

Схема квантовых коммуникаций, описываемая регулярным четырехмерным комплексным политопом

А.Ю. Власов^{1,2,*}

¹ Санкт-Петербургский научно-исследовательский институт радиационной гигиены имени профессора П.В. Рамзаева
Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека
Россия, 197101, Санкт-Петербург, ул. Мира, 8

² Лаборатория теоретической физики им. А.А. Фридмана
Россия, 191186, Санкт-Петербург, наб. р. Мойки, 48

(Поступила в редакцию 03.12.2024; после доработки 09.12.2024; подписана в печать 16.12.2024)

В настоящее время обобщения протоколов квантовых коммуникаций с кубитов на системы с более высокой размерностью пространства состояний (кудиты) обычно используют взаимно несмещённые базисы, конструкция которых известна в любой размерности равной степени простого числа. Однако в небольших размерностях также существуют формально более симметричные системы состояний, описываемые регулярными комплексными политопами, являющимися обобщением идеи правильных многогранников на комплексные пространства. В данной работе рассматривается применение модели, изначально предложенной Р. Пенроузом и построенной на основе геометрии додекаэдра и двух квантово-запутанных частиц со спином $3/2$. В более общем случае вместо них можно использовать две произвольные квантовые системы с четырьмя базисными состояниями (кукварты). В дальнейшем было показано, что эта система из 40 состояний эквивалентна конфигурации Виттинга и связана с четырехмерным комплексным политопом, описанным Кокстером. В работе предложен использующий данную конфигурацию протокол квантового распределения ключей, основанный на контекстуальности.

PACS: 03.67.-a, 03.67.Bg, 03.67.Dd, 03.67.Ac, 02.20.-a УДК: 539

Ключевые слова: квантовая запутанность, квантовые коммуникации, контекстуальность, квантовая информация, кукварты, додекаэдр Пенроуза, политоп Виттинга.

DOI: [10.55959/MSU0579-9392.80.2530405](https://doi.org/10.55959/MSU0579-9392.80.2530405)

ВВЕДЕНИЕ

Модель «нелокальности Белла без вероятностей», основанная на геометрии додекаэдра и двух частицах со спином $3/2$, была предложена Р. Пенроузом и получила дальнейшее развитие в ряде публикаций [1–3]. При этом было использовано так называемое представление Майораны [4], позволяющее представить состояние системы с произвольным спином $n/2$ в виде набора из n точек на сфере.

В дальнейшем другими авторами были найдены эквивалентные упрощённые выражения для 40 квантовых состояний данной модели [5], не использующие представление Майораны. При этом связь с геометрической моделью додекаэдра уже оказывалась менее естественной и наглядной.

Однако такое представление упрощает использование более общего подхода к описанию модели и позволяет более естественно использовать произвольные квантовые системы с размерностью пространства состояний равной четырём (кукварты), а не только частицы со спином $3/2$. Помимо этого, у данного представления была найдена связь с уже

известной и достаточно хорошо изученной геометрической структурой, регулярным комплексным политопом Виттинга [6].

В данной работе рассматривается протокол квантового распределения ключей (КРК), основанный на модели додекаэдров Пенроуза и политопе Виттинга. В разделе 1 рассмотрен политоп Виттинга и связанная с ним конфигурация Виттинга, а также два способа индексации её состояний. В разделе 2 с использованием этой конфигурации построен протокол КРК, основанный на контекстуальности. Чтобы продемонстрировать некоторые характерные свойства такого протокола КРК, в разделе 3 проанализированы взаимоотношения между связанными с ним классическими и квантовыми моделями. В Заключение приведены основные выводы и обсуждаются некоторые дополнительные вопросы.

1. ПОЛИТОП И КОНФИГУРАЦИЯ ВИТТИНГА

Регулярные комплексные политопы были предложены Кокстером как обобщения правильных многоугольников и многогранников на комплексные пространства различной размерности [8]. Четырех-

* E-mail: qubeat@mail.ru, a.vlasov@niirg.ru

мерный комплексный политоп Виттинга имеет 240 вершин, которые могут быть описаны выражениями [8]:

$$\begin{aligned} (0, \pm\omega^\mu, \mp\omega^\nu, \pm\omega^\lambda), & \quad (\mp\omega^\mu, 0, \pm\omega^\nu, \pm\omega^\lambda), \\ (\pm\omega^\mu, \mp\omega^\nu, 0, \pm\omega^\lambda), & \quad (\mp\omega^\mu, \mp\omega^\nu, \mp\omega^\lambda, 0), \\ (\pm i\omega^\lambda\sqrt{3}, 0, 0, 0), & \quad (0, \pm i\omega^\lambda\sqrt{3}, 0, 0), \\ (0, 0, \pm i\omega^\lambda\sqrt{3}, 0), & \quad (0, 0, 0, \pm i\omega^\lambda\sqrt{3}), \end{aligned} \quad (1)$$

где $\omega = (-1 + i\sqrt{3})/2 = e^{2\pi i/3}$, $\omega^3 = 1$ и $\lambda, \mu, \nu \in \{0, 1, 2\}$.

Если исходя из принципов квантовой механики не различать вектора, отличающиеся только общим фазовым множителем, то получается набор из 40 квантовых состояний, аналогичный конфигурации, описанной Виттингом в 1887 г. [9], в честь которой и был назван упомянутый выше политоп. Этот набор включает 4 состояния базиса:

$$(1, 0, 0, 0), \quad (0, 1, 0, 0), \quad (0, 0, 1, 0), \quad (0, 0, 0, 1) \quad (2a)$$

и 36 состояний, которые могут быть представлены как четыре группы по 9 состояний:

$$\begin{aligned} \frac{1}{\sqrt{3}}(0, 1, -\omega^\mu, \omega^\nu), & \quad \frac{1}{\sqrt{3}}(1, 0, -\omega^\mu, -\omega^\nu), \\ \frac{1}{\sqrt{3}}(1, -\omega^\mu, 0, \omega^\nu), & \quad \frac{1}{\sqrt{3}}(1, \omega^\mu, \omega^\nu, 0), \end{aligned} \quad (2b)$$

где $\mu, \nu \in \{0, 1, 2\}$, $\omega = e^{2\pi i/3}$.

В более развёрнутом виде, используя нумерацию из работы [7], все 40 состояний приведены в табл. 1, где из типографских соображений все компоненты умножены на корень из трёх. Для определённости данная нумерация названа здесь «блочной» из-за структуры алгоритма построения, который может быть найден в приложении к данной работе [7].

Структура табл. 1 также отражает связь конфигурации Виттинга с взаимно несмещёнными базисами в трехмерном пространстве [7]. Один из таких наборов представлен векторами состояний из первой строки и последнего столбца таблицы: $\{|\phi_0^0\rangle, |\phi_0^1\rangle, |\phi_0^2\rangle\}$, $\{|\phi_3^1\rangle, |\phi_3^2\rangle, |\phi_3^3\rangle\}$, $\{|\phi_3^4\rangle, |\phi_3^5\rangle, |\phi_3^6\rangle\}$, $\{|\phi_3^7\rangle, |\phi_3^8\rangle, |\phi_3^9\rangle\}$, последняя компонента которых равна нулю. Эти тройки состояний соответствуют «строительным блокам» таблицы. Все столбцы этой таблицы с точностью до расстановки знаков и несущественного общего фазового множителя могут быть получены друг из друга циклическими сдвигами компонент векторов.

Однако такой способ индексации плохо отражает симметрию конфигурации. Чтобы сделать модель более наглядной, далее используется отображение 40 состояний в наборы из десяти карт четырёх мастей, представленное в табл. 2. Правило формирования строки в этой таблице основано не на циклическом сдвиге, а на требовании, чтобы все состояния в каждой строке были взаимно ортогональны.

Преимущество «карточной» индексации заключается в некоторой дополнительной регулярности,

которая проявляется при описании наборов из 40 ортогональных состояний (базисов), используемых в модели додекаэдров Пенроуза, которые будут описаны далее и представлены в табл. 3.

2. КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ

Рассмотрим систему двух куквартов, описываемых состоянием

$$|\Sigma\rangle = \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle + |3\rangle|3\rangle). \quad (3)$$

Если рассмотреть некую идеализацию реальной ситуации, то многократное приготовление данного состояния с последующим разделением между двумя участниками после измерений приведёт к появлению у них случайной последовательности пар одинаковых целых чисел с равной вероятностью распределённых в диапазоне от нуля до трёх, которые в дальнейшем могут быть использованы ими для обмена шифрованными сообщениями. Следует отметить, что в работе Пенроуза вместо данного симметричного состояния использовалось антисимметричное, но это не влияет принципиально на дальнейший ход изложения.

Измерение с использованием двух фиксированных базисов $|0\rangle, \dots, |3\rangle$ не защищено от перехвата сообщения у одного из участников с дальнейшей пересылкой ему квантового состояния $|j\rangle$, $j = 0, \dots, 3$ в зависимости от результата измерения. В этом случае формально происходит подмена состояния $|\Sigma\rangle$ на набор пар $|j\rangle|j\rangle$, посылаемых с равной вероятностью. Чтобы обнаружить данную подмену, необходимо производить измерения в разных базисах.

Рассмотрим достаточно естественное обобщение протокола E91, основанного на квантовой запутанности и предложенного А. Экертом [10] на системы более высокой размерности [11]. Прежде всего отметим, что состояние (3) можно переписать в виде

$$|\Sigma\rangle = \frac{1}{2}(|\chi_0\rangle|\chi_0^*\rangle + |\chi_1\rangle|\chi_1^*\rangle + |\chi_2\rangle|\chi_2^*\rangle + |\chi_3\rangle|\chi_3^*\rangle), \quad (4)$$

где $|\chi_k\rangle = \sum_{j=0}^3 \chi_{kj}|j\rangle$, $j, k = 0, \dots, 3$ — некий ортогональный набор состояний (один из возможных альтернативных базисов), а $|\chi_k^*\rangle$ — «комплексно-сопряжённый» базис, полученный по формуле $|\chi_k^*\rangle = \sum_{j=0}^3 \bar{\chi}_{kj}|j\rangle$. Следует отметить, что в частном случае, когда все коэффициенты χ_{kj} вещественны, оба базиса совпадают, что соответствует обычному выбору, используемому в случае кубитов. Набор коэффициентов χ_{kj} можно также отождествить с матрицей преобразования от стандартного к альтернативному базису.

В более простой версии КРК, не основанной на квантовой запутанности и не используемой в данной работе (так называемый *протокол подготовки и измерения*), в качестве набора базисов часто выбирают взаимно несмещённые [12, 13]. Аналогичный выбор кажется естественным и в случае

Таблица 1. «Блочная» нумерация

n	$\sqrt{3} \phi_0^n\rangle$	$\sqrt{3} \phi_1^n\rangle$	$\sqrt{3} \phi_2^n\rangle$	$\sqrt{3} \phi_3^n\rangle$
0	$(\sqrt{3}, 0, 0, 0)$	$(0, \sqrt{3}, 0, 0)$	$(0, 0, \sqrt{3}, 0)$	$(0, 0, 0, \sqrt{3})$
1	$(0, 1, -1, 1)$	$(1, 0, -1, -1)$	$(1, -1, 0, 1)$	$(1, 1, 1, 0)$
2	$(0, 1, -\omega, \bar{\omega})$	$(1, 0, -\omega, -\bar{\omega})$	$(1, -\omega, 0, \bar{\omega})$	$(1, \omega, \bar{\omega}, 0)$
3	$(0, 1, -\bar{\omega}, \omega)$	$(1, 0, -\bar{\omega}, -\omega)$	$(1, -\bar{\omega}, 0, \omega)$	$(1, \bar{\omega}, \omega, 0)$
4	$(0, 1, -\omega, 1)$	$(1, 0, -1, -\omega)$	$(1, -\bar{\omega}, 0, \bar{\omega})$	$(1, \omega, 1, 0)$
5	$(0, 1, -\bar{\omega}, \bar{\omega})$	$(1, 0, -\omega, -1)$	$(1, -1, 0, \omega)$	$(1, \bar{\omega}, \bar{\omega}, 0)$
6	$(0, 1, -1, \omega)$	$(1, 0, -\bar{\omega}, -\bar{\omega})$	$(1, -\omega, 0, 1)$	$(1, 1, \omega, 0)$
7	$(0, 1, -\bar{\omega}, 1)$	$(1, 0, -1, -\bar{\omega})$	$(1, -\omega, 0, \omega)$	$(1, \bar{\omega}, 1, 0)$
8	$(0, 1, -1, \bar{\omega})$	$(1, 0, -\omega, -\omega)$	$(1, -\bar{\omega}, 0, 1)$	$(1, 1, \bar{\omega}, 0)$
9	$(0, 1, -\omega, \omega)$	$(1, 0, -\bar{\omega}, -1)$	$(1, -1, 0, \bar{\omega})$	$(1, \omega, \omega, 0)$

Таблица 2. Индексация состояний «квантовыми картами»
(в квадратных скобках показан соответствующий «блочный» индекс)

n	$\sqrt{3} \mathfrak{n}_{\blacktriangle}\rangle$	$\sqrt{3} \mathfrak{n}_{\blacktriangleright}\rangle$	$\sqrt{3} \mathfrak{n}_{\blacktriangleleft}\rangle$	$\sqrt{3} \mathfrak{n}_{\blacktriangledown}\rangle$
1	$(\sqrt{3}, 0, 0, 0)_{[0]}$	$(0, \sqrt{3}, 0, 0)_{[0]}$	$(0, 0, \sqrt{3}, 0)_{[0]}$	$(0, 0, 0, \sqrt{3})_{[0]}$
2	$(0, 1, -1, 1)_{[1]}$	$(1, 0, -1, -1)_{[1]}$	$(1, -1, 0, 1)_{[1]}$	$(1, 1, 1, 0)_{[1]}$
3	$(0, 1, -\omega, \bar{\omega})_{[2]}$	$(1, 0, -\bar{\omega}, -1)_{[9]}$	$(1, -\omega, 0, 1)_{[6]}$	$(1, \omega, \bar{\omega}, 0)_{[2]}$
4	$(0, 1, -\bar{\omega}, \omega)_{[3]}$	$(1, 0, -\omega, -1)_{[5]}$	$(1, -\bar{\omega}, 0, 1)_{[8]}$	$(1, \bar{\omega}, \omega, 0)_{[3]}$
5	$(0, 1, -1, \omega)_{[6]}$	$(1, 0, -\omega, -\bar{\omega})_{[2]}$	$(1, -\omega, 0, \bar{\omega})_{[2]}$	$(1, \omega, \omega, 0)_{[9]}$
6	$(0, 1, -\omega, 1)_{[4]}$	$(1, 0, -1, -\bar{\omega})_{[7]}$	$(1, -\bar{\omega}, 0, \bar{\omega})_{[4]}$	$(1, \bar{\omega}, 1, 0)_{[7]}$
7	$(0, 1, -\bar{\omega}, \bar{\omega})_{[5]}$	$(1, 0, -\bar{\omega}, -\bar{\omega})_{[6]}$	$(1, -1, 0, \bar{\omega})_{[9]}$	$(1, 1, \bar{\omega}, 0)_{[8]}$
8	$(0, 1, -1, \bar{\omega})_{[8]}$	$(1, 0, -\bar{\omega}, -\omega)_{[3]}$	$(1, -\bar{\omega}, 0, \omega)_{[3]}$	$(1, \bar{\omega}, \bar{\omega}, 0)_{[5]}$
9	$(0, 1, -\omega, \omega)_{[9]}$	$(1, 0, -\omega, -\omega)_{[8]}$	$(1, -1, 0, \omega)_{[5]}$	$(1, 1, \omega, 0)_{[6]}$
10	$(0, 1, -\bar{\omega}, 1)_{[7]}$	$(1, 0, -1, -\omega)_{[4]}$	$(1, -\omega, 0, \omega)_{[7]}$	$(1, \omega, 1, 0)_{[4]}$

протоколов, основанных на квантовой запутанности. Действительно, для такого набора для любых двух состояний из разных базисов верна формула $|\langle\psi|\varphi\rangle|^2 = 1/4$ и в случае неправильного выбора результат измерений будет полностью случайным и равновероятным.

Для разных векторов конфигурации Виттинга величина $|\langle\psi|\varphi\rangle|^2$ может быть равна либо нулю, либо $1/3$, что хотя и затрудняет анализ протокола, но при неправильном выборе базиса тоже делает результат измерений случайным и равновероятным, если не учитывать, что один из элементов базиса (для которого вероятность равна нулю) не может появиться в результате измерения. Действительно, конфигурация Виттинга может быть рассмотрена, как некое симметричное вложение в четырехмерное пространство четырёх наборов взаимно несмещённых трехмерных базисов [7], что уже было упомянуто ранее при описании «блочной» индексации.

Заметным отличием конфигурации Виттинга от неперекрывающихся наборов базисов, обычно ис-

пользуемых в КРК, является то, что одно и то же состояние может входить сразу в четыре разных базиса, и общее количество базисов, которые можно составить из этих состояний, достигает 40.

Протокол, базирующийся на модели додекаэдров Пенроуза и конфигурации Виттинга, можно классифицировать, как *КРК, основанное на контекстуальности*. Данная терминология может быть понятна из работ, связанных с данной моделью [1–3, 5, 6] и более подробно раскрывается далее в разделе 3. Существуют и другие примеры таких протоколов [14, 15]. Предлагаемый протокол достаточно естественно связан с обобщениями протокола E91. Рассмотрим более подробно схему квантовых коммуникаций основанную на конфигурации Виттинга.

Два участника (обозначаемые в дальнейшем как А и В) производят измерения квантово запутанного состояния $|\Sigma\rangle$, причем в качестве измерительного базиса $|\chi_j\rangle$, $j = 0, \dots, 3$, указанного в выражении (4), первый участник использует один из 40 бази-

сов, приведённых в табл. 3, а второй участник — соответствующий базис, состоящий из «сопряжённых» состояний $|\chi_j^*\rangle$.

Для удобства можно предполагать, что В использует вместо индексации состояний, приведённой в табл. 2, альтернативную таблицу, все коэффициенты в которой заменены на комплексно-сопряжённые. Можно заметить, что для этого достаточно произвести в таблице перестановку строк по схеме $3 \leftrightarrow 4$, $5 \leftrightarrow 8$, $7 \leftrightarrow 9$ и $6 \leftrightarrow 10$. Базисы для В тоже должны состоять из «сопряжённых» состояний. Это гарантирует, что при измерении состояния $|\Sigma\rangle$ в любой из таких 40 согласованных пар базисов оба участника получают пару состояний, отмеченных одним и тем же индексом.

Состояниям в каждой четвёрке, приведённой в табл. 3, можно сопоставить числа от нуля до трёх, соответствующие позиции внутри этой четвёрки в данной таблице. В первой части таблицы, состоящей из 28 базисов, четвёрки проиндексированы в порядке возрастания, выбранном для «мастей» ($\spadesuit, \heartsuit, \diamondsuit, \clubsuit$), а у оставшихся 12 базисов, состоящих из карт одинаковых мастей, — в порядке возрастания числовых значений.

В определённом смысле такое соответствие между числами и состояниями является результатом предварительного соглашения. Число, соответствующее данному состоянию, может зависеть не только от него, но и от базиса. Например, состояние $|\spadesuit_3\rangle$ будет соответствовать нулю в трёх базисах из первой части таблицы, но в четвёртом базисе оно соответствует двум. При этом $|\heartsuit_3\rangle$ соответствует единице во всех четырёх базисах.

Два участника после серии измерений в согласованных базисах получают одинаковый набор случайных чисел от нуля до трёх, которые могут быть использованы для обмена зашифрованными сообщениями. Следует отметить, что «наивная» версия протокола с выбором одного из 40 базисов случайным образом приводит к достаточно низкой вероятности совпадения в 2.5%, которую можно увеличить, используя более сложные версии протокола.

Одним из преимуществ протоколов, основанных на контекстуальности, является возможность проконтролировать, что канал действительно работает в «квантовом режиме». Имеется в виду, что из-за неправильной работы оборудования или специфической атаки на протокол, вместо квантовой версии может происходить функционирование в классическом режиме. В таком случае рассуждения о надёжности квантовой связи просто теряют смысл. Происходит так называемая «подмена квантового протокола классическим».

С формальной точки зрения участники используют некие устройства, которые генерируют одинаковые наборы случайных чисел, и может возникнуть необходимость убедиться, что их функционирование основано именно на квантовых свойствах. Следует отметить, что подобные вопросы могут решаться и без использования контекстуальности. На-

пример, уже в протоколе E91 для аналогичной проверки предлагалось использовать дополнительные измерения проверяющие неравенства Белла [10]. Несмотря на это, рассматриваемый здесь протокол, основанный на модели Пенроуза «без вероятностей», может иметь некоторые преимущества.

3. КВАНТОВЫЕ И КЛАССИЧЕСКИЕ МОДЕЛИ

Чтобы оценить варианты «подмены квантового протокола классическим», которые могли бы нарушить безопасность передачи информации, рассмотрим классические версии модели, связанные с рассматриваемым протоколом. Например, два участника получают по набору из 40 карт и каждый набирает из них одну из 40 четвёрок, указанных в табл. 3. После этого в результате неких манипуляций выбирается одна из этих четырёх карт, которая при корректном функционировании протокола должна была бы *всегда* совпадать у обоих участников (если они выбрали из своих колод одну и ту же четвёрку карт).

Если оба участника производят выбор карт независимо и никак не согласуют свои действия, но при любом таком выборе карта должна оказаться одной и той же, то можно заключить, что на картах заранее нанесены метки, которые и позволяют выбрать нужную карту. Чтобы такой способ воспроизводил поведение квантовой модели, необходимо, чтобы распределение меток по 40 картам было произведено таким образом, что в любой четвёрке карт из табл. 3 присутствовала одна и только одна метка.

Однако такое распределение невозможно. В модели Пенроуза демонстрация данного противоречия опиралась на геометрические построения, но для его проверки достаточно просто иметь заданный набор используемых четвёрок состояний, аналогичный приведённому в табл. 3. Покажем на данном примере, как доказать невозможность выбора необходимого распределения меток.

Во-первых, рассмотрим десять наборов карт, подчёркнутых в табл. 3, и состоящих из четырёх карт одного достоинства разных мастей. Очевидно, что каждая из 40 карт входит в эти десять наборов один и только один раз и если бы вместо 40 базисов использовались только эти десять, то расстановка меток стала бы достаточно тривиальной. Нужно было бы просто произвольным образом поставить одну метку на одну из карт в каждом из этих десяти наборов.

Однако такой подход с расстановкой меток может привести к неправильному распределению меток в остальных 30 наборах. Например, предположим, что во всех 10 наборах была выбрана одна и та же масть, например пики. В этом случае выбор любой из 28 четвёрок из первой части таблицы (то есть в 70% случаев) приводит к корректному результату, однако в оставшихся 12 четвё-

Таблица 3. 40 базисов в обозначениях с «квантовыми картами»

1	$\{ 1\rangle, 1\rangle, 1\rangle, 1\rangle \} \equiv \{ 0\rangle, 1\rangle, 2\rangle, 3\rangle \},$		
2	$\{ 2\rangle, 2\rangle, 2\rangle, 2\rangle \},$	3	$\{ 2\rangle, 7\rangle, 6\rangle, 8\rangle \},$
5	$\{ 3\rangle, 3\rangle, 3\rangle, 3\rangle \},$	6	$\{ 3\rangle, 5\rangle, 7\rangle, 9\rangle \},$
8	$\{ 4\rangle, 4\rangle, 4\rangle, 4\rangle \},$	9	$\{ 4\rangle, 6\rangle, 5\rangle, 10\rangle \},$
11	$\{ 5\rangle, 5\rangle, 5\rangle, 5\rangle \},$	12	$\{ 5\rangle, 10\rangle, 9\rangle, 2\rangle \},$
14	$\{ 6\rangle, 6\rangle, 6\rangle, 6\rangle \},$	15	$\{ 6\rangle, 8\rangle, 10\rangle, 3\rangle \},$
17	$\{ 7\rangle, 7\rangle, 7\rangle, 7\rangle \},$	18	$\{ 7\rangle, 9\rangle, 8\rangle, 4\rangle \},$
20	$\{ 8\rangle, 8\rangle, 8\rangle, 8\rangle \},$	21	$\{ 8\rangle, 4\rangle, 3\rangle, 5\rangle \},$
23	$\{ 9\rangle, 9\rangle, 9\rangle, 9\rangle \},$	24	$\{ 9\rangle, 2\rangle, 4\rangle, 6\rangle \},$
26	$\{ 10\rangle, 10\rangle, 10\rangle, 10\rangle \},$	27	$\{ 10\rangle, 3\rangle, 2\rangle, 7\rangle \},$
29	$\{ 1\rangle, 2\rangle, 3\rangle, 4\rangle \},$	30	$\{ 1\rangle, 5\rangle, 6\rangle, 7\rangle \},$
32	$\{ 1\rangle, 2\rangle, 5\rangle, 8\rangle \},$	33	$\{ 1\rangle, 3\rangle, 6\rangle, 9\rangle \},$
35	$\{ 1\rangle, 2\rangle, 5\rangle, 8\rangle \},$	36	$\{ 1\rangle, 3\rangle, 6\rangle, 9\rangle \},$
38	$\{ 1\rangle, 2\rangle, 3\rangle, 4\rangle \},$	39	$\{ 1\rangle, 5\rangle, 6\rangle, 7\rangle \},$
		40	$\{ 1\rangle, 8\rangle, 9\rangle, 10\rangle \}.$

ках сразу все четыре карты либо отмечены, либо не имеют меток.

Далее, используя выбранные 10 карт как основу, можно перебрать все $4^{10} = 1048576$ возможных способов расстановки меток и посмотреть, как они расположатся в остальных 30 четвёрках карт. Прямой перебор подтверждает, что всегда найдутся четвёрки карт, для которых распределение меток не будет корректным. Расчёт также показывает, что при случайном выборе вероятность получить корректную четвёрку карт с одной меткой составляет около 57%, что даже меньше, чем в примере, приведённом выше.

Максимально возможное количество корректных четвёрок составляет 34 (то есть 85% случаев). Примером является набор меток, соответствующих состояниям

$$\{ |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle, |8\rangle, |9\rangle, |10\rangle \},$$

при котором в 34 базисах, как положено, будет отмечено только одно состояние, но в трёх базисах будет сразу две метки, а в других трёх — ни одной. В табл. 3 это базисы с номерами 6, 7, 29 и 15, 25, 38 соответственно. Подобных наборов существует всего 720, и их доля из всех возможных 4^{10} вариантов составляет менее 0.07%, а доля комбинаций, для которых количество корректных четвёрок будет 70% и выше, оказывается менее 4%. Так что при использовании такого типа классических моделей нарушение необходимых требований проявится после не очень большого количества тестов с различными комбинациями карт.

Однако воспроизвести корректные результаты можно при использовании контекстуальных классических моделей. Например, вместо одного набора из 40 карт, выдаваемых каждому участнику, можно использовать по четыре таких набора из которых нужно сразу составить все 40 необходимых комбинаций, приведённых в табл. 3, и при этом в каждой из них отметить одну и ту же карту в наборах обоих участников. В этом случае каждый участник не выбирает по одной карте, а сразу берёт одну из 40 четвёрок карт и находит в них заранее отмеченную.

Такая модель даже более приближена к обычной процедуре измерения используемой в формализме квантовых вычислительных цепей (КВЦ) и их симуляторах, в которых обычно не предусмотрены промежуточные измерения, что приводит к некой сложности с реализацией идеи используемой Пенроузом. Но только что описанная реализация модели формально является контекстуальной, так как одна и та же карта может быть либо отмеченной, либо нет, в зависимости от того, в четвёрку с какими другими картами она попадёт. Избежать такой ситуации можно, если потребовать выполнения определённой процедуры измерений, аналогичной используемой в модели, рассмотренной Пенроузом [1–3].

Реализация данной процедуры в модифицированной версии данной модели, основанной на конфигурации Виттинга, уже рассматривалась ранее [7]. Для этого на первом шаге необходимо выбрать одно из 40 состояний и произвести измерение, результат которого можно интерпретировать как ответ на вопрос, находится ли система в данном состоянии или нет, и уже после этого выбрать один из четырёх ба-

зисов, к которому принадлежит данное состояние и закончить процедуру измерения, получив в результате этого окончательную информацию о состоянии системы.

В модели Пенроуза такую поэтапную схему измерений предлагается сделать способом, аналогичным используемому в квантовых коммуникациях *кодированию номером пути*. Однако соответствующая процедура измерения не очень естественна в стандартном подходе с использованием КВЦ, поэтому могут потребоваться два вспомогательных кубита, чтобы осуществить первый этап измерения [7].

При этом, чтобы использовать стандартную процедуру измерений, принятую в теории КВЦ, можно использовать идею отложенного запроса, при котором вместо измерения производится взаимодействие состояния с дополнительным кубитом. Каждый такой кубит будет соответствовать «неразрушающему» (отложенному) запросу, находится ли система (кукварт) в некоем состоянии $|\psi\rangle$, и унитарный оператор, выполняющий необходимое взаимодействие, может быть выражен как

$$T_\psi = |\psi\rangle\langle\psi| \otimes X + (\mathbb{1} - |\psi\rangle\langle\psi|) \otimes \mathbb{1}. \quad (5)$$

Если закодировать кукварт набором из двух кубитов, то простейшим примером такого оператора является вентиль Тоффли, соответствующий $|\psi\rangle$ равному $|1\rangle|1\rangle$ или $|3\rangle$.

Подход со вспомогательными кубитами позволяет проще моделировать данный протокол на симуляторах. В любом случае в «наивной» версии протокола в таком двухшаговом подходе уже упомянутая проблема с низкой эффективностью проявляется ещё сильнее. Вероятность того, что оба участника выберут одно и то же состояние, равна $1/40$, а после этого ещё выбирается один из четырёх базисов, доводя вероятность совпадения до $1/160$.

Правда, вероятность того, что после двухшаговой процедуры оба участника выберут один и тот же базис, опять составляет $1/40$, и даже несмотря на то, что при этом в $3/4$ случаев они выбирали разные состояния на первом шаге, согласованный базис всегда позволяет им использовать результат измерений для выработки одинакового ключа.

ЗАКЛЮЧЕНИЕ

В данной работе был рассмотрен основанный на квантовой запутанности протокол распределения ключей, использующий контекстуальность. В основе оригинальной идеи протокола лежит модель, предложенная Пенроузом и основанная на геометрии додекаэдра. Использование конфигурации Виттинга упрощает выражения для квантовых состояний, но теряет прямую связь с геометрией и связанную с ней наглядность.

Чтобы частично исправить этот недостаток, выбрана схема нумерации состояний, использующая набор из 40 карт четырёх мастей достоинствами

от одного («туз») до десяти. Как видно из табл. 3, наборы из четырёх карт, соответствующие 40 базисам, имеют определённую регулярность, отсутствующую при альтернативной индексации, используемой ранее в [7].

В работе не были затронуты вопросы, связанные с практической реализацией протокола. Например, отдельной темой заслуживает анализ, какие именно квантовые системы возможно использовать в качестве куквартов.

Была упомянута низкая эффективность протокола, обратно пропорциональная количеству базисов, перебираемых участниками в процессе обмена. Следует отметить, что измерение с использованием всех 40 наборов необходимо только для проверки условий, связанных с контекстуальностью. Кроме того, даже в этом случае минимально необходимое количество наборов в исходной модели может быть уменьшено до 28 [2].

Помимо этого, в упрощённой версии протокола максимальную эффективность можно обеспечить, если предположить, что хотя и выбор состояний и выбор базисов производится случайно, он может быть согласован для обоих участников. Например, они оба могут использовать один и тот же генератор (псевдо)случайных чисел. Хотя сложно представить, как использовать такую версию для секретных коммуникаций, она может быть полезна для экспериментов связанных с фундаментальными вопросами квантовой теории. Также может быть полезен промежуточный случай, когда выбор, производимый обоими участниками не обязательно одинаков, но некоторым образом коррелирован, чтобы увеличить вероятность совпадения.

Ещё одна возможность сильно повысить эффективность связана с модификацией протокола, кратко описанной далее. Как уже было отмечено, в первоначальной двухшаговой версии протокола участники сначала используют проверку, находится ли система в одном из 40 состояний.

Предположим, участники независимо выбрали для этого какие-то два состояния и у них имеется возможность отложить второе измерение и за это время обменяться информацией, какие именно состояния они выбрали. В этом случае вероятность, что оба состояния одновременно принадлежат какому-нибудь из 40 базисов, составляет $13/40$ (то есть 32.5% и из них 2.5% — вероятность совпадения состояний и 30% — вероятность попадания двух разных состояний в один и тот же базис). В этом случае участники могут использовать этот базис на втором шаге для получения согласованных результатов измерений.

Только что описанный подход скорее похож на *протокол совместной выработки ключа*, хотя в классической криптографии это происходит совсем на других принципах. С технической точки зрения реализация такого квантового протокола может усложнить реализацию, так как требует поддержки между двумя этапами квантового протокола, необходимой для обмена классическими сообще-

ниями, несущими информацию о выбранных состояниях. Необходимо отметить, что перехват только этих сообщений не приводит к утечке информации, так как неизвестно, какие именно результаты измерений будут получены уже после этого обмена в результате выбора согласованного базиса.

БЛАГОДАРНОСТИ

Автор выражает благодарность организаторам и спонсорам XII семинара Клышко за предоставленную возможность участвовать в нём и выступить с приглашённым докладом.

- [1] Penrose R. On Bell non-locality without probabilities: some curious geometry. препринт, Oxford, 1992; перепечатано в: J. Ellis, D. Amati Quantum Reflections. 1–27, CUP, 2000.
- [2] Zimba J., Penrose R. // *Stud. Hist. Phil. Sci.* **24**, 697 (1993).
- [3] Penrose R. // *Shadows of the Mind*, OUP, 1994.
- [4] Majorana E. // *Nuovo Cimento* **9**, 43 (1932).
- [5] Massad J., Aravind P.K. // *Am. J. Phys.* **67**, 631 (1999).
- [6] Waegell M., Aravind P.K. // *Phys. Lett. A* **381**, 1853 (2017); Erratum: *Phys. Lett. A* **384**, 126331 (2020).
- [7] Vlasov A.Y. Penrose dodecahedron, Witting configuration and quantum entanglement. Препринт arXiv:2208.13644 (2022); *Quanta* **13**. 38 (2024).
- [8] Coxeter H.S.M. // *Regular Complex Polytopes*, CUP, 1991.
- [9] Witting A. // *Math. Ann.* **29**, 157 (1887).
- [10] Ekert A. // *Phys. Rev. Lett.* **67**, 661 (1991).
- [11] Durt T., Kaszlikowski D., Chen J.-L., Kwek L.C. // *Phys. Rev. A* **69**, 032313 (2004).
- [12] Cerf N.J., Bourennane M., Karlsson A., Gisin N. // *Phys. Rev. Lett.* **88**, 127902 (2002).
- [13] Кулик С.П., Шурупов А.П. // *ЖЭТФ* **131**, 842 (2007) (Kulik S.P., Shurupov A.P. *J. Exp. Theor. Phys.* **104**, 736 (2007)).
- [14] Cabello A., D'Ambrosio V., Nagali E., Sciarrino F. // *Phys. Rev. A* **84**, 030302(R) (2011).
- [15] Singh J., Bharti K., Arvind // *Phys. Rev. A* **95**, 062333 (2017).

Scheme of quantum communications described by a regular 4D complex polytope

A. Yu. Vlasov^{1,2}

¹*P. V. Ramzaev Research Institute of Radiation Hygiene. St. Petersburg, 197101, Russia*

²*Alexander Friedmann Laboratory for Theoretical Physics. St. Petersburg, 191186, Russia*

E-mail: qubeat@mail.ru, a.vlasov@niirg.ru

Currently, generalizations of quantum communication protocols from qubits to systems with higher-dimensional state spaces (qudits) typically use mutually unbiased bases (MUB), the construction of which is known in any dimension equal to a prime power. However, in small dimensions, there also exist formally more symmetric systems of states, described by regular complex polytopes, which are a generalization of the idea of regular polytopes to complex spaces. This work considers the application of a model originally proposed by R. Penrose and based on the geometry of dodecahedron and two entangled particles with spin 3/2. In a more general case, two arbitrary quantum systems with four basis states (ququarts) can be used instead. It was later shown that this system with 40 states is equivalent to the Witting configuration and is related to the four-dimensional complex polytope described by Coxeter. Presented paper describes how to use this configuration for a quantum key distribution protocol based on contextuality.

PACS: 03.67.-a, 03.67.Bg, 03.67.Dd, 03.67.Ac, 02.20.-a

Keywords: quantum entanglement, quantum communications, contextuality, quantum information, ququarts, Penrose dodecahedron, Witting polytope.

Received 03 December 2024.

English version: *Moscow University Physics Bulletin*. 2025. **80**, No. , pp.

Сведения об авторе

Александр Юрьевич Власов — научный сотрудник; e-mail: qubeat@mail.ru.