации о ключе k, поскольку результат 0 более вероятен для значения ключа 0 в базисе (4) или значения ключа 1 в базисе (3); аналогично, результат 1 может свидетельствовать о вероятном значении бита ключа 1 в базисе (4) или 0 в базисе (3), поэтому может создаться впечатление, что измерение бесполезно. Но важно, что когда легитимные стороны объявят базисы, перехватчик сможет обработать результат измерения и понять, какой бит ключа наиболее вероятен. Поэтому переобозначение битов ключа в рамках одного базиса не усложняет перехватчику задачу получения информации.

Если фотон был приготовлен в базисе (1) или в базисе (2), то измерение в базисе $\{|m_0^{(2)}\rangle, |m_1^{(2)}\rangle\}$ приводит к вероятностям исходов

$$\begin{aligned}
q_0 &= |\langle m_0^{(2)}|\varepsilon_0^{(1)}\rangle|^2 = |\langle m_1^{(2)}|\varepsilon_1^{(1)}\rangle|^2 =\\
&= \left|\frac{1}{\sqrt{2}}\left(\cos\frac{\eta}{2} + e^{i\frac{3\pi}{8}}\sin\frac{\eta}{2}\right)\right|^2,\\
q_1 &= |\langle m_1^{(2)}|\varepsilon_0^{(1)}\rangle|^2 = |\langle m_0^{(2)}|\varepsilon_1^{(1)}\rangle|^2 =\\
&= 1 - \left|\frac{1}{\sqrt{2}}\left(\cos\frac{\eta}{2} + e^{i\frac{3\pi}{8}}\sin\frac{\eta}{2}\right)\right|^2,
\end{aligned} \tag{19}$$

и они ближе к равномерному распределению вероятностей, следовательно это измерение дает мало информации о соответствующем бите ключа.

В простом варианте атаки можно принимать во внимание только “удачные” вероятности p_0 и p_1, т.е. после объявления базисов, Ева игнорирует результаты одного из измерений, и использует лишь результаты измерения, подходящего для данного базиса, что дает ей информацию $1 - h_2(p_0)$. Но Ева может получить больше информации, если также примет во внимание результаты измерения и в “плохо подходящем” базисе. Поэтому рассмотрим один из базисов и учтем все 4 возможных результата измерения. Для каждого измеряемого состояния вероятности исходов образуют распределение вероятностей $P_{Y|X} = \{p_0q_0,\ p_0q_1,\ p_1q_0,\ p_1q_1\}$. В среднем же распределение вероятностей исходов, если учесть, что на вход были поданы два фотона, с учетом знания базиса записывается как $P_Y = \{\frac{1}{2}(p_0q_0 + p_1q_1),\ \frac{1}{2}(p_0q_1 + p_1q_0),\ \frac{1}{2}(p_0q_1 + p_1q_0),\ \frac{1}{2}(p_0q_0 + p_1q_1)\}$, и для информации перехватчика после объявления базисов имеем

$$I_{AE} = H(Y) - H(Y \mid X) = \\ = 1 + h_2(p_0 q_0 + p_1 q_1) - h_2(p_0) - h_2(q_1), \qquad (20)$$

что превосходит величину $1 - h_2(p_0)$, которая соответствует игнорированию одного из исходов измерения.

На рисунке 3 штриховой линией показана информация перехватчика согласно (20), то есть при измерении в отсутствие квантовой памяти. Видно, что уже начиная примерно с 50 км она становится выше величины Холево исходных состояний. На рисунке 5 штриховой линией показана доля ключа, которую перехватчик знает при применении данной атаки в отсутствие квантовой памяти. Начиная с 50 км, перехватчик и в отсутствие квантовой памяти получает частичную информацию о ключе, что соответствует потере стойкости и свидетельствует о некорректной оценке информации перехватчика. Также для сравнения приведена доля известного ключа при применении атаки с использованием квантовой памяти из предыдущего раздела.

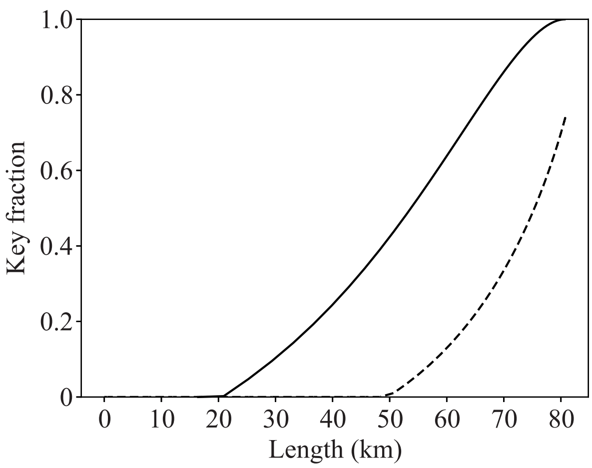

Рис. 5. Доля ключа, известная перехватчику при применении описанной атаки. Сплошной линией показаны данные при наличии квантовой памяти у Евы, штриховой линией – при отсутствии. Число состояний $N = 8$, исходная интенсивность 0.025

Отметим, что штриховые линии на рис. 3 и 5 не следует экстраполировать, несмотря их на резкий рост в правой части. Правые точки рисунков соответствует значению $\eta = \pi/2$, но дальнейшее увеличение параметра η не увеличивает информацию перехватчика. Поэтому обобщение атаки без квантовой памяти на более протяженные линии связи между легитимными сторонами нетривиально, и нельзя утверждать, что на 90 км перехватчику в отсутствие квантовой памяти будет известна существенно большая доля ключа, чем на 80 км.

6. Заключение и обсуждение результатов. В работе была построена атакующая стратегия для протокола квантовой криптографии на боковых частотах, которая для актуальных параметров протокола дает перехватчику частичную информацию о ключе уже начиная с 20 км, а полную информацию – примерно при 80 км.

Предложенная стратегия подслушивания использует отображение состояния на два однофотонных состояния перехватчика, которые несут много информации о ключе, когда базис приготовления состояний оказывается известен. В этом атака очень схожа с атакой разделением по числу фотонов (PNS-атакой), но существенным физическим отличием является то, что перехватчику достается не фотон из исходного импульса, а новый фотон, скоррелированный с сигналом. Поэтому построенную атаку можно назвать обобщением атаки разделением по числу фотонов. Важно подчеркнуть, что для подсушивания не обязательно проводить именно те физические действия, которые были указаны в оригинальной статье про PNS-атаку, поэтому ad hoc методы защиты от этих действий не обязательно эффективны. Если целью является доказательство стойкости против всех атак перехватчика, то возможны любые атаки, не запрещенные законами Природы, и физическая их реализация не играет большой роли.

Принципиальное отличие представленной здесь атаки от атаки безошибочным различением состояний – более экономное расходование перехватчиком ресурса затухания в линии связи. Задача различения всех состояний – очень сложная задача, и имеет малую вероятность успеха, в то время как представленная в данной работе атака не пробует различать все состояния. Для полной информации перехватчику достаточно получить ортогональные состояния для каждого базиса, что и происходит в предложенной атаке. Также было рассмотрено обобщение, при котором перехватчик получает не полностью ортогональные состояния, что делает атаку применимой на относительно небольших расстояниях между легитимными пользователями.

Был также рассмотрен случай отсутствия долговременной квантовой памяти у перехватчика. В этих условиях перехватчик вынужден совершать измерение сразу после взаимодействия с сигналами, еще не зная базис, что затрудняет извлечение информации. Но при построенной атаке и при отсутствии квантовой памяти у перехватчика, как было показано, протокол также демонстрирует уязвимость, но уже начиная с длины линии связи в 50 км. Это говорит об эффективности предложенного преобразования. Построение более эффективных атак без использования долговременной квантовой памяти, однако, представляется нетривиальной задачей.

Причина уязвимости протокола на боковых частотах против предложенной атаки состоит в использовании величины Холево для оценки информации перехватчика. Действительно, теорема Холево очень важна для квантовой теории информации, но она не применима в условиях постселекции [23, 24], а в квантовой криптографии при затухании перехватчик может провести постселекцию, отбросив посылки с неудачными результатами атакующего преобразования. Примером атаки с постселекцией является атака безошибочным различением состояний, но важно, что это не единственная подобная атака, поэтому методы борьбы с безошибочным различением состояний не обязательно помогают бороться с другими атаками с постселекцией.

Предложенная атака хорошо применима к случаю фазового сдвига π между состояниями внутри каждого базиса, что соответствует предложению разработчиков протокола, но теряет свою эффективность, если легитимные пользователи используют другой фазовой сдвиг. Соответственно, применение другого фазового сдвига можно формально считать ad hoc методом борьбы с представленной атакой, но важно, что поднятые в данной работе проблемы несовершенной оценки информации перехватчика в протоколе на боковых частотах остаются.

Можно также формализовать обобщение атаки для других фазовых сдвигов внутри базиса, см. [24] для более подробного описания задачи. Для получения полной информации Еве требуется сделать ортогональными свои состояния внутри каждого базиса, что меняет матрицу Грама G_E перехватчика, в то время как матрица Грама G_B принимающей стороны не претерпевает изменений. Для этой задачи, несмотря на простую формулировку, не обязательно существует простое решение. В целом поиск состояний перехватчика и принимающей стороны является нетривиальной задачей. В данной работе использовалась физическая интуиция, основанная на оригинальной атаке разделением по числу фотонов, и предложены состояния перехватчика в плоскости XZ сферы Блоха (при получении полной информации) или в плоскости XY (для более общего случая получения перехватчиком неполной информации). В общем же случае состояния должны быть принципиально физически реализуемы, что соответствует неотрицательной матрице Грама, но не обязательно имеют столь простой вид. Таким образом, дальнейшая работа по сокращению разрыва между верхними и нижними оценками стойкости актуальна для протокола КРК на боковых частотах.

В статье не рассматривался вопрос сложности построенного преобразования перехватчика, если реализовывать его с помощью квантовых вентилей, таких как “контролируемое НЕ” (CNOT) и вентиль Тоффоли. Вопрос построения квантовой схемы атаки также может быть темой будущих исследований, см. смежные результаты для другой атаки в работах [25, 26].

Автор выражает благодарность А. А. Гайдашу и А. В. Козубову за обсуждение протокола КРК на боковых частотах, а также Т. Р. Клевцову за проверку некоторых вычислений.

Финансирование работы. Исследование выполнено за счет гранта Российского научного фонда # 24-11-00145, https://rscf.ru/project/24-11-00145/.

Конфликт интересов. Автор данной работы заявляет, что у него нет конфликта интересов.

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**(1), 145 (2002).
2. P. W. Shor and J. Preskill, ‘Phys. Rev. Lett. **85**(2), 441 (2000).
3. R. Renner, N. Gisin, and B. Kraus, Physical Review A – Atomic, Molecular, and Optical Physics **72**(1), 012332 (2005).
4. C. Portmann and R. Renner, Rev. Mod. Phys. **94**(2), 025008 (2022).
5. R. Renner and R. Wolf, AIAA J. **61**(5), 1895 (2023).
6. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**(6), 1330 (2000).
7. G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, and D. B. Horoshko, Opt. Express **26**(9), 11292 (2018).
8. A. Gaidash, G. Miroshnichenko, and A. Kozubov, J. Opt. Soc. Am. B **39**(2), 577 (2022).
9. V. Chistiakov, A. Kozubov, A. Gaidash, A. Gleim, and G. Miroshnichenko, Opt. Express **27**(25), 36551 (2019).
10. А. С. Холево, Проблемы передачи информации **9**(3), 3 (1973).
11. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**(10), 686 (2010).
12. A. Chefles, R. Jozsa, and A. Winter, Int. J. Quantum Inf. **2**(01), 11 (2004).
13. D. A. Kronberg, Phys. Rev. A **106**(4), 042447 (2022).
14. С. Н. Молотков, Письма в ЖЭТФ **101**(8), 637 (2015).
15. K. S. Kravtsov and S. N. Molotkov, Phys. Rev. A **100**(4), 042329 (2019).

16. C. H. Bennett, Phys. Rev. Lett. **68**(21), 3121 (1992).
17. A. Peres, Phys. Lett. A **128**(1–2), 19 (1988).
18. A. N. Klimov, S. P. Kulik, S. N. Molotkov, and T. A. Potapova, Laser Phys. Lett. **14**(3), 035201 (2017).
19. A. Acin, N. Gisin, and V. Scarani, Phys. Rev. A **69**(1), 012309 (2004).
20. A. S. Avanesov and D. A. Kronberg, Phys. Rev. A **111**(4), 042601 (2025).
21. M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, Phys. Rev. A **58**(1), 146 (1998).
22. V. A. Pastushenko and D. A. Kronberg, Entropy **25**(6), 956 (2023).
23. N. R. Kenbaev and D. A. Kronberg, Phys. Rev. A **105**(1), 012609 (2022).
24. Д. А. Кронберг, А. С. Холево, Вопросы кибербезопасности **3**(67), 110 (2025).
25. Д. А. Кронберг, Теоретическая и математическая физика **214**(1), 140 (2023).
26. Д. А. Кронберг, Математические вопросы криптографии **15**(2), 91 (2024).