

Подход к оценке вычислительного потенциала квантовых компьютеров

А.А. Крючков

Аннотация — Современный этап развития технологии квантовых вычислений предполагает взаимодействие с квантовыми компьютерами преимущественно через облачные сервисы, что исключает возможность физического доступа к удаленным устройствам. В то же время предоставляемые вендорами квантового оборудования калибровочные данные квантовых процессоров могут не соответствовать актуальному техническому состоянию целевого устройства, в том числе в виду функционального отставания некоторых методов оценки качества кубит в современных масштабируемых системах. Работа посвящена формализации подхода по оценке вычислительного потенциала квантовых компьютеров с помощью некоторых прикладных задач, моделирование которых задействует основные ресурсы исследуемых вычислительных систем. Важность вопроса независимого бенчмаркинга приобретает в рамках использования облачных вычислителей, где от достоверности калибровочных данных напрямую зависит структура квантовой схемы и, следовательно, точность генерируемого результата. Результатом оценки предлагаемого подхода является набор квантовых состояний, рекомендуемый к использованию в проектируемых квантовых схемах.

В качестве инструментального средства анализа качества облачных квантовых процессоров использован разработанный автором программный комплекс «QISs_Benchmark», возможности которого позволяют верифицировать технологический портрет вычислителей как до, так и после запуска квантовых схем.

Ключевые слова — квантовые вычислительные устройства, кубит, квантовый регистр, оценка, верификация, вычислительный потенциал, «QISs_Benchmark».

I. ВВЕДЕНИЕ

В настоящее время ведутся активные работы в сфере исследовательских проектов по стандартизации и разработке универсальных методов анализа технических возможностей квантовых вычислительных устройств (КВУ) [1, 2, 3]. Однако, на текущий момент единый регламент проведения соответствующей оценки характеристик квантовых процессоров не принят, в то время как потребность в независимой верификации качества кубит возрастает одновременно с повышением сложности архитектуры исполнения целевых устройств

[4]. Особую важность вопрос независимого бенчмаркинга КВУ приобретает в рамках использования облачных вычислителей, предоставляемых исключительно на коммерческой основе, где от достоверности калибровочных данных напрямую зависит структура квантовой схемы и, следовательно, точность генерируемого результата [5, 6].

К ключевым ресурсам КВУ [7], подлежащим оценке, относят процедуры инициализации квантового состояния, суперпозиции (одиночных) и запутывания (нескольких) кубит. В таком случае, видится закономерной необходимость в разработке подхода по анализу точности выполнения представленных низкоуровневых операций, совокупный итог работы которых может послужить независимой оценкой актуального технологического портрета КВУ, а также способен выступить в качестве метода верификации калибровочных данных, поставляемых производителем квантового оборудования.

Результатом оценки предлагаемого подхода является набор квантовых состояний, рекомендуемый к использованию в проектируемых квантовых схемах.

II. МАТЕМАТИЧЕСКАЯ ПОСТАНОВКА ЗАДАЧИ

A. Исследование ресурса инициализации

Для выявления качества кубит квантового процессора с точки зрения точности выполнения операции инициализации предлагается следующий алгоритм действий:

1. Применить квантовый вентиль *Init-gate* к одиночному кубиту $|q_i\rangle$ k раз, где k – количество повторений квантовой схемы (параметр «shots»)¹. Накопить статистические данные по результатам выполнения покубитной инициализации всего регистра (число ожидаемых «0» и побочных «1» с каждого кубита последовательности $c \in \{0,1\}^k$).

2. Применить квантовый вентиль *Init-gate* ко всему регистру. Накопить статистические данные по результатам инициализации всего регистра.

3. Сопоставить количество побочных бит «1» с каждого кубита для обоих случаев. В случае наблюдения существенных расхождений (на несколько порядков) сделать вывод о неустойчивом состоянии кубита и исключить его из проектируемой схемы.

Аномальное поведение квантовых состояний [при

Статья получена 20 марта 2026.

Крючков Андрей Андреевич, МИРЭА – Российский технологический университет, Москва, Российская Федерация (kryuchkov_a@mirea.ru).

¹ На выходе квантовой схемы [в идеальных условиях] ожидается получение с кубита двоичных бит «0» в количестве k .

инициализации всего регистра] зачастую вызвано влиянием соседних кубит, что проявляется при их активации, не прогнозируется посредством анализа калибровочных данных КВУ и объясняется аппаратным несовершенством архитектуры квантового процессора.

Накопленный массив информации покубитной инициализации предлагается сопоставить с векторами технических параметров регистра КВУ и использовать в качестве обучающей выборки для разработки модели множественной регрессии, с помощью которой для используемого процессора будет возможно проводить предварительный анализ КВУ по актуальным на момент эксперимента калибровочным данным без необходимости запуска квантовой схемы [8].

В. Исследование ресурса суперпозиции

В рамках оценки качества процедуры установки кубита в состояние суперпозиции, предлагается использовать модель квантового генератора случайных чисел (КГСЧ). Вопрос реализации физических датчиков случайных чисел (ДСЧ) имеет прикладное значение [9, 10] и может найти свое практическое применение в т.ч. в рамках моделирования КГСЧ на квантовых компьютерах [11, 12].

Первичный анализ (с запуском квантовой схемы).

1. Моделирование КГСЧ на одиночном кубите.

В некоторых исследованиях для выработки случайной последовательности (СП) задействуется несколько кубит, либо квантовый регистр целиком [13]. Данный подход видится несколько некорректным в виду отличающихся свойств каждого квантового состояния, вследствие чего может возникнуть ситуация, при которой в итоговую последовательность будут подмешиваться слабые с точки зрения распределения двоичные данные, генерируемые нестабильным кубитом с высоким уровнем ошибок вентиляционных преобразований.

Математическая модель КГСЧ на КВУ описывается применением операции Уолша-Адамара (*H-gate*) к одиночному квантовому состоянию, в результате чего генерируется один случайный бит – «0» или «1»:

$$H: |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H: |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Квантовая схема КГСЧ представлена на рисунке 1.

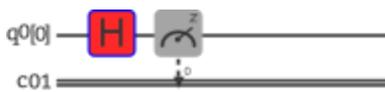


Рис. 1. Квантовая схема КГСЧ на одном кубите.

Имея в распоряжении КВУ разрядностью в *N* кубит при циклическом повторении предложенной квантовой схемы на каждом кубите, будет получено *N* двоичных строк $\{z_i\}_{i=1}^k$ длины $k \in N$.

Для оценки качества ресурса суперпозиции конкретного кубита можно провести анализ статистических свойств распределения каждой СП. Но

учитывая, что самостоятельный анализ больших объемов выборки двоичных данных представляет собой нетривиальную задачу, возникает закономерная потребность в разработке автоматизированных методов исследования на накапливаемых массивов информации.

2. Частотный побитовый тест.

Данный тест подсчитывает наблюдаемую статистику количества бит «0» и «1», определяя степень равномерности распределения двоичных данных для рассматриваемой последовательности длины *k*:

$$s_{obs} = \frac{|S_k|}{\sqrt{k}} \tag{1}$$

Тогда при $X_i = 2x_i - 1$:

$$S_k = \sum_{i=1}^k X_i \tag{2}$$

Через дополнительную функцию ошибок вычисляется значение *P-value*:

$$P_{value} = \text{erfc}\left(\frac{s_{obs}}{\sqrt{2}}\right) \tag{3}$$

P-value сравнивается на уровне значимости α , заданным пользователем.

В случае, если *P-value* превосходит α , принимается гипотеза о равномерности распределения СП (на заданном уровне значимости) и, следовательно, заключается, что ресурс суперпозиции для выбранного кубита является надежным и приемлемым.

Если *P-value* меньше α – рассматриваемый кубит исключается из рассмотрения и не рекомендуется к дальнейшему использованию в проектируемых квантовых схемах.

Преимуществом использования данного подхода является вариативность метода отбора квантовых состояний, что достигается за счет возможности самостоятельной настройки параметра α , изменение которого ужесточает или смягчает предъявляемые требования к равномерности распределения СП, т.е. – к ресурсу суперпозиции для каждого кубита КВУ.

3. Корреляционный анализ.

Корреляционный анализ генерируемых СП сможет показать, являются ли одиночные кубиты самостоятельными (независимыми) источниками случайных данных.

В то же время архитектура квантовых процессоров зачастую предусматривает прямую аппаратную связь между квантовыми состояниями. Тогда для выявления возможного наличия негативного низкоуровневого побочного влияния между кубитами проведение корреляционного анализа также сможет выявить те пары кубит, использование которых не рекомендуется до момента восстановления функциональных свойств КВУ (очевидно, что для выяснения природы подобного влияния и его устранения необходим прямой физический доступ к квантовому устройству).

Для двух СП $\{x_i\}_{i=1}^k$ и $\{z_i\}_{i=1}^k$ корреляционная функция может быть записана как:

$$F_{corr(i)} = \frac{1}{k} \sum_{j=1}^k s_j, i = \overline{0, k}$$

где $s_j = 1$, если $\overline{x(i) \oplus z(i)} = 1$; и $s_j = -1$, если

$x(i) \oplus z(i) = 0$. Для более полного исследования выявления зависимости между СП следует рассчитывать корреляцию для последовательностей с циклическим сдвигом и нормировкой полученных значений. Инверсия, применяемая в вычислениях, необходима для наглядности последующей графической интерпретации результатов.

4. Статистические тесты NIST STS.

Вспомогательным инструментом оценки качества ресурса суперпозиции может выступить набор статистических тестов NIST STS [14], предназначенный для проверки свойств распределения случайных последовательностей, полученных с программных ДСЧ. Чем больше тестов последовательность проходит, тем лучше работает связка «кубит – H-gate». Формирование пограничных значений по определению приемлемого уровня доли прохождения тестов отдается на усмотрение пользователя.

Методики анализа СП, полученных с физических ДСЧ [15] предусматривают обладание математической моделью физического генератора (в данном случае – кубита), однако данная информация вендорами КВУ не распространяется.

Вторичный анализ (по калибровочным данным КВУ).

Накопление результатов моделирования задачи КГСЧ позволит в дальнейшем проводить оценку вычислительного потенциала КВУ по актуальным калибровочным данным без необходимости запуска квантовых схем. Для этого достаточно сопоставить результаты выработки СП с вектором технических параметров соответствующего кубита.

Калибровочные данные, требуемые для регрессионного анализа, представлены в таблице 1.

Таблица 1 – Калибровочные данные как признаки модели

Параметр	Readout	Meas1 Prep0	Meas0 Prep1	(sx)
Значение	Ошибка чтения	Получение значения, ортогональному заданному		Ошибка вентиля (sx)
Признак	X_1	X_2	X_3	X_4

Для оценки ресурса суперпозиции предлагаются следующие подходы:

1. Предсказание количества бит «0».

Модель предсказания числа двоичных бит «0» на всю длину последовательности может быть записана как:

$$Y_{zeropred} = \beta_0 + \beta_1 X_1 + \beta_2 X_3 + \beta_3 X_4.$$

Параметр X_2 в данном контексте не рассматривается, так как является обратным предложенной постановке задачи.

2. Предсказание количества бит «1».

По аналогии, модель множественной линейной регрессии примет следующую форму записи:

$$Y_{onepred} = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_4.$$

В данном случае параметр X_3 заменяется на X_2 , что также следует из логики формулировки отклика модели.

3. Предсказание доли успешного прохождения тестов NIST STS.

Каждому тесту NIST STS методом экспертных оценок ставится в соответствие числовая характеристика $\lambda_1, \lambda_2,$

..., λ_m (где m – число проводимых тестов). Для каждого j -ого теста вычисляется весовой коэффициент:

$$\alpha_j = \lambda_j \left(\sum_{i=1}^m \lambda_i \right)^{-1},$$

где $\sum_{i=1}^m \alpha_i = 1$, тогда $0 < \alpha_j < 1$.

После распределения весовых коэффициентов рассчитывается величина p , отражающая долю прохождения тестов последовательностью с кубита:

$$p = \sum_{i=1}^m \alpha_i \chi(T_i),$$

где $\chi(T_i)$ - индикатор теста T_i такой, что:

$$\chi(T_i) = \begin{cases} 1, \text{ тест пройден} \\ 0, \text{ тест не пройден} \end{cases}$$

При разрядности КВУ в N кубит пользователь получит N числовых характеристик p , значение которого тем лучше характеризует качество ресурса суперпозиции, чем ближе оно к единице.

Модель множественной регрессии по определению ресурса суперпозиции с точки зрения доли прохождения тестов NIST STS примет вид:

$$P_{NISTpred} = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_4.$$

Опытным путем установлено – выбор между параметрами X_2 и X_3 не оказывает значительного влияния на прогностические свойства модели, в связи с чем использование конкретного признака отдается на усмотрение пользователя.

4. Кубит как категориальная переменная.

Одним из вспомогательных инструментов исследования взаимодействия «кубит – H-gate» может послужить рассмотрение квантового состояния в категориальной плоскости, где в случае, если СП с кубита удовлетворяет правилу (1) – (3), ему ставится в соответствие значение «1» (надежный кубит), если нет – «0» (ненадежный кубит).

Для решения поставленной задачи используется логистическая регрессия:

$$F(w_i) = \frac{1}{1 + e^{-w_i}},$$

где $w_i = \beta_0 + \beta_1 X_{i1} + \beta_2 X_{i2} + \dots + \beta_p X_{ip} + \varepsilon_i$.

Вычисление коэффициентов логит-модели происходит в процессе решения системы нелинейных уравнений:

$$\begin{cases} \sum_{i=1}^n (1 + e^{-w_i})^{-1} X_{ji} = \sum_{i=1}^n Y_i X_{ji}, \quad j = \overline{0, p} \\ \sum_{i=1}^n (1 + e^{-w_i})^{-1} = \sum_{i=1}^n Y_i \end{cases}$$

Решение данной системы может быть выполнено итерационным [вычислительным] методом вручную, а также с помощью задействования ресурсов классического и графического процессоров [16].

С. Исследование ресурса запутывания

Для оценки ресурса запутывания двух квантовых состояний, имеющих прямую аппаратную связь, предлагается использовать модель КГСЧ в базисе Белла:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle).$$

В результате моделирования один кубит выступает в роли КГСЧ и передает результирующую последовательность на соседний кубит, запутанный с искомым с помощью применения вентиля преобразования *CNOT-gate*.

Квантовая схема предложенной задачи представлена на рисунке 2.

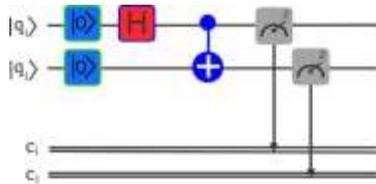


Рис. 2. Квантовая схема КГСЧ в базисе Белла

На выходе работы квантовой схемы ожидается получение двух идентичных последовательностей, однако, в виду аппаратного несовершенства современных КВУ, вероятнее всего будут наблюдаться расхождения в полученных данных. По числу расхождений между двумя СП можно оценить ресурс запутывания двух квантовых состояний по формуле:

$$err = \frac{\sum_{i=1}^k (x_i \oplus z_i)}{k} \cdot 100\%. \quad (4)$$

D. Совокупный анализ ресурсов КВУ

Наконец, проведя независимый анализ качества отдельных квантовых операций, к использованию предлагается метод, объединяющий в себе основные ресурсы КВУ воедино и отражающий более полную информацию о наборе квантовых состояний в количестве от 5 до 7 кубит [17].

Идея метода заключается в распределение СП между двумя или тремя кубитами, что отчасти может соотноситься с модификацией протокола BB84 [18].

В случае использования пяти кубит, СП распределяется между двумя квантовыми состояниями и должна быть идентичной на выходе квантовой схемы для каждого из двух целевых кубит.

При работе с семью кубитами, СП распределяется между тремя квантовыми состояниями таким образом, что в результирующих СП с первого и третьего кубитов степень расхождений в двоичных строках должен сохраняться на уровне около 25%.

Все оставшиеся квантовые состояния выступают в роли КГСЧ, необходимых для выбора базиса кодируемого квантового бита для каждого отдельного повторения моделирования сформулированной задачи. Операция запутывания (*CNOT-gate*) заменена на квантовый вентиль перестановки (*SWAP-gate*). Несоответствия в СП вычисляются по формуле (4).

Квантовая схема расширенной модификации метода на 7 кубит представлена на рисунке 3.

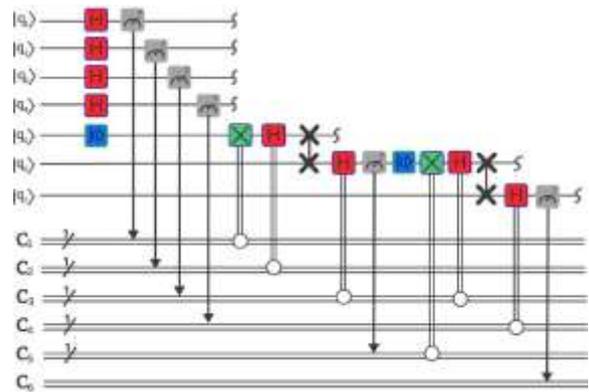


Рис. 3. Квантовая схема распределения СП между кубитами

III. РЕЗУЛЬТАТЫ ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА ДЛЯ ОБЛАЧНЫХ КВУ КОМПАНИИ IBM

В целях практической реализации изложенного подхода с помощью библиотеки квантовых вычислений Qiskit и фреймворка QT5 доработан программный комплекс «QISs_Benchmark» [19], предусматривающий возможность низкоуровневой настройки квантовых схем сформулированных прикладных задач и их моделей, а также содержащий инструментальные средства по накоплению, предобработке и анализу статистических массивов информации. Период проведения экспериментов: январь – июнь 2025 года. Некоторые из результатов тематических исследований были ранее представлены в работах [8, 20, 21].

A. Исследование инициализации квантового регистра

В рамках вычислительного эксперимента были проведены запуски процедуры инициализации КВУ «ibm_brisbane» и «ibm_kyvi» (127 кубит каждый). Количество запусков квантовых схем $2 \cdot 10^4$ повторений.

На рисунке 4 для КВУ «ibm_brisbane» приведены результаты покубитной инициализации (белый маркер), инициализации всего регистра (красный маркер), а также результаты предсказания двух разработанных регрессионных моделей (синий и фиолетовый маркер), где в качестве отклика выступает число бит «1».

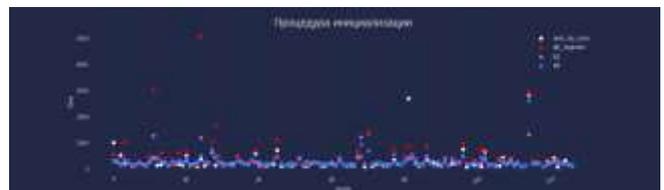


Рис. 4. Инициализация КВУ «ibm_brisbane»

Можно заметить, что при инициализации **всего регистра** на квантовых состояниях «11», «24» и «28» наблюдаются аномально высокие показатели числа зафиксированных бит «1», которые противоречат как результатам покубитной инициализации, так и предсказаниям разработанных моделей. Впоследствии установлено, что подобное поведение обусловлено негативным влиянием некоторых соседних квантовых состояний, имеющих прямую аппаратную связь и оказывающих побочное влияние на целевые кубиты при их активации.

Аналогичные исследования для КВУ «ibm_kyvi»

(рисунок 5) продемонстрировали согласованность наблюдаемых отклонений и предсказаний моделей, за редкими исключениями, которые могут быть обусловлены недостаточностью объема обучающей выборки.

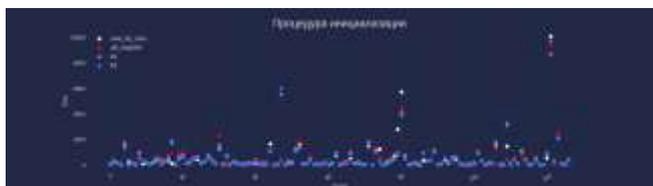


Рис. 5. Инициализация КВУ «ibm_kyvi»

В. Исследование ресурса суперпозиции

Первичный анализ.

Результаты моделирования задачи КГСЧ на одиночных кубитах показали, что равномерность распределения бинарных данных в генерируемых СП, а также число успешно преодолеваемых тестов NIST STS напрямую зависят от вектора технических параметров конкретного кубита – чем ниже уровень ошибок квантовых операций, тем лучше статистические свойства вырабатываемых СП. В то же время, корреляционный анализ показал, что кубиты могут выступать в роли самостоятельных и независимых КГСЧ независимо от калибровочных данных по каждому квантовому состоянию (F_{corr} ни в одном из экспериментов не превышала значения 17×10^{-2}).

Вторичный анализ.

1. Предсказание количества встречаемости бит «0».

На рисунке 6 приведены экспериментальные результаты для КВУ «ibm_brisbane». Белый и фиолетовый маркеры – фактически наблюдаемое число бит «0» для СП длин 2×10^4 и 10^5 бит соответственно, красный и синий – результаты предсказаний (аналогично).

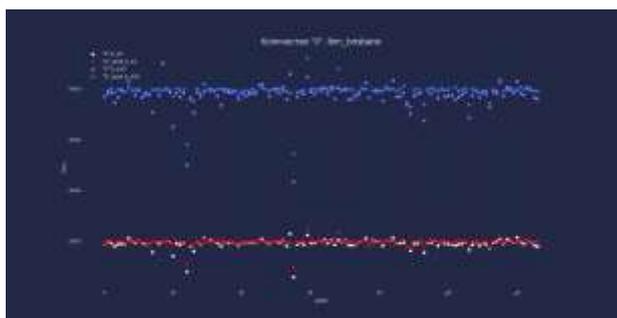


Рис. 6. Количество бит «0» для КВУ «ibm_brisbane»

Погрешность предсказаний для указанных длин не превышала 2%, что демонстрирует хорошие предикативные свойства моделей (для «ibm_kyvi» погрешность составила 3%).

2. Предсказание количества встречаемости бит «1».

На рисунке 7 представлены результаты с идентичными установочными данными за исключением того, что прогнозировалось число встречаемости бит «1» для КВУ «ibm_kyvi».

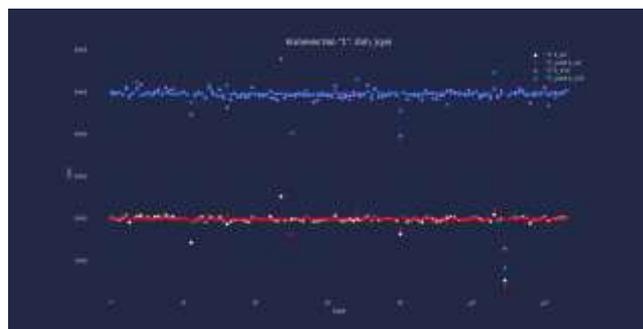


Рис. 7. Количество бит «1» для КВУ «ibm_kyvi»

Погрешность предсказаний сохранялась на уровне 3% (для «ibm_brisbane» – 2%).

3. Предсказание доли успешного прохождения тестов NIST STS.

На рисунке 8 приведены зафиксированные значения прохождения тестов NIST STS (белый маркер) и предсказанные (красный маркер) для длин последовательностей КВУ «ibm_kyvi» в 2×10^4 бит.

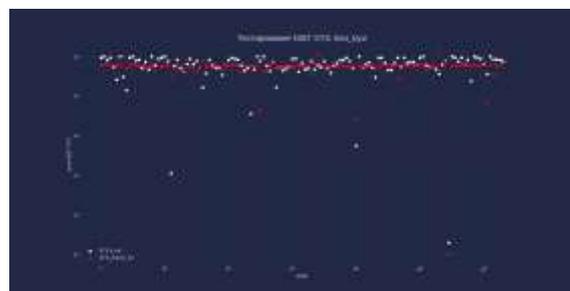


Рис. 8. Прохождение тестов NIST STS «ibm_kyvi»

С увеличением длины последовательностей качество предсказаний ухудшается, что можно видеть из рисунка 9 (длина СП 10^5 бит).

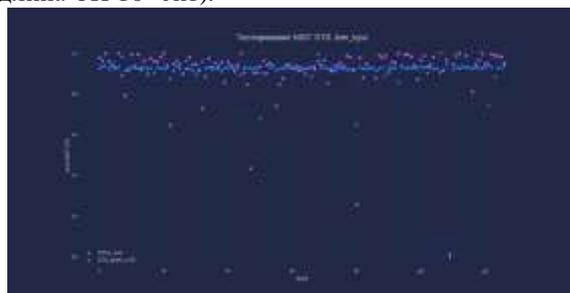


Рис. 9. Прохождение тестов NIST STS «ibm_kyvi»

Расчетная погрешность увеличилась с 4% до 9%. Для КВУ «ibm_brisbane» – с 3% до 9% на аналогичных длинах СП. Предполагается, что с увеличением объема обучающей выборки можно снизить данные показатели. Тем не менее, представленный метод не должен использоваться обособленно и является дополнением к изложенному подходу по оценке вычислительного потенциала КВУ.

4. Предсказание качества кубита по правилу (1) – (3)

Предварительные исследования показали неудовлетворительные результаты анализа таблицы промахов и попаданий. Однако, при постепенной настройке порогового критерия (уровня значимости α) замечено выравнивание показателей попадания. Ожидается, что в рамках дальнейших исследований

удастся улучшить изложенный метод классификации квантовых состояний на предмет выработки равномерных последовательностей.

C. Исследование ресурса запутывания

В ходе экспериментов генерировались СП на кубитах, имеющих разные параметры ошибки вентиляционной операции *CNOT-gate*, *(sx)-gate*, ошибки чтения (*Readout error*). Результаты некоторых из них (длинами 2×10^4 бит) для КВУ «*ibm_brisbane*» приведены в таблице 2.

Таблица 2. Моделирование КГСЧ в базе Белла

Readout error	(sx) error	ECR error	Кубиты	err. %
0,041	3,2e-4	0,004	0	4,60
0,033	1,6e-4		1	
0,086	1,3e-4	0,025	70	25,56
0,215	1,1e-3		74	
0,119	2,2e-4	0,182	24	68,52
0,034	1,9e-4		34	

Замечено, что калибровочные данные в достаточной мере отражают качество запутывания квантовых состояний. Для автоматизации оценки вычислительного потенциала следует разработать соответствующую модель множественной регрессии.

D. Объединенное исследование ресурсов КВУ

Испытания проводились на КВУ «*ibm_brisbane*» для СП длинами $2 \cdot 10^4$ бит.

При распределении СП между «81» и «82» кубитами процент расхождений в СП составил 3,68%. При назначении «82» кубита промежуточным состоянием и добавлении конечного состояния «83» несоответствия увеличились до 28,56%.

Аналогичный опыт проведен для кубит «124», «125», «126», где отличия в СП увеличились с 3,44% до 28,00%.

Данные результаты свидетельствуют, что:

– Теоретические предпосылки верны и добавление промежуточного состояния при распределении СП между кубитами увеличивает процент несоответствий на ~25% (к уже имеющимся расхождениям).

– Сопоставление результатов экспериментов с калибровочными данными может послужить фундаментом для разработки регрессионных моделей, обеспечивающих превентивный анализ КВУ на обособленных группах квантовых состояний.

IV. ЗАКЛЮЧЕНИЕ

Предложен комплексный подход по оценке вычислительного потенциала КВУ, с учетом ключевых ресурсов квантовых компьютеров.

Продемонстрированы результаты экспериментальных исследований, последовательность действий при составлении технологического портрета КВУ, приведены примеры анализа и интерпретации получаемых результатов.

На момент проведения экспериментов для КВУ «*ibm_brisbane*» из 127 кубит приемлемые характеристики демонстрировали порядка ~60 кубит, для «*ibm_kyvi*» – около ~80 квантовых состояний.

БЛАГОДАРНОСТИ

Автор благодарит заведующего базовой кафедрой РТУ МИРЭА №252, к.т.н., член-корреспондента Академии криптографии Российской Федерации Королькова Андрея Вячеславовича за многолетнюю вовлеченность в проводимые исследования, формирование научного фундамента, бесценный опыт, свободу творческого самовыражения. Автор выражает особую благодарность Сергею Ивановичу С., Анатолию Анатольевичу К., Александру Викторовичу Х., Геннадию Николаевичу М., много лет выступающих в качестве строгих, но честных оппонентов, искренне поддерживающих начинания автора. Представленные исследования являются промежуточным законченным результатом научных изысканий, которые оказались возможными во многом благодаря всесторонней поддержке перечисленных коллег, наставников и старших товарищей.

БИБЛИОГРАФИЯ

- [1] Information technology. Quantum computing. Vocabulary. ISO/IEC 4879. 2024. [Электронный ресурс] Дата обращения: 21.03.2026. <https://cdn.standards.iteh.ai/samples/80432/2735b24c77494248b92d91c333dbcb0/ISO-IEC-4879-2024.pdf>.
- [2] Altpeter J. *Quantum Benchmarking Initiative (QBI)*. DARPA. 2024. [Электронный ресурс] Дата обращения: 21.03.2026. <https://www.darpa.mil/sites/default/files/attachment/2024-12/qbi-proposers-day-2024-program-manager.pdf>.
- [3] Darwish A., Grossi M., Vallecorsa S., et al. *A scalable, more extensible architecture for ABAQUS*. 2023. [Электронный ресурс] Дата обращения: 21.03.2026. <https://zenodo.org/records/7528880>.
- [4] McKay D., Hincks I., Pritchett E., et al. Benchmarking Quantum Processor Performance at Scale. // *arxiv*. 2023. [Электронный ресурс] Дата обращения: 21.03.2026. <https://arxiv.org/pdf/2311.05933>.
- [5] Lubinski T., Coffrin C., McGeoch C., et al. Optimization Applications as Quantum Performance Benchmarks. // *ACM Transactions on Quantum Computing*. 2024. Vol. 5. Iss. 3. Pp. 1–14.
- [6] Крючков А.А., Комогоров К.Е. *Неочевидные аспекты бенчмарка квантовых вычислительных устройств на примере генерации случайных чисел*. // Правовая информатика. 2024. №4. С. 42–51.
- [7] Алиев Ф.К., Корольков А.В., Матвеев В.А. *Несепарабельные состояния многокубитных квантовых систем*. Монография / Под ред. Ф. К. Алиева. М.: Радиотехника, 2017. 320 с.
- [8] Крючков А.А., Пастухова Ю. И. *Выявление неустойчивых кубит квантового компьютера на стадии инициализации квантового регистра* // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. 2025. №06/2. С. 114–122 DOI 10.37882/2223-2966.2025.06-2.17
- [9] Петренко А.А., Ковалев А.В., Бугров В.Е. *Генерация случайных чисел с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками* // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 6. С. 962–968.
- [10] Бальгин К.А., Кулик С.П., Молотков С.Н., *Реализация квантового генератора случайных чисел: экстракция доказуемо случайных битовых последовательностей из коррелированных марковских цепочек* // Письма в ЖЭТФ. 2024. Т. 119. №7. С. 533–544.
- [11] Li Y., Fei Y., Wang W. et al. Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol. // *Sci Rep*. 2021. Vol. 11. Iss. 1. Pp. 23873
- [12] Salehi R., Razaghi M., Fotouhi B. Hybrid Hadamard and Controlled-Hadamard Based Quantum Random Number Generators in IBM QX. // *Physica Scripta*. 2022. Vol. 97. Iss. 6. Pp. 065101.
- [13] Орлов М., Нечаев К., Резниченко С. *Оценка статистических свойств и криптографической стойкости случайных последовательностей, полученных квантовым компьютером IBM* // Безопасность информационных технологий. 2023. Т. 30. № 1. С. 14–26.
- [14] NIST SP 800-22. Набор статистических тестов проверки генераторов случайных чисел. NIST STS. 2010. Дата обращения:

22.03.2026. <https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software>.

- [15] Проект методики по криптографической защите информации. ТК-26. 2025. Дата обращения: 22.03.2026 <https://tc26.ru/forum/viewtopic.php?f=61&t=1299&p=3441&hilit=ФСЧ#p3441>
- [16] Недожогин Н.С., Копысов С.П., Новиков А.К. *Параллельное решение систем линейных уравнений на гибридной архитектуре CPU+GPU* // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика. 2020. Т. 9/ № 2. С. 40–54.
- [17] A.A. Kryuchkov, A.V. Korolkov. Simulation of some security tasks for secure telecommunications using a quantum-computing simulator in one of the quantum programming languages. // *XIX International Workshop on New Approaches to High-Tech: Nano-Design, Technology, Computer Simulations*. 2021. Pp. 116-117.
- [18] Bennett C., Francois B., Brassard G. Experimental quantum cryptography. // *Journal of Cryptology*. 1991. Vol. 5. Pp. 3–28.
- [19] Свидетельство о регистрации программы для ЭВМ № RU2025613655 Российская Федерация, QISs_v.0.3.9 : N 2025611456 : заявл. 28.01.2025 : опубли. 13.02.2025.
- [20] Корольков А.В., Крючков А.А. *Подход к выявлению оптимального набора кубит квантовых вычислительных устройств на примере модели генерации случайных двоичных последовательностей* // Российский технологический журнал. 2025. Т. 13, Вып. 6. С. 25–46.
- [21] Крючков А.А., Пастухова Ю.И. *Подходы к прогнозированию результатов выработки случайных двоичных последовательностей, генерируемых на квантовых вычислительных устройствах* // Доклады ТУСУР. Т. 28, Вып. 2. С. 96–105.

An approach to assessing the computational potential of quantum computers

Andrey A. Kryuchkov

Annotation — The current stage of development of quantum computing technology involves interaction with quantum computers mainly through cloud services, which eliminates the possibility of physical access to remote devices. At the same time, the calibration data of quantum processors provided by vendors of quantum equipment may not correspond to the current technical condition of the target device, including due to the functional lag of some methods for evaluating the quality of qubits in modern scalable systems. The paper is devoted to the formalization of an approach to assessing the computational potential of quantum computers using some applied tasks, the modeling of which uses the main resources of the studied computing systems. The issue of independent benchmarking is becoming increasingly important in the context of cloud computing, where the reliability of calibration data directly affects the structure of the quantum circuit and, consequently, the accuracy of the generated results. The evaluation of the proposed approach yields a set of quantum states recommended for use in the designed quantum circuits. The software package "QISs_Benchmark" developed by the author is used as a tool for analyzing the quality of cloud quantum processors, the capabilities of which allow verifying the technological portrait of computers both before and after the launch of quantum circuits.

Keywords — quantum computing devices, qubit, quantum register, evaluation, verification, computing potential, «QISs_Benchmark».

REFERENCES

- [1] Information technology. Quantum computing. Vocabulary. ISO/IEC 4879. 2024. Available at: <https://cdn.standards.itech.ai/samples/80432/2735b24c77494248b92d91c333dbcdb0/ISO-IEC-4879-2024.pdf>.
- [2] Altepeter J. Quantum Benchmarking Initiative (QBI). DARPA. 2024. Available at: <https://www.darpa.mil/sites/default/files/attachment/2024-12/qbi-proposers-day-2024-program-manager.pdf>.
- [3] Darwish A., Grossi M., Vallecorsa S., et al. A scalable, more extensible architecture for ABAQUS. 2023. Available at: <https://zenodo.org/records/7528880>.
- [4] McKay D., Hincks I., Pritchett E., et al. Benchmarking Quantum Processor Performance at Scale. arxiv. 2023.
- [5] Lubinski T., Coffrin C., McGeoch C., et al. Optimization Applications as Quantum Performance Benchmarks. ACM Transactions on Quantum Computing, vol. 5, no. 3, pp. 1–14, 2024.
- [6] Kryuchkov A.A., Komogorov K.E. Non-obvious aspects of the benchmark of quantum computing devices using the example of random number generation. Pravovaya informatika, no. 4, pp. 42–51, 2024. [Rus]
- [7] Aliev F.K., Korolov A.V., Matveev V.A. Non-separable states of multi-qubit quantum systems. M., Radio engineering. 2017. [Rus]
- [8] Kryuchkov A.A., Pastuhova Y.I. Identification of unstable qubits of a quantum computer at the initialization stage of a quantum register. Modern Science: actual problems of theory & practice. Series Natural & Technical Science, №06/2, pp. 114–122, 2025. doi: 10.37882/2223-2966.2025.06-2.17 [Rus]
- [9] Petrenko A.A., Kovalev A.V., Bougrov V.E. Random number generation with arrays of coupled quantum-dot micropillar lasers. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 21, no. 6, pp. 962–968, 2021 doi: 10.17586/2226-1494-2021-21-6-962-968. [Rus]
- [10] Balygin, K.A., Kulik, S.P., Molotkov, S.N. Implementation of a Quantum Generator of Random Numbers: Extraction of Provably Random Bit Sequences from Correlated Markov Chains. Jetp Lett., vol. 119, pp. 538–548, 2024. doi:10.1134/S0021364024600575
- [11] Li Y., Fei Y., Wang W. et al. Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol. Sci Rep., vol. 11, no. 1, p. 23873, 2021.
- [12] Salehi R., Razaghi M., Fotouhi B. Hybrid Hadamard and Controlled-Hadamard Based Quantum Random Number Generators in IBM QX. Physica Scripta, vol. 97, no. 6, p. 065101, 2022.
- [13] Orlov M.A., Nechaev K.A., Reznichenko S.A. Evaluation of statistical properties and cryptographic strength of random sequences obtained by an IBM quantum computer. IT Security, vol. 30, no. 1, pp. 14–26, 2023. doi: 10.26583/bit.2023.1.01. [Rus]
- [14] NIST SP 800-22. Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. 2010. Available at: <https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software>.
- [15] Draft methodology for cryptographic information protection. Technical Committee 26. 2025. Available at: <https://tc26.ru/forum/viewtopic.php?f=61&t=1299&p=3441&hilit=ФГЧ#p3441>.
- [16] Nedozhgin N.S., Kopysov S.P., Novikov A.K. Parallel Solving of Linear Equations Systems on Hybrid Architecture CPU+GPU. Bulletin of the South Ural State University. Series: Computational Mathematics and Software Engineering, vol. 9, no. 2, pp. 40–54, 2020. doi: 10.14529/cmse200203.
- [17] A.A. Kryuchkov, A.V. Korolov. Simulation of some security tasks for secure telecommunications using a quantum-computing simulator in one of the quantum programming languages. In XIX International Workshop on New Approaches to High-Tech: Nano-Design, Technology, Computer Simulations. 2021. Pp. 116–117. [Rus]
- [18] Bennett C., Francois B., Brassard G. Experimental quantum cryptography. Journal of Cryptology, vol. 5, pp. 3–28, 1991.
- [19] Kryuchkov A.A., QISs_v.0.3.9. Patent RF, no. RU2025613655, 2025. [Rus]
- [20] Korolov A.V., Kryuchkov A.A. Approach for identifying the optimal set of qubits of quantum computing devices based on a model for generating binary random sequences. Russian Technological Journal, vol. 13, no. 6, pp. 25–46, 2025. doi: 10.32362/2500-316X-2025-13-6-25-46
- [21] Kryuchkov A.A., Pastuhova Y.I. Approaches to predicting the results of generating random binary sequences generated on quantum computing devices. Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki, vol. 28, no. 2, pp. 96–105, 2025. [Rus]

About of Author

Andrey Andreevich Kryuchkov, MIREA – Russian Technological University, Moscow, Russian Federation (kryuchkov_a@mirea.ru).