НОВЫЕ ПОДХОДЫ К ОЦЕНКАМ ИНФОРМАЦИИ ПЕРЕХВАТЧИКА В ПРОБЛЕМАХ КВАНТОВОЙ КРИПТОГРАФИИ

Кронберг Д. А.[1], Холево А. С.[2]

DOI: 10.21681/2311-3456-2025-3-110-117

Цель работы: *провести обзор новых аспектов вопроса извлечения информации из ансамблей квантовых состояний, продиктованных практическими задачами квантовой криптографии.*

Метод исследования: *использованы математические методы квантовой теории информации, в частности, процедура безошибочного различения квантовых состояний.*

Результаты исследования: *в работе проведен анализ литературы по теме оценок информации перехватчика в квантовой криптографии при наличии затухания в линии связи, в том числе в отсутствие квантовой памяти. Указаны особенности применения фундаментального информационного ограничения к количеству информации перехватчика в условиях затухания, продемонстрированы угрозы применения «ad hoc» методов борьбы с атакой безошибочным различением состояний. Сформулированы задачи нахождения эффективного преобразования перехватчика, использующего постселекцию, а также проведения измерения в условиях отсутствия квантовой памяти у перехватчика.*

Научная новизна: *научная новизна заключается в интеграции разрозненных подходов к задаче оценки информации перехватчика в квантовой криптографии и борьбы с атаками в условиях затухания. Обзор описывает особенности применения информационного ограничения к вопросам квантовой криптографии и формализует задачи, стоящие перед перехватчиком в условиях затухания.*

Ключевые слова: *квантовая криптография, квантовая теория информации, квантовые преобразования с постселекцией.*

1. Введение

Отличительное свойство квантовой информации, содержащейся в ансамбле квантовых состояний, – невозможность ее копирования [1]. Другое важное свойство – запрет на получение полной информации из ансамбля неортогональных чистых квантовых состояний, вытекающий из ограничения на количество классической информации, извлекаемой из ансамбля квантовых состояний [2]. Эти особенности квантовой информации лежат в основе протоколов передачи квантовой информации, препятствующих ее перехвату.

Уникальной чертой квантовой криптографии является принципиальная возможность математического доказательства безусловной стойкости протокола, в отличие от классической криптографии, где стойкость доказывается лишь против ряда известных атак. При этом представляют интерес как нижние, так и верхние оценки стойкости протоколов квантового распределения ключей.

Часто действия перехватчика в квантовой криптографии сводят к попыткам провести наилучшее измерение над ансамблем передаваемых состояний. Однако в данном обзоре мы хотим привлечь внимание к двум другим ресурсам перехватчика, важным для стойкости практических систем квантового распределения ключей:

1. Линии связи имеют затухание, и легитимные пользователи ожидают, что не все посылки будут зафиксированы на принимающей стороне. Это позволяет перехватчику проводить квантовые преобразования с постселекцией, при которых он иногда извлекает много информации, а иногда ему это не удается, и у перехватчика есть возможность блокировать посылки в последнем случае, что не будет обнаружено легитимными пользователями.
2. Легитимные пользователи общаются между собой, при этом они раскрывают некоторую информацию о ключе или об особенностях приготовлениях сигнала.

В статье будет рассмотрено то, как указанные ресурсы могут быть использованы перехватчиком и как их наличие изменяет формулировку и решение некоторых задач квантовой теории информации. Мы концентрируемся на случае большого затухания в линии связи, и поэтому рассматриваем атаки с нулевой ошибкой, значимые при большом затухании. В рамках данной работы мы не рассматриваем

1 Кронберг Д. А., кандидат физико-математических наук, старший научный сотрудник, Математический институт им. В. А. Стеклова Российской академии наук, г. Москва, Россия. ORCID: https://orcid.org/0000-0003-1652-6376. Scopus Author ID: 26648798700. E-mail: dmitry.kronberg@gmail.com

2 Холево Александр Семенович, доктор физико-математических наук, профессор, академик РАН, заведующий отделом, главный научный сотрудник, Математический институт им. В. А. Стеклова Российской академии наук, г. Москва, Россия. ORCID: https://orcid.org/0000-0001-5699-521X. Scopus Author ID: 6603727683. E-mail: holevo@mi-ras.ru

атаки, которым сопутствует внесение ошибки перехватчиком, актуальные при малых длинах линии связи; этот случай существенно сложнее из-за появления смешанных состояний.

2. Информация в условиях постселекции

Информационное ограничение [2] гласит, что при любом квантовом измерении из ансамбля квантовых состояний $\{p_j, \rho_j\}$ нельзя извлечь больше информации, чем $\mathcal{X}$-величина этого ансамбля

$$\mathcal{X} = H(\sum_j p_j \rho_j) - \sum_j p_j H(\rho_j),$$

где $H(\rho) = -Tr\rho \log \rho$ энтропия фон Неймана оператора плотности ρ. Мы хотим здесь подчеркнуть, что этот результат применим в условиях, когда учитываются все исходы измерения. Однако в квантовой криптографии в условиях сильного затухания не все сигналы доходят до принимающей стороны. Поэтому представляет интерес ситуация, при которой некоторые исходы измерения можно отбросить, заблокировав соответствующие сигналы, так что они не будут вносить вклад в распределяемый ключ. В такой ситуации $\mathcal{X}$-величина исходного ансамбля уже не может использоваться как верхняя оценка информации перехватчика.

Рассмотрим этот вопрос подробнее.

Самым простым примером нарушения информационного ограничения в условиях постселекции является так называемое безошибочное различение состояний [3, 4, 5]. В простейшем варианте при таком измерении двух неортогональных состояний $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ можно добиться в случае успеха их безошибочного различения. Но это достигается ценой возможности неудачи, которая имеет вероятность $|\langle\varphi_0|\varphi_1\rangle|$ (в несимметричном случае эту вероятность можно уменьшить для одного состояния, но тогда для другого состояния она увеличится; такая асимметрия может представлять интерес при различных исходных вероятностях состояний и максимизации средней вероятности успеха). Информационное ограничение выполняется в среднем в смысле математического ожидания классической информации, если учесть нулевую информацию в случае неудачи различения, но не выполняется, если рассматривать только успешные исходы.

На основе безошибочного различения состояний можно рассмотреть атаку в квантовой криптографии, при которой перехватчик проводит попытку безошибочного различения для каждого сигнала, и в случае неудачи блокирует посылку, а в случае удачи отправляет ее на принимающую сторону (в последнем случае перехватчик может применить дополнительные методы увеличения вероятности обнаружения посылки, такие как усиление сигнала). При такой атаке некоторые сигналы из-за блокировки не будут достигать принимающей стороны, но при передаче данных на большие расстояния легитимные пользователи и в отсутствие перехватчика ожидают потери существенной части сигналов. Поэтому начиная с некоторой критической длины линии связи атака безошибочным различением состояний оказывается возможной, то есть перехватчик не вносит больше затухания, чем ожидается легитимными сторонами. При этом перехватчик обладает полной информацией о ключе, поскольку посылал на принимающую сторону только те сигналы, о которых он получил полную информацию.

Возникает естественное предложение рассматривать безошибочное различение состояний как отдельную операцию, принципиально отличную от других атак в квантовой криптографии, и защищаться именно от нее. Возможные методы защиты [6] ставят своей целью уменьшить вероятность успеха безошибочного различения состояний, что приводит к увеличению критической длины линии связи, или вовсе сделать безошибочное различение невозможным. Они включают увеличение количества состояний [7, 8, 9], для которых в симметричном случае существуют верхние оценки вероятности успеха безошибочного различения [10], или линейную зависимость состояний [11]. Однако даже если безошибочное различение состояний невозможно, эффект превышения информационного ограничения за счет постселекции может иметь место [12].

Приведем простой пример ансамбля состояний, для которых невозможна операция безошибочного различения, но имеет место эффект превышения информационного ограничения. Рассмотрим двумерную систему (кубит) и два смешанных равновероятных квантовых состояния $\{\rho_0, \rho_1\}$. Для таких состояний невозможно безошибочное различение [13], поскольку их носители совпадают, и не существует элемента квантовой наблюдаемой, для которого соответствующая вероятность исхода была бы равна нулю для одного состояния и не равна нулю для другого состояния.

Рассмотрим, однако, разложение состояний $\{\rho_0, \rho_1\}$ по двум чистым состояниям

$$\begin{aligned} \rho_0 &= (1 - \alpha_0)\,|\varphi_0\rangle\langle\varphi_0| + \alpha_0\,|\varphi_1\rangle\langle\varphi_1|, \\ \rho_1 &= \alpha_1|\varphi_0\rangle\langle\varphi_0| + (1 - \alpha_1)\,|\varphi_1\rangle\langle\varphi_1|, \end{aligned} \qquad (1)$$

которое соответствует разложению по крайним точкам хорды на сфере Блоха. Для неортогональных состояний $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ возможно безошибочное различение, которое точно определит состояние в случае успеха. Если сопоставить успешным исходам безошибочного различения ортогональные состояния $\{|e_0\rangle, |e_1\rangle\}$, то в случае успеха имеем отображение

$$\rho_0 \longrightarrow \sigma_0 = (1-\alpha_0)\,|e_0\rangle\langle e_0| + \alpha_0\,|e_1\rangle\langle e_1|,$$
$$\rho_1 \longrightarrow \sigma_1 = \alpha_1\,|e_0\rangle\langle e_0| + (1-\alpha_1)\,|e_1\rangle\langle e_1|, \quad (2)$$

для которого коэффициенты $\{\alpha_0,\alpha_1\}$ не изменяются в случае равных вероятностей успеха для обоих состояний $\{|\varphi_0\rangle, |\varphi_1\rangle\}$.

Теперь можно построить квантовый канал, который отображает состояния $\{\sigma_0, \sigma_1\}$ в состояния $\{\rho_0, \rho_1\}$:

$$\Phi[\rho] = |\varphi_0\rangle\langle e_0|\rho|e_0\rangle\langle\varphi_0| + |\varphi_1\rangle\langle e_1|\rho|e_1\rangle\langle\varphi_0|. \quad (3)$$

Это канал с операторами Крауса $\{K_0 = |\varphi_0\rangle\langle e_0|, K_1 = |\varphi_1\rangle\langle e_1|\}$.

Следовательно, в силу свойства монотонности, $\mathcal{X}$-величина состояний $\{\sigma_0, \sigma_1\}$ строго превосходит $\mathcal{X}$-величину состояний $\{\rho_0, \rho_1\}$, если последние не коммутируют (то есть в случае, когда состояния $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ неортогональны). Таким образом, $\mathcal{X}$-величина монотонна относительно детерминированных преобразований, но не обязательно монотонна относительно постселективных. В силу ортогональности $|e_0\rangle$ и $|e_1\rangle$ $\mathcal{X}$-величина состояний $\{\sigma_0, \sigma_1\}$ в точности равна информации, которая извлекается из этих состояний при измерении в базисе $\{|e_0\rangle, |e_1\rangle\}$, и только что было показано, что эта информация больше $\mathcal{X}$-величины исходных состояний $\{\rho_0, \rho_1\}$, несмотря на то что для этих состояний невозможно безошибочное различение. Таким образом, эффект увеличения информации при постселективных измерениях, в том числе превышение $\mathcal{X}$-величины, это более общее явление, чем безошибочное различение состояний.

Эти рассуждения можно обобщить на два произвольных некоммутирующих квантовых состояния: для них также будет явное постселективное измерение, которое дает больше информации, чем $\mathcal{X}$-величина. Но для трех состояний это, вообще говоря, уже не так, и существует пример [12], когда $\mathcal{X}$-величина исходных состояний больше, чем информация, которую можно извлечь с помощью индивидуальных постселективных измерений: это одно из проявлений того эффекта, что коллективные измерения над состояниями эффективнее, чем индивидуальные [14, 15]. Информационное ограничение включает возможность коллективных измерений, а индивидуальные постселективные действия такой возможностью не обладают.

3. Постселективные действия перехватчика

В предыдущем разделе в качестве примера рассматривались постселективные измерения квантовых состояний, на выходе которых появляются классические (т.е. коммутирующие) сигналы, которые можно описать распределениями вероятностей. Но множество преобразований квантовых состояний шире, и в этом разделе будут рассмотрены постселективные преобразования с квантовыми состояниями на выходе. Они актуальны для построения успешных стратегий перехвата, использующих затухание.

Упомянутая выше атака безошибочным различением состояний, при которой перехватчик (Ева) пытается получить полную информацию о сигнале, передаваемом от легитимного участника (Алисы) другому легитимному участнику (Бобу), и блокирует состояния в случае неудачи, не очень эффективна для современных протоколов квантовой криптографии, поскольку они используют явные методы защиты от этой атаки, и вероятность успешного безошибочного различения состояний оказывается очень малой, что означает применимость атаки только на очень больших длинах линии связи.

Более эффективной атакой с нулевой ошибкой является атака, при которой Ева в случае успеха получает квантовое состояние, скоррелированное с сигналом Алисы, и после объявления базисов может совершить над ними нужное измерение. Будем стремиться построить такую атаку, но сначала рассмотрим задачу нахождения вероятности успеха довольно общего постселективного преобразования состояний. Преобразование, при котором состояния Алисы переходят в состояния Боба и Евы, можно описать так:

$$|\varphi_i\rangle_A \longrightarrow |\psi_i\rangle_B \otimes |\varepsilon_i\rangle_E, \quad (4)$$

где $\{|\varphi_i\rangle_A\}_i$ – набор состояний Алисы на входе, а $\{|\psi_i\rangle_B\}_i$ и $\{|\varepsilon_i\rangle_E\}_i$ – наборы состояний Боба и Евы соответственно.

Если учитывать состояния и в случае неудачи, то итоговое преобразование будет отображать состояния Алисы в сцепленные состояния на выходе:

$$|\varphi_i\rangle_A \longrightarrow \sqrt{p_{succ}}\,|\psi_i\rangle_B \otimes |\varepsilon_i\rangle_E \otimes |s\rangle_D + \sqrt{1-p_{succ}}\,|f_i\rangle_{BE} \otimes |f\rangle_D, \quad (5)$$

где p_{succ} – вероятность успеха, а $|s\rangle_D$ и $|f\rangle_D$ – взаимно ортогональные флаги успеха или неудачи во вспомогательном пространстве H_D. Их можно измерить, чтобы получить данные об успехе или неудаче преобразования. В случае успеха в пространстве $H_B \otimes H_E$ получается результат преобразования (4).

Условие изометричности отображения (5), которое отвечает его принципиальной реализуемости [15], записывается как

$$\langle\varphi_i|\varphi_j\rangle \longrightarrow p_{succ}\langle\psi_i|\psi_j\rangle\langle\varepsilon_i|\varepsilon_j\rangle + (1-p_{succ})\langle f_i|f_j\rangle \quad (6)$$

для всех возможных индексов $\{i, j\}$, что можно записать в матричной форме:

$$G_A = p_{succ}\,G_B \circ G_E + (1-p_{succ})\,G_F, \quad (7)$$

где G_A, G_B и G_E – матрицы Грама соответственно Алисы, Боба и Евы, то есть матрицы, составленные

из скалярных произведений, а $G_B \circ G_E$ – поэлементное (адамарово) произведение матриц. Матрица G_F соответствует скалярным произведениям в случае неудачи.

Состояния $\{|f_i\rangle_{BE}\}_{ij}$ в случае неудачи не столь важны, но требуется, чтобы этот набор состояний существовал, и это означает неотрицательную определенность соответствующей матрицы G_F. Поэтому для вероятности успеха p_{succ} преобразования (4) имеем условие (подробности, в том числе для более общего случая различных вероятностей успеха см. в [16, 17])

$$G_A - p_{succ}\, G_B \circ G_E \geq 0, \tag{8}$$

или следующую верхнюю оценку на вероятность успеха [17]

$$p_{succ} = \max_{G_E \geq 0} 2^{-D_{max}(G_B \circ G_E \| G_A)}, \tag{9}$$

где

$$D_{\max}(\rho\|\sigma) = -\log_2 \max\{\lambda : \sigma - \lambda\rho \geq 0\},$$

– max – относительная энтропия [18].

Теперь можно рассмотреть математическую задачу построения эффективной атаки в условиях затухания. Как уже отмечалось выше, это, с одной стороны, атака, дающая перехватчику много информации при малых вносимых помехах, а с другой – соответствующее преобразование (4) должно иметь большую вероятность успеха, чтобы атака была применима при небольших расстояниях между легитимными сторонами. Для этого нужно подобрать подходящие состояния для принимающей стороны $\{|\psi_i\rangle_B\}_i$ и для перехватчика $\{|\varepsilon_i\rangle_E\}_i$.

Состояния принимающей стороны должны вносить мало ошибок, давать высокую вероятность детектирования сигналов и при этом позволять построить преобразование (4) с высокой вероятностью успеха. С учетом этих требований их поиск может быть нетривиальной задачей, связанной с конкретными протоколами квантовой криптографии и используемой в них аппаратурой для детектирования состояний. Ниже мы рассмотрим важный частный случай когерентных состояний, а пока просто фиксируем состояния $\{|\psi_i\rangle_B\}_i$, тогда будет зафиксирована и матрица G_B, и требуется подобрать матрицу G_E, что проще формализовать математически.

Рассмотрим сначала случай получения Евой полной информации. Тогда для каждого базиса протокола соответствующие состояния Евы должны быть взаимно ортогональны. Если протокол использует N состояний, разделенных на $N/2$ базисов, то это означает, что матрица G_E содержит N нулей в позициях, соответствующих скалярным произведениям состояний одного базиса. Тогда остальные внедиагональные элементы матрицы G_E требуется заполнять числами, которые минимизируют величину $D_{\max}(G_B \circ G_E \| G_A)$, с учетом требования неотрицательности G_E. Это формализует построение эффективной атаки в квантовой криптографии, дающей полную информацию перехватчику для данных состояний $\{|\psi_i\rangle_B\}_i$ принимающей стороны, при этом мы не утверждаем оптимальность построенной атаки.

В более общем случае перехватчик может не стремиться получить полную информацию о ключе, что может быть невозможно для данной величины затухания. Тогда задачей перехватчика является поиск матрицы G_E, для которой его информация $I_{AE} \in (0,1]$ принимает фиксированное значение, и при этом максимизируется вероятность успеха преобразования. Рассмотрим случай симметричной атаки, при которой информация перехватчика в каждом базисе совпадает. Параметром атаки является модуль скалярного произведения $s \in [0,1)$ состояний каждого базиса, от которого информация перехватчика, равная $\mathcal{X}$-величине двух состояний базиса, зависит как

$$I_{AE} = h_2\left(\frac{1-s}{2}\right), \tag{10}$$

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

Это означает, что соответствующие N элементов матрицы G_E в общем случае заполняются уже не нулями (как это происходило в случае требования полной информации перехватчика), а числами, равными по модулю s, и задачей является поиск остальных элементов матрицы G_E, которые бы максимизировали вероятность успеха преобразования (9) с учетом требования $G_E \geq 0$.

Для состояний Боба $\{|\psi_i\rangle_B\}_i$ уже нельзя учитывать лишь скалярные произведения и соответствующие матрицы Грама, поскольку сам вид состояний ограничен физическими характеристиками измеряемой аппаратуры: эти состояния не должны приводить к ошибке, либо, в более общем случае, должны давать небольшую ошибку. Поэтому математическая формализация имеет смысл именно для задачи поиска матрицы G_E.

Важным частным случаем является использование легитимными сторонами чистых когерентных состояний, которые характеризуются в том числе исходной интенсивностью μ_A. Тогда на стороне Боба логично использовать состояния того же вида, но с интенсивностью μ_B, которая является параметром атаки для оптимизации. Если обозначить вероятность детектирования состояния в зависимости от интенсивности как $P_{det}(\mu)$ (конкретная формула зависит от протокола), то условием применимости атаки для длины линии связи l является

$$p_{succ}\, P_{det}(\mu_B) = P_{det}(\mu_A\, 10^{-\frac{\delta l}{10}}), \tag{11}$$

где слева стоит вероятность детектирования сигналов при применении атаки, а справа – в отсутствие

атаки, но с затуханием в линии связи длины l с коэффициентом пропускания δ дБ/км. Отметим, что в этом случае также не утверждается оптимальность построенного преобразования.

Условие вида (11) можно привести и в других ситуациях для других параметров, таких как количество фотонов. В общем случае в задачу вмешивается физика возможных состояний Боба и ошибка в зависимости от оптической схемы на принимающей стороне.

Таким образом, главная практическая задача перехватчика в квантовой криптографии состоит в получении максимальной информации при данной длине линии связи l. Для решения этой задачи нужно найти как подходящие состояния Боба, что сопряжено с протоколом и аппаратурой, так и состояния Евы. Если состояния Боба фиксированы, то нахождение состояний Евы можно представить как математическую задачу поиска значений элементов матрицы Грама G_E, которые максимизируют вероятность (9) с учетом заполнения ряда элементов G_E фиксированными числами, равными по модулю s (параметр атаки, отвечающий различимости состояний внутри базиса, от которого информация перехватчика зависит согласно (10)).

4. Измерения с учетом дополнительной информации

Традиционно в квантовой криптографии предполагается, что перехватчик никак не ограничен технически. Но возможны подходы, при которых предполагается очень высокий, но все же не безграничный технологический уровень перехватчика [19]. Одним из предположений в этой модели является отсутствие у перехватчика долговременной квантовой памяти [20]. Это означает, прежде всего, что перехватчик не может совершить измерение, дождавшись объявления базисов, а должен делать это раньше, еще не зная базис, так что измерение не может зависеть от базиса.

В самом деле, легитимные пользователи могут просто задержать объявление базисов на некоторое время [21], скажем, на сутки, а предположение, что перехватчик может в течение суток хранить квантовые состояния в идеальной квантовой памяти это предположение о чрезвычайно высоком уровне перехватчика, которое может быть избыточным для существующих коммерческих приложений квантовой криптографии.

Рассмотрим перехватчика, который обладает состояниями $\{|\varepsilon_i\rangle_E\}_i$, что соответствует атаке (4) из предыдущего раздела (про некоторые отличия от этой атаки будет сказано ниже). Состояния с учетом битов ключа и базиса можно записать как

$$|\Psi_i\rangle = |k_i\rangle_K|b_i\rangle_B|\varepsilon_i\rangle_E, \tag{12}$$

где k_i – значение бита ключа, b_i – базис в данной позиции, $|\varepsilon_i\rangle$ – измеряемое состояние. Например, для протокола BB84, использующего 4 состояния $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, разделенные на базисы Z (это состояния $\{|0\rangle,|1\rangle\}$) и X (состояния $\{|+\rangle,|-\rangle\}$), исходные состояния Алисы в этих обозначениях

$$\begin{aligned}
|\Phi_0\rangle &= |0\rangle_K|Z\rangle_B|0\rangle_A,\\
|\Phi_1\rangle &= |1\rangle_K|Z\rangle_B|1\rangle_A,\\
|\Phi_2\rangle &= |0\rangle_K|X\rangle_B|+\rangle_A,\\
|\Phi_3\rangle &= |1\rangle_K|X\rangle_B|-\rangle_A,
\end{aligned} \tag{13}$$

а состояния перехватчика после взаимодействия

$$\begin{aligned}
|\Psi_0\rangle &= |0\rangle_K|Z\rangle_B|\varepsilon_0\rangle_E,\\
|\Psi_1\rangle &= |1\rangle_K|Z\rangle_B|\varepsilon_1\rangle_E,\\
|\Psi_2\rangle &= |0\rangle_K|X\rangle_B|\varepsilon_2\rangle_E,\\
|\Psi_3\rangle &= |1\rangle_K|X\rangle_B|\varepsilon_3\rangle_E.
\end{aligned} \tag{14}$$

Важно, что перехватчик, совершая измерение над подсистемой E, стремится получить информацию о ключе K, но при этом он знает, что получит информацию B о базисе, и эта информация может увеличить информацию о ключе. Но измерение при этом не может зависеть от подсистемы B, поскольку на момент измерения доступа к этой подсистеме нет. Следовательно, стоит задача подбора наблюдаемой над E, которая бы максимизировала информацию

$$I(K;E|B), \tag{15}$$

но которая сама бы не зависела от B.

Эта задача отличается от максимизации $I(K;E)$ без учета B; последняя в приведенном примере является задачей получения максимума информации при измерении смешанных состояний

$$\begin{aligned}
\rho_0 &= \frac{1}{2}\left(|\varepsilon_0\rangle\langle\varepsilon_0| + |\varepsilon_2\rangle\langle\varepsilon_2|\right),\\
\rho_1 &= \frac{1}{2}\left(|\varepsilon_1\rangle\langle\varepsilon_1| + |\varepsilon_3\rangle\langle\varepsilon_3|\right),
\end{aligned} \tag{16}$$

Также задача отличается и от максимизации $I(K;E)$ в условиях знания B, поскольку в последнем случае речь уже идет о различении либо состояний $\{|\varepsilon_0\rangle, |\varepsilon_1\rangle\}$ (в базисе Z), либо состояний $\{|\varepsilon_2\rangle, |\varepsilon_3\rangle\}$ (в базисе X).

В качестве примера рассмотрим ситуацию, которая может возникнуть при атаке разделением по числу фотонов [22] на реализацию протокола BB84 на когерентных состояниях. Пусть исходная посылка содержала 3 фотона, и перехватчик отвел два фотона себе, а один фотон направил на принимающую сторону. Состояния Евы (14) в таком случае принимают вид

$$\begin{aligned}
|\Psi_0\rangle &= |0\rangle_K|Z\rangle_B|0\rangle_E^{\otimes 2},\\
|\Psi_1\rangle &= |1\rangle_K|Z\rangle_B|1\rangle_E^{\otimes 2},\\
|\Psi_2\rangle &= |0\rangle_K|X\rangle_B|+\rangle_E^{\otimes 2},\\
|\Psi_3\rangle &= |1\rangle_K|X\rangle_B|-\rangle_E^{\otimes 2}.
\end{aligned} \tag{17}$$

Если обращаться с этими состояниями как в задаче Хелстрома о различении двух смешанных состояний [23], то при различении состояний

$$\rho_0 = \frac{1}{2}\ (|00\rangle\langle 00| + |{+}{+}\rangle\langle{+}{+}|),$$
$$\rho_1 = \frac{1}{2}\ (|11\rangle\langle 11|+|{-}{-}\rangle\langle{-}{-}|) \qquad (18)$$

неизбежна ошибка. В то же время, если учесть, что базис потом станет известен, то полную информацию о ключе дает наблюдаемая

$$M_{0Z} = |0\rangle\langle 0| \otimes I,$$
$$M_{1Z} = |1\rangle\langle 1| \otimes I,$$
$$M_{0X} = I \otimes |+\rangle\langle +|, \qquad (19)$$
$$M_{1X} = I \otimes |-\rangle\langle -|,$$

соответствующая измерению первого фотона в базисе Z, а второго фотона в базисе X. После объявления базиса Ева получает информацию о том, в каком базисе исход соответствует биту ключа, а в каком базисе он неинформативен.

Этот пример показывает, что оптимальная по Хелстрому наблюдаемая не обязательно оптимальна в смысле максимизации величины (15).

Отметим, что мы использовали преобразование вида (4) и выходные состояния Евы $\{|\varepsilon_i\rangle_E\}_i$, как и в предыдущем разделе. Но следует иметь в виду, что если раньше эффективность этого преобразования понималась в том смысле, что нужно добиться наибольшей $\mathcal{X}$-величины внутри базиса, то в условиях отсутствия квантовой памяти у перехватчика преобразование вида (4) или его обобщение должны строиться из расчета на увеличение величины (15), что может привести к другому виду эффективного преобразования.

Говоря об отсутствии квантовой памяти у перехватчика, мы в первую очередь рассматривали его незнание базиса на момент измерения. Но есть еще одно, менее тривиальное, следствие отсутствия квантовой памяти, а именно то, что перехватчику уже не имеет смысла совершать коллективные измерения. Известно, что коллективные измерения дают больше информации, чем индивидуальные [14, 15, 24], именно поэтому в квантовой криптографии для учета информации перехватчика используется $\mathcal{X}$-величина, а не достижимая информация при индивидуальных измерениях. Но для эффективного применения коллективных измерений необходимо знание набора кодовых слов для проектирования больших кортежей состояний. Если же перехватчик не знает набор кодовых слов, он уже не может извлечь выгоду из коллективных измерений, даже если кратковременная квантовая память позволяет ему собрать несколько состояний и провести над ними коллективное измерение (см. теорему 2 в [24]). Поэтому в условиях отсутствия квантовой памяти для оценки информации перехватчика следует использовать информацию, достижимую при индивидуальных измерениях.

5. Заключение

В этой статье рассматривалась задача извлечения информации из ансамбля квантовых состояний и был дан обзор новых подходов к этой задаче, которые становятся актуальными в практических условиях квантовой криптографии.

При квантовом распределении ключей на большие расстояния неизбежно затухание в линии связи, и легитимные пользователи предполагают возможность детектирования на принимающей стороне не всех отправленных сигналов. В этих условиях перехватчик может блокировать часть посылок, и эта блокировка не будет замечена. Возможность отбирать часть посылок для отправки на принимающую сторону (т.е. проводить постселекцию) – важный ресурс перехватчика в квантовой криптографии, и в разделе 2 рассматривалось, как этот ресурс влияет на ограничения информации, извлекаемой из ансамбля квантовых состояний. Фундаментальное информационное ограничение выполняется в смысле математического ожидания информации, когда все исходы (в том числе неудачные для перехватчика) были приняты во внимание, но уже не выполняется, если был произведен отбор удачных результатов. Приведен пример, когда информация после постселекции оказывается больше, чем $\mathcal{X}$-величина исходных состояний. Было продемонстрировано, что указанное явление более общее, чем хорошо известное в квантовой теории информации безошибочное различение состояний, так как в приведенном примере оно невозможно. Следовательно, те меры, которые в протоколах квантовой криптографии используются для противодействия атаке безошибочным различением состояний, не обязательно эффективны против общей атаки с использованием постселекции. Важным выводом является то, что $\mathcal{X}$-величина исходных состояний не является верхней оценкой информации перехватчика при использовании им постселекции в условиях затухания.

Раздел 3 посвящен вопросу эффективного использования затухания перехватчиком. Было построено постселективное преобразование, которое дает перехватчику много информации о ключе в случае успеха. При этом становится актуальным использование еще одного важного ресурса, а именно информации, которую легитимные стороны раскрывают при объявлении базисов. Перехватчик не может построить преобразование с учетом этой информации, потому что не обладает ей на момент совершения преобразования, но строит преобразование с учетом дальнейшего получения этой информации.

Поэтому задача перехватчика состоит в том, чтобы сделать состояния каждого базиса как можно более различимыми, в то время как соотношения между векторами разных базисов не играют роли и могут быть любыми. В терминах матриц Грама это означает заполнение матрицы G_E рядом элементов с фиксированным модулем, и остальных позиций числами, при которых вероятность успеха оказывается максимальной. Эффективные состояния Боба при этом сложнее формализовать, так как их вид продиктован в том числе физическими аспектами протокола квантовой криптографии.

В разделе 4 была рассмотрена задача построения эффективного измерения, с учетом последующего объявления информации о базисах. Эта задача актуальна при отсутствии у перехватчика долговременной квантовой памяти, что в настоящее время является одной из допустимых моделей в квантовой криптографии. В этом случае оптимальной наблюдаемой уже не обязательно будет наблюдаемая оптимального различения двух смешанных квантовых состояний, соответствующих разным битам ключа. Это связано с тем, что перехватчик получает информацию о базисе приготовления состояний, и может улучшить результаты измерения в соответствии с этой информацией.

Темой будущих исследований может быть как решение задач, рассмотренных в настоящей статье, так и исследование ситуации с внесением перехватчиком ошибки при построении атаки, что означает дальнейшее сближение верхних и нижних оценок стойкости в квантовой криптографии.

Исследование выполнено за счет гранта Российского научного фонда № 24-11-00145, https://rscf.ru/project/24-11-00145/

Литература

1. W. K. Wootters, W. H. Zurek, A single quantum cannot be cloned. Nature, 299(5886). 802-803 (1982).
2. Холево А. С. Некоторые оценки для количества информации, передаваемого квантовым каналом связи // Проблемы передачи информации, 9(3), 3–11 (1973).
3. D. Ivanovic, How to differentiate between non-orthogonal states. Physics Letters A. 123(6), 257–259 (1987).
4. D. Dieks, Overlap and distinguishability of quantum states. Physics Letters A, 126(5-6), 303–306 (1988).
5. Peres, How to differentiate between non-orthogonal states. Physics Letters A. 128(1-2), 19 (1988).
6. Gaidash, A. Kozubov, G. Miroshnichenko, Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems. JOSA B, 36(3), B16-B19 (2019).
7. Молотков С. Н. О секретности волоконных систем квантовой криптографии без контроля интенсивности квазиоднофотонных когерентных состояний // Письма в ЖЭТФ, 101(8), 637–643 (2015).
8. K. S. Kravtsov, S. N. Molotkov, Practical quantum key distribution with geometrically uniform states. Physical Review A, 100(4), 042329 (2019). https://arxiv.org/pdf/1906.10978.
9. Gaidash, G. Miroshnichenko, A. Kozubov, Subcarrier wave quantum key distribution with leaky and flawed devices. JOSA B, 39(2), 577–585 (2022). DOI:10.1364/JOSAB.439776.
10. Chefles, S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states. Physics letters A, 250(4–6), 223–229 (1998). https://arxiv.org/pdf/quant-ph/9807023.
11. Gaidash, A. Kozubov, G. Miroshnichenko, Overcoming unambiguous state discrimination attack with the help of Schrödinger Cat decoy states. arXiv preprint arXiv:1808.08145 (2018).
12. N. R. Kenbaev, D. A. Kronberg, Quantum postselective measurements: Sufficient condition for overcoming the Holevo bound and the role of max-relative entropy. Physical Review A, 105(1), 012609 (2022). DOI:10.1103/PhysRevA.105.012609.
13. U. Herzog, J. A. Bergou, Optimum unambiguous discrimination of two mixed quantum states. Physical Review A, 71(5), 050301 (2005).
14. Холево А. С. Квантовые теоремы кодирования // Успехи математических наук, 53(6) (324), 193–230 (1998).
15. Холево А. С. Математические основы квантовой информатики // Лекц. курсы НОЦ, 30, МИАН, М., 2018, 118 с.
16. Chefles, R. Jozsa, A. Winter, On the existence of physical transformations between sets of quantum states. International Journal of Quantum Information, 2(01), 11–21 (2004).
17. D. A. Kronberg, Success probability for postselective transformations of pure quantum states. Physical Review A, 106(4), 042447 (2022). DOI:10.1103/PhysRevA.106.042447.
18. N. Datta, Min- and max-relative entropies and a new entanglement monotone. IEEE Transactions on Information Theory, 55(6), 2816–2826 (2009).
19. B. Damgård, S. Fehr, L. Salvail, C. Schaffner, Cryptography in the bounded-quantum-storage model. SIAM Journal on Computing, 37(6), 1865–1890 (2008).
20. H. Bechmann-Pasquinucci, Eavesdropping without quantum memory. Physical Review A Atomic, Molecular, and Optical Physics, 73(4), 044305 (2006).
21. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. Reviews of modern physics, 74(1), 145 (2002).
22. G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, Limitations on practical quantum cryptography. Physical Review Letters, 85(6), 1330 (2000).
23. К. Хелстром, Квантовая теория проверки гипотез и оценивания. Мир, 1979.
24. M. Sasaki, K. Kato, M. Izutsu, O. Hirota, Quantum channels showing superadditivity in classical capacity. Physical Review A, 58(1), 146 (1998).

NEW APPROACHES TO EAVESDROPPER INFORMATION BOUNDS IN QUANTUM CRYPTOGRAPHY PROBLEMS

Kronberg D. A.[3], Holevo A. S.[4]

Keywords: *quantum cryptography, quantum information theory, postselective quantum transformations.*

Purpose of work *is to review new aspects for the task of information extraction from ensembles of quantum states, dictated by practical tasks of quantum cryptography.*

Research methods: *mathematical methods of quantum information theory, in particular, unambiguous discrimination of quantum states.*

Results of the study: *the paper analyzes the literature on the topic of eavesdropper information bounds in quantum cryptography in the presence of channel attenuation, including in the absence of quantum memory. The features of application of the fundamental information bound to the eavesdropper information in the presence of attenuation, the threats of application of ad hoc countermeasures for unambiguous state discrimination attack are demonstrated. The problems of finding an effective postselective eavesdropping transformation, as well as measurement in the absence of eavesdropper's quantum memory, are formulated.*

Scientific novelty: *the scientific novelty consists in the integration of disparate approaches to the problem of eavesdropper information bounds in quantum cryptography and resisting attacks in case of lossy channel. The review describes the peculiarities of applying information bound to quantum cryptography problems and formalizes the challenges facing the eavesdropper under attenuation conditions.*

References

1. W. K. Wootters, W. H. Zurek, A single quantum cannot be cloned. Nature, 299(5886). 802-803 (1982).
2. Holevo A. S. Nekotorye ocenki dlja kolichestva informacii, peredavaemogo kvantovym kanalom svjazi // Problemy peredachi informacii, 9(3), 3–11 (1973).
3. D. Ivanovic, How to differentiate between non-orthogonal states. Physics Letters A. 123(6), 257–259 (1987).
4. D. Dieks, Overlap and distinguishability of quantum states. Physics Letters A, 126(5-6), 303–306 (1988).
5. Peres, How to differentiate between non-orthogonal states. Physics Letters A. 128(1-2), 19 (1988).
6. Gaidash, A. Kozubov, G. Miroshnichenko, Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems. JOSA B, 36(3), B16-B19 (2019).
7. Molotkov S. N. O sekretnosti volokonnyh sistem kvantovoj kriptografii bez kontrolja intensivnosti kvaziodnofotonnyh kogerentnyh sostojanij // Pis'ma v ZhJeTF, 101(8), 637–643 (2015).
8. K. S. Kravtsov, S. N. Molotkov, Practical quantum key distribution with geometrically uniform states. Physical Review A, 100(4), 042329 (2019). https://arxiv.org/pdf/1906.10978
9. Gaidash, G. Miroshnichenko, A. Kozubov, Subcarrier wave quantum key distribution with leaky and flawed devices. JOSA B, 39(2), 577–585 (2022). DOI:10.1364/JOSAB.439776.
10. Chefles, S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states. Physics letters A, 250(4–6), 223–229 (1998). https://arxiv.org/pdf/quant-ph/9807023.
11. Gaidash, A. Kozubov, G. Miroshnichenko, Overcoming unambiguous state discrimination attack with the help of Schrödinger Cat decoy states. arXiv preprint arXiv:1808.08145 (2018).
12. N. R. Kenbaev, D. A. Kronberg, Quantum postselective measurements: Sufficient condition for overcoming the Holevo bound and the role of max- relative entropy. Physical Review A, 105(1), 012609 (2022). DOI:10.1103/PhysRevA.105.012609.
13. U. Herzog, J. A. Bergou, Optimum unambiguous discrimination of two mixed quantum states. Physical Review A, 71(5), 050301 (2005).
14. Holevo A. S. Kvantovye teoremy kodirovanija // Uspehi matematicheskih nauk, 53(6) (324), 193–230 (1998).
15. Holevo A. S. Matematicheskie osnovy kvantovoj informatiki // Lekc. kursy NOC, 30, MIAN, M., 2018, 118 s.
16. Chefles, R. Jozsa, A. Winter, On the existence of physical transformations between sets of quantum states. International Journal of Quantum Information, 2(01), 11–21 (2004).
17. D. A. Kronberg, Success probability for postselective transformations of pure quantum states. Physical Review A, 106(4), 042447 (2022). DOI:10.1103/PhysRevA.106.042447.
18. N. Datta, Min- and max-relative entropies and a new entanglement monotone. IEEE Transactions on Information Theory, 55(6), 2816–2826 (2009).
19. B. Damgård, S. Fehr, L. Salvail, C. Schaffner, Cryptography in the bounded-quantum-storage model. SIAM Journal on Computing, 37(6), 1865–1890 (2008).
20. H. Bechmann-Pasquinucci, Eavesdropping without quantum memory. Physical Review A Atomic, Molecular, and Optical Physics, 73(4), 044305 (2006).
21. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. Reviews of modern physics, 74(1), 145 (2002).
22. G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, Limitations on practical quantum cryptography. Physical Review Letters, 85(6), 1330 (2000).
23. K. Helstrom, Kvantovaja teorija proverki gipotez i ocenivanija. Mir, 1979.
24. M. Sasaki, K. Kato, M. Izutsu, O. Hirota, Quantum channels showing superadditivity in classical capacity. Physical Review A, 58(1), 146 (1998).

3 Kronberg D.A., PhD in Physics and Mathematics, Senior Researcher, Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow, Russia. ORCID: https://orcid.org/0000-0003-1652-6376. Scopus Author ID: 26648798700. E-mail: dmitry.kronberg@gmail.com

4 Kholevo Alexander Semenovich, Doctor of Physical and Mathematical Sciences, Professor, Academician of the Russian Academy of Sciences, Head of Department, Chief Researcher, Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow, Russia. ORCID: https://orcid.org/0000-0001-5699-521X. Scopus Author ID: 6603727683, E-mail: holevo@mi-ras.ru