НЕОЧЕВИДНЫЕ АСПЕКТЫ БЕНЧМАРКА КВАНТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ НА ПРИМЕРЕ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ

Крючков А.А.[1], Комогоров К.Е.[2]

Ключевые слова: *квантовый компьютер, генератор случайных чисел, бенчмарк, кубит, квантовое программирование, случайная последовательность, статистический анализ, вентиль Адамара.*

Аннотация

Цель работы: формирование последовательности действий при проведении и анализе результатов бенчмарка квантовых вычислительных устройств на примере использования квантовых компьютеров в задачах генерации случайных чисел.

Методы: системный анализ, классификация, практическое моделирование, графический и табличный методы анализа.

Результаты: реализован подход по исследованию и предварительной оценке возможностей квантовых компьютеров с помощью инструментов разработанного программного комплекса проведения бенчмарка квантовых вычислительных устройств, в рамках которого квантовый процессор используется для генерации случайных двоичных последовательностей. На основании полученных данных пользователю предлагается оптимальный набор квантовых состояний, которые в последующем могут использоваться для решения более трудоемких прикладных задач.

Сформулированы и на практическом примере продемонстрированы некоторые неочевидные следствия результатов бенчмарка, заслуживающие более предметного анализа для формирования полной картины о технических характеристиках и производительности исследуемого квантового компьютера.

DOI: 10.24412/1994-1404-2024-4-42-51

Введение

Нарастающий интерес к квантовым вычислениям[3] во многом вызван актуальностью и характером гипотетически решаемых задач, которые в обозримом будущем могут быть успешно выполнены на масштабируемых и устойчивых к ошибкам квантовых компьютерах, в то время как классическая вычислительная техника справится с подобными вызовами за приемлемое время [в теории] будет не способна по причине физической ограниченности исполнения классической технологии.

Одной из наиболее актуальных областей применения квантовых вычислительных устройств (КВУ) является криптоанализ [24-28]. Однако, по некоторым оценкам[4], как минимум до 2030 года уровень технического развития отрасли квантовых вычислений не предполагает решения сколь-нибудь практически значимых задач [в области информационной безопасности (ИБ)], что обусловлено некоторыми трудностями преодоления барьера между чувствительностью квантовых процессоров к внешнему воздействию и аппаратному

[3] Квантовая экономика // WEF, 2024. URL: https://www.weforum.org/publications/quantum-economy-blueprint/ (дата обращения: 30.11.2024).

[4] Квантовые технологии в Дании // KPMG, 2021. URL: https://assets.kpmg.com/content/dam/kpmg/dk/pdf/dk-2020/11/Quantum-technology-in-Denmark.pdf (дата обращения: 30.11.2024).

[1] ***Крючков Андрей Андреевич****, старший преподаватель ФГБОУ ВО «МИРЭА – Российский технологический университет», Институт Искусственного Интеллекта, кафедра информационной безопасности, Российская Федерация, г. Москва.*

E-mail: kryuchkov_a@mirea.ru

[2] ***Комогоров Кирилл Евгеньевич****, студент 5 курса ФГБОУ ВО «МИРЭА – Российский технологический университет», Институт Искусственного Интеллекта, кафедра информационной безопасности, специалист по тестированию на проникновение BI.ZONE, Российская Федерация, г. Москва.*

E-mail: komogorovk@mail.ru

несовершенству NISQ-устройств и степенью масштабируемости КВУ [1].

Тем не менее в перспективе большинством специалистов, опрошенных аналитическими агентствами[5], ожидается, что квантовые компьютеры будут постепенно модернизированы и выведены на достаточный уровень готовности технологии, чтобы успешно использоваться для работы в качестве одного из незаменимых инструментов в руках профильных криптоаналитиков.

С учетом вышесказанного непосредственный интерес представляет разработка метода первичной оценки технических возможностей квантовых компьютеров, который бы с минимальными вычислительными затратами и с некоторыми допущениями отражал наиболее близкий к реальности уровень вычислительного потенциала исследуемого устройства.

По мнению авторов, одним из таких подходов может выступить бенчмарк КВУ в контексте выполнения типовых задач ИБ, где в состав комплекса в качестве независимых алгоритмов тестирования могут войти: процесс генерации случайных чисел (ГСЧ), моделирование протокола квантовой криптографической системы выработки и распределения ключа (ККС ВРК), квантовое преобразование Фурье.

В представленном исследовании будет продемонстрирован метод анализа КВУ на примере его использования в качестве квантового ГСЧ (КГСЧ), а также акцентированы некоторые неочевидные следствия, вытекающие из интерпретации полученных результатов.

Подходы к стандартизации бенчмарков квантовых компьютеров

На сегодняшний день в индустрии квантовых вычислений отсутствует единый общепринятый стандарт оценки производительности и достоверности заявляемых характеристик произвольного квантового компьютера с помощью наборов специализированных тестов – бенчмарка. Известно о проведении подобных научных работ в военном исследовательском институте США[6] и в Ассоциации стандартизации Института IEEE[7], однако информация о результатах исследований не публиковалась. Оба проекта стартовали в 2021 году сроком на 4 года.

В Российской Федерации развитие квантовых технологий выполняется под контролем государственных организацией в соответствии с принятой в 2019 году Дорожной картой[8]. На данный момент в области стандартизации рассматриваемой отрасли в России уже представлены предварительные национальные стандарты по квантовым коммуникациям[9] и квантовому Интернету вещей[10], в то время как аналогичные документы по квантовым вычислениям отсутствуют – возможно, по причине недостаточного уровня готовности технологии в нашей стране, а также в связи с уделением бóльшего внимания первоочередным вопросам обеспечения защиты информации со стороны регулятора РФ и профильных организацией[11] [23].

Глобально отсутствие стандартов по проведению комплексного тестирования квантовых процессоров обусловлено двумя причинами.

Во-первых, до конца неизвестно, по какой технологической карте пойдет развитие квантовых компьютеров в среднесрочной перспективе. Каждая из четырех имеющихся технологий [ионы, атомы, фотоны, сверхпроводники] имеет свои особенности и принципиальные, местами непересекающиеся отличия от конкурентных направлений.

Во-вторых, начиная с 2016 года, когда был представлен первый в мире облачный квантовый компьютер на 1 кубит, темпы развития зарождающейся отрасли квантовых вычислений только увеличиваются, в связи с чем некоторые метрики и характеристики КВУ за короткий промежуток времени теряют свою актуальность и репрезентативность, в связи с чем необходим периодический пересмотр принятых подходов по оценке производительности КВУ, что усложняет разработку долгосрочного регламента.

Таким образом, с одной стороны, на начальных этапах не стоит торопиться с принятием итогового стандарта по исследованию потенциала квантовых компьютеров. В то же время, без возможности достоверной и однозначно-интерпретируемой оценки характеристик произвольного КВУ существует вероятность замедления процесса исследований, развитие технологии по ложному пути, извлечение коммерческой выгоды на разработках и эксплуатации устройств, не соответствующих предъявляемым требованиям.

Вопрос о необходимости принятия единого стандарта по оценке производительности и верификации [сертификации] квантовых вычислительных устройств поднимался в работе [2]. Современные тенденции по методикам выполнения и проведения бенчмарков квантовых компьютеров подробно изложены в исследованиях [3-6]. С бенчмарками, разработанными

[5] См., напр.: Quantum Technology Monitor // McKinsey Digital, 2024. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage#/ (дата обращения: 30.11.2024).

[6] Количественная оценка полезности квантовых компьютеров // DARPA, 2021. URL: https://www.darpa.mil/news-events/2021-04-02 (дата обращения 30.11.24).

[7] P7131. Стандарт показателей производительности квантовых вычислений и сравнительный анализ производительности // IEEE SA, 2021. URL: https://standards.ieee.org/ieee/7131/10681/ (дата обращения: 30.11.2024).

[8] Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» // МинЦифры РФ, 2019. URL: https://digital.gov.ru/ru/documents/6650/

[9] ПНСТ 829-2023; ПНСТ 830-2023.

[10] ПНСТ 831-2023; ПНСТ 832-2023; ПНСТ 906-2023; ПНСТ 907-2023.

[11] См., напр., ТК-26: «В России разработан криптографический механизм, способный выдерживать атаки квантовых компьютеров», 2024. URL: https://tc26.ru/news/novosti-kriptografii/v-rossii-razrabotan-kriptograficheskiy-mekhanizm-sposobnyy-vyderzhivat-ataki-kvantovykh-kompyuterov.html?sphrase_id=84911 (дата обращения 30.11.24).

независимыми исследовательскими группами, можно ознакомиться в научных трудах [7-13].

Бенчмарк КВУ для специалистов в области ИБ

Основываясь на перспективной, но пока нереализуемой на практике области применения квантовых компьютеров, подразумевая задачи криптоанализа, авторам видится закономерным и обоснованным разработка бенчмарка, нацеленного на специалистов в области информационной безопасности. Для этого предлагается объединить в единый программный комплекс три типовых алгоритма: КГСЧ, моделирование протокола ККС ВРК, квантовое преобразование Фурье.

Генерация случайных чисел на квантовом компьютере призвана разрешить один из парадоксов квантовых вычислений – как из классического мира, находясь в классе сложности BPP, оценить правильность выполнения алгоритмической задачи, запускаемой в квантовом мире – классе сложности BQP. Другими словами, каким образом можно оценить корректность получаемого результата, в условиях отсутствия возможности смоделировать задачу на классическом устройстве и вычислить верный ответ.

Единственный очевидный вариант верификации квантового устройства – переход к анализу классических данных, поддающихся однозначной обработке и интерпретации. В контексте КГСЧ – проверка генерируемой случайной последовательности (СП) на статистическую (не)зависимость (например, тестами NIST STS), что может косвенно говорить о «квантовости» квантового компьютера.

Второй не менее актуальной задачей, с точки зрения практического применения сгенерированных последовательностей в сфере ИБ, выступает создание ключа шифрования для алгоритмов симметричной криптографии. Очевидно, что двоичные последовательности, полученные на облачном устройстве (независимо от его квантовой природы), в действующих криптографических системах применять запрещено. Однако для демонстрации такой возможности в будущих квантовых компьютерах, которые, предположительно, могут стать более доступными, переносимыми и универсальными – практическое моделирование потенциальной возможности применения КВУ в качестве КГСЧ может послужить отправной точкой для будущих испытаний.

Для более детального изучения вопроса КГСЧ в области информационной безопасности можно обратиться к научной литературе, в которой представлены исследования аппаратных устройств, нацеленных и реализующих исключительно функции квантовых генераторов случайных чисел [19-22].

Моделирование протоколов ККС ВРК на КВУ преследует две цели.

Во-первых, предлагает практическое исследование существующих и перспективных способов распределения ключей без необходимости конструирования опытного макета, реализующего весь функционал «квантового» оборудования.

Во-вторых, расширяет область покрытия тестируемых технических характеристик квантового процессора. В схему включаются вентили связывания квантовых состояний, которые принципиальным образом меняют весь процесс тестирования функциональных возможностей устройства [по сравнению с КГСЧ]. Увеличивается глубина квантовой схемы и добавляются новые параметры, влияющие на результат тестирования (напр. ошибка подготовки квантового состояния, метрика EPLG).

Квантовое преобразование Фурье является завершающим элементом бенчмарка, который более других приближен к целевым задачам, использующим весь вычислительный потенциал квантового компьютера. Схема QFT (Quantum Fourier Transform) заложена в основу алгоритма Шора, раскладывающего числа на простые множители.

Таким образом, итоговый алгоритм и ожидаемый результат работы предлагаемого бенчмарка для ИБ-специалистов будет следующим.

Тест 1 : КГСЧ. Предварительная проверка устойчивости кубит квантового регистра и корректности применения преобразования Уолша-Адамара (частный случай QFT). По результатам тестирования формируется оптимальный набор кубит, сохраняемый в качестве промежуточного результата.

Тест 2 : ККС ВРК. Определение лучших сочетаний кубит при использовании вентилей спутывания квантовых состояний с одновременной проверкой корректности использования операции инициализации. Итог тестирования – корректировка сформированного в рамках первого теста набора кубит с учетом полученных данных на втором шаге исследования КВУ.

Тест 3 : QFT. По результатам двух первых испытаний итоговый набор кубит подается на вход завершающего теста. В зависимости от количества рекомендованных квантовых состояний и степени их удаления друг от друга генерируется схема квантового преобразования Фурье. Проверяется корректность его выполнения.

Подведение итогов. В качестве числовых показателей, отражающих характеристики и потенциал исследуемого КВУ, предлагаются метрики:

- *скорость выполнения квантовой схемы*. Помимо демонстрации скорости работы КВУ, при прочих равных показателях метрика будет полезной при выборе квантового компьютера, на котором планируется запуск квантовых программ, что становится особенно актуальным, учитывая коммерциализацию отрасли квантовых вычислений, где стоимость одной минуты работы облачного КВУ может начинаться от 10 тыс. рублей[12].
- *оптимальный набор кубит* [всего регистра КВУ]. Отражает количество квантовых состояний,

[12] Платформа облачных квантовых вычислений // IBM Quantum Platform. URL: https://quantum.ibm.com/ (дата обращения 30.11.24).

успешно справляющихся с поставленными задачами в области информационной безопасности.

– *точность получаемых результатов*. Позволяет оценить, насколько приближенны вычисленные данные к ожидаемым. Информация окажется полезной при масштабировании квантовой схемы.

Определив цель и задачи бенчмарка квантовых вычислительных устройств, перейдем к практическому моделированию и демонстрации работы системы оценки КВУ на примере задачи генерации двоичной СП.

Квантовый компьютер и задача генерации случайных чисел

Порядок разработки программного обеспечения и правила построения квантовых схем для квантовых компьютеров имеют существенные отличия от привычных и устоявшихся классических подходов. Некоторые особенности методов квантового программирования по отношению к технологиям и методам классического программирования были рассмотрены в работах [14-17].

Для создания программного комплекса «QISs_v.0.3», задачей которого является проведение бенчмарка квантовых компьютеров, задействованы:

– библиотека для разработки с открытым исходным кодом «Qiskit»;
– кроссплатформенный набор инструментов и виджетов «Qt5»;
– набор статистических тестов NIST STS[13].

Для выполнения исследований использованы облачные квантовые компьютеры компании IBM[14]. Программная реализация «QISs_v.0.3» расположена в репозитории GitHub[15].

В более ранних научных работах была продемонстрирована возможность и реализуемость выполнения подобных экспериментов, однако малое количество квантовых состояний не позволяло должным образом масштабировать квантовую схему и проводить полноценные исследования вариаций использования и анализа генерируемых СП [18].

На сегодняшний день в облачном доступе находятся КВУ, имеющие 127 кубит, что предоставляет значительно больше полезной информации о способах генерации случайных двоичных последовательностей на квантовых компьютерах. Первые предварительные результаты КГСЧ на современных масштабируемых облачных КВУ были представлены в ноябре 2024 года на конференции «Радиоинфоком-2024»[16].

Перейдем к математической постановке задачи. Фундаментальной единицей произвольного КВУ является кубит, представляющий собой единичный вектор в двумерном комплексном векторном пространстве:

$$|y\rangle = c_1|0\rangle + c_2|1\rangle, \quad (1)$$

где c_1, c_2 – произвольные комплексные числа, амплитуды вероятностей кубита с базисом в виде ортогональных векторов $|0\rangle, |1\rangle$, связанные отношением:

$$|c_1|^2 + |c_2|^2 = 1. \quad (2)$$

Амплитуды вероятностей выступают в качестве координат квантового состояния в гильбертовом пространстве. Они могут быть заданы в различных эквивалентных представлениях, связанных друг с другом унитарными преобразованиями, которые описывают эволюцию системы в процессе работы квантовой схемы/алгоритма.

$$|y'\rangle = U|y\rangle, \quad (3)$$

где матрица *U* удовлетворяет требованию однородности во времени:

$$U(t_1 + t_2) = U(t_1)U(t_2). \quad (4)$$

Из всего доступного набора унитарных преобразований отдельного внимания заслуживает однокубитное преобразование Уолша-Адамара, задающееся матрицей:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (5)$$

Преобразование (5) устанавливает кубит в состояние суперпозиции, в результате чего измерение кубита [в идеальных условиях] выдает с равной вероятностью либо классический бит '0', либо '1':

$$\begin{aligned} H:|0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H:|1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}. \quad (6)$$

Как можно видеть из (2) и (6), не имеет значения, в каком состоянии кубит был инициализирован перед применением к нему оператора (5). В таком случае, тест КГСЧ может отразить совокупную точность выполнения преобразования (5), успех временного поддержания кубита в состоянии (6) и корректность завершающих измерений с последующим коллапсом волновой функции до классического состояния ['0' или '1'].

В рамках сформулированной модели квантовый процессор не является самостоятельным генератором случайных чисел – КВУ разбивается на отдельные независимые КГСЧ, в качестве которых выступают отдельные кубиты, находящиеся в квантовом регистре исследуемого устройства.

Выполним практическое моделирование теста КГСЧ. Интерфейс программы «QISs_v.0.3» [Quantum Information Security] представлен на рис. 1.

Заметим – программа проводит исследования на квантовых компьютерах компании IBM, построенных на технологии сверхпроводников. В связи с этим полу-

[13] SP 800-22. NIST STS // NIST. URL: https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final

[14] Платформа облачных квантовых вычислений // IBM Quantum Platform. URL: https://quantum.ibm.com/ (дата обращения 30.11.24).

[15] Облачный репозиторий проектов GitHub / «QISs» : [Электронный ресурс]. — Режим доступа: https://github.com/KomogorovKirill/QISs (дата обращения 30.11.24).

[16] VIII МНПК «Актуальные проблемы и перспективы радиотехнических и инфокоммуникационных систем». URL: https://forum.mirea.ru/_(дата обращения 30.11.24).

чаемые в ходе экспериментов результаты могут отличаться от аналогичных опытов, выполненных на КВУ с иным аппаратным обеспечением.

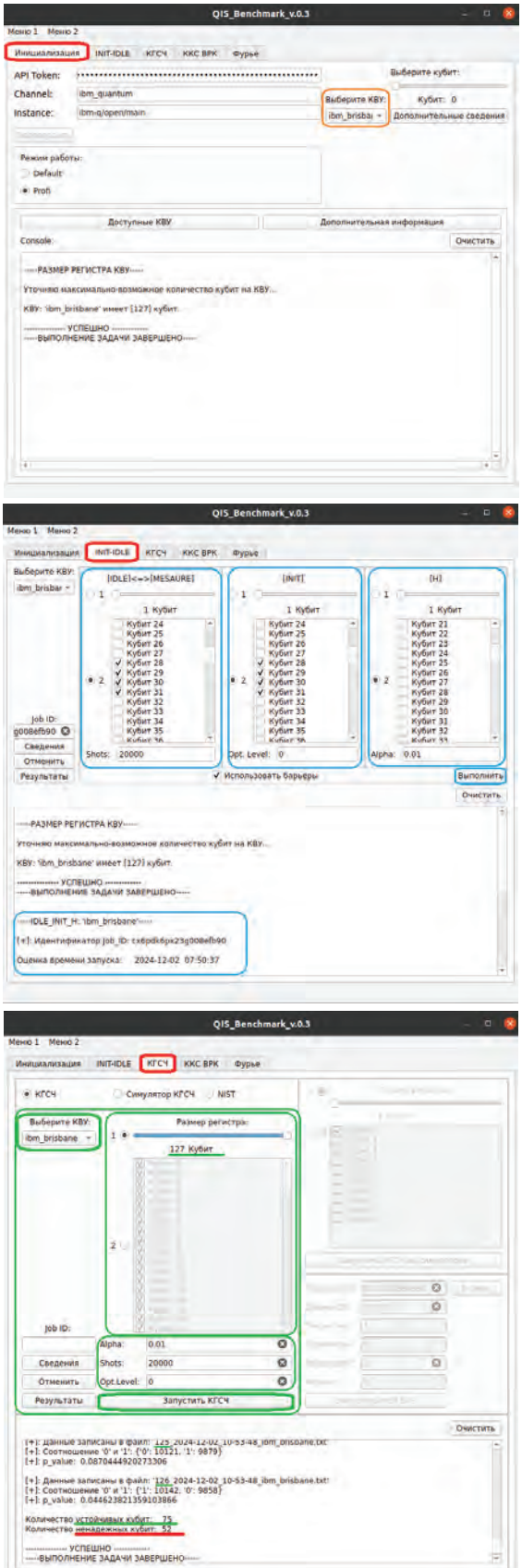

Рис. 1. Интерфейс бенчмарка «QISs_v.0.3»

Для возможности запуска квантовых схем на облачных КВУ необходимо предварительно пройти процедуру регистрации на официальном сайте компании, после чего пользователю будет присвоен персональный API-токен.

Первая вкладка программного комплекса «QISs_v.0.3» (рис. 1, слева) предназначена для установления соединения с удаленным сервером, предоставляющим облачные КВУ по уникальному API-токену пользователя. Вкладка «INIT-IDLE» (рис. 1, центр) полезна при проведении диагностики квантового регистра («точечные» исследования отдельных кубит). Необходимость данной функциональной возможности подтвердилась по результатам анализа многочисленных серий экспериментов запуска теста КГСЧ на облачном КВУ. Вкладка «КГСЧ» (рис. 1, справа) отображает все настраиваемые параметры, требуемые для реализации квантовой схемы и анализа получаемых результатов в ходе тестирования КВУ на работу в режиме КГСЧ.

Настраиваемые параметры моделируемой схемы:

– *уровень значимости* ‘Alpha’ равен ‘0.01’. Отвечает за принимаемое решение о случайности генерируемой СП на основании частотного побитового теста (см. NIST STS);
– *количество запусков* ‘max_shots’ равняется ‘20.000’ повторений квантовой схемы (предельное значение);
– *уровень оптимизации* схемы может принимать значения от ‘0’ (без изменений) до ‘3’ (максимально возможная оптимизация схемы). Установим параметр в значение ‘0’.

Приведенные исходные данные отвечают за генерацию случайной последовательности длиной в ~0,3МБ ($127 \cdot 2 \cdot 10^4$ бит: 127 – разрядность КВУ, $2 \cdot 10^4$ – количество запусков схемы). Однако в связи с тем, что с одного кубита (самостоятельного КГСЧ) будет получена двоичная строка размером $2 \cdot 10^4$ бит, все 127 полученных СП необходимо проверить на корреляцию и в случае ее отсутствия – объединить последовательности в один файл с итоговым случайным ключом, получив [в идеальных условиях] искомую СП.

Тем не менее на сегодняшний день на практике это нереализуемо по причине несовершенства современного квантового оборудования NISQ-устройств. Эксперименты на трех облачных КВУ показали, что как минимум половина из имеющихся в распоряжении исследователя кубит будет выдавать «слабые» СП, в которых числовой разрыв между количеством ‘0’ и ‘1’ будет негативно сказываться на статистических свойствах СП.

Тем не менее важно понимать, в каких целях проводится исследование.

Если СП необходима для ее дальнейшего применения в задачах, где распределение ‘0’ и ‘1’ является критичным – следует жертвовать количеством в размен на качество, увеличивая параметр ‘Alpha’ и получая СП меньшей длины, но с лучшим распределением.

В случае, если необходимо проверить время когерентности кубита, корректность применения вентиля

Адамара (5) и вероятность ошибки чтения квантового состояния, свойствами случайности СП можно пренебречь, уменьшая уровень значимости ['Alpha'] и используя максимально возможное количество кубит, одновременно отбрасывая те квантовые состояния, которые выдают однозначно плохие последовательности.

Запустим процесс КГСЧ на облачном квантовом компьютере «ibm_brisbane» и проанализируем результаты работы квантовой схемы.

Интерпретация результатов и скрытые параметры

В ходе тестирования квантового процессора «ibm_brisbane» при уровне значимости 0.01 в рамках трех экспериментов[17] по результатам работы квантовой схемы каждый раз формировался перечень из более чем 70 кубит, генерирующих устойчивые СП.

При анализе независимых испытаний установлено, что итоговые списки рекомендуемых к использованию квантовых состояний отличаются номерами выбранных [в качестве оптимальных] кубит.

Некоторые из таких несоответствий в порядковых номерах квантовых состояний и их включении/исключении в итоговый перечень «хороших» кубит вызваны влиянием незначительных отклонений в соотношении '0' и '1', где отличие даже на одно значение автоматически способно привести к неудовлетворительному результату прохождения частотного теста (под «хорошими» понимаются кубиты, прошедшие частотный тест, под «плохими» - не удовлетворяющие предъявляемым требованиям).

Тем не менее, когда такие несоответствия незначительны, полученными результатами можно пренебречь, вернув кубит в список рекомендуемых для использования в рамках работы произвольной квантовой схемой (но не для генерации случайных чисел). В других, более очевидных случаях, где разница между '0' и '1' при выборке в $2 \cdot 10^4$ может достигать $5 \cdot 10^3$ отклонений, квантовое состояние однозначно не рекомендуется к применению как для работы в режиме ГСЧ, так и для иных пользовательских программ.

По завершению генерации СП программный комплекс «QISs_v.0.3» предлагает возможность тестирования полученных последовательностей на статистические свойства инструментами NIST STS (см. рис. 1) как с каждого кубита, так и после объединения последовательностей в единый ключ, что может быть полезным для определения максимального числа кубит КВУ, генерирующих наилучшую СП наибольшей длины.

При подведении итогов практического моделирования процесса КГСЧ на облачном КВУ, следует уделить более подробное внимание интерпретации полученных результатов. Эмпирическим путем установлено, что предложенный подход по исследованию КВУ может является необходимым, но недостаточным способом анализа возможностей квантового вычислительного устройства.

На рис. 2 представлена цепочка кубит квантового регистра, поведение которой в ходе первичного тестирования не полностью отражает имеющиеся технические возможности элементов квантового процессора.

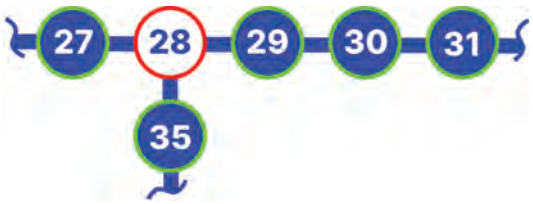

Рис. 2. Цепочка кубит квантового процессора «ibm_brisbane»

На первый взгляд, при анализе результатов выполнения схемы КГСЧ можно предположить, что квантовое состояние № 28 дает не самые лучшие, но в определенной степени приемлемые результаты: '0' – 9.105, '1' – 10.895. Разброс значений достаточно высок, но остается в допустимых пределах, что предполагает потенциальную возможность использования кубита в более сложных квантовых схемах.

Однако учитывая, что применение вентиля Адамара не зависит от исходного значения произвольного кубита, высока вероятность, что для программ, где необходима предварительная строгая инициализация, состояние № 28 окажется слабым местом программируемой схемы.

Проверим данное предположение с помощью исследования выбранного участка квантового регистра диагностическими средствами разработанной программы «QISs_v.0.3».

Исходные данные, отражающие технические параметры заданных кубит, представлены в табл. 1.

Можно видеть, что ряд параметров 28 кубита в сравнении с соседними состояниями имеет приблизительно равные значения, за исключением ошибки чтения. Следовательно, ожидается, что выбранный кубит будет выдавать результаты, не сильно отличающиеся от рядом стоящих кубит.

Проверим это, выполнив на облачном КВУ три квантовые схемы:

- работа кубита № 28 на холостом ходу;
- работа связки кубит № 28,29,30 на холостом ходу;
- работа связки кубит № 27,28,29,30,31 на холостом ходу.

Проведенные исследования показали неочевидные результаты – побочные возникновения классического бита '1' на 28 кубите [объяснимые несовершенством его технических параметров] остаются приблизительно в одном диапазоне ровно до тех пор, пока не будет активировано квантовое состояние под номером 27.

[17] Результаты всех экспериментов расположены в облачном репозитории проектов GitHub // QISs/Experiments/IDLE-INIT. URL: https://github.com/KomogorovKirill/QISs (дата обращения 30.11.24).

Таблица 1

Актуальные характеристики исследуемых кубит КВУ «ibm_brisbane»

№ кубита	Параметр КВУ «ibm_brisbane»					
	T1, µs	T2, µs	Readout error	meas0 prep1	meas1 prep0	(ID), (X), (sx) error
27: 30.11.24	277.32	155.81	0.055	0.05	0.06	1e-04
28: 30.11.24	160.44	89.55	0.04	0.009	0.07	2e-04
29: 30.11.24	84.28	105.13	0.02	0.03	0.01	5e-04
30: 30.11.24	182.8	49.4	0.007	0.009	0.006	3e-04
31: 30.11.24	223.12	66.77	0.005	0.007	0.003	2e-04
35: 30.11.24	289.98	132.37	0.014	0.013	0.01	3e-04

Данное наблюдение было проверено серией экспериментов, когда поочередно приводились в действие 27, 35, 28 кубиты в разных комбинациях, с попеременной активацией смежных состояний «в ширину». Результат всегда оставался неизменным, и отклонения от оптимальных значений на кубите № 28 происходили всегда и в прямой зависимости исключительно от кубита № 27. Более того, в ходе исследований обнаружено – даже задействовав весь квантовый регистр (127 кубит), но без состояния № 27, значения, считываемые с 28 элемента, всегда остаются в привычном интервале. И только после активации расположенного слева кубита результат измерения искомого неизменно ухудшается в разы.

С исходными последовательностями и статистическими графиками выполненных серий экспериментов можно ознакомиться в папке проекта[18].

В пользу неочевидности наблюдаемого поведения квантового состояния указывает тот факт, что операция связывания двух кубит друг с другом не производится, и при прочих равных условиях побочное воздействие шумов от работы соседних квантовых состояний не может оказывать столь существенного влияния на итоговые значения.

В таком случае, пользователю, не имеющему прямого физического доступа к исследуемому квантовому компьютеру, при отсутствии подробной технической документации на устройство, остается лишь предполагать возможное наличие скрытых параметров, обусловленных особенностями аппаратной реализации и технологии исполнения квантового процессора. В таком случае для пользователей особенно важно иметь быстрое, качественное и легко масштабируемое средство проведения предварительной оценки вычислительных возможностей исследуемого квантового компьютера, выраженное в виде комплексного набора специализированных тестов в рамках единого бенчмарка.

Заключение

В работе предложен подход по проведению исследования технических возможностей квантовых компьютеров для специалистов в области информационной безопасности.

На примере теста, анализирующего облачное квантовое вычислительное устройство в режиме работы КГСЧ, показано, каким образом с минимальными вычислительными затратами может быть проведено предварительное исследование квантовых состояний искомого квантового процессора, а также продемонстрированы некоторые неочевидные следствия, наблюдаемые при анализе и интерпретации итоговых результатов.

Предложенный подход является простым, масштабируемым и «дешевым» с точки зрения затрачиваемых ресурсов используемого КВУ. Представленные в ходе проведения бенчмарка результаты являются содержательными и однозначно интерпретируемыми.

Сформулированный алгоритм может послужить полезным инструментом анализа современных NISQ-устройств и является функциональным расширением существующего на сегодняшний день множества алгоритмов квантовых бенчмарков.

[18] Репозиторий проекта «QISs/Expierements/IDLE-INIT». URL: https://github.com/KomogorovKirill/QISs (дата обращения 30.11.24).

Литература

1. Балыгин К.А., Зайцев В.И., Климов А.Н., Кулик С.П., Молотков С.Н. Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью ≈100 Мбит/с, Письма в ЖЭТФ, 153:6 (2018), 879–894. Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью около 100 мбит/с / К.А. Балыгин, В.И. Зайцев, А.Н. Климов [и др.] // Журнал экспериментальной и теоретической физики. 2018. Т. 153, № 6. С. 879-894.
2. Балыгин 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, 119:7 (2024), 533–544.
3. Букашкин С.А., Черепнев М.А. Квантовые устройства в криптографии // International Journal of Open Information Technologies. 11:1 (2023). 104–108.
4. Гайдаш А.А., Гончаров Р.К., Козубов А.В., Яковлев П.В. Математическая модель квантового генератора случайных чисел на основе флуктуации вакуума // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 20:2 (2024), 136–153.
5. Евсиков К.С. Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета имени О.Е. Кутафина, 4:92 (2022). 46–58.
6. МР 26.4.004–2021. Информационная технология. Криптографическая защита информации. Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации. // Методические рекомендации ТК 26. 2021.
7. Кравцов К.С., Кулик С.П., Радченко И.В. Квантовый генератор случайных чисел, Мат. Вопр. Крипт., 7:2 (2016), 111–114.
8. Крючков А.А. О необходимости принятия единого стандарта по оценке производительности и сертификации квантовых вычислительных устройств / Научно-практическая конференция, посвященная 100-летию деятельности ФГБУ «Институт стандартизации»: «Стандартизация: траектория науки», Санкт-Петербург, 2024 // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 6(81).
9. Лукашев А.В., Шабуня В.В., Сарафанников В.С. [и др.]. Тенденции повышения уязвимости современных информационных систем со стороны квантовых компьютеров. // Известия Тульского государственного университета. Технические науки, 11 (2023). 324–331. DOI:10.24412/2071-6168-2023-11-324–325
10. Минбалеев А.В., Берестнев М.А., Евсиков К.С. Обеспечение информационной безопасности оборудования добывающей промышленности в квантовую эпоху // Известия Тульского государственного университета. Науки о земле, 1 (2023). 567–584.
11. Орлов М.А., Нечаев К.А., Резниченко С.А. Оценка статистических свойств криптографической стойкости случайных последовательностей, полученных квантовым компьютером IBM // Безопасность информационных технологий, [S.l.], v. 30, n. 1 (2023), 14-26. DOI: 10.26583/bit.2023.1.01
12. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ. // Вопросы кибербезопасности, 3:49 (2022). 2–22.
13. Соловьев В.М. Квантовые компьютеры и квантовые алгоритмы. Часть 1. Квантовые компьютеры // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2015. Т. 15, № 4. С. 462–477.
14. Соловьев В.М. Квантовые компьютеры и квантовые алгоритмы. Часть 2. Квантовые алгоритмы // Изв. Сарат. ун-та. Новая серия. Серия: Математика. Механика. Информатика. 2016. Т. 16, № 1. С. 104–112.
15. Acuaviva A., Aguirre D., Pena R., Sanz M. Benchmarking Quantum Computers: Towards a Standard Performance Evaluation Approach : [Электронный ресурс]. 2024. Режим доступа: https://doi.org/10.48550/arXiv.2407.10941
16. Amico M., Zhang H., Jurcevic P. [и др.]. Defining Standard Strategies for Quantum Benchmarks : [Электронный ресурс]. 2023. Режим доступа: https://research.ibm.com/publications/defining-standard-strategies-for-quantum-benchmarks
17. Chatterjee A., Rappaport S., Giri A. [и др.]. A Comprehensive Cross-Model Framework for Benchmarking the Performance of Quantum Hamiltonian Simulations. 2024. DOI: 10.48550/arXiv.2409.06919
18. Darwish A., Grossi M., Vallecorsa S., Di Meglio A. A scalable, more extensible architecture for ABAQUS. // EU open Research Repository. 2023. URL: https://zenodo.org/records/7528880 (дата обращения 20.09.24).
19. Eisert, J., Hangleiter, D., Walk, N. [и др.]. Quantum certification and benchmarking. Nat Rev Phys, 2, (2020), 382–390.
20. Li A., Stein S., Krishnamoorthy S. [и др.]. QASMBench: A Low-level QASM Benchmark Suite for NISQ Evaluation and Simulation. 2020. DOI: 10.48550/arXiv.2005.13018
21. Larose, R. Overview and Comparison of Gate Level Quantum Software Platforms. (2018). ArXiv, abs/1807.02500.
22. Lubinski T., Coffrin C., McGeoch C. [и др.]. Optimization Applications as Quantum Performance Benchmarks. 2023. DOI: 10.48550/arXiv.2302.02278
23. Lubinski T., Goings J., Mayer K. [и др.]. Quantum Algorithm Exploration using Application-Oriented Performance Benchmarks. 2024. DOI: 10.48550/arXiv.2402.08985
24. Mesman K., Al-Ars Z., Moller M. QPack: Quantum Approximate Optimization Algorithms as universal benchmark for quantum computers. 2021. DOI: 10.48550/arXiv.2103.17193

25. Preskill J. Quantum computing in the NISQ era and beyond. Quantum 2, 79. DOI: 10.22331/q-2018-08-06-79 (2018).
26. Proctor T., Young K., D. Baczewski A. [и др.]. Benchmarking quantum computers. 2024. DOI: 10.48550/arXiv.2407.08828
27. Tomesh T., Gookhale P., Omole V. [и др.]. SupermarQ: A Scalable Quantum Benchmark Suite. 2022. DOI: 10.48550/arXiv.2202.11045
28. Valiron B. On Quantum Programming Languages. 2024. DOI: 10.48550/arXiv.2410.13337

NON-OBVIOUS ASPECTS OF THE BENCHMARK OF QUANTUM COMPUTING DEVICES ON THE EXAMPLE OF QUANTUM RANDOM NUMBER GENERATION

Andrey A. Kryuchkov, *Senior Lecturer, MIREA – Russian Technological University, Institute of Artificial Intelligence, Department of Information Security, Moscow, Russian Federation.*
E-mail: kryuchkov_a@mirea.ru

Kirill E. Komogorov, *5th year student of MIREA – Russian Technological University, Institute of Artificial Intelligence, Department of Information Security, BI. ZONE, Russian Federation, Moscow.*
E-mail: komogorovk@mail.ru

Keywords*: quantum computer, random number generator, benchmark, qubit, quantum programming, random sequence, statistical analysis, Hadamard gate.*

Abstract

Purpose of the work: the formation of an algorithm for conducting and analyzing the results of the benchmark of quantum computing devices on the example of using quantum computers in the tasks of generating random numbers.

Methods used: system analysis, classification, practical modeling, graphical and tabular analysis methods.

Results obtained: An approach has been implemented to investigate and pre-evaluate the capabilities of quantum computers using the tools of the developed software package for conducting a benchmark of quantum computing devices, in which a quantum processor is used to generate random binary sequences. Based on the data obtained, the user is offered an optimal set of quantum states, which can later be used to solve more time-consuming applied tasks.

Some non-obvious consequences of the benchmark results are formulated and demonstrated by a practical example, which deserve a more substantive analysis to form a complete picture of the technical characteristics and performance of the quantum computer under study.

References

1. Balygin K.A., Zajcev V.I., Klimov A.N., Kulik S.P., Molotkov S.N. Kvantovyj generator sluchajnyh chisel, osnovannyj na puassonovskoj statistike fotootschetov, so skorost'ju ≈100 Mbit/c, Pis'ma v ZhJeTF, 153:6 (2018), 879–894. Kvantovyj generator sluchajnyh chisel, osnovannyj na puassonovskoj statistike fotootschetov, so skorost'ju okolo 100 mbit/c / K. A. Balygin, V. I. Zajcev, A. N. Klimov [i dr.] // Zhurnal jeksperimental'noj i teoreticheskoj fiziki. 2018. T. 153, № 6. S. 879-894.
2. Balygin K.A., Kulik S.P., Molotkov S.N. Realizacija kvantovogo generatora sluchajnyh chisel: jekstrakcija dokazuemo sluchajnyh bitovyh posledovatel'nostej iz korrelirovan-nyh markovskih cepochek // Pis'ma v ZhJeTF, 119:7 (2024), 533–544.
3. Bukashkin S.A., Cherepnev M.A. Kvantovye ustrojstva v kriptografii // International Jour-nal of Open Information Technologies. 11:1 (2023). 104–108.
4. Gajdash A.A., Goncharov R.K., Kozubov A.V., Jakovlev P.V. Matematicheskaja model' kvantovogo generatora sluchajnyh chisel na osnove fluktuacii vakuuma // Vestnik Sankt-Peterburgskogo universiteta. Prikladnaja matematika. Informatika. Processy upravlenija. 20:2 (2024), 136–153.
5. Evsikov K.S. Informacionnaja bezopasnost' cifrovogo gosudarstva v kvantovuju jepohu // Vestnik Universiteta imeni O.E. Kutafina, 4:92 (2022). 46–58.

6. MR 26.4.004–2021. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Zashhishhennyj protokol vzaimodejstvija kvantovo-kriptograficheskoj apparatury vyra-botki i raspredelenija kljuchej i sredstva kriptograficheskoj zashhity informacii // Metodicheskie rekomendacii TK 26. 2021.
7. Kravcov K.S., Kulik S.P., Radchenko I.V. Kvantovyj generator sluchajnyh chisel, Mat. Vopr. Kript., 7:2 (2016), 111–114.
8. Krjuchkov A.A. O neobhodimosti prinjatija edinogo standarta po ocenke proizvoditel'no-sti i sertifikacii kvantovyh vychislitel'nyh ustrojstv / Nauchno-prakticheskaja konfe-rencija, posvjashhennaja 100-letiju dejatel'nosti FGBU «Institut standartizacii»: «Standartizacija: traektorija nauki», Sankt-Peterburg, 2024 // Informacionno-jekonomicheskie aspekty standartizacii i tehnicheskogo regulirovanija. 2024. № 6(81).
9. Lukashev A.V., Shabunja V.V., Sarafannikov V.S. [i dr.]. Tendencii povyshenija ujazvimosti sovremennyh informacionnyh sistem so storony kvantovyh komp'juterov. // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki, 11 (2023). 324–331. DOI:10.24412/2071-6168-2023-11-324–325
10. Minbaleev A.V., Berestnev M.A., Evsikov K.S. Obespechenie informacionnoj bezopasno-sti oborudovanija dobyvajushhej promyshlennosti v kvantovuju jepohu // Izvestija Tul'sko-go gosudarstvennogo universiteta. Nauki o zemle, 1 (2023). 567–584.
11. Orlov M.A., Nechaev K.A., Reznichenko S.A. Ocenka statisticheskih svojstv kriptograficheskoj stojkosti sluchajnyh posledovatel'nostej, poluchennyh kvantovym komp'juterom IBM // Bezopasnost' informacionnyh tehnologij, [S.l.], v. 30, n. 1 (2023), 14-26. DOI: 10.26583/bit.2023.1.01
12. Petrenko A.S., Petrenko S.A. Metod ocenivanija kvantovoj ustojchivosti blokchejn-platform. // Voprosy kiberbezopasnosti, 3:49 (2022). 2–22.
13. Solov'ev V.M. Kvantovye komp'jutery i kvantovye algoritmy. Chast' 1. Kvantovye kom-p'jutery // Izvestija Saratovskogo universiteta. Novaja serija. Serija: Matematika. Mehanika. Informatika. 2015. T. 15, № 4. S. 462–477.
14. Solov'ev V.M. Kvantovye komp'jutery i kvantovye algoritmy. Chast' 2. Kvantovye algo-ritmy // Izv. Sarat. un-ta. Novaja serija. Serija: Matematika. Mehanika. Informatika. 2016. T. 16, № 1. S. 104–112.
15. Acuaviva A., Aguirre D., Pena R., Sanz M. Benchmarking Quantum Computers: Towards a Standard Performance Evaluation Approach. 2024. URL: https://doi.org/10.48550/arXiv.2407.10941
16. Amico M., Zhang H., Jurcevic P. [i dr.]. Defining Standard Strategies for Quantum Bench-marks. 2023. URL: https://research.ibm.com/publications/defining-standard-strategies-for-quantum-benchmarks
17. Chatterjee A., Rappaport S., Giri A. [i dr.]. A Comprehensive Cross-Model Framework for Benchmarking the Performance of Quantum Hamiltonian Simulations. 2024. DOI: 10.48550/arXiv.2409.06919
18. Darwish A., Grossi M., Vallecorsa S., Di Meglio A. A scalable, more extensible architecture for ABAQUS. // EU open Research Repository. 2023. URL: https://zenodo.org/records/7528880 (data obrashhenija 20.09.24).
19. Eisert, J., Hangleiter, D., Walk, N. [i dr.]. Quantum certification and benchmarking. Nat Rev Phys, 2, (2020), 382–390.
20. Li A., Stein S., Krishnamoorthy S. [i dr.]. QASMBench: A Low-level QASM Benchmark Suite for NISQ Evaluation and Simulation. 2020. DOI: 10.48550/arXiv.2005.13018
21. Larose, R. Overview and Comparison of Gate Level Quantum Software Platforms. (2018). ArXiv, abs/1807.02500.
22. Lubinski T., Coffrin C., McGeoch C. [i dr.]. Optimization Applications as Quantum Perfor-mance Benchmarks. 2023. DOI: 10.48550/arXiv.2302.02278
23. Lubinski T., Goings J., Mayer K. [i dr.]. Quantum Algorithm Exploration using Application-Oriented Performance Benchmarks. 2024. DOI: 10.48550/arXiv.2402.08985
24. Mesman K., Al-Ars Z., Moller M. QPack: Quantum Approximate Optimization Algorithms as universal benchmark for quantum computers. 2021. DOI: 10.48550/arXiv.2103.17193
25. Preskill J. Quantum computing in the NISQ era and beyond. Quantum 2, 79. DOI: 10.22331/q-2018-08-06-79 (2018).
26. Proctor T., Young K., D. Baczewski A. [i dr.]. Benchmarking quantum computers. 2024. DOI: 10.48550/arXiv.2407.08828
27. Tomesh T., Gookhale P., Omole V. [i dr.]. SupermarQ: A Scalable Quantum Benchmark Suite. 2022. DOI: 10.48550/arXiv.2202.11045
28. Valiron B. On Quantum Programming Languages. 2024. DOI: 10.48550/arXiv.2410.13337