Роль коллективного приготовления и измерения состояний в некоторых квантовых коммуникационных протоколах

Д.А.Кронберг

Рассматриваются связанные задачи в квантовых коммуникациях: распределение информации и секретного ключа между отправителем и несколькими получателями. Исследуется выгода участников коммуникационных протоколов как от использования коллективных измерений, так и от коллективных действий на передающей стороне, связанных с использованием сцепленных состояний и различными действиями над ними.

Ключевые слова: *квантовая информация, классически-квантовый канал связи, коммуникационный протокол, супераддитивность, сцепленное состояние, секретный ключ.*

1. Введение

Важным объектом исследований в квантовой информации является ансамбль двух неортогональных состояний, для которого существенны следующие свойства квантовой механики:

– для таких состояний невозможно клонирование [1], а при попытке провести приближенное клонирование выходные состояния будут отличаться от исходных [2];

– недоступна операция вещания (broadcasting) таких состояний [3], т. е. нельзя раздать исходные состояния нескольким участникам (с допустимой сцепленностью между ними) так, чтобы частичное состояние каждого участника совпадало с исходным;

– передаваемая с помощью таких состояний информация супераддитивна [4, 5], т. е. коллективные измерения над всей передаваемой последовательностью дают больше информации, чем индивидуальные измерения с последующей классической обработкой результатов;

– возможно распределение секретного ключа по протоколу квантовой криптографии B92 [6].

Эти явления связаны с невозможностью достоверного различения между неортогональными квантовыми состояниями: если бы это было возможно, то, в частности, можно было бы приготовить копию исходного состояния, а перехватчик в квантовой криптографии мог бы сделать такую копию для себя, оставшись незамеченным. В то же время квантовая механика оставляет возможность частично «обойти» запрет на достоверное различение между неортогональными состояниями как с помощью безошибочного измерения, которое используется в квантовой криптографии и способно с некоторой вероятностью успеха дать полную информацию о сигнале, так и с помощью коллективных измерений, которые способны дать больше информации по сравнению с индивидуальными измерениями, в чем и состоит явление супераддитивности.

Количественное описание связи этих явлений с характеристиками ансамбля квантовых состояний является актуальной научной задачей, для которой, насколько нам известно, еще не было получено полного решения, несмотря на ряд важных результатов, таких как введение квантового дискорда как меры «квантовости» корреляций, не всегда связанной со сцепленностью. Оригинальное определение дискорда [7] имеет связь с явлением квантовой супераддитивности, поскольку рассматривает разность между максимумом достижимой информации и максимумом информации, достижимой при индивидуальных измерениях. Позже были предложены другие подходы к определению дискорда [8], например связанные с различными метриками на множестве квантовых состояний, но до сих пор открыт вопрос о возможности количественного описания многих квантовых явлений через дискорд.

Явление супераддитивности связано с возможностью применять коллективные наблюдаемые, в то время как ансамбль состояний состоит из разделимых состояний-произведений [9]. Представляет интерес ситуация, когда на вход канала также подаются сцепленные состояния. Важным результатом является то, что кодирование с помощью сцепленных состояний в общем случае может дать увеличение взаимной информации [10], но оно достигается в довольно сложных условиях.

В настоящей работе рассматриваются более простые ситуации, в которых используются сцепленные состояния для коммуникации с несколькими получателями, и сцепленность позволяет преодолеть ограничения, обусловленные независимой друг от друга работой получателей, а также с их возможным недоверием друг к другу при распределении секретных ключей. Для различных ситуаций получены оценки на суммарную публичную взаимную информацию между отправителем и несколькими получателями, а также на суммарную длину секретного ключа в случае идеального канала между отправителем и получателями.

Д.А.Кронберг. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул.Губкина, 8; Российский квантовый центр, Россия, 121353 Москва, Сколковское ш., 45; Московский физико-технический институт (национальный исследовательский университет), Россия, Московская обл., 141701 Долгопрудный, Институтский пер., 9; e-mail: dmitry.kronberg@gmail.ru

Поступила в редакцию 15 ноября 2019 г.

В разд.2 вводятся основные понятия, а также дается описание явления супераддитивности и рассмотрен выигрыш от применения коллективных наблюдаемых для одной из простых ситуаций – использования кода с повторением. В разд.3 рассматриваются задачи распределения публичной информации и секретного ключа между несколькими пользователями, в которых использование кода с повторением оказывается связанным с задачей приближенного клонирования квантовых состояний. Разд.4 посвящен тем же задачам, но с использованием сцепленных состояний вместо разделимых, что отвечает преобразованию приближенного вещания, а в разд.5 рассматривается использование разбавления сцепленности для создания независимых ансамблей для каждого участника. В Заключении приведены основные результаты работы.

2. Выигрыш от использования коллективных наблюдаемых

Рассмотрим простой бинарный классически-квантовый (c-q) канал, т.е. канал, имеющий на выходе квантовые состояния $\{|\psi_0\rangle,|\psi_1\rangle\}$, соответствующие входным классическим сигналам 0 и 1, при этом выходные состояния неортогональны и не совпадают: $\langle\psi_0|\psi_1\rangle=\kappa\in(0,1)$. Отправитель выбирает сигналы, а получатель проводит измерение и делает вывод о том, какое состояние было послано. Наблюдаемая П в квантовой механике описывается набором неотрицательных эрмитовых операторов, суммирующихся в единичный оператор: $\Pi=\{M_i\}_i$: $M_i=M_i^*\geqslant 0$, $\sum_i M_i=I$. Вероятность исхода i при измерении состояния ρ наблюдаемой П определяется как $p(i)=\mathrm{Tr}(\rho M_i)$.

При передаче информации центральной задачей является максимизация взаимной информации между передающей и приемной стороной в условиях многократной передачи состояний, при этом важным является использование кодовых слов (см. [9]). При бинарном кодировании классическое кодовое слово $w=(x_1,\ldots,x_N)$, где $x_i\in(0,1)$ отображается в состояние-произведение $S_w=|\psi_{x_1}\rangle\otimes\ldots\otimes|\psi_{x_N}\rangle$. Кодом (W, M) называется набор из K классических кодовых слов $\{w^{(i)}\}$ длины N и наблюдаемой M с $K+1$ исходами $\{0,1,\ldots,K\}$, где исход 0 соответствует уклонению от принятия решения. Скорость кода R определяется как

$$R=\frac{\log K}{N}.$$

Взаимная информация между входом и выходом при использовании кодовых слов длины N задается величиной

$$I_N(\{\hat p_i\},M)=\sum_i\hat p_i\sum_k p_N(k|i)\times\Big[\log p_N(k|i)-\log\sum_{i'}p_N(k|i')\hat p_{i'}\Big],\qquad(1)$$

где $p_N(k|i)=\mathrm{Tr}S_{w(i)}M_k$ – вероятность получения k-го исхода при отправке i-го кодового слова, а $\hat p_i$ – вероятность отправки i-го кодового слова. Можно определить пропускную способность при использовании кодовых слов длины N как максимум взаимной информации при использовании лучшего кода и измерения:

$$C_N=\max_{\{\hat p_i\},M}I_N(\{\hat p_i\},M).\qquad(2)$$

Если для классического случая всегда выполняется $C_N=NC_1$, то в квантовом случае возможно явление супераддитивности: $C_N>NC_1$. Это явление заключается в том, что пропускная способность c-q каналов может увеличиться при использовании коллективных измерений над всей последовательностью, что не достигается в классическом случае. Важную роль играет величина C_1 – максимальная взаимная информация, достижимая при индивидуальных измерениях, называемая пропускной способностью за один шаг (one-shot capacity).

Простой пример ситуации, когда указанный выше c-q канал демонстрирует супераддитивность, приведен в [11]: был построен конкретный код с $K=4$ кодовыми словами длины $N=3$, для которого $I_3>3C_1$, т.е. взаимная информация при коллективном измерении таких кодовых слов более чем втрое превышает пропускную способность при индивидуальных измерениях.

Величина $C=\lim_{N\to\infty}N^{-1}C_N$ называется пропускной способностью классически-квантового канала связи. Квантовая теорема кодирования [4, 5] утверждает, что эта величина равна максимуму величины Холево (или χ-величины), которая в общем случае ансамбля $(\{\rho_i\},\{p_i\})$, где каждое состояние ρ_i имеет вероятность p_i, принимает вид

$$\chi(\{\rho_i\},\{p_i\})=S\Big(\sum_i p_i\rho_i\Big)-\sum_i p_iS(\rho_i).\qquad(3)$$

Здесь $S(\rho)$ – энтропия фон Неймана квантового состояния.

Для двух чистых равновероятных состояний, $\{|\psi_0\rangle,|\psi_1\rangle\}$, величина Холево записывается как

$$\chi\Big(\{|\psi_0\rangle,|\psi_1\rangle\},\Big\{\frac12,\frac12\Big\}\Big)=S\Big(\frac12(|\psi_0\rangle\langle\psi_0|+|\psi_1\rangle\langle\psi_1|)\Big)=h_2\Big(\frac{1-\kappa}{2}\Big),\qquad(4)$$

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

Для супераддитивности важны как коллективные измерения, так и кодовые слова, не распадающиеся на применение кодов с меньшей длиной кодового слова [12]. Задача построения «хороших» кодов в классической теории кодирования является весьма нетривиальной, поэтому имеет смысл отдельное рассмотрение явления увеличения взаимной информации при использовании коллективной наблюдаемой. Сделаем это на примере простого кода – кода с повторением. Этот код содержит два кодовых слова

$$W=\{|w_0\rangle,|w_1\rangle\}=\{|\psi_0\rangle^{\otimes N},|\psi_1\rangle^{\otimes N}\},\qquad(5)$$

для этих слов $\langle w_0|w_1\rangle=\kappa^N$. Состояния $|w_0\rangle$ и $|w_1\rangle$ попрежнему являются неортогональными квантовыми состояниями, и легко найти наблюдаемую оптимального различения между ними.

Будем использовать наблюдаемую, получаемую из квадратного корня оператора Грама [13]. Оператор Грама ансамбля равновероятных состояний $\{|w_0\rangle,|w_1\rangle\}$

$$G = \frac{1}{2}\left(|w_0\rangle\langle w_0| + |w_1\rangle\langle w_1|\right),$$

и его нормированные собственные векторы имеют вид

$$|\lambda_0\rangle = \frac{1}{\sqrt{2}\sqrt{1+\kappa^N}}\left(|\psi_0\rangle^{\otimes N} + |\psi_1\rangle^{\otimes N}\right),$$

$$|\lambda_1\rangle = \frac{1}{\sqrt{2}\sqrt{1-\kappa^N}}\left(|\psi_0\rangle^{\otimes N} - |\psi_1\rangle^{\otimes N}\right),$$

с соответствующими собственными значениями $\frac{1}{2}(1 \pm \kappa^N)$. Поэтому

$$G^{-1/2} = \frac{1}{\sqrt{2}\sqrt{1+\kappa^N}}\,|\lambda_0\rangle\langle\lambda_0| + \frac{1}{\sqrt{2}\sqrt{1-\kappa^N}}\,|\lambda_1\rangle\langle\lambda_1|,$$

и измерительный базис задается векторами

$$\begin{aligned} |e_0\rangle &= \frac{1}{\sqrt{2}}G^{-1/2}|w_0\rangle = \frac{1}{\sqrt{2}}\left(|\lambda_0\rangle + |\lambda_1\rangle\right), \\ |e_1\rangle &= \frac{1}{\sqrt{2}}G^{-1/2}|w_1\rangle = \frac{1}{\sqrt{2}}\left(|\lambda_0\rangle - |\lambda_1\rangle\right), \end{aligned} \tag{6}$$

где множитель $1/\sqrt{2}$ является квадратным корнем вероятности состояний.

Несложно видеть, что при таком кодировании вероятность ошибки

$$\begin{aligned} Q &= |\langle\psi_0|^{\otimes N}|e_1\rangle|^2 = \frac{1}{2}\left(\sqrt{\frac{1+\kappa^N}{2}} - \sqrt{\frac{1-\kappa^N}{2}}\right)^2 \\ &= \frac{1}{2}\left(1 - \sqrt{1-\kappa^{2N}}\right). \end{aligned} \tag{7}$$

И для взаимной информации при коллективном измерении имеем

$$I_{N,\mathrm{col}}(A,B) = 1 - h_2(Q) = 1 - h_2\left(\frac{1}{2}\left(1 - \sqrt{1-\kappa^{2N}}\right)\right). \tag{8}$$

Аналогичными действиями можно вычислить вероятность ошибки q при индивидуальном различении состояний $\{|\psi_0\rangle, |\psi_1\rangle\}$ в каждой позиции:

$$q = \frac{1}{2}\left(1 - \sqrt{1-\kappa^2}\right),$$

при этом вычисление взаимной информации с учетом неравномерного распределения вероятностей сигналов на выходе менее тривиально – для $N = 2$ взаимная информация

$$\begin{aligned} I_{2,\mathrm{ind}}(A,B) &= H(Y) - H(Y|X) = 1 + h_2(2q(1-q)) \\ &\quad - 2h_2(q) = 1 + h_2\left(\frac{\kappa^2}{2}\right) - 2h_2\left(\frac{1-\sqrt{1-\kappa^2}}{2}\right). \end{aligned} \tag{9}$$

Из (8) и (9) несложно видеть, что $I_{2,\mathrm{col}}(A,B) > I_{2,\mathrm{ind}}(A,B)$, т. е. при использовании тех же кодовых слов коллективные измерения дают выигрыш по взаимной информации, в то же время код с повторением не дает в данном случае возможности достижения общей супераддитивности ($I_{2,\mathrm{col}}(A,B) > 2C_1$), для этого необходимы более сложные коды [11, 12]. В следующих разделах мы рассмотрим применение кода с повторением для задач передачи информации нескольким пользователям и для распределения секретного ключа и покажем, что там его применение может быть более оправданным.

Представляет интерес мера сцепленности векторов измерения (6), поскольку именно наличие векторов, не распадающихся на индивидуальные измерения, дает возможность получать больше информации при измерении. В многочастичной системе определение меры сцепленности неоднозначно [14], поэтому рассмотрим случай $N = 2$. Мера сцепленности одинакова для обоих состояний $|e_0\rangle$ и $|e_1\rangle$, поэтому рассмотрим одно из них:

$$\begin{aligned} |e_0\rangle = \frac{1}{2}\Bigg[&\left(\frac{1}{\sqrt{1+\kappa^2}} + \frac{1}{\sqrt{1-\kappa^2}}\right)|\psi_0\rangle|\psi_0\rangle \\ &+ \left(\frac{1}{\sqrt{1+\kappa^2}} - \frac{1}{\sqrt{1-\kappa^2}}\right)|\psi_1\rangle|\psi_1\rangle\Bigg], \end{aligned}$$

частичное состояние первой подсистемы имеет вид

$$A = \mathrm{Tr}_2\,|e_0\rangle\langle e_0| = \frac{1}{2}\begin{pmatrix} 1 + \dfrac{1}{\sqrt{1+\kappa^2}} & \dfrac{\kappa}{\sqrt{1+\kappa^2}} \\ \dfrac{\kappa}{\sqrt{1+\kappa^2}} & 1 - \dfrac{1}{\sqrt{1+\kappa^2}} \end{pmatrix}.$$

Мера сцепленности этого состояния задается энтропией фон Неймана состояния подсистемы и равна

$$h_2\left[\frac{1}{2}\left(1 - \frac{\sqrt{1+2\kappa^2}}{1+\kappa^2}\right)\right]. \tag{10}$$

Эта мера тем больше, чем больше κ, т. е. чем менее различимы состояния $\{|\psi_0\rangle, |\psi_1\rangle\}$. С точки зрения выражений для взаимных информаций (8) и (9) мера сцепленности может иметь следующий смысл: члены $h_2(Q)$ и $2h_2(q)$ в выражениях для коллективной и индивидуальной взаимной информации означают меру сцепленности системы и окружения после совершения измерения, и эта мера оказывается меньше в случае коллективных измерений. Вычисления показывают, что мера сцепленности вектора измерений является монотонной функцией от разности $2h_2(q) - h_2(Q)$, и наоборот: указанная разность – монотонная функция от сцепленности. Это может говорить о том, что сцепленность операторов наблюдаемой помогает снизить ошибку, т. е. сцепленность состояния и окружения после измерения. Данное явление представляет интерес для дальнейших исследований.

3. Задача клонирования и распределение информации между несколькими получателями

Код с повторением примечателен также тем, что при его использовании отправитель работает с двумя квантовыми состояниями $|\psi_0\rangle^{\otimes N}$ и $|\psi_1\rangle^{\otimes N}$ (далее предполагается, что $N \geqslant 2$), и их можно считать действием преобразования

$$\begin{aligned} |\Phi_0\rangle &\to |\psi_0\rangle^{\otimes N}, \\ |\Phi_1\rangle &\to |\psi_1\rangle^{\otimes N} \end{aligned} \tag{11}$$

на исходные векторы $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ в двумерном пространстве, где $\langle\Phi_0|\Phi_1\rangle=\alpha$. Операция (11) – это операция приближенного клонирования состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$. Как известно, неортогональные квантовые состояния не могут быть клонированы [1], но приближенное клонирование возможно [2]. В данном случае важным ограничением является условие унитарности операции (11), из которого следует соотношение между скалярными произведениями $\alpha=\kappa^N$.

На применение кода с повтроением можно взглянуть следующим образом: отправитель обладает состояниями $\{|\Phi_0\rangle,|\Phi_1\rangle\}$, но решает отправить их не в исходном виде, а произведя их приближенное клонирование, которое разбивает состояния на несколько частей, и отправляет эти части по одной. Коллективное измерение получателя можно трактовать как совершение им обратного преобразования, при котором он собирает частичные состояния вместе. В то же время при индивидуальных измерениях получатель имеет множество «лишних» исходов, которые уменьшают его информацию.

Такой подход позволяет рассмотреть задачу отправления состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ нескольким получателям, при этом каждый получатель может совершать свое измерение, в том числе коллективным образом, но получатели действуют независимо друг от друга, и им уже недоступна обратная операция «сборки» состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$. Несложно определить величину Холево состояний каждого получателя в такой ситуации:

$$\chi_{\text{part}}=\chi\left(\{|\psi_0\rangle,|\psi_1\rangle\}\right)=h_2\left(\frac{1-\kappa}{2}\right)=h_2\left(\frac{1-\sqrt[N]{\alpha}}{2}\right). \quad (12)$$

Видно, что при фиксированном α с увеличением числа получателей N максимальная информация каждого из них стремится к нулю, при этом общая переданная информация, задаваемая суммой информаций получателей, является при $\alpha\in(0,1)$ и достаточно больших N супераддитивной величиной:

$$N\chi_{\text{part}}>\chi\left(\{|\psi_0\rangle,|\psi_1\rangle\}\right). \quad (13)$$

Получатели, однако, не могут после измерения объединиться и совместными действиями (например, обработкой результатов их измерений) получить информацию, превышающую исходную величину Холево состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$, т.к. их результаты измерений будут дублироваться.

Операция приближенного клонирования состояний для отправки нескольким пользователям представляет интерес и с точки зрения криптографии. В самом деле, можно поставить задачу создания секретного ключа между отправителем и несколькими получателями, когда отправитель посылает неортогональные состояния нескольким получателям сразу, и итогом становится получение своего ключа каждым участником. В этом случае между отправителем и каждым из получателей возникает подобие протокола B92 [6], при котором каждый получатель измеряет состояние с помощью безошибочного измерения, задаваемого наблюдаемой:

$$M_0=\frac{I-|\psi_1\rangle\langle\psi_1|}{1+\kappa},\ M_1=\frac{I-|\psi_0\rangle\langle\psi_0|}{1+\kappa},$$
$$M_?=I-M_0-M_1. \quad (14)$$

Такое измерение либо дает полную информацию о состоянии с вероятностью $p_{\text{conc}}=1-\kappa$ (такой исход (0 или 1) называют определенным (conclusive)), либо с вероятностью $p_?=\kappa$ оно дает неопределенный (inconclusive) результат, который говорит о том, что извлечь информацию не удалось.

Дальнейшие действия участников таковы: каждый получатель сообщает отправителю позиции, в которых он получил определенный исход. Если в данной позиции только один получатель смог получить информацию, он использует это значение как бит «сырого» ключа, в случае же определенных результатов у нескольких получателей отправитель случайным образом решает, кто из получателей использует это значение бита, а остальные его не используют и вычеркивают из своей памяти. Такая схема действий требует доверия между получателями, что все они ведут себя по протоколу и, в частности, действительно «забывают» значения общих битов.

При полном доверии между участниками и при отсутствии ошибок и затухания в канале все пользователи получают независимые ключи. Длина секретного ключа каждого участника определяется вероятностью получения полной информации и вероятностью коллизии с другими участниками, когда они тоже получили определенные результаты. Вероятность получения ключа в данной позиции одним из участником при полном доверии равна вероятности того, что хотя бы один из участников получит определенный исход:

$$l_{\text{key,all}}=1-p_?^N=1-\kappa^N=1-\alpha. \quad (15)$$

Это вероятность равна вероятности получения определенного результата при отправке состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ одному отправителю. Отсюда следует, что при полном доверии и идеальном канале сумма длин секретных ключей участников в точности равна длине ключа одного участника, как если бы он получил все состояния.

В то же время если один из получателей подозревает, что часть других получателей действует не по протоколу, то и при отсутствии ошибки ему следует предполагать, что перехватчик имеет частичную информацию о ключе, задаваемую величиной Холево состояний недобросовестных участников (им выгоднее объединиться вместе и использовать общие измерения над своими подсистемами). Тогда суммарная длина ключа, передаваемого всем доверенным пользователям при наличии F недоверенных пользователей и при идеальном канале удовлетворяет неравенству

$$l_{\text{key,trusted}}\geqslant(1-p_?^{N-F})p_?^F\{1-h_2[\tfrac{1}{2}(1-\kappa^F)]\}. \quad (16)$$

Эта вероятность включает в себя вероятность получения определенного исхода хотя бы у одного из $N-F$ доверенных пользователей, отсутствие определенного исхода у F недоверенных пользователей, а также исключение информации, которую могли получить недоверенные пользователи при лучшем измерении. В (16) дана консервативная оценка: если часть пользователей решили совершать оптимальное коллективное измерение для получения величины Холево, равной $1-h_2[\frac{1}{2}(1-\kappa^F)]$, то они уже лишены возможности провести безошибочное измерение своих состояний и либо не смогут просигнализировать отправителю об определенном исходе в ожидаемом количестве позиций, либо обнаружат себя по ошибочному зна-

чению этих битов на этапе раскрытия части последовательности. Отметим, что при наличии ошибки между некоторыми пользователями оценка (16) уже не является верной, т. к. внесение ошибки дает недобросовестным участникам новые возможности: в частности, они могут совершать измерение с безошибочным различением состояний и, наоборот, сигнализировать об определенном результате, когда результат был неопределенным, чтобы исключить такие позиции из ключа. Также не были учтены вероятность затухания в канале и то, как она может быть использована перехватчиком [15], поскольку для идеального канала затухания нет. Полный анализ подобной системы с учетом возможности внесения ошибки и блокирования части состояний может быть темой будущих исследований; в настоящей работе имеет значение общий принцип: при использовании подобной схемы большое число доверенных пользователей способно увеличить длину ключа, получаемого каждым из них.

Также отметим, что в рассматриваемой схеме отправитель не знает, кто из получателей ведет себя недобросовестно, и не способен не отправлять состояния именно этим участникам. В то же время для каждого получателя набор недоверенных участников может быть различным, в том числе может быть разным, вообще говоря, и их число, и только от числа таких участников зависит длина ключа каждого пользователя.

Следует также упомянуть схожие задачи, связанные с криптографическими протоколами нескольких участников: распределение общего секретного ключа между группой удаленных пользователей [16, 17], а также разделение секретного сообщения между несколькими участниками, при котором они вместе могут прочитать сообщение, но любое их подмножество уже не будет иметь доступа к секрету [18].

4. Задача вещания квантовых состояний и использовние сцепленных состояний в канале

Если ставить целью распределение максимальной публичной информации среди не связанных между собой пользователей при наличии исходных состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ у отправителя, то можно видеть, что преобразование приближенного клонирования (11) не является оптимальным. Рассмотрим операцию вещания, при которой выходные состояния могут быть сцепленными:

$$\begin{aligned}|\Phi_0\rangle &\to \sqrt{1-p}|\varphi_0\rangle^{\otimes N} + \sqrt{p}|\varphi_0^{\perp}\rangle^{\otimes N},\\ |\Phi_1\rangle &\to \sqrt{1-p}|\varphi_1\rangle^{\otimes N} + \sqrt{p}|\varphi_1^{\perp}\rangle^{\otimes N},\end{aligned} \tag{17}$$

где $0 \leqslant p < 1$, и из соображений унитарности следует

$$\begin{aligned}\alpha = (1-p)\langle\varphi_0|\varphi_1\rangle^N + p\langle\varphi_0^{\perp}|\varphi_1^{\perp}\rangle^N\\ + \sqrt{p}\sqrt{1-p}\,(\langle\varphi_0|\varphi_1^{\perp}\rangle^N + \langle\varphi_0^{\perp}|\varphi_1\rangle^N),\end{aligned} \tag{18}$$

что дает другие скалярные соотношения для векторов $|\varphi_i\rangle$ относительно векторов $|\psi_i\rangle$, отвечающих операции приближенного клонирования (11).

Задача квантового вещания обобщает задачу клонирования, т. к. последнее не допускает сцепленности выходных состояний. Для двух некоммутирующих матриц плотности также имеет место запрет вещания [3], т. е. полученные частичные состояния

$$\begin{aligned}\rho_0 &= (1-p)|\varphi_0\rangle\langle\varphi_0| + p\,|\varphi_0^{\perp}\rangle\langle\varphi_0^{\perp}|,\\ \rho_1 &= (1-p)|\varphi_1\rangle\langle\varphi_1| + p\,|\varphi_1^{\perp}\rangle\langle\varphi_1^{\perp}|\end{aligned} \tag{19}$$

каждого участника обязательно будут отличаться от исходных состояний $\{|\Phi_0\rangle\langle\Phi_0|,|\Phi_1\rangle\langle\Phi_1|\}$.

Для частичных состояний (19) важным является то, что их величина Холево уже не стремится к нулю при росте числа получателей. В самом деле, существует индивидуальное измерение состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$, которое различает их с вероятностью ошибки

$$Q = \frac{1}{2}(1 - \sqrt[2]{1-\alpha^2}),$$

совпадающей с (7). После такого измерения копированием классических взаимно ортогональных состояний $\{|e_0\rangle,|e_1\rangle\}$, соответствующих результатам измерения 0 и 1, можно получить состояния

$$\begin{aligned}|\Phi_0\rangle &\to \sqrt{1-Q}|e_0\rangle^{\otimes N} + \sqrt{Q}|e_1\rangle^{\otimes N},\\ |\Phi_1\rangle &\to \sqrt{1-Q}|e_1\rangle^{\otimes N} + \sqrt{Q}|e_0\rangle^{\otimes N}\end{aligned} \tag{20}$$

для произвольного N.

Таким образом, величину Холево каждого участника после преобразования (17) можно сделать не меньше величины взаимной информации при индивидуальном измерении состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$:

$$\chi(\{\rho_0,\rho_1\}) \geqslant 1 - h_2(Q).$$

Имеет смысл рассмотреть задачу максимизации информации $\chi(\{\rho_0,\rho_1\})$, которая может быть распределена между отправителем и каждым из независимых получателей, при условии унитарности (18). Запрет полного вещания говорит о том, что при $\alpha \in (0,1)$ она меньше исходной χ-величины:

$$\chi(\{\rho_0,\rho_1\}) < \chi(\{|\Phi_0\rangle,|\Phi_1\rangle\}).$$

Это явление можно назвать запретом информационного вещания: нельзя имеющиеся квантовые состояния использовать для передачи информации произвольному числу пользователей без потери информации при этом. Такой запрет можно рассматривать как двойственное явление к супераддитивности классической пропускной способности с-q канала. Если супераддитивность связана с возможностью совершить коллективные измерения над всей передаваемой последовательностью, то запрет информационного вещания связан с невозможностью нескольких пользователей совершить совместное коллективное измерение, в то время как каждый из них совершает коллективные измерения над своей последовательностью состояний, полученной за несколько сеансов связи, что позволяет использовать χ-величину частичных состояний при оценке информации участника.

При приближенном вещании хорошо решается задача распределения публичной информации, однако такое преобразование, как легко видеть, плохо подходит для рас-

пределения ключей, поскольку получатели из-за их сцепленности будут получать совпадающий ключ, и распределение независимых ключей оказывается крайне неэффективным. Это можно интерпретировать так: низкая «квантовость» ансамблей состояний, которые получает каждый участник, делает распределение ключей плохо реализуемым.

Рассмотрим также ситуацию, когда отправитель выполнил преобразование (17), но после этого отправил все состояния одному получателю. Тогда в силу соотношения унитарности (18) взаимная информация между отправителем и получателем при коллективных измерениях последнего над всеми N состояниями неизменна и равна пропускной способности за один шаг для состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$:

$$I_{\rm col}(A,B) = C_1(\{|\Phi_0\rangle,|\Phi_1\rangle\}) = 1 - h_2(Q) = 1 - h_2\left(\frac{1-\sqrt{1-\alpha^2}}{2}\right),$$

что совпадает с (8). При индивидуальных же измерениях взаимная информация оказывается выше, чем это позволяет сделать клонирование (см. (9)), и определяется как

$$I_{\rm ind}(A,B) = C_1(\{\rho_0,\rho_1\}).$$

Если ставить задачу максимизации $I_{\rm ind}(A, B)$, то легко видеть, что максимум достигается при измерении состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ и приготовлении нескольких копий (20) и не отличается от пропускной способности $I_{\rm ind}(A, B)$ при коллективном измерении получателя над N посылками. Таким образом, выигрыш от использования коллективных измерений в этом случае отсутствует.

В итоге, сцепленность между состояниями различных участников действует как конструктивно для задачи информационного вещания и максимизации информации получателя при индивидуальных измерениях, так и деструктивно для задачи распределения независимых ключей среди нескольких пользователей.

5. Разбавление сцепленности на передающей стороне

В двух предыдущих разделах рассматривались действия отправителя, при которых он изначально обладает набором неортогональных состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ и совершает с ними действия, результатом чего оказываются состояния в новом пространстве, вообще говоря, другой размерности. Эту ситуацию можно обобщить на случай, когда отправитель обладает сцепленным состоянием системы AB

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|\Phi_0\rangle_B + |1\rangle_A|\Phi_1\rangle_B) \qquad (21)$$

и производит действия над ним. Для получения состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ в подсистеме B достаточно измерить подсистему A в базисе $\{|0\rangle,|1\rangle\}$, но это не единственное возможное действие.

Для состояния (21) можно записать разложение Шмидта

$$|\Psi\rangle_{AB} = \sqrt{\frac{1+\alpha}{2}}\,|\bar{0}\rangle_A|\bar{0}\rangle_B + \sqrt{\frac{1-\alpha}{2}}\,|\bar{1}\rangle_A|\bar{1}\rangle_B, \qquad (22)$$

где по-прежнему $\alpha = \{|\Phi_0\rangle,|\Phi_1\rangle\}$, а базис Шмидта задается векторами

$$|\bar{0}\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A), \qquad |\bar{1}\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A - |1\rangle_A),$$

$$|\bar{0}\rangle_B = \frac{1}{\sqrt{2(1+\alpha)}}(|\Phi_0\rangle_B + |\Phi_1\rangle_B), \quad |\bar{1}\rangle_B = \frac{1}{\sqrt{2(1-\alpha)}}(|\Phi_0\rangle_B - |\Phi_1\rangle_B).$$

Мерой сцепленности двухчастичного состояния (21) является энтропия квадратов коэффициентов Шмидтas

$$E(|\Psi\rangle_{AB}) = H\left(\left\{\frac{1+\alpha}{2},\frac{1-\alpha}{2}\right\}\right) = h_2\left(\frac{1-\alpha}{2}\right) = \mu_\alpha. \qquad (23)$$

Важными операциями в квантовой информации являются концентрация (concentration, также используются термины distillation и purification) и разбавление (dilution) сцепленности [14, 19]. Концентрация сцепленности позволяет из большого числа частично сцепленных состояний получить меньшее число полностью сцепленных состояний, разбавление же сцепленности – обратная операция, которая из небольшого числа состояний высокой сцепленности делает большее число состояний меньшей сцепленности.

Мера сцепленности состояния (21) равна μ_α, и это означает, что из него можно получить N состояний $|\Psi\rangle_{AB}$, мера сцепленности каждого из которых равна μ_α/N:

$$|\Psi\rangle_{AB} \to |\Psi'\rangle_{AB}^{\otimes N}. \qquad (24)$$

Рассмотрим ситуацию, когда отправитель совершает такое разбавление и затем измеряет подсистему A каждого из состояний $|\Psi'\rangle_{AB}$ в базисе $\{|0\rangle,|1\rangle\}$, после чего в системе B образуются N независимых ансамблей состояний $\{|\omega_0\rangle,|\omega_1\rangle\}$, для которых $\langle\omega_0|\omega_1\rangle$ определяется из уравнения

$$h_2\left(\frac{1-\alpha}{2}\right) = Nh_2\left(\frac{1-\langle\omega_0|\omega_1\rangle}{2}\right).$$

Снова отметим, что скалярные соотношения между $|\omega_i\rangle$ отличаются от соотношений между $|\psi_i\rangle$ и $|\varphi_i\rangle$, введенных для операций приближенного клонирования и вещания соответственно. Также обратим внимание, что состояния $|\omega_i\rangle$ отличаются от кодовых слов $|w_i\rangle$ (5), рассмотренных в разд.2.

С точки зрения распространения публичной информации этот подход хуже описанных выше, так как суммарная величина Холево ансамблей $\{|\omega_0\rangle,|\omega_1\rangle\}$ равна величине Холево состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ и оказывается меньше аналогичной суммы для других случаев.

В то же время такая ситуация хорошо подходит для распределения ключей с несколькими получателями при отсутствии доверия между ними, так как они получают независимые ключи, о которых другие участники не имеют информации вне зависимости от их добросовестности. При отсутствии ошибки длина секретного ключа каждого участника

$$l_{\rm key,\,part} = 1 - \langle\omega_0|\omega_1\rangle. \qquad (25)$$

Сумма ключей участников будет несколько ниже, чем сумма ключей при приближенном клонировании состояний и наличии достаточного количества доверенных участни-

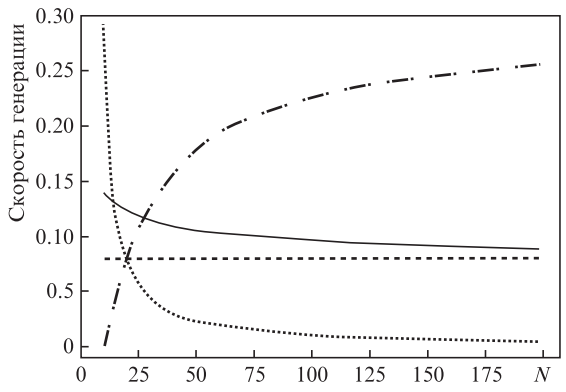

Рис.1. Зависимость скорости генерации секретного ключа на один бит посылки от числа получателей N при операции приближенного клонирования и при разбавлении сцепленности. Сплошной кривой показана сумма ключей пользователей при разбавлении сцепленности, когда длина ключа каждого участника дается формулой (25). Другие кривые соответствуют операции приближенного клонирования и вычисляются согласно (16): пунктирная – при 10 доверенных пользователей, штриховая – при половине доверенных пользователей, штрих-пунктирная – при 10 недоверенных пользователей. Исходная мера сцепленности состояний отправителя равна $h_2[0.5(1-1/\sqrt{2})]$, что соответствует $\langle\Phi_0|\Phi_1\rangle = \cos(\pi/4)$.

ков, но выше, чем при малом количестве доверенных пользователей.

На рис.1 показана скорость генерации ключа при разбавлении сцепленности и при операции приближенного клонирования в случае разного числа доверенных пользователей. Видно, что при большом числе получателей разбавление сцепленности обеспечивает скорость генерации ключа, сопоставимую со скоростью при приближенном клонировании и половине недоверенных пользователей.

Представляет интерес ситуация, когда все N состояний отправляются одному получателю. Если получатель не имеет возможности совершать коллективные измерения над всей последовательностью, которые давали бы величину Холево состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$, то ему не имеет смысла совершать коллективные измерения над словами длины N, т. к. из-за независимости общий ансамбль квантовых состояний распадается на N ансамблей состояний $\{|\omega_0\rangle,|\omega_1\rangle\}$, относящихся к подсистемам, и, как отмечалось выше, коллективное измерение не дает выигрыша по сравнению с индивидуальным измерением каждого состояния [12]. Отметим, что с ростом N увеличивается разность между информацией, доступной при коллективных и индивидуальных измерениях, при этом измерения над всеми N состояниями не дают выигрыша по сравнению с индивидуальными. Для будущих исследований представляет интерес связь этого падения информации с характеристиками наблюдаемой над состояниями $|\Psi'\rangle_{AB}^{\otimes N}$ после разбавления сцепленности, поскольку, как было отмечено в [20], когерентность (способная служить мерой «квантовости») ансамбля, получаемого при измерении части сцепленного состояния, зависит от степени неопределенности применяемой наблюдаемой.

6. Заключение

В работе рассмотрены ситуации передачи публичных данных и распределения секретных ключей при фиксированном ресурсе между удаленными пользователями. В роли ресурса выступала мера сцепленности состояния отправителя, из которого можно получить ансамбль состояний или несколько независимых ансамблей. Рассмотрены три основных направления при работе с полученным ансамблем: приготовление нескольких чистых состояний (приближенное клонирование), приготовление смешанных состояний (вещание) и разбавление сцепленности с приготовлением независимых ансамблей. Для каждой ситуации исследовалась задача передачи публичной информации как одному, так и нескольким пользователям, а также задача распределения секретного ключа.

При передаче всех состояний одному участнику и возможности совершать коллективные измерения способ передачи данных не имеет значение, т. к. максимальная взаимная информация дается величиной Холево исходных состояний $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ или, что эквивалентно, мерой сцепленности состояния $|\Psi\rangle_{AB}$. Однако при возможности совершать измерения над N состояниями для трех рассмотренных ситуаций результаты различны. При приближенном клонировании состояний возникает выигрыш от коллективных измерений, который эквивалентен выигрышу при применении кода с повторением в ситуации c-q канала. В случае приближенного вещания выигрыш от измерений над N состояниями невелик, а при достаточной сцепленности между состояниями он оказывается нулевым. При разбавлении сцепленного состояния с последующим его измерением выигрыша от измерения всех N состояний нет вовсе.

Если ставить задачу передачи публичной информации нескольким участникам, совершающим независимые измерения, то приближенное вещание справляется с такой задачей лучше всего, тем не менее нахождение оптимального преобразования (информационного вещания) над произвольным исходным ансамблем является нетривиальной задачей, для которой нет общего решения. Если участники ограничены индивидуальными измерениями, то такая задача решается путем оптимального измерения исходного состояния и приготовления классических состояний на основе результатов измерения.

При распределении независимых ключей между N получателями плохо подходит операция приближенного вещания из-за дублирования сигналов, которое вызвано сцепленностью состояний. В качестве основного преобразования логично взять разбавление сцепленности, которое позволит создать независимый ключ с каждым участником. Однако любопытна ситуация, возникающая при приближенном клонировании: скорость распределения ключей с каждым участником зависит от доверия между участниками. Чем больше доверенных пользователей, относительно которых участник уверен, что они ведут себя по протоколу, тем выше скорость распределения ключа для данного участника.

По мнению автора, эти ситуации имеет смысл принять во внимание при количественном описании явлений квантовой физики и работы протоколов квантовой коммуникации. Также стоит обратить внимание на ряд сопутствующих задач: исследование влияния сцепленности на выигрыш от коллективных измерений, нахождение оптимального преобразования информационного вещания для передачи максимума публичной информации нескольким получателям при данных исходных квантовых состояниях, а также на строгую оценку длины секретного ключа при его распределении между отправителем и несколькими получателями в зависимости от числа доверенных

получателей, в том числе при неидеальном канале и наличии ошибок.

Автор благодарит А.Н.Печеня за плодотворные обсуждения.

Исследование выполнено за счет гранта Российского научного фонда (проект № 17-11-01388-П) в Математическом институте им. В.А.Стеклова РАН.

1. Wootters W.K., Zurek W.H. *Nature*, **299** (5886), 802 (1982).
2. Scarani V., Iblisdir S., Gisin N., Acin A. *Rev. Mod. Phys*., **77** (4), 1225 (2005).
3. Barnum H., Caves C.M., Fuchs C.A., Jozsa R., Schumacher B. *Phys. Rev. Lett*., **76** (15), 2818 (1996).
4. Holevo A.S. *IEEE Trans. Inform. Theory*, **44** (1), 269 (1998).
5. Schumacher B., Westmoreland M.D. *Phys Rev A*, **56** (1), 131 (1997).
6. Bennett C.H. *Phys. Rev. Lett. A*, **68**, 3121 (1992).
7. Ollivier H., Zurek W.H. *Phys. Rev. Lett*., **88** (1), 017901 (2001).
8. Bera A., Das T., Sadhukhan D., Roy S.S., De A.S., Sen U. *Rep. Prog. Phys*., **81** (2), 024001 (2017).
9. Холево А.С. *Квантовые системы, каналы, информация* (М.: МЦНМО, 2010).
10. Hastings M.B. *Nature Phys*., **5** (4), 255 (2009).
11. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Lett. A*, **236**, 1 (1997).
12. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Rev. A*, **58** (1), 146 (1998).
13. Hausladen P., Jozsa R., Schumacher B., Westmoreland M., Wootters W.K. *Phys. Rev. A*, **54** (3), 1869 (1996).
14. Bennett C.H., Popescu S., Rohrlich D., Smolin J.A., Thapliyal A.V. *Phys. Rev. A*, **63** (1), 012307 (2000).
15. Кронберг Д.А., Курочкин Ю.В. *Квантовая электроника*, **48** (9), 843 (2018) [*Quantum Electron*., **48** (9), 843 (2018)].
16. Bose S., Vedral V., Knight P.L. *Phys. Rev. A*, **57** (2), 822 (1998).
17. Chen K., Lo H.K. arXiv preprint quant-ph/0404133 (2004).
18. Hillery M., Bužek V., Berthiaume A. *Phys. Rev. A*, **59** (3), 1829 (1999).
19. Bennett C.H., Bernstein H.J., Popescu S., Schumacher B. *Phys. Rev. A*, **53** (4), 2046 (1996).
20. Kronberg D.A. *Lobachevskii J. Mathematics*, **40** (10), 1507 (2019).