

# Вычислительные задачи моделирования элементной базы квантовых компьютеров

Ю.И. Богданов, Н.А. Богданова, В.Ф. Лукичев,  
А.А. Орликовский, И.А. Семенихин, А.С. Холево, А.Ю. Чернявский

**Аннотация.** Работа посвящена задачам моделирования элементной базы квантовых компьютеров. Дается краткое введение в математический формализм описания квантовых вентилей – логических элементов квантового компьютера. Рассматриваются важные задачи моделирования элементной базы квантового компьютера и некоторые примеры их численного решения. Описываются вычислительные особенности таких задач и причины необходимости использования высокопроизводительных систем. Приводятся результаты моделирования многокубитового квантового преобразования Фурье и алгоритма Гровера, полученные с использованием персональных компьютеров и суперкомпьютера МВС-100К РАН.

**Ключевые слова:** кубит, квантовый вентиль, деполаризующий шум, амплитудная и фазовая релаксация квантовое преобразование Фурье, алгоритм Гровера.

## Введение

В настоящее время активно обсуждаются десятки различных моделей квантовых компьютеров. В числе наиболее перспективных и интересных предложений по реализации квантовых регистров – проекты на ионах в ловушках, на ядерных спинах, на квантовых точках, на фотонах, на зарядовых, потоковых и фазовых состояниях в сверхпроводниковых структурах, на состояниях ридберговских атомов, на квантовых состояниях вакансионных центров в алмазе и др. [1-6]. Основное достижение проведенных до сих пор исследований состоит в практической демонстрации справедливости физических принципов, лежащих в основе идеи квантовых вычислений. Основные препятствия на пути реализации концепции полномасштабных квантовых компьютеров состоят в недостаточной разработке соответствующей необхо-

димым требованиям технологии изготовления квантовых регистров, в трудностях измерения и контроля квантовых состояний, а также в обеспечении необходимой степени подавления декогерентизации, обусловленной квантовыми шумами. Достигнутая в настоящее время в экспериментах точность реализации, характеризующая вероятностью совпадения между теоретическим и экспериментальным квантовыми состояниями, составляет всего 60-80%, в то время как требуемая точность должна быть 99.99% и более.

С целью существенного повышения уровня исследований в рассматриваемой области в Физико-технологическом институте РАН совместно с Московским государственным университетом им. Ломоносова и Математическим институтом им. В.А. Стеклова РАН разработана новая методология оценивания качества и эффективности квантовых информационных технологий, осно-

<sup>1</sup> Работа частично поддержана Программой Президиума РАН в области фундаментальных исследований, а также РФФИ проект № 12-01-31274 мол\_а и № 13-07-00711

ванная на анализе полноты, адекватности и точности реализации квантовых вентиляей. Методы численного анализа и статистического моделирования с учётом влияния квантовых шумов, а также результатов технологических и экспериментальных исследований позволяют дать исчерпывающую оценку качеству и эффективности проектируемых квантовых регистров, сформулировать требования к экспериментальному оборудованию и технологии, посредством обратной связи развитый подход позволяет наилучшим образом распорядиться имеющимися ресурсами для оптимизации процесса разработки квантовых информационных технологий. Эффективность предложенного подхода уже была продемонстрирована нами в течение последних нескольких лет в работах с оптическими и сверхпроводниковыми кубитами [7-11].

Целью данной работы является оценка влияния квантовых шумов в задачах моделирования элементной базы квантовых компьютеров. Работа имеет следующую структуру. В разделе 1 кратко рассматриваются математические методы описания квантовых вентиляей с учетом квантовых шумов. Общие математические методы иллюстрируются в разделе 2 результатами моделирования важных в практическом отношении вентиляей "Контролируемое-НЕ" (CNOT) и "Корень из  $i$ -SWAP" (SQiSW). В разделе 3 рассматривается влияние квантовых шумов на точность реализации квантовых алгоритмов. Представлены результаты численного анализа в приложении к двум важным алгоритмам квантовой информатики (квантовое преобразование Фурье и алгоритм Гровера). Акцент сделан на квантовых системах высокой размерности, которые доступны для моделирования на персональных компьютерах, а также на суперкомпьютере МВС-100 РАН. В разделе 4 представлены выводы и результаты работы.

## 1. Математический формализм описания квантовых вентиляей

Ниже мы ограничимся очень кратким описанием формализма квантовых вычислений и квантовых операций, которое необходимо для лучшего представления результатов численного моделирования. Более подробное описание

рассматриваемых здесь вопросов можно найти в [3, 5, 12, 13].

**Идеальный квантовый компьютер.** Основным элементом квантового компьютера является квантовый бит (кубит), представляющий собой двухуровневую квантовую систему. Так же как и классический бит, кубит может находиться в двух базисных состояниях  $|0\rangle$  и  $|1\rangle$ . Однако, в отличие от классической системы, кубит может находиться в суперпозиции этих состояний  $c_0|0\rangle + c_1|1\rangle$ , где  $c_i$ ,  $i = 0,1$  - комплексные числа, называемые амплитудами вероятности. Таким образом, состояние кубита задается вектором в пространстве  $\mathbb{C}^2$  (согласно принятой в физике терминологии, это двумерное гильбертово пространство). Амплитуды имеют вероятностный физический смысл: вероятность обнаружить кубит в состоянии  $|i\rangle$  равна  $|c_i|^2$ . Важный аспект квантовой механики, играющий ключевую роль в квантовых вычислениях, определяется тем фактом, что состояние двух кубитов принадлежит пространству, которое задается тензорным произведением однокубитовых пространств  $\mathbb{C}^2 \otimes \mathbb{C}^2$ . Общий вид такого состояния будет  $c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ . Аналогично, состояние  $n$  кубитов лежит в пространстве  $(\mathbb{C}^2)^{\otimes n}$  и описывается уже  $2^{2n} - 2$  действительными числами (два параметра являются избыточными в силу нормировки полной вероятности и не имеющей физического смысла общей фазы  $e^{i\varphi}$ ). Мы видим, что размерность пространства растет экспоненциально, поэтому даже в идеальном случае для моделирования уже небольшого числа кубитов необходимы значительные вычислительные ресурсы.

Аналогом логических элементов классических компьютеров в квантовом случае выступают унитарные преобразования состояний. Как и в классических вычислениях, практически важны преобразования, действующие лишь на небольшое число кубитов. Некоторые вентиляи (gates) имеют классический аналог (например,  $NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ), в то время как другие

(например, фазовое преобразование  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ) такого аналога не имеют. Но даже

если некоторое преобразование  $U$  действует лишь на несколько кубитов, оно меняет *все* амплитуды  $n$  – кубитового квантового состояния. Матрица такого преобразования имеет вид  $U \otimes I$ , где  $I$  – единичная матрица, действующая на незатронутые кубиты. Несмотря на большой размер  $2^n \times 2^n$ , такая матрица сильно разрежена, что позволяет заметно сокращать вычислительные затраты и используемую память при моделировании.

**Зашумленные квантовые вентили.** Рассмотренные выше векторы-состояния описывают идеальный случай так называемых *чистых* состояний. При наличии шумов, возникающих вследствие взаимодействия с окружением, появляется дополнительная стохастическая неопределенность. Теперь состояния системы уже не могут быть описаны вектором – вместо этого используются так называемые матрицы плотности. Матрицей плотности смеси квантовых состояний  $|\psi_i\rangle$ , взятых с соответствующими вероятностями  $p_i$  является матрица  $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ . Рассматриваемые

объекты есть неотрицательно-определенные эрмитовы матрицы с единичным следом. Согласно квантовой механике, унитарные преобразования приводят к следующей эволюции:  $\rho \rightarrow U\rho U^\dagger$ . Отметим, что переход от векторов состояния к матрицам плотности приводит к тому, что число параметров, необходимых для хранения состояний, увеличивается квадратично.

Как и векторы-состояния, унитарные преобразования являются лишь идеализацией. Более реалистично преобразования описываются при помощи формализма, развитого в теории открытых квантовых систем. По аналогии с формализмом случайных марковских процессов, с помощью которого обычно описываются ошибки, возникающие в классических компьютерах, квантовый шум с достаточной для многих приложений точностью также представляет собой марковский процесс (только объектом, который

подвержен эволюции, является не распределение вероятностей, а матрица плотности). С математической точки зрения такой подход ведет к концепции *вполне положительных преобразований*. Такие преобразования сохраняют положительность матрицы плотности при действии на подсистемы (например, на часть кубитов многокубитовой системы). Рассматриваемая концепция в настоящее время широко признана и хорошо обоснована (Краус [14], Линдبلاد [15], Горини и др. [16], Эванс и Льюис [17] в статистической механике и А.С. Холево [18] в квантовой теории сообщений).

Важно отметить, что вполне положительные отображения могут быть представлены в различных эквивалентных математических формах.

1) **Операторы Крауса.** Квантовая эволюция задается операторной суммой  $E(\rho) = \sum_k E_k \rho E_k^\dagger$ , где  $E_k$  – элементы преобразования (так называемые операторы Крауса),  $\sum_k E_k^\dagger E_k = I$ .

В пространстве размерности  $S$  операторы  $E_k$  могут быть представлены матрицами размерности  $s \times S$ . В случае унитарного преобразования в операторной сумме имеется всего одно слагаемое, задаваемое оператором  $U$ .

2) **Расширенная динамика.** Неунитарное преобразование, действующее в гильбертовом пространстве размерности  $s$ , можно интерпретировать как следствие унитарного преобразования  $U$  в пространстве более высокой размерности. Пусть имеется  $m$  операторов преобразования  $E_k$  ( $k = 1, \dots, m$ ). Тогда унитарная матрица  $U$  размерности  $ms \times ms$  может быть представлена в следующем блочном виде:

$$U = \begin{pmatrix} E_1 & : & : \\ : & : & : \\ E_m & : & : \end{pmatrix}.$$

Унитарная матрица  $U$  описывает взаимодействие вспомогательной  $m$  – уровневой системы (среды) с изучаемой физической  $s$  – уровневой системой.

Преобразование системы описывается при помощи редукции по окружению:

$$\rho \rightarrow \text{Tr}_E (U |0_E\rangle\langle 0_E| \otimes \rho U^\dagger)$$

3) **Изморфизм Чоя-Ямилковского.** Каждому квантовому преобразованию можно сопоставить некоторую матрицу плотности в пространстве большей размерности.

Пусть рассматриваемое квантовое преобразование  $\mathbf{E}$  действует на систему  $A$  размерности  $s$ . Добавим вспомогательную систему  $B$  такой же размерности и рассмотрим совместную систему  $AB$ , на вход которой подадим состояние:

$$|\Phi\rangle = \frac{1}{\sqrt{s}} \sum_{j=1}^s |j\rangle \otimes |j\rangle.$$

Здесь первый множитель в тензорном произведении относится к подсистеме  $B$ , а второй – к подсистеме  $A$ . Пусть в подсистеме  $B$  осуществляется тождественное преобразование  $\mathbf{I}$ . Тогда в системе  $AB$  будет действовать преобразование  $(\mathbf{I} \otimes \mathbf{E})$ . Преобразованию  $\mathbf{E}$  можно однозначно сопоставить матрицу плотности  $\rho_\chi = (\mathbf{I} \otimes \mathbf{E})(|\Phi\rangle\langle\Phi|)$  – состояние Чоя-Ямилковского.

Такое представление весьма важно, т.к. дает возможность использовать хорошо разработанный аппарат анализа матриц плотности для квантовых вентилях.

4) **Матрица эволюции.** Пусть входная и выходная матрицы плотности  $\rho_{in}$  и  $\rho_{out}$  вытянуты в столбцы длины  $s^2$ . Тогда, в силу линейности квантовой операции, можно записать:  $\rho_{out} = G\rho_{in}$ , где  $G$  – некоторая матрица размера  $s^2 \times s^2$ , называемая *матрицей эволюции*

Важный частный случай представляют собой однородные во времени марковские процессы. Пусть  $G(\Delta t)$  – матрица эволюции системы за время  $\Delta t$ . Тогда  $N$  шагов такой эволюции, т.е. эволюция за время  $t = N\Delta t$ , будет определяться оператором  $G(t)$ , который имеет следующий простой вид:  $G(t) = (G(\Delta t))^N$ . Такое представление очень удобно для моделирования.

Отметим, что все перечисленные представления могут быть эффективно пересчитаны друг в друга. Различные представления необхо-

димы на различных этапах моделирования: например, для расчета инфинитезимальной операции действующей под влиянием некоторой модели квантового шума необходимы операторы Крауса или расширенная динамика (в зависимости от модели шума). Для расчета эволюции вентиля на фиксированном промежутке времени необходима матрица эволюции. Для дальнейшего анализа полученной модели вентиля и сравнения с экспериментом широко используются состояния Чоя-Ямилковского.

Рассмотрим, как растет необходимый для моделирования объем памяти. Как можно видеть из пунктов 1-4, переход к зашумленным вентилям эффективно удваивает число рассматриваемых кубитов. Действительно, квантовые  $n$ -кубитовые операции сводятся к состояниям Чоя-Ямилковского, которые эффективно представляют собой  $2n$ -кубитовые матрицы плотности, в результате оказывается, что для  $n$ -кубитового вентиля необходимо оперировать примерно с  $2^{4n}$  комплексными параметрами. В такой же пропорции, очевидно, растут и временные вычислительные затраты.

Отметим также еще один важный вычислительный аспект: задачи моделирования квантовых вентилях представляют собой задачи линейной алгебры высокой размерности. Это предоставляет хорошие перспективы для использования готовых суперкомпьютерных программных средств (Scalapack, Matlab distributed computing и т.п.). Кроме этого, рассматриваемые задачи дают широкие возможности для разработки различных алгоритмов вычислительной математики и использования нестандартных методов оптимизации.

## 2. Анализ точности квантовых операций и схем

Как говорилось во введении, для успешного развития квантовых информационных технологий критически важна точность квантовых операций. В связи с этим встает задача моделирования квантовых вентилях и схем с учетом различных моделей квантового шума и дальнейшим анализом точности. Одним из удобных способов является визуальный анализ графического представления матрицы Чоя-Ямилковского.

Далее рассматриваются различные типы квантовых шумов (деполярирующий шум, амплитудная и фазовая релаксация), а также результаты моделирования некоторых важных квантовых вентилях под влиянием данных шумов.

## 2.1. Модели квантовых шумов

### Деполярирующий шум

Квантовое преобразование в условиях деполярирующего квантового шума действует на матрицу плотности  $\rho$  размерности  $s \times s$  следующим образом:

$$\rho \rightarrow \frac{pI}{s} + (1-p)U\rho U^\dagger.$$

Здесь  $I$  – единичная матрица размерности  $s \times s$ . С вероятностью  $p$  происходит замена исходного состояния на совершенно хаотичное, а с вероятностью  $1-p$  осуществляется унитарное преобразование с помощью матрицы  $U$ , отвечающей заданному вентилю.

### Амплитудная и фазовая релаксация

Начнем с рассмотрения простейшего, но очень важного случая чистой дефазировки.

Операторы Крауса для чистой дефазировки есть:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\gamma} \end{pmatrix}.$$

Произвольная матрица плотности  $\rho_{in} = \begin{pmatrix} a & b \\ b^* & 1-a \end{pmatrix}$ , где  $a$  – некоторое действительное число, а  $b$  – некоторое комплексное число, под действием такого преобразования

перейдет в  $\rho_{out} = \begin{pmatrix} a & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & 1-a \end{pmatrix}$ .

Мы видим, что чистая дефазировка не приводит к изменению диагональных элементов матрицы плотности, которые описывают населенности энергетических уровней.

Исторически одним из первых процессов, в котором была подробно изучена дефазировка квантовых состояний, была спин-спиновая релаксация ядерных спинов. Опыты с ядерными спинами и другими физическими системами показывают, что недиагональные элементы, характеризующие когерентность, убывают, как

правило, экспоненциально во времени. Этот факт делает естественной следующую параметризацию:

$$\sqrt{1-\gamma} = \exp\left(-\frac{t}{T_2^{pure}}\right), \quad \gamma = 1 - \exp\left(-\frac{2t}{T_2^{pure}}\right).$$

Здесь введенный параметр времени  $T_2^{pure}$  характеризует чистую дефазировку.

Следующим важным процессом является так называемая амплитудная релаксация. Операторы Крауса в этом случае имеют вид:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}.$$

Параметр  $\gamma$  определяет вероятность релаксации (скачка), связанного с переходом из возбужденного состояния  $|1\rangle$  в основное состояние  $|0\rangle$ . Мы предполагаем, что конечным итогом амплитудной релаксации является состояние  $|0\rangle$ .

Пусть снова  $\rho_{in} = \begin{pmatrix} a & b \\ b^* & 1-a \end{pmatrix}$ , тогда

$$\rho_{out} = \begin{pmatrix} a + \gamma(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & (1-\gamma)(1-a) \end{pmatrix}.$$

Мы видим, что амплитудная релаксация затрагивает как диагональные, так и недиагональные элементы. Заметим попутно, что в общем случае нельзя обеспечить затухание населенности верхнего уровня без изменения когерентности – это привело бы к потере положительной определенности матрицы плотности.

Введем параметр времени  $T_1$ , характеризующий экспоненциальную во времени релаксацию верхнего уровня

$$\gamma = 1 - \exp\left(-\frac{t}{T_1}\right), \quad \sqrt{1-\gamma} = \exp\left(-\frac{t}{2T_1}\right).$$

Отметим некоторое отличие представленных формул от аналогичных формул для чистой дефазировки. Время  $T_1$  параметризует скорость релаксации диагональных элементов матрицы плотности, при этом скорость релаксации недиагональных элементов оказывается вдвое ниже.

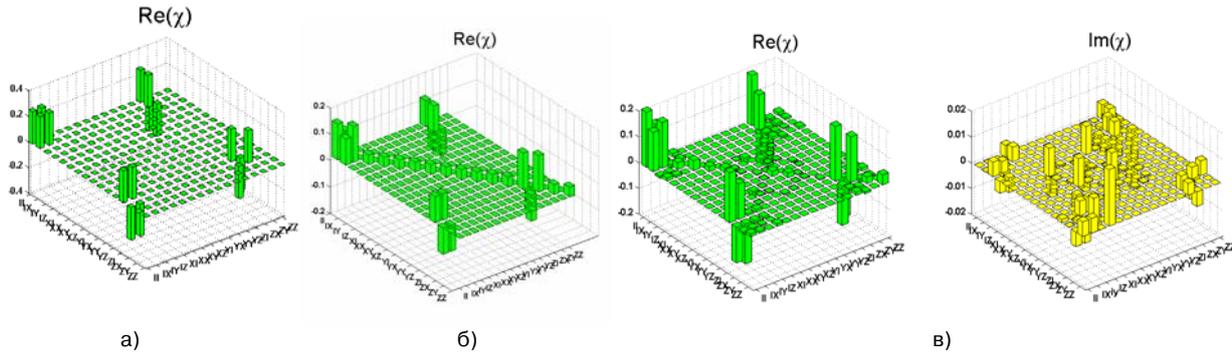


Рис. 1. Состояние Чоя-Ямилковского (хи-матрица) вентиля CNOT

а) идеальный случай отсутствия шума; б) деполяризующий квантовый шум ( $\rho=0,6$ ); в) амплитудная и фазовая релаксация с параметрами  $T_1=5$  и  $T_2=3$  (время операции выбрано за единицу)

Нетрудно заметить, что одновременное действие двух рассмотренных выше процессов приведет к следующему результату:

$$\rho_{out} = \begin{pmatrix} 1 - (1-a)\exp\left(-\frac{t}{T_1}\right) & b \exp\left(-\frac{t}{T_2}\right) \\ b^* \exp\left(-\frac{t}{T_2}\right) & (1-a)\exp\left(-\frac{t}{T_1}\right) \end{pmatrix}.$$

Здесь мы ввели новый параметр  $T_2$  такой, что

$$\frac{1}{T_2} = \frac{1}{T_2^{pure}} + \frac{1}{2T_1}.$$

Из этого определения получаем, что всегда должно выполняться неравенство:

$$T_2 \leq 2T_1.$$

При моделировании необходимо учитывать, что процессы релаксации действуют одновременно с гамильтоновой эволюцией. В связи с этим целесообразно представление релаксации в формализме расширенной унитарной динамики.

Гамильтонианы для моделирования амплитудной и фазовой релаксации, описывающие взаимодействие физического кубита с фиктивным вспомогательным кубитом, имитирующим окружение, есть, соответственно:

$$H_{ampl} = i(\mathbf{b}^+ \otimes \mathbf{a} - \mathbf{b} \otimes \mathbf{a}^+),$$

$$H_{phase} = (\mathbf{b} + \mathbf{b}^+) \otimes \mathbf{a}^+ \mathbf{a}.$$

Здесь  $\mathbf{a}, \mathbf{a}^+, \mathbf{b}, \mathbf{b}^+$  – операторы уничтожения и рождения для основного и вспомога-

тельного кубитов соответственно,  $\mathbf{a} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ,

$\mathbf{a}^+ = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ , и аналогично для  $\mathbf{b}, \mathbf{b}^+$ .

## 2.2. Результаты моделирования

### Вентиль CNOT

В качестве первого примера на Рис. 1 представлен идеальный и зашумленный (под действием деполяризующего шума, а также амплитудной и фазовой релаксации) вентиль CNOT (controlled-NOT), который меняет состояние второго кубита в зависимости от состояния первого CNOT:  $|i\rangle|j\rangle \rightarrow |i\rangle|i \oplus j\rangle$ . Гамильтониан, осуществляющий это преобразование за время  $t = 1$ , имеет вид

$$H_{CNOT} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \pi/2 & -\pi/2 \\ 0 & 0 & -\pi/2 & \pi/2 \end{pmatrix}.$$

### Вентиль SQiSW

Преобразование SQiSW (квадратный корень из i-SWAP) непосредственно возникает в результате емкостной связи сверхпроводниковых кубитов [19-21]

$$H_{int} = \hbar(g/2)(|01\rangle\langle 10| + |10\rangle\langle 01|),$$

где  $g$  – константа взаимодействия.

Отметим, что рассматриваемый гамильтониан отвечает XY-модели обменного взаимодействия Гейзенберга.

Эволюция системы задается посредством следующей унитарной матрицы:

$$U_{\text{int}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(gt/2) & -i \sin(gt/2) & 0 \\ 0 & -i \sin(gt/2) & \cos(gt/2) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Пи-импульс, удовлетворяющий условию  $gt = \pi$ , обеспечивает обмен (i-swap):  $|01\rangle \rightarrow -i|10\rangle$ ,  $|10\rangle \rightarrow -i|01\rangle$ . Импульс вдвое меньшей длительности, когда  $gt = \pi/2$ , обеспечивает искомую операцию SQiSW.

Результаты моделирования приведены на Рис. 2. Время амплитудной релаксации равно  $T_1 = 3$ , а время фазовой релаксации равно  $T_2 = 1.5$ . В качестве единицы времени снова выбрано время выполнения операции.

### 3. Моделирование квантовых алгоритмов

В настоящем разделе рассматривается моделирование зашумленного квантового преобразования Фурье и квантового алгоритма Гровера.

Учитывая, что моделирование на уровне квантовых преобразований увеличивает экспоненциальную степень размерности в четыре раза, для работы с многими кубитами было проведено моделирование на уровне векторов-состояний с простыми моделями шума.

Основной трудностью подобного моделирования является экспоненциальный рост размерности в зависимости от числа кубитов. Так, для моделирования всего лишь 50 кубитов необходимо работать с векторами из  $2^{50}$  комплексных чисел; при использовании чисел с одинарной точностью для хранения такого вектора потребуется 18.014.398.509.481.984 байт.

На современных персональных компьютерах, используя оперативную память, можно моделировать примерно 30 кубитов. Так, в работе [22] реализовано моделирование схем с 32 кубитами при 16Gb оперативной памяти. Использование суперкомпьютеров позволяет увеличить число моделируемых кубитов примерно до 40. Например, в Германии на суперкомпьютере Jugene [23] проведена симуляция работы 42-кубитного квантового компьютера, а в России на суперкомпьютере «Ломоносов» реали-

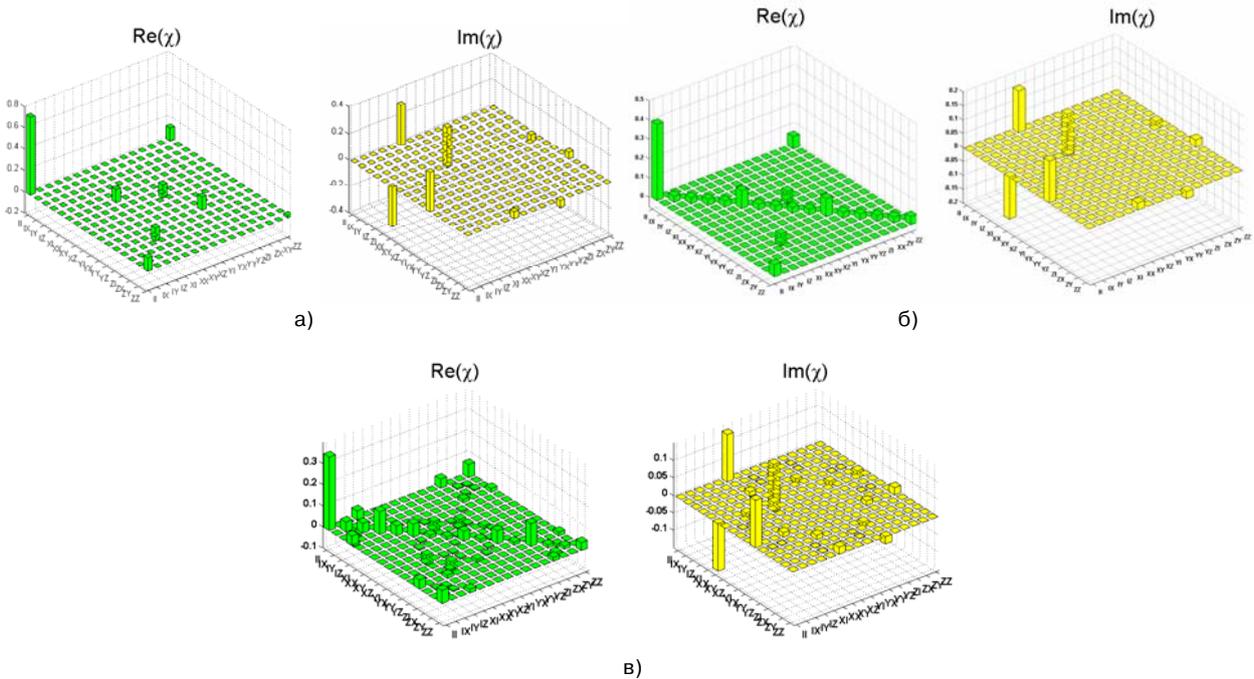


Рис. 2. Состояние Чоя-Ямилковского (хи-матрица) вентиля SQiSW

- а) идеальный случай; б) случай деполаризующего квантового шума ( $p=0,5$ );
- в) хи-матрица в условиях амплитудной и фазовой релаксации

зованы 39 кубитов [24]. В работе [25] представлено моделирование 37-кубитных схем со скоростью одна квантовая операция за 10 сек. Известна библиотека QSMPI [26], способная моделировать некоторые квантовые вентили и схемы на кластере. Библиотека основана на технологии MPI.

**3.1. Алгоритм Шора и квантовое преобразование Фурье**

Квантовое преобразование Фурье является квантовым аналогом дискретного преобразования Фурье. Оно играет ключевую роль в алгоритме Шора [27], который позволяет разложить число на простые множители экспоненциально быстрее по сравнению с известными классическими аналогами. Так наилучший известный классический алгоритм решета числового поля решает задачу за время порядка  $O[\exp((64/9)^{1/3} n^{1/3} (\ln(n))^{2/3})]$ , а алгоритм Шора за  $O(n^2 \ln(n) \ln(\ln(n)))$  (здесь  $n$  - двоичная длина раскладываемого числа).

Помимо алгоритма Шора квантовое преобразование Фурье играет ключевую роль в еще одном важнейшем классе квантовых алгоритмов, а именно в алгоритмах моделирования квантовых систем [28].

Опишем само преобразование. На базисных состояниях оно действует следующим образом:

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{i2\pi jk}{N}\right) |k\rangle,$$

где  $N=2^n$ ,  $n$  – число кубитов.

Оказывается, что на амплитудах состояния производится стандартное дискретное преобразование Фурье. Такое преобразование можно реализовать квантовой схемой (Рис. 3), требующей всего лишь  $O(\log^2 N)$  шагов, в то время как классическое быстрое преобразование Фурье требует  $O(N \log N)$ .

В схеме используется преобразование Адамара  $H = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  и контролируемый

поворот фазы: поворот  $R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp(\frac{2\pi i}{2^k}) \end{pmatrix}$

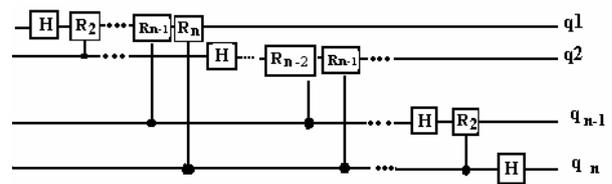


Рис. 3. Схема квантового преобразования Фурье

производится на управляемом кубите при условии, что управляющий кубит находится в состоянии  $|1\rangle$  (управляющий кубит на схеме обозначается жирной точкой, связь между кубитами указывается соответствующей линией).

**3.2. Зашумление квантовых вентиляей**

В работе было проведено моделирование не только идеальных, но и зашумленных квантовых алгоритмов. Для вентиляей были выбраны следующие модели шума.

Зашумленный вентиль Адамара:

$$H_e = HU(\theta), U(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix},$$

$$\theta = e \cdot \xi, \xi \sim N(0,1).$$

Здесь  $e$  - уровень ошибки,  $N(0,1)$  – нормальная случайная величина с нулевым средним и единичной дисперсией.

Зашумленное фазовое преобразование

$$R_{ke} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(\frac{2\pi i}{2^k} + e \cdot \xi) \end{pmatrix}.$$

Начальные векторы состояний выбирались случайными. Действительные и мнимые части всех амплитуд вероятности представляли собой независимые нормальные случайные величины с нулевыми средними и одинаковыми дисперсиями.

На Рис. 4. представлены результаты численных экспериментов, нацеленных на оценку влияния квантовых шумов на точность реализации квантового алгоритма Фурье. В качестве меры точности выбрана так называемая вероятность совпадения  $F$  (Fidelity) между идеальным  $|c_{ideal}\rangle$  и зашумленным  $|c_{noise}\rangle$  векторами состояния. Рассматриваемая величина может

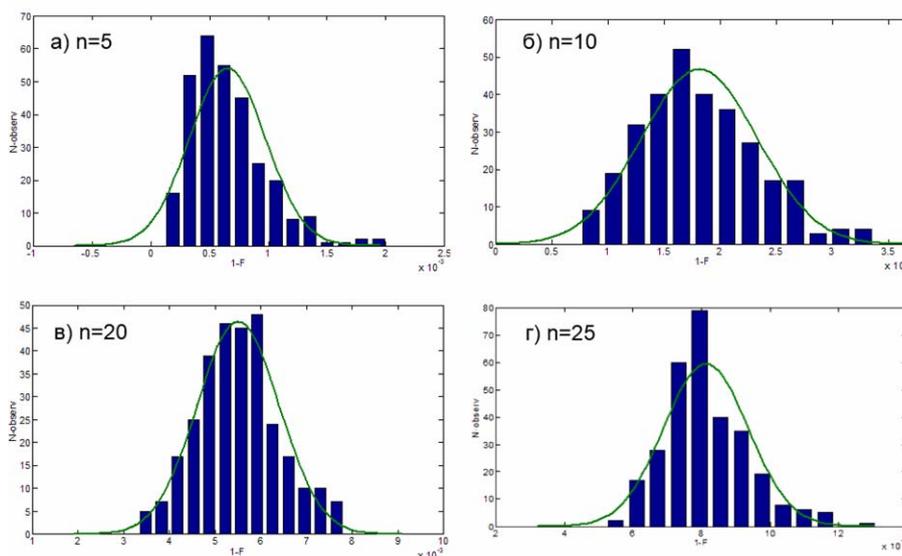


Рис. 4. Распределение потерь точности  $1 - F$  для алгоритма квантового преобразования Фурье с различным числом кубитов

быть вычислена как квадрат модуля скалярного произведения соответствующих векторов:

$$F = |\langle c_{noise} | c_{ideal} \rangle|^2.$$

В условиях нулевого шума вероятность совпадения равна единице ( $F=1$ ). В качестве меры потери точности естественно выбрать величину  $1-F$ . Для всех представленных на Рис. 4 случаев уровень шума  $\epsilon=0.01$ . Для алгоритмов с числом кубитов от 5 до 25 было выполнено по 300 численных экспериментов (гистограммы), для случая 29 кубитов – 142 эксперимента, для 32 кубитов – 25 экспериментов, кривые представляют собой гауссову аппроксимацию. Итоговые статистические характеристики представлены в Табл. 1.

Результаты этих и других численных экспериментов суммированы на Рис. 5. Здесь представлена зависимость средней точности реализации квантового алгоритма Фурье от числа кубитов для уровня шума  $\epsilon=0.01$ . Для различ-

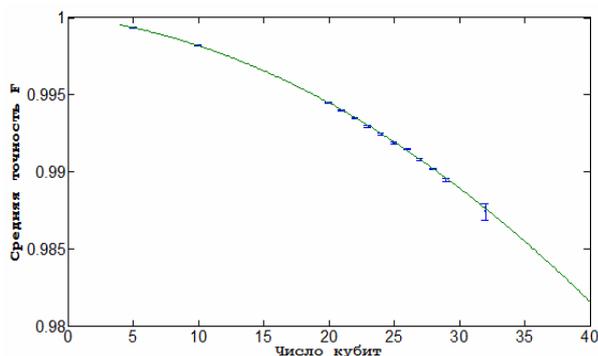


Рис. 5. Зависимость точности QFT от числа кубит  
Уровень шума  $\epsilon=0.01$

ного числа кубитов в квантовой схеме фактически было выполнено различное число численных экспериментов. Данные очень хорошо аппроксимируются параболической регрессионной зависимостью, которая была построена взвешенным методом наименьших квадратов.

### 3.3. Моделирование на суперкомпьютере МВС-100К РАН

Программа моделирования квантового преобразования Фурье была реализована для компьютера МВС-100К Российской академии наук. Реализация использует стандартную библиотеку обмена сообщениями MPI версии 1.1. Особенностью реализации является накопление

Табл. 1: Результаты моделирования зашумленного квантового преобразования Фурье

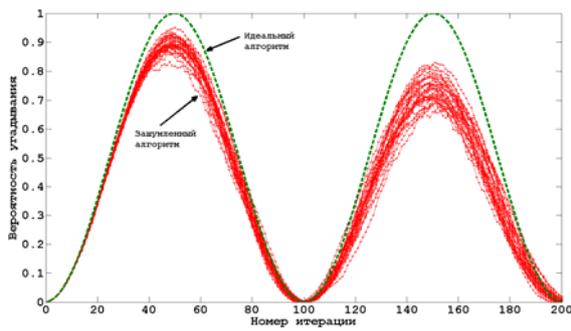
Число кубитов	Средние потери	Стандартное отклонение
5	0.000653	0.000325
10	0.00182	0.000519
20	0.00550	0.000896
25	0.00814	0.00123
29	0.01050	0.00133
32	0.0126	0.00164

Табл. 2. Скорость моделирования квантового преобразования Фурье на суперкомпьютере MBC-100K

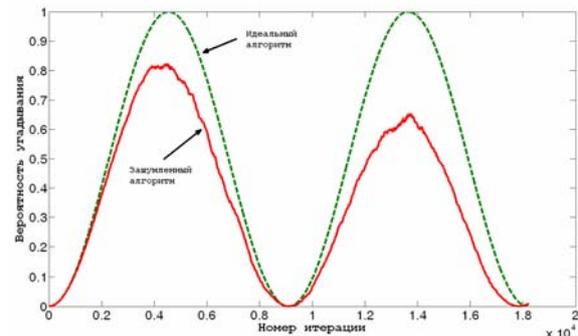
Число кубитов	Время выполнения, секунд	Число процессоров
24	29	4
25	50.5	8
26	74	16
27	119	32
28	214	64
29	412	128
32	3460	128

Табл. 3. Время выполнения 28-кубитного зашумленного квантового преобразования Фурье в зависимости от числа процессоров

Число процессоров	Время выполнения, секунд
16	333
32	252
64	214
128	166
256	68



а)



б)

Рис. 6. Моделирование алгоритма Гровера

а) 12 кубит,  $\epsilon=0.01$ , 30 численных реализаций, б) 25 кубит,  $\epsilon=0.001$ , одна численная реализация

результатов вычислений в узлах суперкомпьютера с дальнейшей их массовой отправкой необходимым процессорам, что позволяет бороться с латентностью обращения. Однако, активное использование данных заметно сказывается на скорости вычислений из-за ограниченности пропускной способности.

В Таб. 2 и Таб. 3 приведены данные о времени моделирования.

### 3.4. Моделирование алгоритма Гровера

Алгоритм Гровера, предложенный в 1996 году [29], позволяет с существенным ускорением решать переборные задачи. Пусть имеется булева функция  $f: \{0,1\}^n \rightarrow \{0,1\}$ , такая, что  $f(x)=1$  для искомого решения и  $f(x)=0$  для всех остальных  $x$ . Очевидно, что классический алгоритм находит решение за  $O(2^n)$  обращений к функции  $f$ . Алгоритм Гровера позволяет решить задачу за  $O(2^{n/2})$ , т.е. корень квадратный из классического времени. Важно отметить, что для работы алгоритма Гровера

необходим так называемый квантовый оракул, переводящий базисное квантовое состояние  $|x\rangle$  в  $(-1)^{f(x)}|x\rangle$ . Несложно показать, что такой оракул может быть создан в виде квантовой схемы, для любой булевой функции, заданной в виде схемы из функциональных элементов. В данной работе при моделировании алгоритма Гровера зашумлялись только элементы Адамара, остальная часть схемы предполагалась идеальной.

На Рис. 6 представлены результаты численного моделирования алгоритма квантового поиска Гровера. Представлена зависимость вероятности правильного решения по поиску искомого элемента в неструктурированной базе данных от числа итераций. Заметим, что идеальная реализация алгоритма Гровера, характеризуемая нулевым уровнем шума, обеспечивает вероятность угадывания, практически равную единице. Наличие шума приводит к тому, что рассматриваемая вероятность становится случайной величиной, существенно отличающейся от единицы. Так, для 30 численных экспери-

ментов для 12 кубитового алгоритма с уровнем ошибки  $\epsilon=0.01$  (Рис. 6а) соответствующая вероятность варьируется в диапазоне от 0.81 до 0.93. Заметим, что искомая вероятность быстро падает с увеличением числа кубитов в квантовой схеме. Например, уровень шума  $\epsilon=0.01$  делает практически бесполезной реализацию алгоритма Гровера для 25 кубитов. В этом случае уровень шума должен быть снижен на порядок. На Рис. 6б представлена одна реализация для 25-кубитовой квантовой схемы с уровнем шума  $\epsilon=0.001$ , соответствующая вероятность правильного решения составила 0.82. Заметим, что реализация одной итерации Гровера проще, чем реализация квантового алгоритма Фурье, однако для решения задачи требуется большое число таких реализаций (порядка  $\sqrt{2^n}$ , где  $n$  – число кубитов в квантовой схеме).

## Заключение

Сформулируем кратко основные выводы и результаты настоящей работы.

Рассмотрены методы моделирования элементной базы квантовых компьютеров с учетом влияния квантовых шумов.

Выполнено моделирование важных в практическом отношении вентилей "Контролируемое-HE" (CNOT) и "Корень из  $i$ -SWAP" (SQiSW). Рассмотрены процессы декогерентизации под действием деполаризирующего шума, а также амплитудной и фазовой релаксации.

Представлены результаты моделирования многокубитового квантового преобразования Фурье и алгоритма Гровера, полученные с использованием персональных компьютеров и суперкомпьютера МВС-100К РАН.

Авторы выражают благодарность Межведомственному Суперкомпьютерному Центру (МСЦ) РАН за предоставленные вычислительные ресурсы.

## Литература

1. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежда и реальность. Ижевск. РХД. 2001. 352с.
2. Ю.И.Богданов, К.А.Валиев, А.А.Кокин. Квантовые компьютеры: достижения, трудности реализации и перспективы // Микроэлектроника. 2011. Т.40. №4. С.243-255.
3. Нильсен М, Чанг И. Квантовые вычисления и квантовая информация. М. Мир. 2006. 824с.
4. Chen G, Church D.A., Englert B.-G., Henkel C., Rohwedder B., Scully M.O., Zubairy M.S. Quantum Computing Devices. Principles, Designs, and Analysis. Chapman & Hall. 2007. 542p. Прескилл Дж. Квантовая информация и квантовые вычисления. Том.1. М.-Ижевск. РХД. 2008. 464с.
6. Ю.И. Богданов, А.А. Кокин, В.Ф. Лукичев, А.А. Орликовский, И.А. Семенихин, А.Ю. Чернявский Квантовая механика и развитие информационных технологий // Информационные технологии и вычислительные системы. 2012. №1. С. 17-31.
7. Bogdanov Yu.I., Brida G, Genovese M., Kulik S.P., Moreva E.V., and Shurupov A.P. Statistical Estimation of the Efficiency of Quantum State Tomography Protocols // Phys. Rev. Lett. 2010. V.105. 010404. 4p.
8. Yu. I. Bogdanov, G. Brida, I. D. Bukeev, M. Genovese, K. S. Kravtsov, S. P. Kulik, E. V. Moreva, A. A. Soloviev, A. P. Shurupov // Statistical Estimation of Quantum Tomography Protocols Quality // Phys. Rev. A. 2011. V.84. 042108. 19 p.
9. Yu. I. Bogdanov, A. A. Kalinkin, S. P. Kulik, E. V. Moreva, V. A. Shershulin Quantum polarization transformations in anisotropic dispersive medium // New Journal of Physics. 2013. V.15. 035012. 24 p.
10. Ю.И. Богданов, С.А. Нуязин Характеристики точности томографии квантовых процессов с использованием сверхпроводниковых фазовых кубитов // Известия РАН. Серия физическая 2012. Т. 76. № 2. С. 164–168.
11. Ю.И. Богданов, В.Ф. Лукичев, С.А. Нуязин, А.А. Орликовский Квантовые шумы и контроль качества элементной базы квантовых компьютеров на сверхпроводниковых фазовых кубитах // Микроэлектроника. 2012. Т.41. №6. с.387-398
12. Холево А.С. Квантовые системы, каналы, информация. М.: МЦНМО 2010. 327 с.
13. Богданов Ю.И., Лукичев В.Ф., Нуязин С.А., Орликовский А.А., Холево А.С., Чернявский А.Ю. Математическое моделирование влияния квантовых шумов на качество элементной базы квантовых компьютеров // Труды ФТИАН. М. Наука. 2012. Т.22. с. 39-77.
14. Kraus States, Effects, and Operations: Fundamental Notions of Quantum Theory. Lecture Notes in Physics, V. 190. Springer- Verlag. Berlin. 1983. 151 p.
15. Lindblad G. Completely positive maps and entropy inequalities// Commun. Math. Phys. 1975. V.40. P.147-151
16. Gorini V., Frigerio A., Verri M., Kossakowski A., Sudarshan E. C. G. Properties of quantum Markovian master equations // Rep. Math. Phys. 1978. V. 13. P. 149-173.
17. Evans D. E., Lewis J. T. Dilations on irreversible evolutions in algebraic quantum theory // Commun. Dublin Inst. Adv. Stud. Ser. A 24. Dublin. 1977.
18. Холево А.С. К математической теории квантовых каналов связи // Проблемы передачи информации. 1972. Т.8. №1. С. 63-71.
19. R. C. Bialczak, M. Ansmann, M. Hofheinz, E. Lucero, M. Neeley, A. D. O'Connell, D. Sank, H. Wang, J. Wenner, M. Steffen, A. N. Cleland and J. M. Martinis Quantum process

- tomography of a universal entangling gate implemented with Josephson phase qubits // *Nature Physics*. 2010. V. 6 P. 409-413
20. T. Yamamoto, M. Neeley, E. Lucero, R. C. Bialczak, J. Kelly, M. Lenander, Matteo Mariantoni, A. D. O'Connell, D. Sank, H. Wang, M. Weides, J. Wenner, Y. Yin, A. N. Cleland, and John M. Martinis Quantum process tomography of two-qubit controlled-Z and controlled-NOT gates using superconducting phase qubits // *Phys. Rev. B*. 2010. V. 82. 184515.
  21. Pinto R.A., Korotkov A.N., Geller M. R., Shumeiko V. S., Martinis J.M. Analysis of a tunable coupler for superconducting phase qubits // *Phys. Rev. B*. 2010. V. 82. 104522.
  22. J.R. Burger New approaches to quantum computer simulation in a classical supercomputer // *arxiv:quant-ph/0308158* (2003)
  23. World record: German supercomputer simulates quantum computer <http://phys.org/news189231849.html> (дата обращения 01.12.2012г.)
  24. Д.Ю. Андреев, О.В. Корж, С.В. Коробков, А.Ю. Чернявский Параллельный алгоритм моделирования идеального квантового алгоритма Гровера // Тезисы конференции ПАВТ-2013
  25. G. Arnold, T. Lippert, N. Pomplun, M. Richter Large Scale Simulation of Ideal Quantum Computers on SMP-Clusters // *PARCO*, pp. 447-454, 2005
  26. F. Tabakin, B. Julia-Diaz QCMPi: A parallel environment for quantum computing // *Computer Physics Communications* n. 180, p. 948. 2009
  27. P. Shor Algorithms for quantum computation: discrete logarithms and factoring // *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. IEEE, 1994.*
  28. C. Zalka Simulating quantum systems on a quantum computer // *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 454.1969 (1998): 313-322.
  29. L.K. Grover A fast quantum mechanical algorithm for database search // *Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996)* p. 212.

**Богданов Юрий Иванович.** Заведующий лабораторией Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский государственный университет им. М. В. Ломоносова в 1986 году. Доктор физико-математических наук. Автор более 120 печатных работ. Область научных интересов: квантовая информатика, физика квантовых компьютеров. E-mail: bogdanov@ftian.ru

**Богданова Надежда Александровна.** Доцент кафедры высшей математики Национального исследовательского университета "МИЭТ". Окончила Московский государственный университет им. М. В. Ломоносова в 1986 году. Кандидат физико-математических наук. Автор более 40 печатных работ. Область научных интересов: цифровая обработка сигналов, математическое моделирование.

**Лукичев Владимир Федорович.** Заместитель директора по научной работе Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский государственный университет им. М. В. Ломоносова в 1978 году. Доктор физико-математических наук, профессор, член-корреспондент РАН. Автор более 70 печатных работ. Область научных интересов: физика сверхпроводников, микроэлектроника. E-mail: lukichev@ftian.ru

**Орликовский Александр Александрович.** Директор Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский инженерно-физический институт в 1961 году. Доктор технических наук, профессор, академик РАН. Автор свыше 300 печатных работ, в том числе двух монографий. Область научных интересов: технологии кремниевой микро- и нанoeлектроники, в том числе технологии МДП-транзисторов с динамичеся длиной канала порядка 10 нм, включая квантовое описание характеристик таких транзисторов; технологии твердотельных квантовых компьютеров. E-mail: orlikovsky@ftian.ru

**Семенihin Игорь Александрович.** Старший научный сотрудник Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский инженерно-физический институт (Технический университет) в 2000 году. Кандидат физико-математических наук. Автор более 30 печатных работ. Область научных интересов: высокопроизводительные вычисления, моделирование квантовых приборов и устройств. E-mail: isemenihin@mail.ru

**Холево Александр Семенович.** Ведущий научный сотрудник Математического института им. В.А. Стеклова РАН (МИАН). Окончил Московский физико-технический институт в 1966 году. Доктор физико-математических наук, профессор. Автор свыше 170 печатных работ, в том числе 5 монографий. Область научных интересов: квантовая теория информации, квантовые вычисления, некоммутативная теория вероятностей, квантовые случайные процессы, динамические (марковские) полугруппы, статистическая структура квантовой теории, квантовые измерения. E-mail: holevo@mi.ras.ru

**Чернявский Андрей Юрьевич.** Старший научный сотрудник Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский государственный университет им. М. В. Ломоносова в 2005 году. Кандидат физико-математических наук. Автор 10 печатных работ. Область научных интересов: квантовые вычисления, квантовая запутанность, искусственный интеллект, параллельные вычисления. E-mail: andrey.chernyavskiy@gmail.com