МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КВАНТОВЫХ ТЕХНОЛОГИЙ

Александр Н. Печень
МИАН им. В.А. Стеклова

11 декабря 2023 года

Квантовые технологии

Квантовые системы (электроны, атомы, фотоны и другие объекты микромира) описываются законами, отличающимися (и нередко противоположными) от законов классической механики, описывающих макроскопические объекты: суперпозиция «взаимоисключающих» состояний, внутренне вероятностный характер квантовых процессов, невозможность неразрушающих измерений, запрет одновременного точного измерения координаты и импульса, туннелирование, запрет копирования квантовых состояний и т.п.

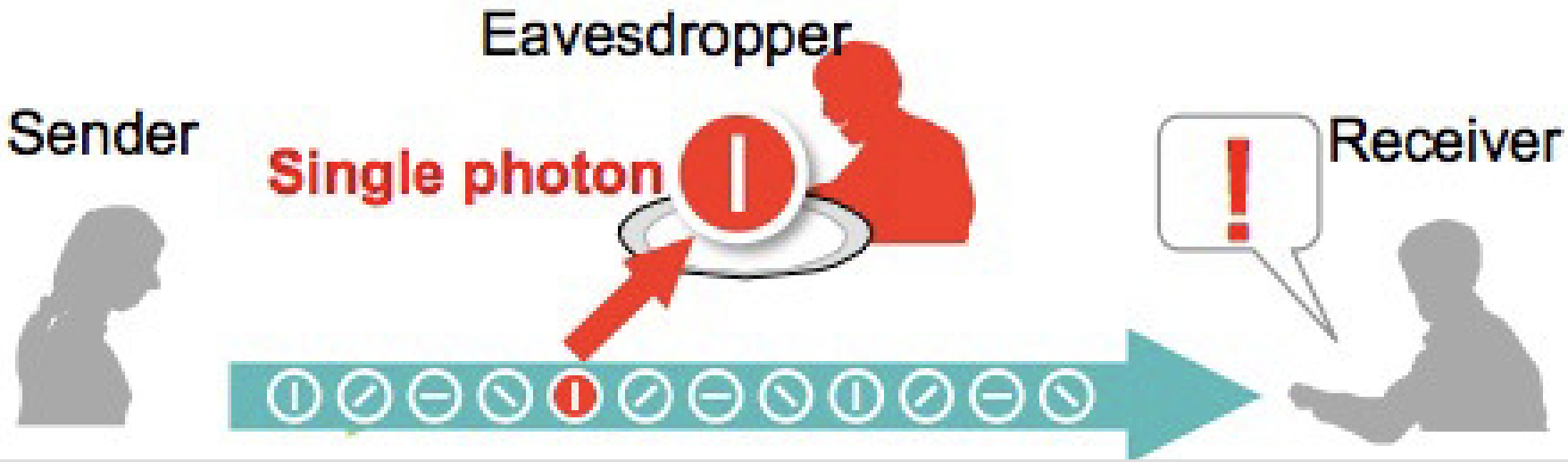
Квантовые технологии — технологии, основанные на использовании свойств индивидуальных квантовых систем.

Законы квантовой механики используют весьма широкий математический аппарат: теорию гильбертовых пространств, операторов, д.у. в частных производных, группы и алгебры Ли, C^*–алгебры, (квантовые) случайные процессы, вещественный и комплексный анализ (функций многих переменных), дифференциальная геометрия, топология, теория сложности и т.д.

Основные направления квантовых технологий

- Квантовые коммуникации и крипрография
- Квантовые алгоритмы, компьютеры и симуляторы
- Квантовые сенсоры и метрология
- Лазерная химия, ЯМР и т.д.

Квантовая криптография



И.М. Гельфанд, М.А. Наймарк (1943), I. Sigal (1947), W. Steinspring, L. Accardi, В.П. Белавкин, И.В. Волович, А.С. Холево, Б. Шумахер, М. Вестмориленд, (квантовая теорема кодирования); П. Шор, Е. Книлл и Р. Лафламм (квантовые коды, исправляющие ошибки), Ч. Беннет и Ж. Брассард (протокол квантового распределения ключа BB84), Д. Майерс (доказательство стойкости протоколов квантовой криптографии)

Квантовая криптография

- Stephen Wisner: Квантовые деньги (1970).
- Протокол BB84 (Криптостойкость: Mayers 1996-1998, Shor and Preskill 2000)
- Протокол E91 (A. Ekert, 1991)
- Протокол B92 (C. Bennett, 1992)
- Другие протоколы
- MagiQ, ID Quantique, Toshiba, ...

Неидеальные источники и детекторы, не строго однофотонные состояния и т.п.

- Доказательства стойкости протоколов КРК.[1]
- Атаки на протоколы КРК.
- Методы быстрой оценки новых протоколов КРК.

[1] Проект ИСП-МИАН 2020-2023.

Квантовые алгоритмы

- Состояние кубита — норм. вектор в $\mathbb{C}^2$.
- Состояние N кубит — норм. вектор в $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$.
- Квантовый k-кубитный гейт (вентиль) — унитарный оператор в Г.П. k кубит.
- Квантовая схема — последовательность кв. гейтов $U_S[i_1, \ldots, i_{k_S}] \ldots U_1[i_1, \ldots, i_{k_1}]$.

Квантовые алгоритмы

1980, 1981: Ю. Манин, Р. Фейнман: использование квантовых систем для ускорения вычислений. Квантовые операции: унитарные.

Квантовые алгоритмы

1980, 1981: Ю. Манин, Р. Фейнман: использование квантовых систем для ускорения вычислений. Квантовые операции: унитарные.

1994: Алгоритм Шора нахождения периода (факторизации числа N). Число квантовых операций (без ошибок):

$$O((\log N)^2(\log\log N)(\log\log\log N)) \text{ v.s. subexp.}$$
$$N^2 < 2^n < 2N^2$$

Квантовые алгоритмы

1980, 1981: Ю. Манин, Р. Фейнман: использование квантовых систем для ускорения вычислений. Квантовые операции: унитарные.

1994: Алгоритм Шора нахождения периода (факторизации числа N). Число квантовых операций (без ошибок):

$$O((\log N)^2(\log\log N)(\log\log\log N)) \text{ v.s. subexp.}$$
$$N^2 < 2^n < 2N^2$$

1996: Алгоритм Гровера решения задачи перебора из N элементов. Число квантовых операций $R = U_\xi U_O$ (включая оракул):

$$\frac{\pi}{4}\sqrt{N} \text{ v.s. } \frac{N}{2}$$
$$n = \lceil \log_2 N \rceil$$

Универсальные наборы квантовых вентилей

Универсальный набор квантовых вентилей: позволяет генерировать с любой точностью любой унитарный оператор.

[2]P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "A new universal and fault-tolerant quantum basis," Information Processing Letters, vol. 75, no. 3, pp. 101–107, 2000

Универсальные наборы квантовых вентилей

Универсальный набор квантовых вентилей: позволяет генерировать с любой точностью любой унитарный оператор.

Теорема Готссмана–Нила: Квантовые вычисления, основанные на

- приготовлении состояний в вычислительном базисе;
- гейтах H, S, CNOT, Паули
- измерениях в вычислительном базисе;
- классическом управлении,

могут быть эффективно симулированы на классическом компьютере.

[2] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "A new universal and fault-tolerant quantum basis," Information Processing Letters, vol. 75, no. 3, pp. 101–107, 2000

Универсальные наборы квантовых вентилей

Универсальный набор квантовых вентилей: позволяет генерировать с любой точностью любой унитарный оператор.

Теорема Готссмана–Нила: Квантовые вычисления, основанные на

- приготовлении состояний в вычислительном базисе;
- гейтах H, S, CNOT, Паули
- измерениях в вычислительном базисе;
- классическом управлении,

могут быть эффективно симулированы на классическом компьютере.

Clifford+T=$\{H, CNOT, T\}$, где $T = Z^{1/4}$ — $\frac{\pi}{8}$-gate. Универсальный набор.[2] Есть много других наборов.

[2] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "A new universal and fault-tolerant quantum basis," Information Processing Letters, vol. 75, no. 3, pp. 101–107, 2000

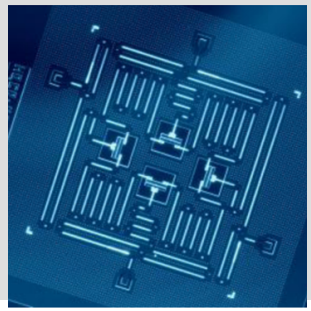
Аппроксимации (без ошибок)

Теорема Соловея-Китаева (аппроксимация однокубитных унитарных операций): Пусть $G \subset SU(2)$ генерирует плотное подмножество в $SU(2)$. Тогда это можно сделать быстро: в ϵ–окрестность любого элемента из $SU(2)$ можно попасть за

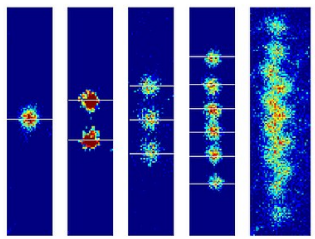
$$l = O(\log^c(1/\epsilon)), \quad c = 3 + \delta \quad ; \quad \text{можно } c \to 1$$

Физические реализации (платформы)

Сверхпроводящие кубиты. Кубиты — трансмоны, флаксониумы. 2021: IBM Eagle (127 кубит, квантовый объем 10^8); 2023 IBM Heron (133); Condor (1121). Rigetti Advantage (128 кубит, КО 1.6×10^9.



Ионы в ловушках. IonQ Quantum Computer (128 кубит, КО 4.8×10^9.); The Enchilada Trap (200 кубит).



Нейтральные атомы. Кубиты — энергетические состояния в нейтральных (ридберговских) атомах. Управление с помощью «оптического пинцета» — сфокусированного пучка света, способного к удержанию микроскопических незаряженных частиц. Atom Computing — ок. 1000 кубит в 2024 г.

Фотонные. University of Science and Technology of China Jiuzhang system (126 фотонных кубит, КО 10^{10}.

Проблема: меры квантовой производительности (квантовый объем)

Квантовое превосходство

Неуниверсальные квантовые вычисления.

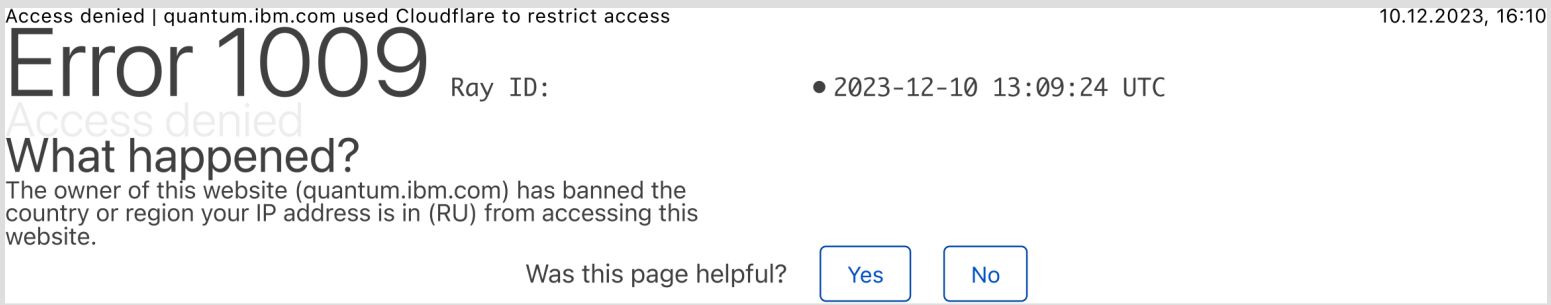
2019: Sampling random circuits on 53(54) transmon qubit processor "Sycamore". Errors:

- Single-qubit: $0.15 - 0.16\%$.
- Two-qubit: $0.36 - 0.93\%$.
- Readout: $3.1 - 3.8\%$.

2020: Boson sampling on Jiuzhang quantum computer; permanent of a matrix. $\mathcal{F} = 0.990(1)$.

Облачные платформы

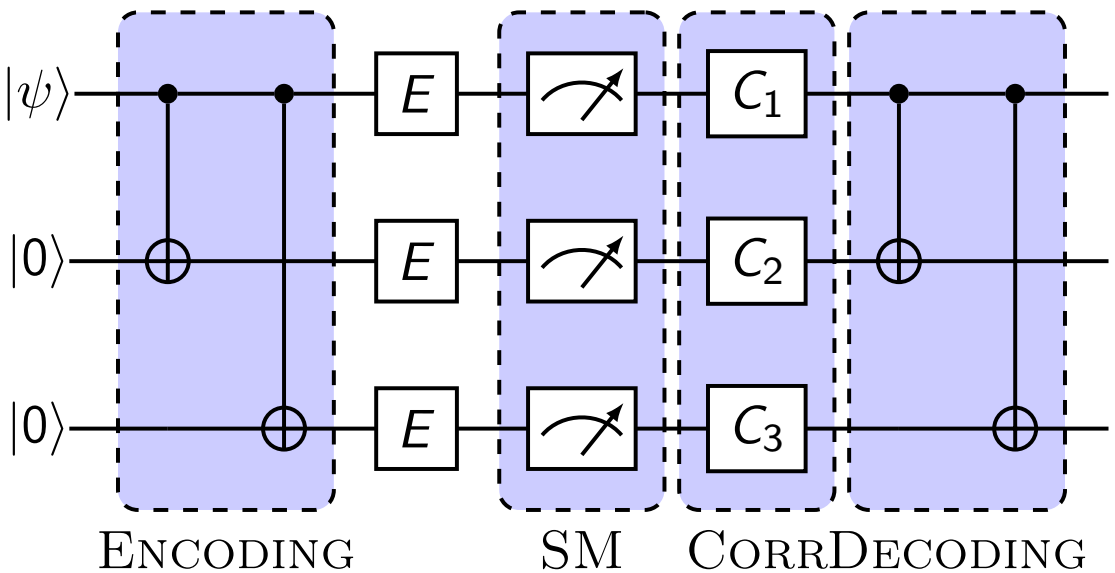
IBM Quantum Platform (сверхпроводящие, трансмоны)



Квантовая коррекция ошибок

Error (bit flip): X with prob. p: $\rho \to \ E(\rho) = (1-p)\rho + pX\rho X$.

- Encoding $|0\rangle \to |0_L\rangle = |000\rangle$, $|1\rangle \to |1_L\rangle = |111\rangle$.
- Syndrome measurement of Z_1Z_2 and Z_2Z_3, error on ith qubit.
- Error correction: $C_i = X$, other $C_j = \mathbb{I}$.



$\rho_{\text{out}} \approx |\psi\rangle\langle\psi|$

Fidelity: $\mathcal{F} = \langle\psi|\rho_{\text{out}}|\psi\rangle = 1 - 3p^2 + 2p^3$ vs $1-p$.

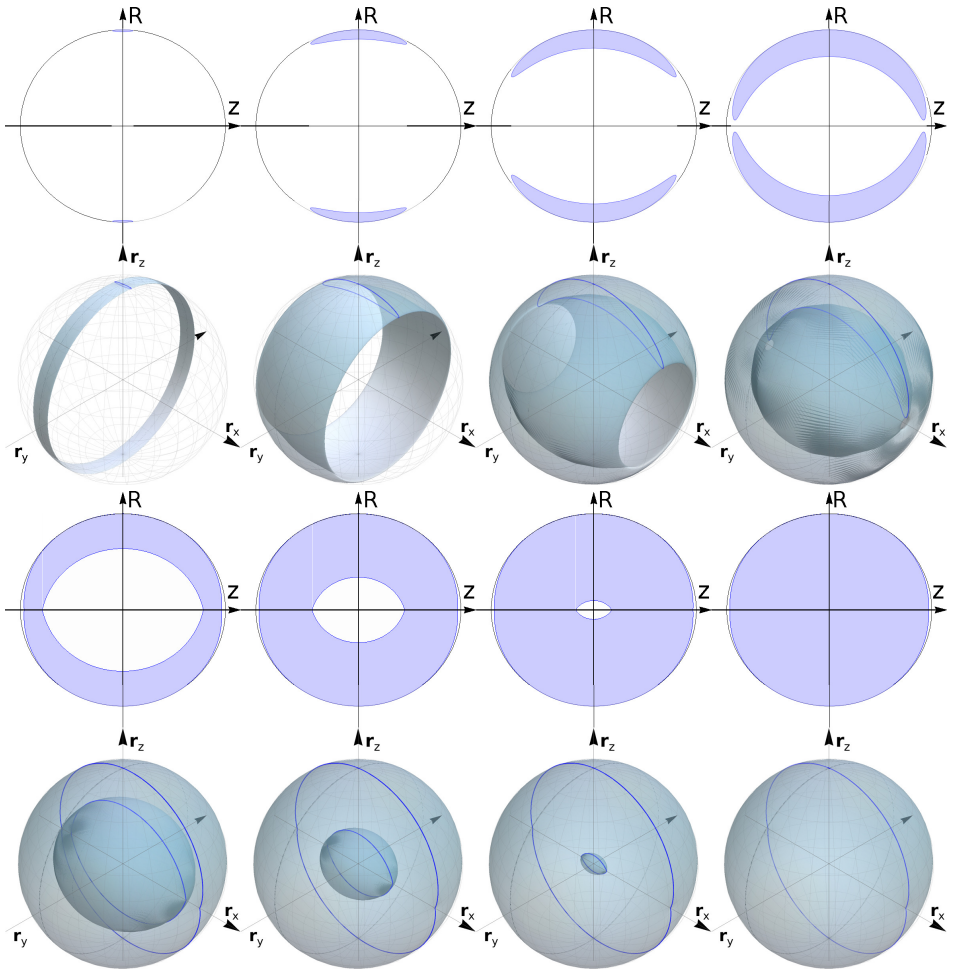
Квантовые коды, исправляющие ошибки

Квантовые коды, исправляющие ошибки: П. Шор (1995), Е. Книлл и Р. Лафламм (1997), А. Кальдербанк, А. Стин, А. Китаев

- 3-qubit bit flip (and phase flip) codes
- 5-qubit code (minimal) correcting any single-qubit errors
- 7-qubit Steane code
- 9-qubit Shor code
- Calderbank–Shor–Steane (CSS) codes
- Stabilizer codes
- Topological, e.g., surface 2D codes
- Бозонные состояния: Schrödinger cat states, Gottesman-Kitaev-Preskill, binomial codes, etc.[3]

[3] Напр.: G.G. Amosov, A.S. Mokeev, A.N. Pechen, "Non-commutative graphs and quantum error correction for a two-mode quantum oscillator", Quantum Information Processing, 19:3, 95 (2020).

Множества достижимости[4]



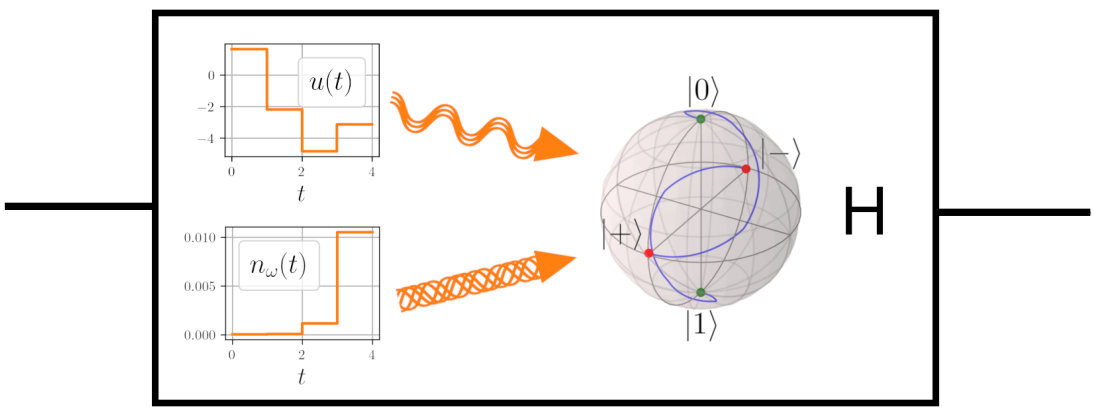
[4] L. Lokutsievskiy, A. Pechen, Reachable sets for two-level open quantum systems driven by coherent and incoherent controls, J. Phys. A: Math. Theor. **54**, 395304 (2021).

Методы оптимизации

$$f \to f + \varepsilon \mathrm{grad}\mathcal{F}$$

- B.O. Volkov, O.V. Morzhin, A.N. Pechen, Quantum control landscape for ultrafast generation of single-qubit phase shift quantum gates, J. Phys. A: Math. Theor. 54, 215303 (2021).
- V. Petruhanov, A. Pechen, GRAPE optimization for open quantum systems with time-dependent decoherence rates driven by coherent and incoherent controls, J. Phys. A 56, 305303 (2023).
- V.N. Petruhanov, A.N. Pechen, Quantum gate generation in two-level open quantum systems by coherent and incoherent photons found with gradient search, Photonics, 10:2, 220 (2023).

$$\frac{d\rho_t^f}{dt} = -i[H_u(t), \rho_t^f] + \sum_i \gamma_i(t)\mathcal{D}_i(\rho_t^f).$$



Управление квантовыми системами

Квантовое управление для оптимального приготовления состояний и генерации квантовых вентилей

Максимизация фиделити:

$$\mathcal{F} = \frac{1}{n^2}|\mathrm{Tr}\, W^+ U_T|^2 \to \max; \quad i\dot{U}_t = (H_0 + f(t)V)U_t$$

$$\mathcal{F} = \mathcal{F}_{\max} - \epsilon\mathcal{D}$$

Вывод мастер-уравнений

- A.S. Trushechkin, Unified Gorini-Kossakowski-Lindblad-Sudarshan quantum master equation beyond the secular approximation, Phys. Rev. A 103, 062226 (2021).
- S.N. Filippov and I.A. Luchnikov, Collisional open quantum dynamics with a generally correlated environment: Exact solvability in tensor networks, Phys. Rev. A, 105, 062410 (2022).
- A.E. Teretenkov, Memory tensor for non-Markovian dynamics with random Hamiltonian, Mathematics 11, 3854 (2023).

Квантовое машинное обучение и ИИ в квантовых технологиях

- Применение методов машинного обучения, генетических алгоритмов,[5] тензорных сетей для задач квантовых технологий, моделирования динамики сложных квантовых систем и повышения информационной безопасности.
- Обобщение методов машинного обучения на квантовый случай.[6]

[5] A. Pechen, H. Rabitz, "Teaching the environment to control quantum systems", Phys. Rev. A, 73 (2006), 062102

[6] D.-Y. Dong, C.-L. Chen, T.-J. Tarn, A. Pechen, H. Rabitz, "Incoherent control of quantum systems with wavefunction controllable subspaces via quantum reinforcement learning", IEEE Transactions on Systems, Man and Cybernetics — Part B: Cybernetics, 38:4 (2008), 957–962

Кадры: Базовая кафедра МИАН — МФТИ

- Математические основы квантовой информатики (А.С. Холево)
- Управление квантовыми системами (А.Н. Печень, О.В. Моржин)
- Классические и квантовые случайные процессы (Г.Г. Амосов)
- Основы теории открытых квантовых систем (А.Е. Теретёнков)
- Введение в теорию сложности (В.В. Подольский)
- Введение в интегрируемые системы (А.В. Зотов)
- Функциональные интегралы и их приложения в квантовой теории и статистической механике (О.Г. Смолянов, В.Ж. Сакбаев)
- Квантовые вычисления (А.С. Трушечкин)
- Квантовые тензорные сети (С.Н. Филиппов)
- Геометрические методы в квантовой информации (Д.С. Агеев)
- Квантовая криптография (Д.А. Кронберг)

Школа по сверхпроводниковых квантовым вычислениям в ПОМИ (2023).

Что было бы полезно организовать

1) Введение в номенклатуру научных специальностей, по которым присуждаются ученые степени, профильной специальности.

2) Обеспечение удаленного доступа к квантовым облачным вычислениям на базе российских вычислительных платформ для всех образовательных, научных и научно-образовательных учреждений Российской Федерации, в которых ведется образовательная деятельность, исследования или разработки в области квантовых технологий.

3) Организация работ, направленных на развитие математических методов управления квантовыми системами для промышленных квантовых вычислительных платформ, перспективных исследований протоколов квантовых коммуникаций и методов машинного обучения в квантовых технологиях.

4) Введение профильной стипендии всем специализирующимся по направлениям, связанным с квантовыми технологиями: (а) студентам старших курсов, обучающимся в образовательных учреждениях Российской Федерации, имеющим оценки не менее «хорошо» и «отлично» по профильным дисциплинам, и (б) аспирантам образовательных и научных организаций Российской Федерации, имеющим профильные публикации в изданиях, индексируемых в российских и международных базах данных.