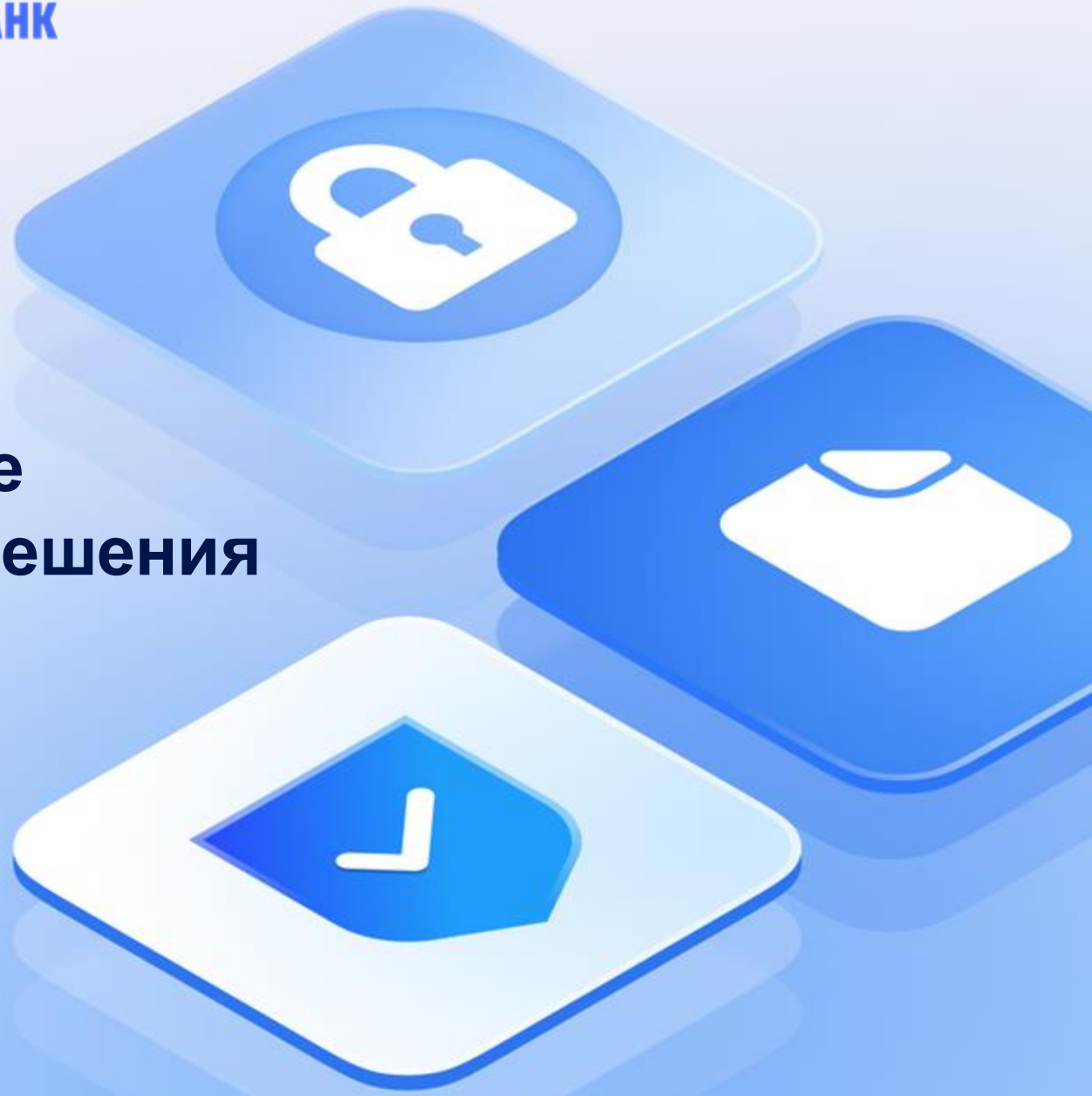
РусКрипто

ГАЗПРОМБАНК



Квантово-устойчивые криптографические решения

Опыт Газпромбанка

Алексей Федоров

РусКрипто ГАЗПРОМБАНК

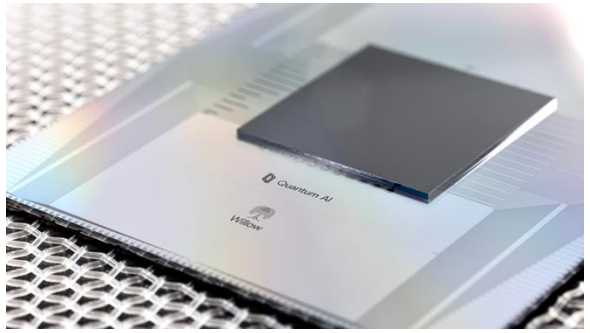
Прогресс в квантовых вычислениях

Развитие квантовых вычислений: прогресс в возможностях и коррекция ошибок

ГАЗПРОМБАНК

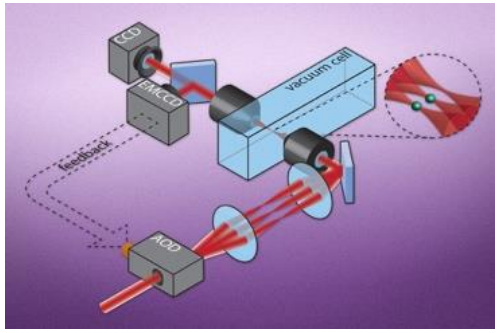
Продолжается параллельная разработка квантовых компьютеров на различных физических принципах

Сверхпроводниковые кубиты



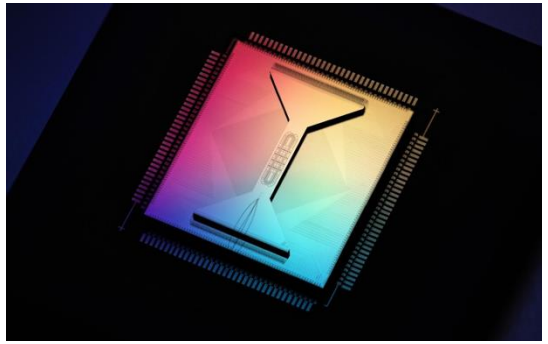
Google

Атомные кубиты



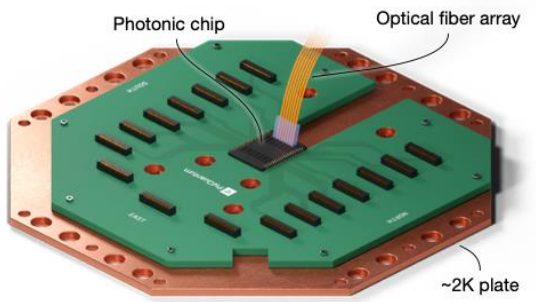
QuEra & Harvard

Ионные кубиты

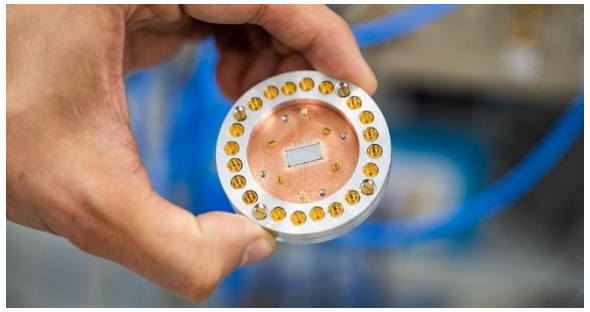


Quantinuum

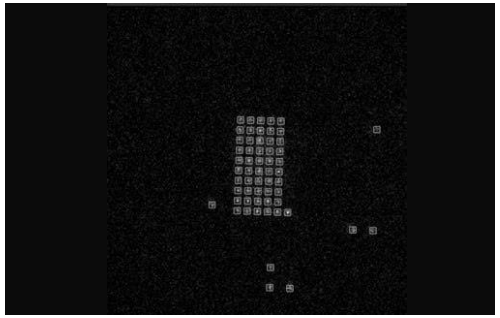
Фотонные кубиты



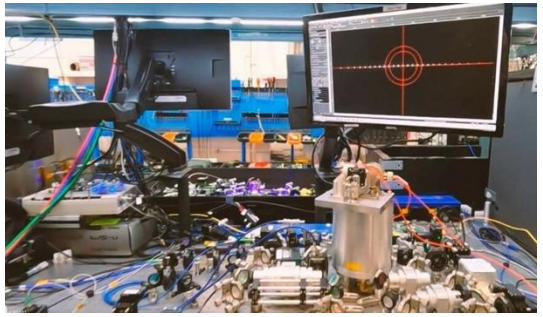
PsiQuantum



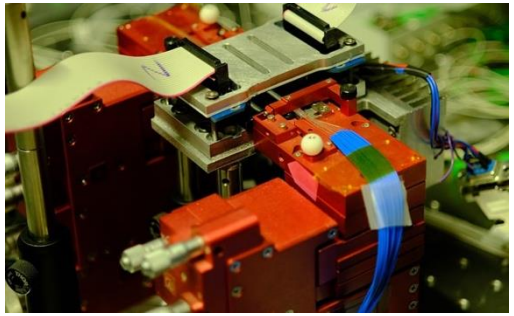
МИСИС



МГУ и РКЦ



ФИАН и РКЦ

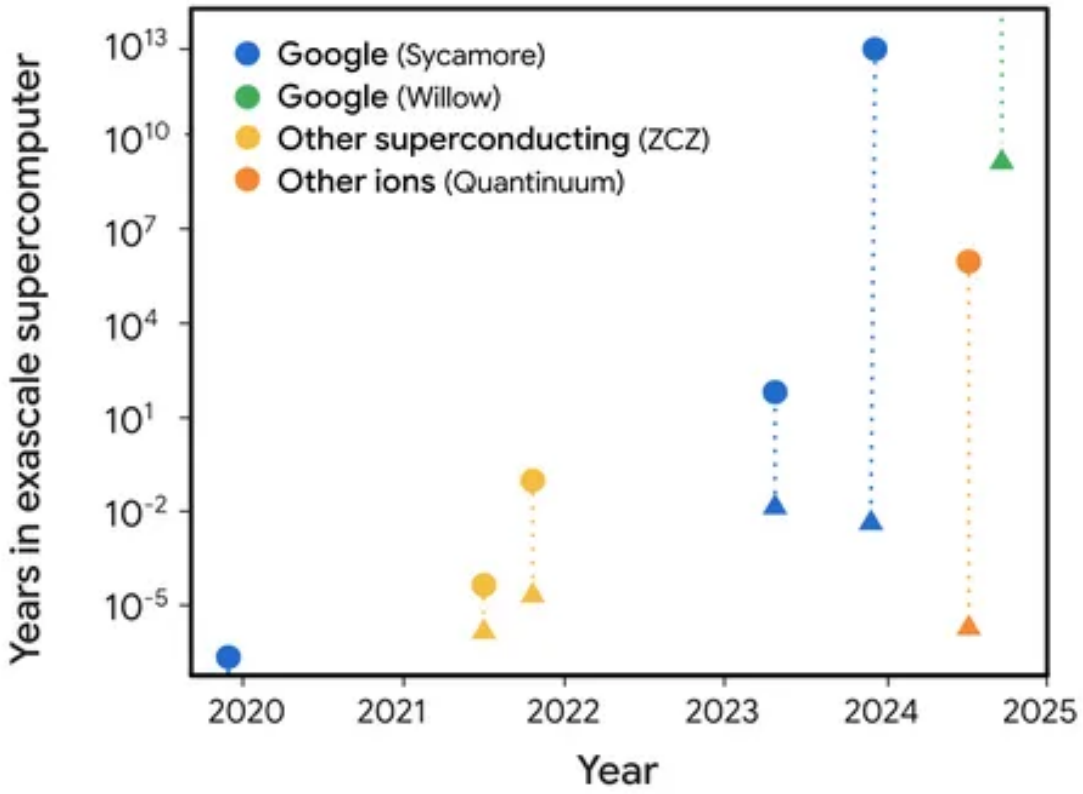


МГУ и РКЦ

Развитие квантовых вычислений: квантовое вычислительное преимущество

ГАЗПРОМБАНК

Willow – 105 сверхпроводниковых кубитов, задача сэмплирования случайных квантовых цепочек



Zuchongzhi 3.0 – 105 сверхпроводниковых кубитов, задача сэмплирования случайных квантовых цепочек

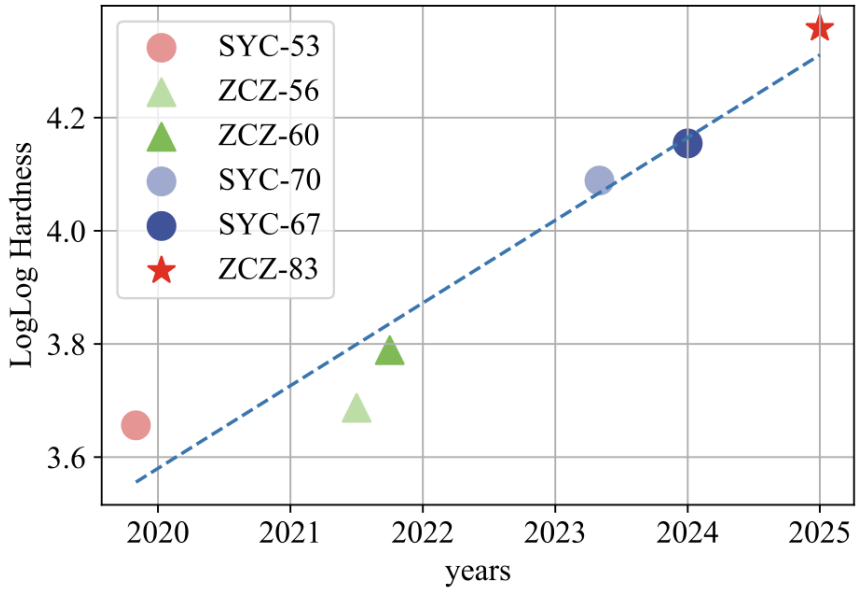


FIG. 4. **Progress on random circuit sampling.** The evolution of the time complexity in random circuit sampling experiments. The dotted line illustrates the pattern of doubly-exponential growth. SYC and ZCZ respectively denote the Sycamore and *Zuchongzhi* processors.

Развитие квантовых вычислений: прогресс в возможностях и коррекция ошибок

ГАЗПРОМБАНК

Демонстрация экспоненциального уменьшения ошибок с ростом кодового расстояния в поверхностном коде
[Google Quantum AI and Collaborators, "Quantum error correction below the surface code threshold", arXiv:2408.13687]

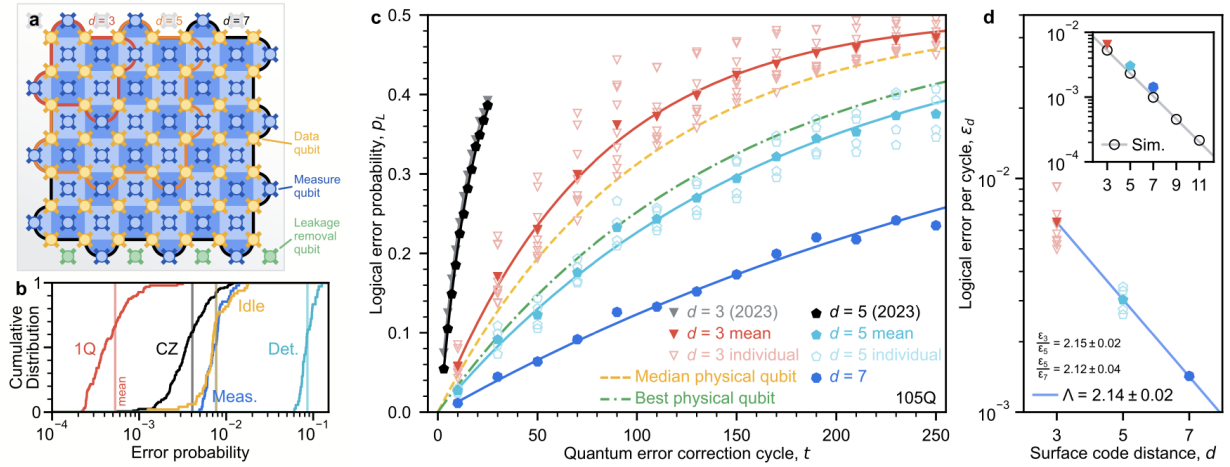
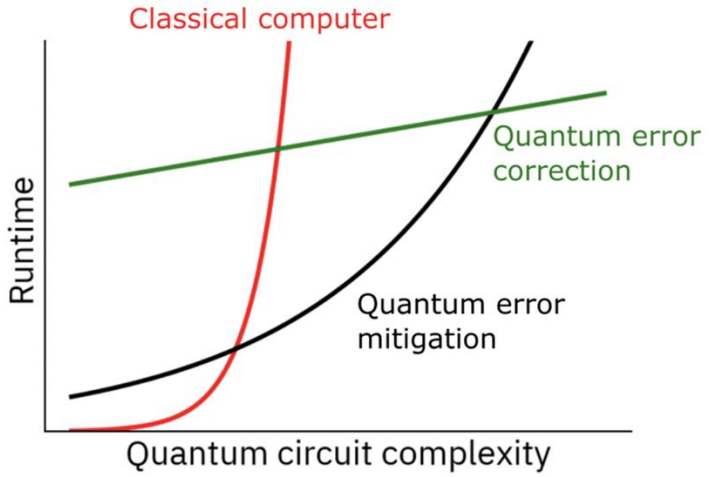


FIG. 1. **Surface code performance. a,** Schematic of a distance-7 surface code on a 105-qubit processor. Each measure qubit (blue) is associated with a stabilizer (blue colored tile). Red outline: one of nine distance-3 codes measured for comparison (3×3 array). Orange outline: one of four distance-5 codes measured for comparison (4 corners). Black outline: distance-7 code. We remove leakage from each data qubit (gold) via a neighboring qubit below it, using additional leakage removal qubits at the boundary (green). **b,** Cumulative distributions of error probabilities measured on the 105-qubit processor. Red: Pauli errors for single-qubit gates. Black: Pauli errors for CZ gates. Blue: Average identification error for measurement. Gold: Pauli errors for data qubit idle during measurement and reset. Teal: weight-4 detection probabilities (distance-7, averaged over 250 cycles). **c,** Logical error probability, p_L, for a range of memory experiment durations. Each datapoint represents 10^5 repetitions decoded with the neural network and is averaged over logical basis (X_L and Z_L). Black and grey: data from Ref. [17] for comparison. Curves: exponential fits after averaging p_L over code and basis. To compute ε_d values, we fit each individual code and basis separately [24]. **d,** Logical error per cycle, ε_d, reducing with surface code distance, d. Uncertainty on each point is less than 5×10^{-5}. Symbols match panel c. Means for $d = 3$ and $d = 5$ are computed from the separate ε_d fits for each code and basis. Line: fit to Eq. 1, determining Λ. Inset: simulations up to $d = 11$ alongside experimental points, both decoded with ensembled matching synthesis for comparison. Line: fit to simulation, $\Lambda_{\text{sim}} = 2.25 \pm 0.02$.

- Базовые принципы коррекции ошибок показаны экспериментально: **вероятность ошибки при использовании кодов коррекции уменьшается**



- **Работы IBM по смягчению ошибок**

Развитие квантовых вычислений: прогресс в возможностях и коррекция ошибок

ГАЗПРОМБАНК

Implementing Fault-tolerant Entangling Gates on the Five-qubit Code and the Color Code

C. Ryan-Anderson, N. C. Brown, M. S. Allman, B. Arkin, G. Asa-Attuah, C. Baldwin, J. Berg, J. G. Bohnet, S. Braxton, N. Burdick, J. P. Campora, A. Chernoguzov, J. Esposito, B. Evans, D. Francois, J. P. Gaebler, T. M. Gatterman, J. Gerber, K. Gilmore, D. Gresh, A. Hall, A. Hankin, J. Hostetter, D. Lucchetti, K. Mayer, J. Myers, B. Neyenhuis, J. Santiago, J. Sedlacek, T. Skripka, A. Slattery, R. P. Stutz, J. Tait, R. Tobey, G. Vittorini, J. Walker, D. Hayes

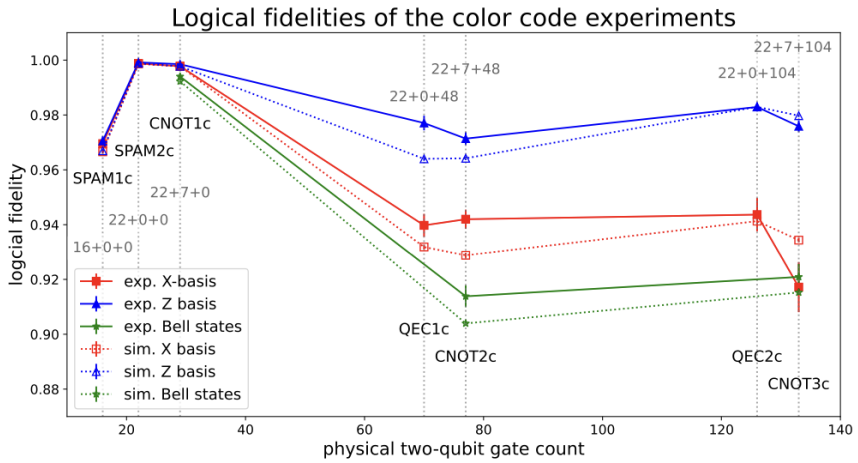


FIG. 6. Experimental and simulated logical fidelity vs the total two-qubit gate count in seven different color code experiments. Note that the ordering here is different than that in Table III, as denoted by the vertical line labels. The red, blue and green markers denote experiments that ideally produce output states in the $\overline{X}$, $\overline{Z}$, and Bell bases respectively. The markers connected with solid lines represent experimental data, and the markers connected with dashed lines represent simulated data.

Demonstrating Bayesian Quantum Phase Estimation with Quantum Error Detection

Kentaro Yamamoto, Samuel Duffield, Yuta Kikuchi, David Muñoz Ramo

Квантовые алгоритмы с помощью логических операций на логических кубитах: 920 физических операций, чтобы оценить энергию основного состояния молекулы с точностью 6×10^{-3}

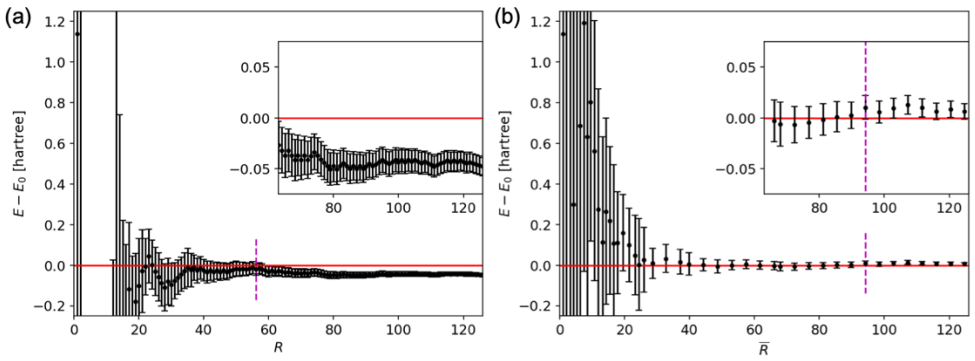
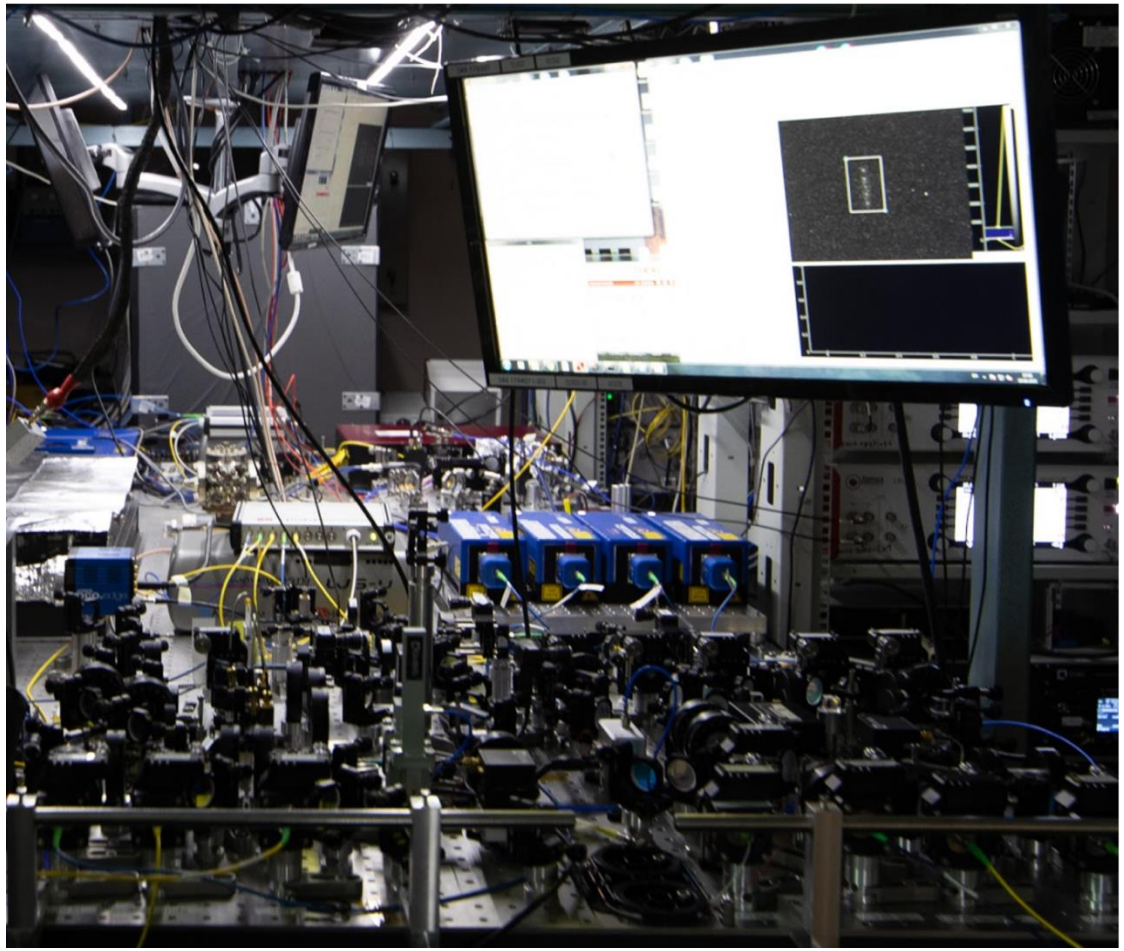


Figure 5. Estimated energies plotted against the number of experiments R for the unencoded QPE (a) and against the rescaled number of experiments $\overline{R}$ for the encoded experiments (b). The black circles represent the estimated energies with the error bars representing $\sqrt{\mathrm{Var}_H[E]}$. The purple dashed lines indicate when the distributions are converted from Fourier to von Mises representations.

Развитие квантовых вычислений: прогресс в возможностях и коррекция ошибок



Работа групп
И.А. Семерикова и Н.Н. Колачевского

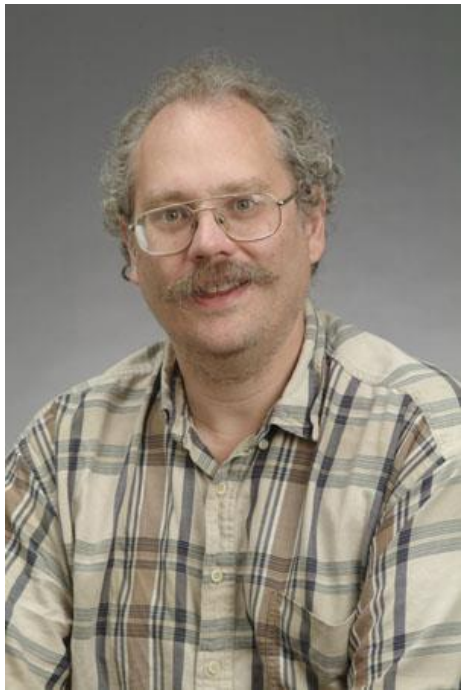
2021-2022:
- 4 кубита (2 кудита)
- точность однокубитных операций — 95%
- точность двухкубитных операций — 70%

2022-2023:
- 16 кубитов (8 кудитов)
- точность однокубитных операций — 99,1%
- точность двухкубитных операций — 95%

2023-2024:
- 20 кубитов (10 кудитов)
- точность однокубитных операций — 99,1%
- точность двухкубитных операций — 95%

2024:
- 50 кубитов (25 кудитов)
- точность однокубитных операций — 99,1%
- точность двухкубитных операций — 95%

Развитие квантовых вычислений: новые алгоритмы факторизации



- Современная асимметричная криптография базируется на сложности решения определенного класс математических задач, например, **факторизации** (разложение числа на простые множители).
- В 1995 году Питер Шор предложил алгоритм для задач факторизации и дискретного логарифмирования за полиноминальное время для квантового компьютера. Число 15 было разложено на множители 3 и 5 при помощи квантового компьютера с помощью компьютера с 7 кубитами.

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2,3]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[3]Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

Physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds.

Развитие квантовых вычислений: новые алгоритмы факторизации

ГАЗПРОМБАНК

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, Lan Luo, Qianheng Duan, Yiting Liu, Wenhao Shi, Yangyang Fei, Xiangdong Meng, Yu Han, Zheng Shan, Jiachen Chen, Xuhao Zhu, Chuanyu Zhang, Feitong Jin, Hekang Li, Chao Song, Zhen Wang, Zhi Ma, H. Wang, Gui-Lu Long

Shor's algorithm has seriously challenged information security based on public key cryptosystems. However, to break the widely used RSA-2048 scheme, one needs millions of physical qubits, which is far beyond current technical capabilities. Here, we report a universal quantum algorithm for integer factorization by combining the classical lattice reduction with a quantum approximate optimization algorithm (QAOA). The number of qubits required is O(logN/loglog N), which is sublinear in the bit length of the integer N, making it the most qubit-saving factorization algorithm to date. We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.

- Выбор факторной базы
- Поиск гладких пар (sr-пар)
- Построение СЛАУ
- Построение сомножителей из решения СЛАУ на основе идеи Ферма

Поиск sr-пар сводится к поиску ближайшего вектора на решетке (CVP), может быть решено с помощью LLL-алгоритма

Факторизация Шнорра

- Для CVP строится функционал QUBO – задача оптимизации
- Задача оптимизации решается с помощью алгоритма квантовой приближенной оптимизации (QAOA), который работает без коррекции ошибок
- В ходе QAOA задействуется классическая оптимизация

Предположение: факторизация ускоряется при решении задачи CVP таким методом

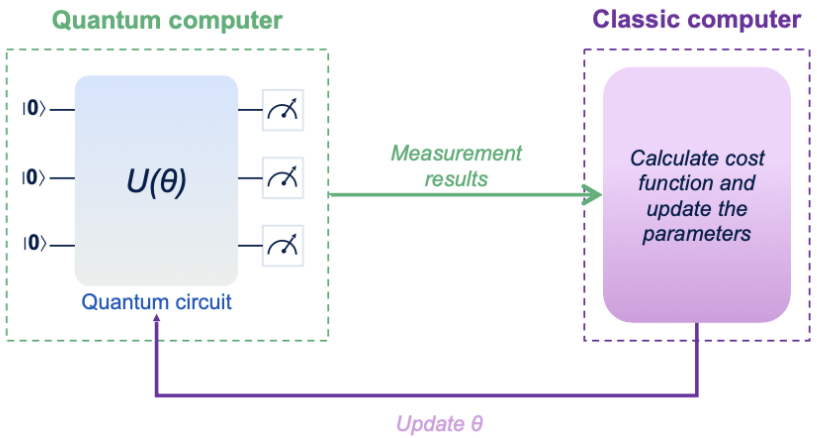
Квантовая приближенная оптимизация

Развитие квантовых вычислений: новые алгоритмы факторизации

ГАЗПРОМБАНК

В России усомнились в скором взломе шифра RSA квантовыми компьютерами

Заведующий кафедрой инженерной кибернетики НИТУ "МИСиС" Альберт Ефимов отметил, что квантовый компьютер все же может стать серьезным риском информационной безопасности в будущем



Pitfalls of the Sublinear QAOA-Based Factorization Algorithm

SERGEY V. GREBNEV[1,2], MAXIM A. GAVREEV[1,2], EVGENIY O. KIKTENKO[1,2], ANTON P. GUGLYA[1,2], ALBERT R. EFIMOV[2,3], AND ALEKSEY K. FEDOROV[1,2]

[1]Russian Quantum Center, Skolkovo, 121205 Moscow, Russia
[2]National University of Science and Technology "MISIS," 119049 Moscow, Russia
[3]Sberbank of Russia, Sber Innovation and Research, 121357 Moscow, Russia

Corresponding author: Aleksey K. Fedorov (akf@rqc.ru)

This work was supported in part by Sberbank, and in part by the Russian Science Foundation under Grant 19-71-10092.

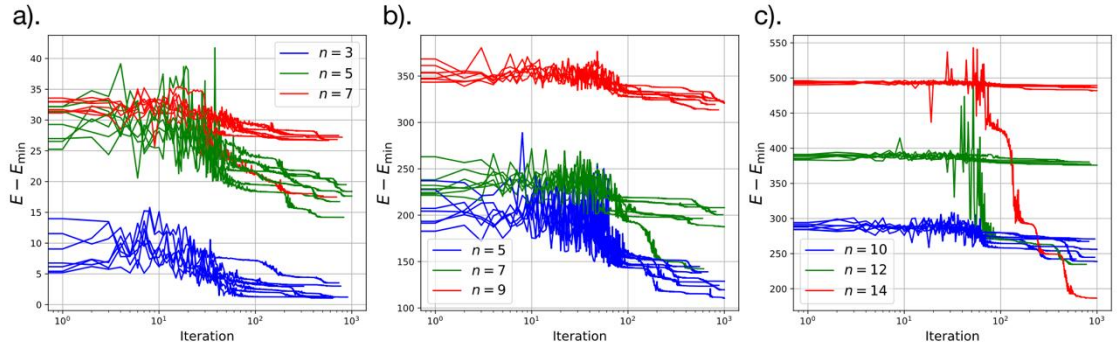


FIGURE 1. Convergence of mean energy E to the minimal energy E_{min} for QAOA circuits consisting of $p = 3$ layers designed for different number of qubits n and different RSA integers $N = 1961$ (a), $N = 48567227$ (b), and $N = 261980999226229$ (c). Each line corresponds to a distinct run of Nelder-Mead optimization algorithm.

Развитие квантовых вычислений: новые алгоритмы факторизации

ГАЗПРОМБАНК

11 марта 2025 года

A Practically Scalable Approach to the Closest Vector Problem for Sieving via QAOA with Fixed Angles

Ben Priestley*
Department of Computer Science, University of Oxford and Quantum Software Lab, School of Informatics, University of Edinburgh

Petros Wallden†
Quantum Software Lab, School of Informatics, University of Edinburgh
(Dated: March 12, 2025)

The NP-hardness of the closest vector problem (CVP) is an important basis for quantum-secure cryptography, in much the same way that integer factorisation's conjectured hardness is at the foundation of cryptosystems like RSA. Recent work with heuristic quantum algorithms [1] indicates the possibility to find close approximations to (constrained) CVP instances that could be incorporated within fast sieving approaches for factorisation. This work explores both the *practicality* and *scalability* of the proposed heuristic approach to explore the potential for a quantum advantage for approximate CVP, without regard for the subsequent factoring claims. We also extend the proposal to include an antecedent "pre-training" scheme to find and fix a set of parameters that generalise well to increasingly large lattices, which both optimises the scalability of the algorithm, and permits direct numerical analyses. Our results further indicate a noteworthy quantum speed-up for lattice problems obeying a certain 'prime' structure, approaching fifth order advantage for QAOA of fixed depth $p = 10$ compared to classical brute-force, motivating renewed discussions about the necessary lattice dimensions for quantum-secure cryptosystems in the near-term.

Scaling advantage

13 марта 2025 года

Experimental factoring integers using fixed-point-QAOA with a trapped-ion quantum processor

Ilia V. Zalivako,[1,2] Andrey Yu. Chernyavskiy,[2] Anastasiia S. Nikolaeva,[1,2,3] Alexander S. Borisenko,[1,2] Nikita V. Semenin,[1,2] Kristina P. Galstyan,[1,2] Andrey E. Korolkov,[1,2] Sergey V. Grebnev,[2] Evgeniy O. Kiktenko,[2,3] Ksenia Yu. Khabarova,[1,2] Aleksey K. Fedorov,[1,2,3] Ilya A. Semerikov,[1,2] and Nikolay N. Kolachevsky[1,2]

[1]*P.N. Lebedev Physical Institute of the Russian Academy of Sciences, Moscow 119991, Russia*
[2]*Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[3]*National University of Science and Technology "MISIS", Moscow 119049, Russia*

Factoring integers is considered as a computationally-hard problem for classical methods, whereas there exists polynomial-time Shor's quantum algorithm for solving this task. However, requirements for running the Shor's algorithm for realistic tasks, which are beyond the capabilities of existing and upcoming generations of quantum computing devices, motivates to search for alternative approaches. In this work, we experimentally demonstrate factoring of the integer with a trapped ion quantum processor using the Schnorr approach and a modified version of quantum approximate optimization algorithm (QAOA). The key difference of our approach in comparison with the recently proposed QAOA-based factoring method is the use of the fixed-point feature, which relies on the use of universal parameters. We present experimental results on factoring $1591 = 37 \times 43$ using 6 qubits as well as simulation results for $74425657 = 9521 \times 7817$ with 10 qubits and $35183361263263 = 4194191 \times 8388593$ with 15 qubits. Alongside, we present all the necessary details for reproducing our results and analysis of the performance of the factoring method, the scalability of this approach both in classical and quantum domain still requires further studies.

1591 = 37 × 43 using 6 qubits (experiment)
35183361263263 = 4194191 × 8388593 with 15 qubits (simulation)

РусКрипто ГАЗПРОМБАНК

Квантово-устойчивая криптография: опыт пилотных проектов

Газпромбанк активно пилотирует квантово-устойчивую защиту данных

ГАЗПРОМБАНК

Завершены проекты по постквантовой криптографии

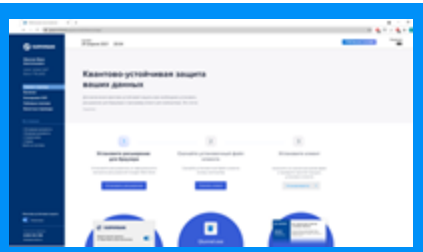
1

Квантово-устойчивые мобильные BLE-платежи

2

Квантово-устойчивая защита информационных систем Host-to-Host банка и бизнес-клиентов

3



Квантово-устойчивая защита дистанционного банковского обслуживания

Конфиденциальные вычисления

1

ОКБ

Конфиденциальное обучение модели оценки вероятности дефолта юридических лиц

Квантово-устойчивая защита информационных систем Host-to-Host Банка и бизнес-клиентов

ГАЗПРОМБАНК

Партнер проекта: QApp

Защищаемые данные: платежные поручения

В 2024 году завершен пилотный проект по постквантовой криптографии

Квантово-устойчивые мобильные BLE-платежи

Партнеры проекта: НСПК QApp

Защищаемые данные: финансовые транзакции

FINOPOLIS

Результаты проекта представлены
Председателю Банка России Набиуллиной Э.С.
в рамках FINOPOLIS 2024

BLE (Bluetooth Low Energy) — беспроводная технология Bluetooth с низким энергопотреблением

В 2024 году завершен пилотный проект по постквантовой криптографии

Квантово-устойчивые мобильные BLE-платежи

ГАЗПРОМБАНК

Партнеры проекта: НСПК QApp

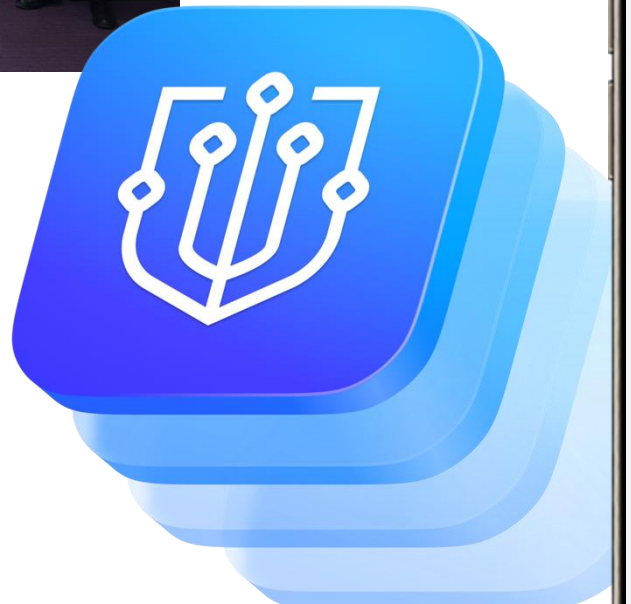
Защищаемые данные: финансовые транзакции

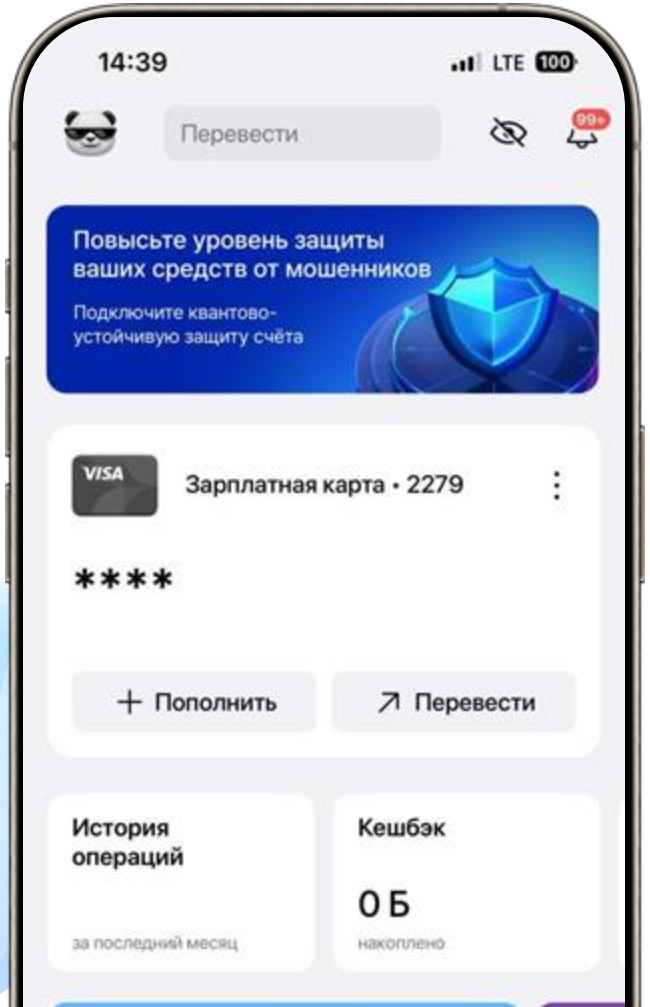
	BLE-соединение	NFC-соединение
Интеграция постквантовой криптографии для повышения уровня кибербезопасности	✓	✗
Проведение платежей в условиях отсутствия интернета	✓	✓
Высокий радиус покрытия: улучшенное взаимодействие при проведении оплаты	✓	✗
Скорость передачи данных	1-2 Мбит/с	106-848 Кбит/с

Планы на 2025 по пилотированию постквантовой криптографии

Одним из финалистов корпоративного акселератор Банка стал проект по квантово-устойчивой защите канала API системы ДБО физических лиц

Предполагается пилотирование открытой программной реализации постквантового алгоритма-кандидата на включение в новые государственные стандарты — «**Гиперикум**»





В 2024 году завершен пилотный проект по конфиденциальным вычислениям

Конфиденциальное обучение модели оценки вероятности дефолта юридических лиц

ГАЗПРОМБАНК

Партнеры проекта: ЭКБ QApp

Решаемая задача: повышение точности моделей кредитного скоринга

Впервые в Газпромбанке удалось протестировать программный подход к конфиденциальным вычислениям (SMPC[1])

SD 24

Результат представлен на Форуме Scoring Day 2024

Получение точности предсказания GINI[2]:

0.58	С SMPC-подходом (Безопасная передача данных)
0.6	Без SMPC-подхода (Небезопасная передача данных)

40 сек

Скорость выдачи предсказаний

*[1] **SMPC** (secure multi-party computation) — протокол конфиденциального вычисления это криптографический протокол, который распределяет вычисления между несколькими сторонами, при этом ни одна из сторон не может видеть данные других сторон*
*[2] **Коэффициент Джини** (Gini coefficient) — метрика качества, которая часто используется при оценке предсказательных моделей в задачах бинарной классификации в условиях сильной несбалансированности классов целевой переменной*

РусКрипто ГАЗПРОМБАНК

Алексей Федоров

aleksey.k.fedorov@gazprombank.ru
+79162970977