Квантовые вычисления: Реализация алгоритма Шора с использованием библиотеки Qiskit от IBM.

Бакалавр группы 3821Б1ПМоп2: Богдашкин Сергей Евгеньевич

Научный руководитель:

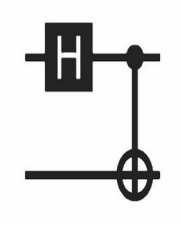
зав. каф. ВВиСП ИИТММ ННГУ

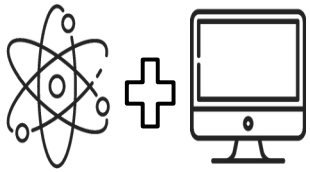
Мееров Иосиф Борисович

Нижегородский государственный университет

им. Н.И. Лобачевского

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ АКТИВНО РАЗВИВАЮТСЯ ПО РАЗЛИЧНЫМ НАПРАВЛЕНИЯМ





Универсальные квантовые вычисления	Адиабатические квантовые вычисления	Гибридные квантовые вычисления	Квантово-вдохновленные вычисления	Облачные платформы доступа
- Ионы - Холодные атомы - Сверхпроводники - Фотоны и фотонные чипы			Программные - CPU/GPU Программно-аппаратные - FPGA/ASIC - ПЛИС	Доступ к квантовым компьютерам и эмуляторам Готовы квантовые алгоритмы и приложения

НАИБОЛЕЕ МОЩНЫЕ КВАНТОВЫЕ ПРОЦЕССОРЫ В МИРЕ

	IBM	Google	IONQ	XANADU	D-Wave The Quantum Computing Company™
Платформа	Сверхпроводники	Сверхпроводники	Ионы в ловушках	Фотоны	Сверхпроводники
Количество кубит	433	54	20 *алгоритмические кубиты*	216 *бозонный сэмплинг*	5000 *алгоритм квантового отжига*

РКЦ Российский Квантовый Центр

QBoard

КВАНТОВОЕ ВЫЧИСЛИТЕЛЬНОЕ ПРЕВОСХОДСТВО

ВОЗМОЖНОСТЬ КВАНТОВОГО КОМПЬЮТЕРА РЕШИТЬ ВЫЧИСЛИТЕЛЬНУЮ ЗАДАЧУ ЗНАЧИТЕЛЬНО БЫСТРЕЕ КЛАССИЧЕСКОГО КОМПЬЮТЕРА

2019

Google

Исследовательская группа компании Google впервые в мире продемонстрировала достижение квантового превосходства в 2019 г. Для примера была выбрана задача расчета случайных квантовых цепочек. По заявлению авторов работы, классический компьютер затратит на решение данной задачи ~10,000 лет.

2020

中國科學院 CHINESE ACADEMY OF SCIENCES

Группа ученых из Китая продемонстрировала достижение квантового превосходства при решении задачи сэмплирования бозонных состояний. По подсчетам авторов работы, классическому компьютеру потребуется несколько миллиардов лет, чтобы решить данную задачу.

SCIENCE
3 Dec 2020
Vol 370, Issue 6523

2021

中國科學院 CHINESE ACADEMY OF SCIENCES

Продемонстрировано квантовое вычислительное превосходство при решении задачи расчета случайных квантовых цепочек на сверхпроводящем квантовом компьютере

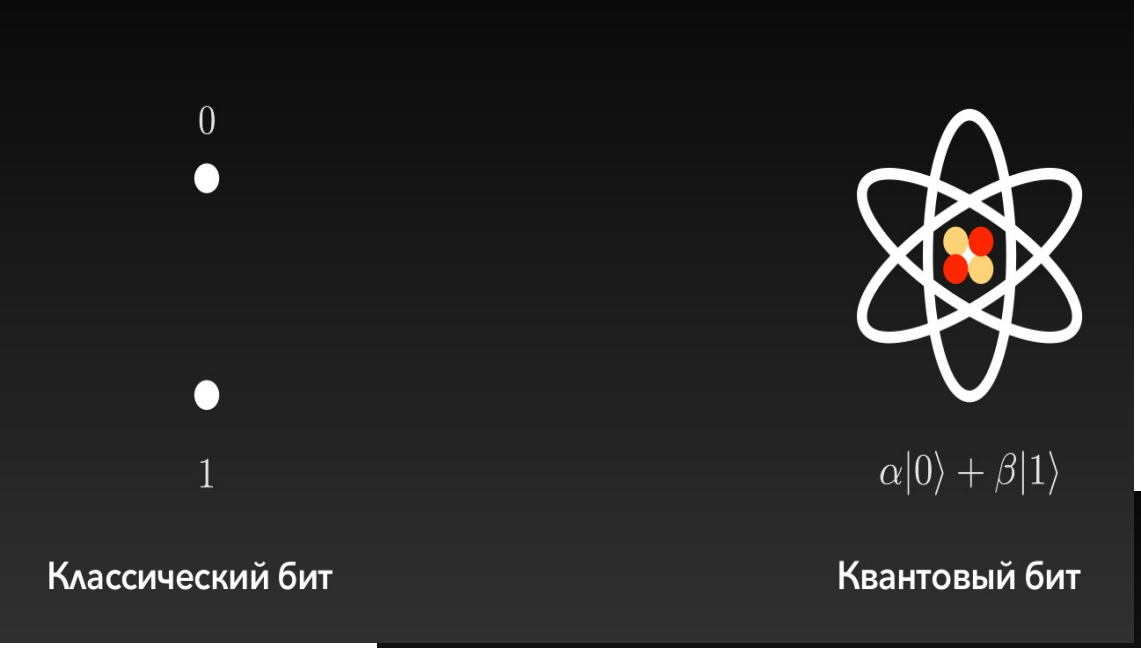
2022

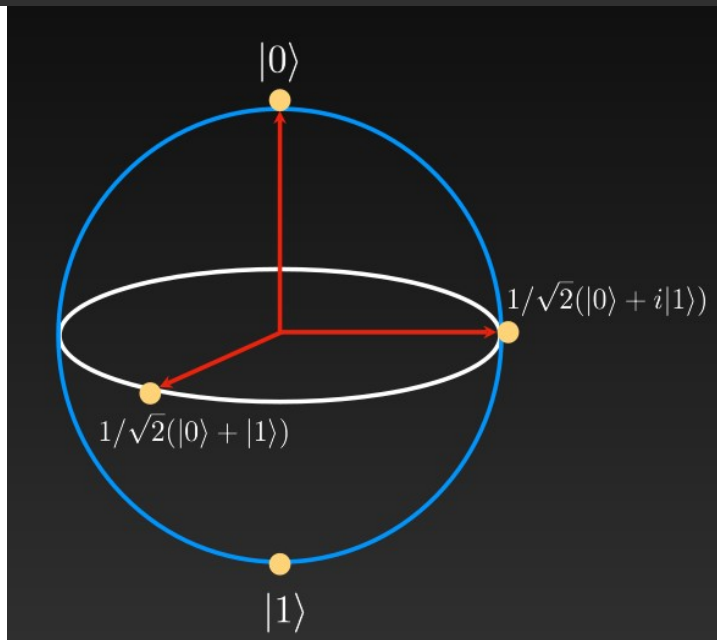
XANADU

Продемонстрировано квантовое превосходство при сэмплировании бозонных состояний на фотонном квантовом компьютере.

Nature 606, 75–81 (2022)

Квантовые биты



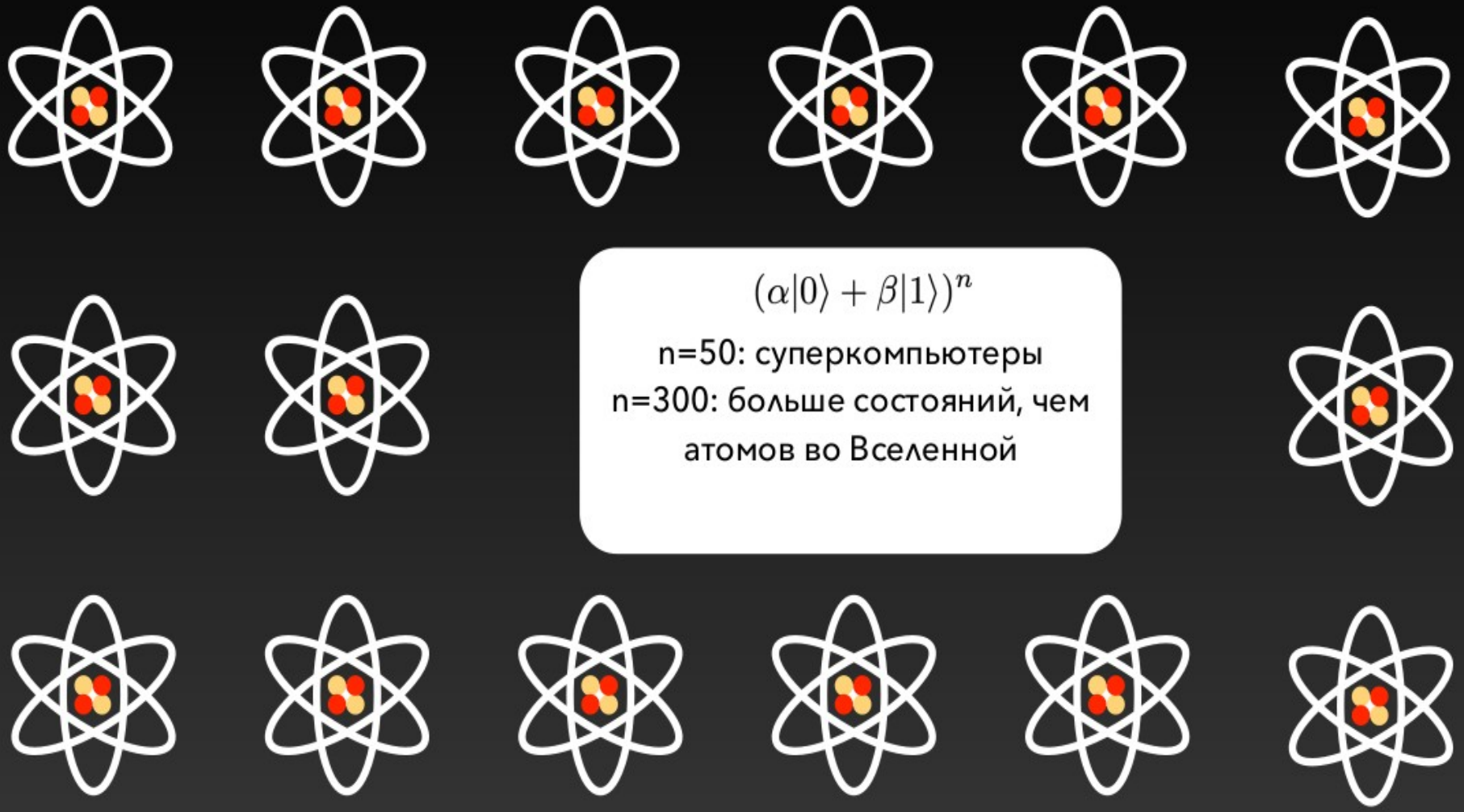


Пространство состояний кубита

$$(\alpha|0\rangle + \beta|1\rangle)^2 = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

Размерность пространства состояний растёт экспоненциально с ростом числа кубитов.

Пространство состояний кубита



$$(\alpha|0\rangle + \beta|1\rangle)^n$$

n=50: суперкомпьютеры

n=300: больше состояний, чем атомов во Вселенной

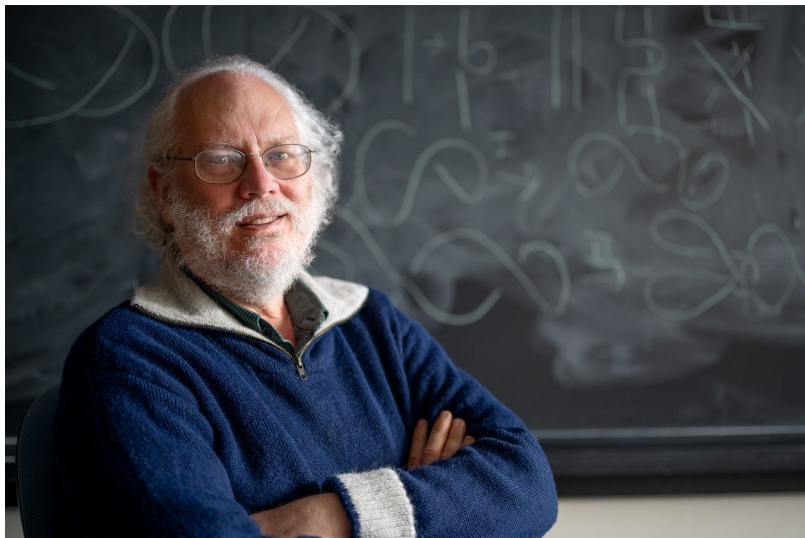
Алгоритм Шора факторизации целого числа

Задача: Дано составное n-битное число, найти нетривиальный множитель.

Наилучший известный детерминистический алгоритм на классическом компьютере имеет вычислительную сложность: $\exp(O(n^{1/3}\log^{2/3} n))$

Квантовый компьютер способен решить эту задачу за $O(n^3)$ операций

Питер Шор – американский математик и профессор Массачусетского технологического института, известный своими значительными вкладами в квантовую информатику, включая разработку алгоритма Шора для факторизации целых чисел



Алгоритм Шора факторизации целого числа

Алгоритм Шора предназначен для факторизации целых чисел и основан на нахождении периода последовательности чисел.

Решение задачи факторизации:
- Сведение к задаче нахождения периода функции f(x) = a^x mod N.

Период функции f(x) = a^x mod N - это наименьшее положительное целое число r, при котором f(x + r) = f(x) . Иначе говоря, это периодичность, с которой значения функции повторяются.

Основные шаги:
- Классическая часть:
  - Выбрать случайное число a, взаимно простое с N.
- Квантовая часть:
  - Подготовить квантовое состояние.
  - Применить квантовое преобразование Фурье для нахождения периода функции
- Классическая обработка:
  - Найти множители N по вычисленному периоду.

Преимущество:
- Алгоритм работает за полиномиальное время на квантовом компьютере O(n^3) операций, что значительно быстрее классических методов.

Цели: реализация универсальной схемы для квантовой части

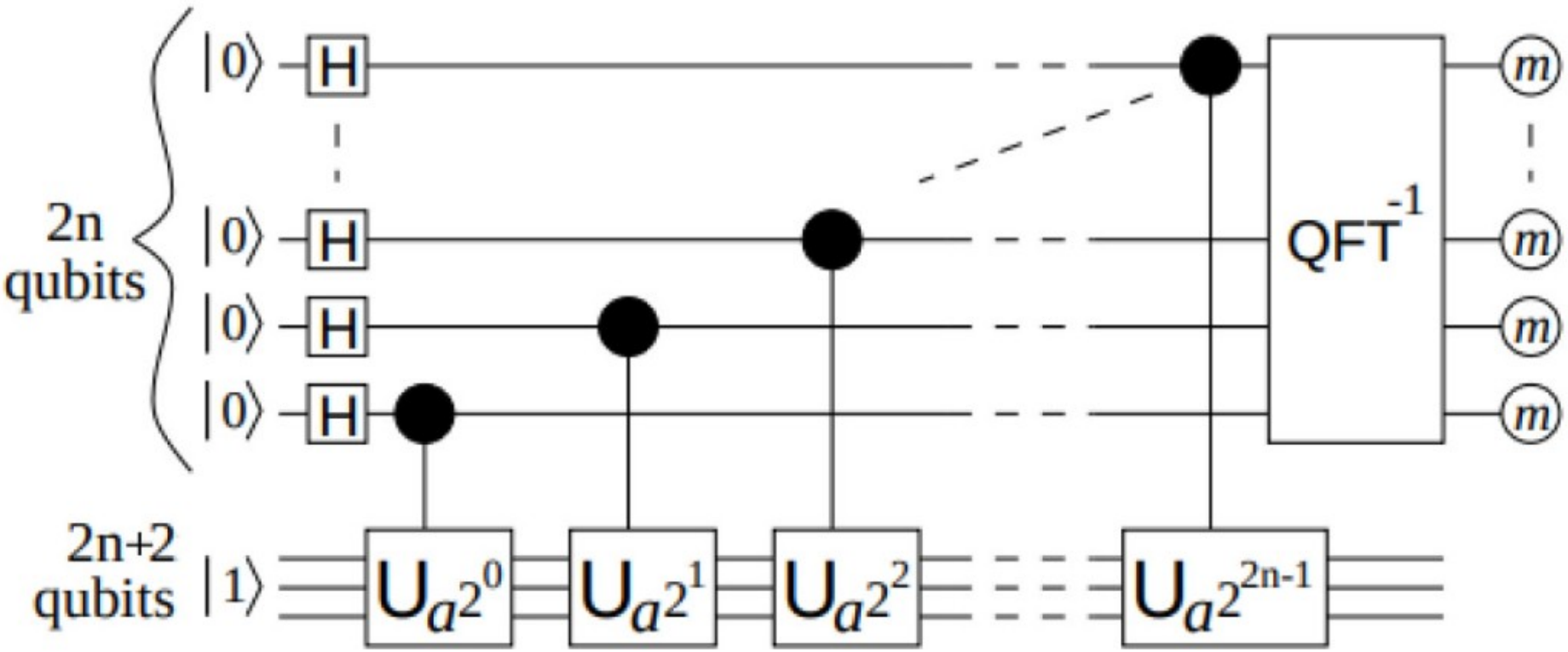


Рис. 9 Квантовая часть алгоритма Шора. U_a реализует $|x> \rightarrow |(ax)\ mod\ N>$.

После измерения и классической постобработки получаем порядок r числа a по модулю N.

Такой алгоритм требует 4n + 2 кубит для разложения n-битного числа

Квантовое сложение

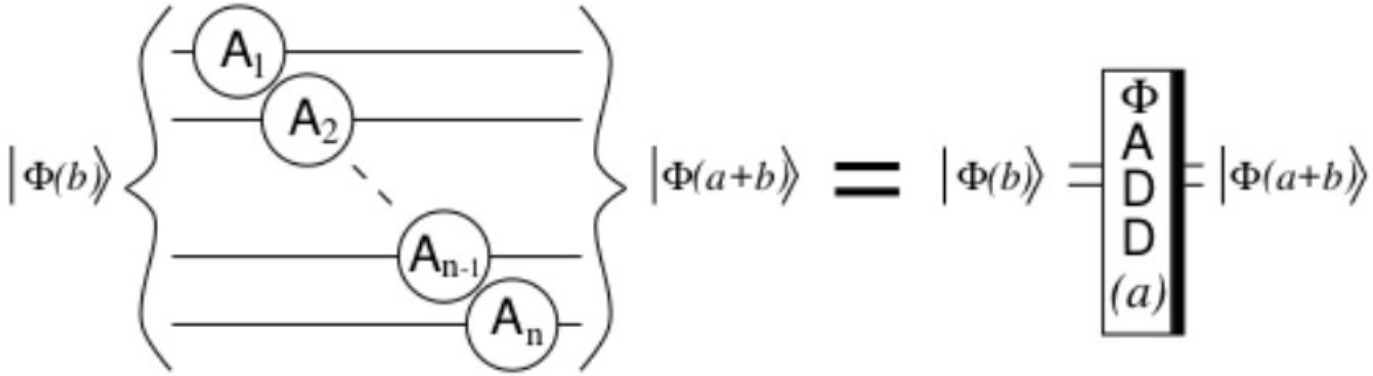


Рис. 3 Схема для сложения классического значения a и квантового значения b в пространстве Фурье. Гейты A_i вычисляются классическими комбинациями фазовых сдвигов..

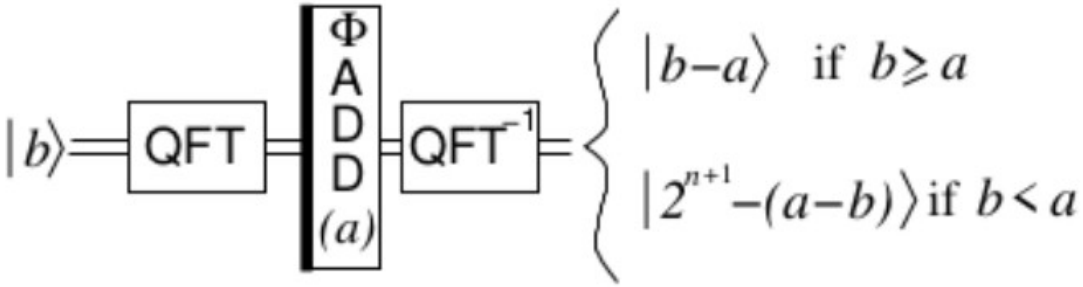


Рис. 4 Эффект обратного гейта ϕADD(a) на |ϕ(b)|

Реализация гейта сложение по модулю .

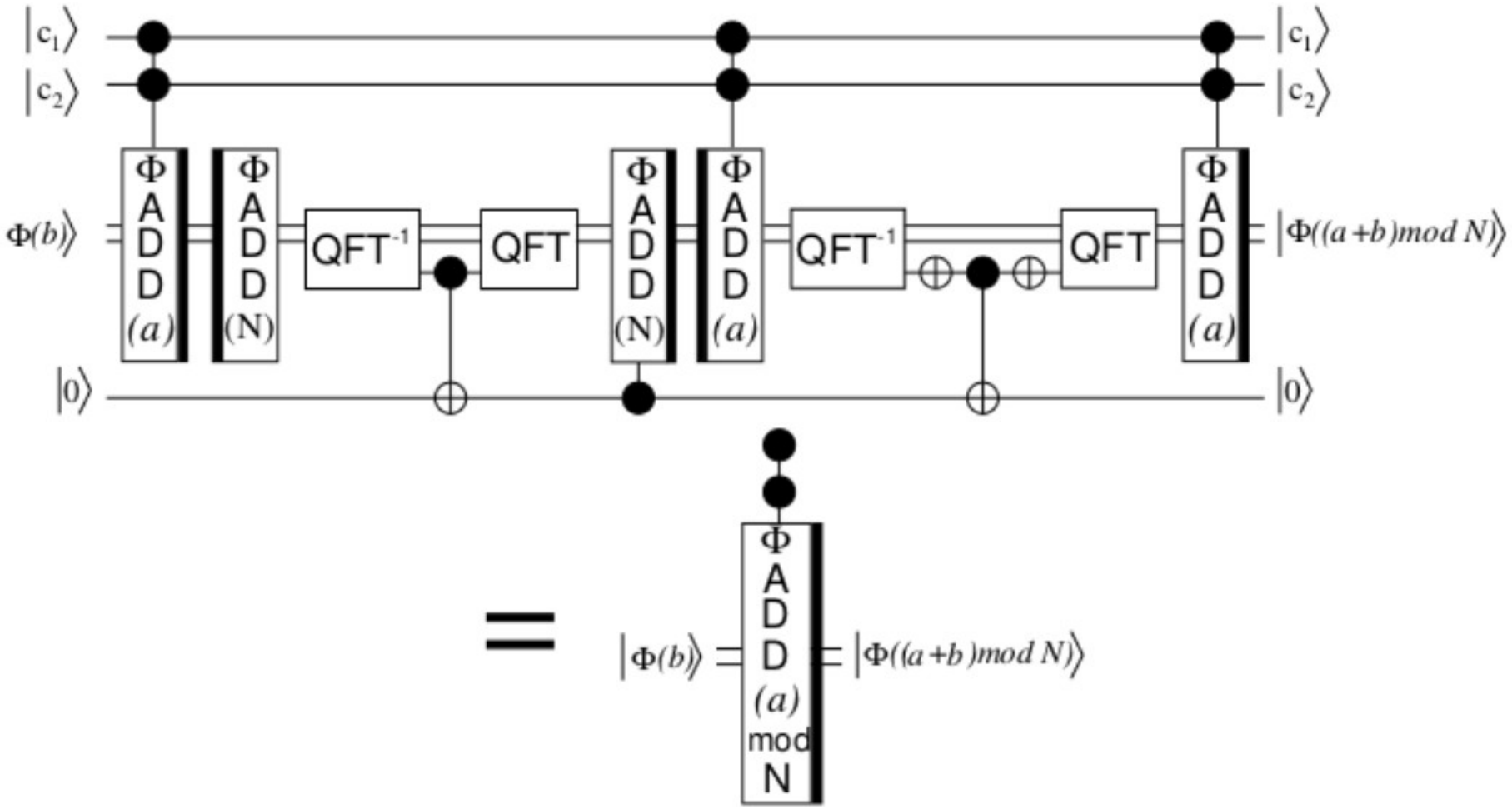


Рис. 5 Дважды контролируемый ΦADD(a)MOD(N) гейт с c1 = c2 = 1. Если один из контролирующих кубитов в состоянии |0i, результат выполнения операции |Φ(b)i при b < N.

Реализация гейта умножения по модулю .

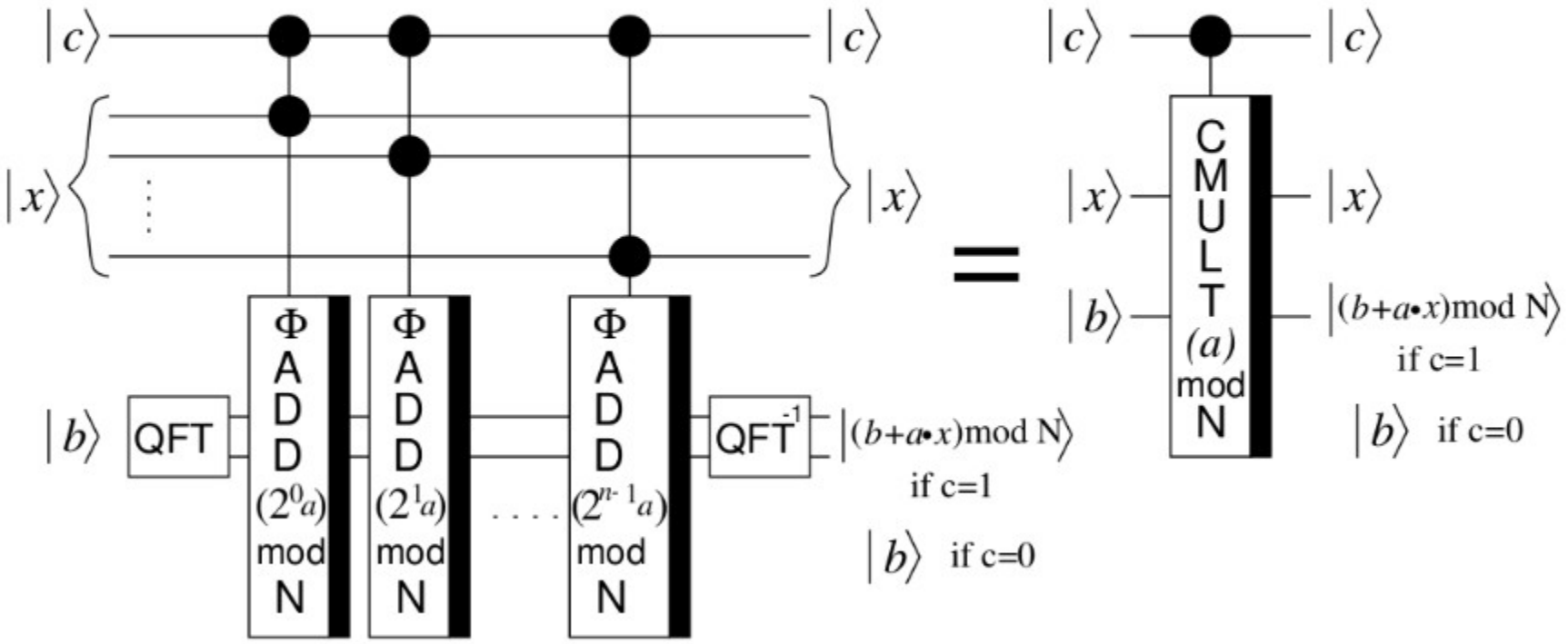


Figure 6: The $CMULT(a)MOD(N)$ gate.

Вышеописанная последовательность гейтов на схеме, позволяет нам реализовать главный в алгоритме Шора **гейт Возведения в степень.**

*Именно эта операция нам и нужна для вычисления периодической функции $f(a) = a^x \ mod \ N$.

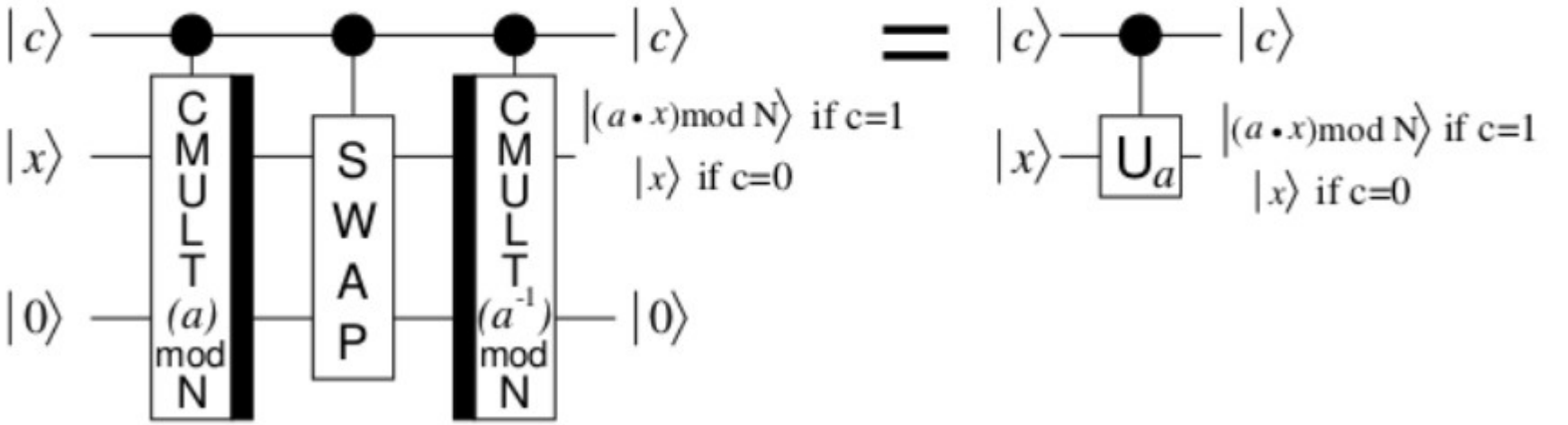
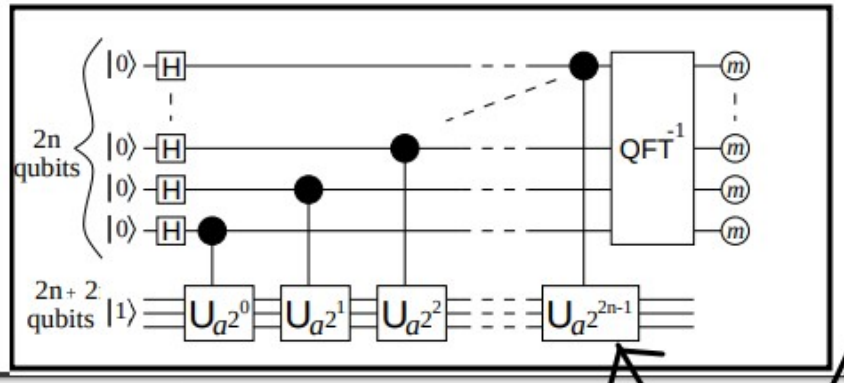


Рис. 8 схема контролируемого U_a гейта.

Общая схема



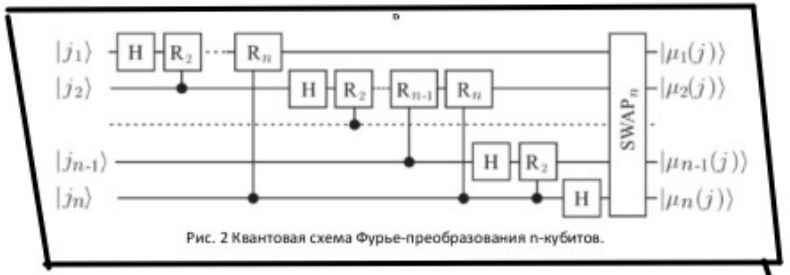
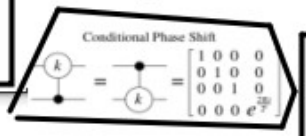
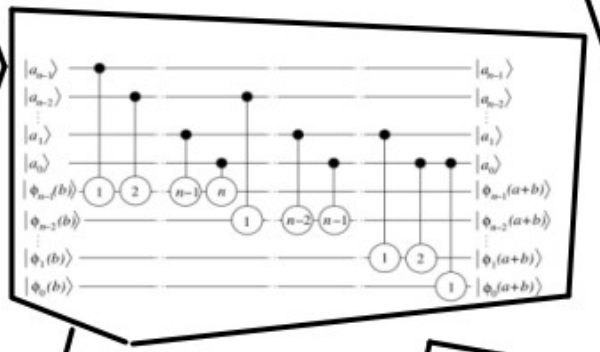
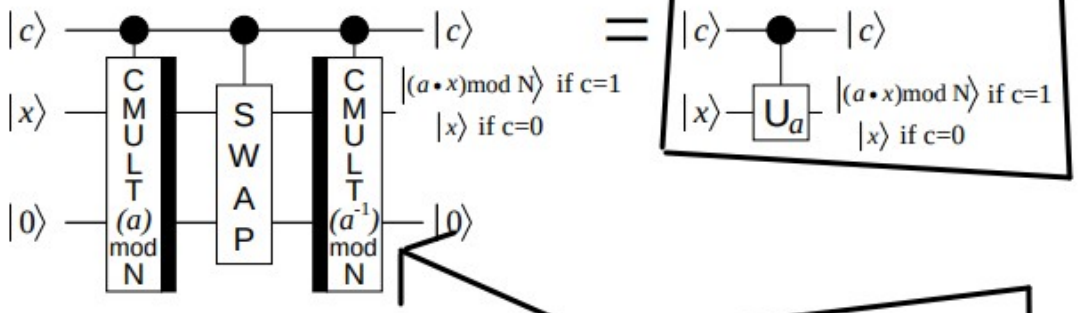
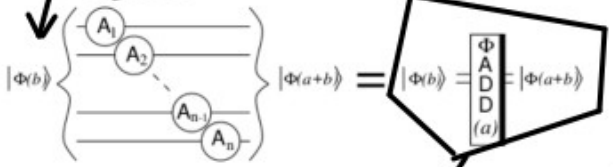


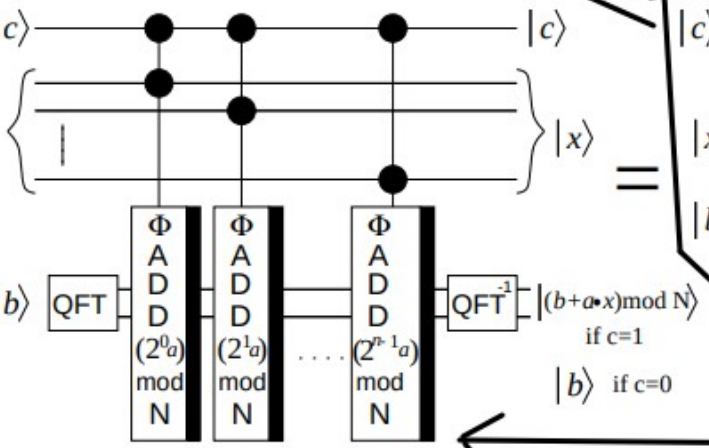
Рис. 2 Квантовая схема Фурье-преобразования n-кубитов.

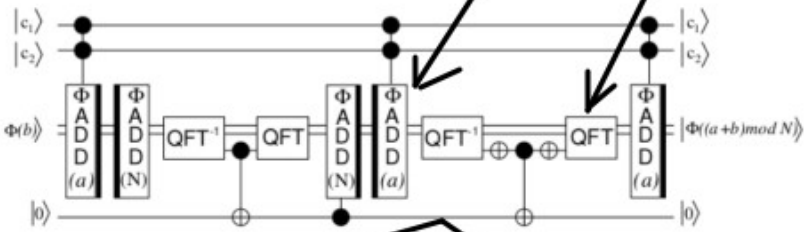


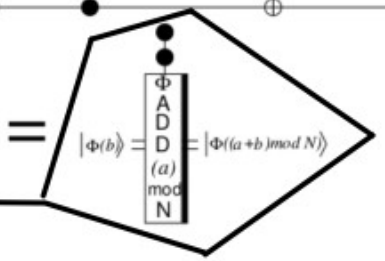












Пример

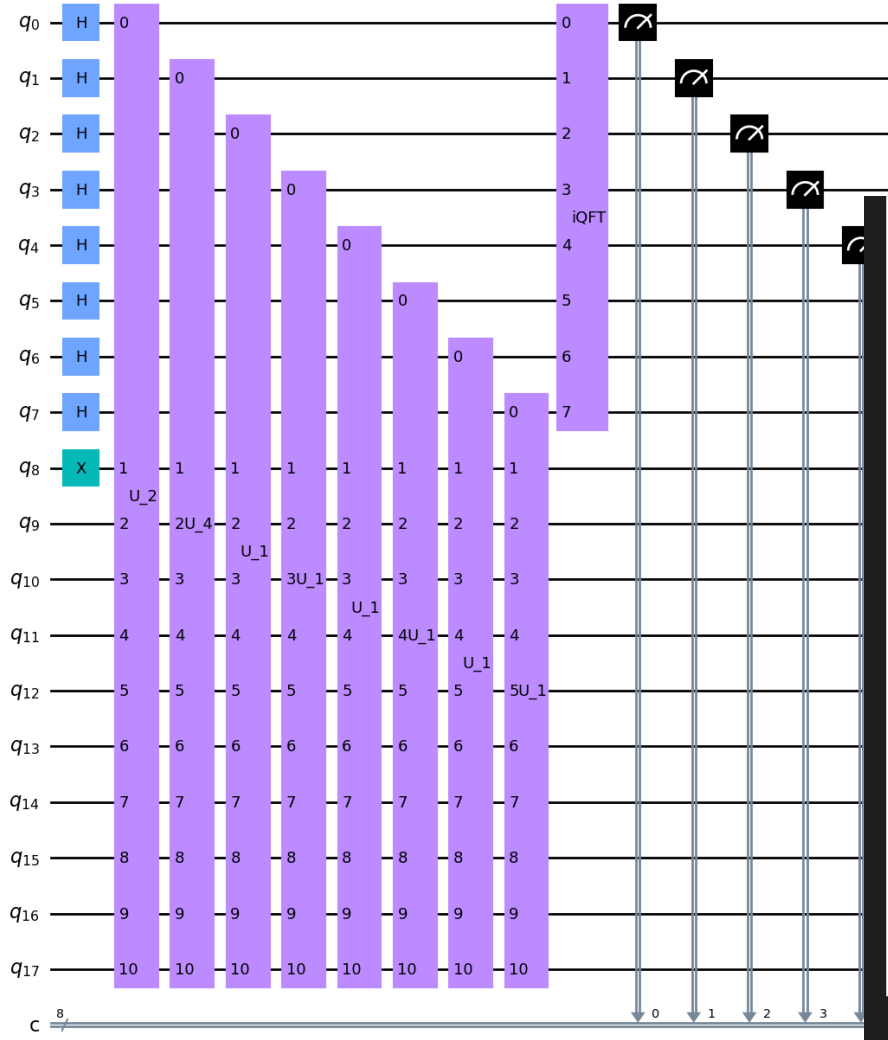
Как отмечалось ранее, для разложения n-битного числа потребуется 4n+2 кубита. В симуляторе это выражается в необходимом размере вектора, содержащего 2^{4n+2} значений. Тестирование алгоритма имеет смысл проводить на составных нечетных числах, которые не являются степенью натурального числа. Ввиду ограничений по физической памяти вычислительных устройств, эксперименты будем проводить только для чисел 15 и 21. Оценки затрат памяти для применения алгоритма Шора к составным нечетным числам приведены в таблице:

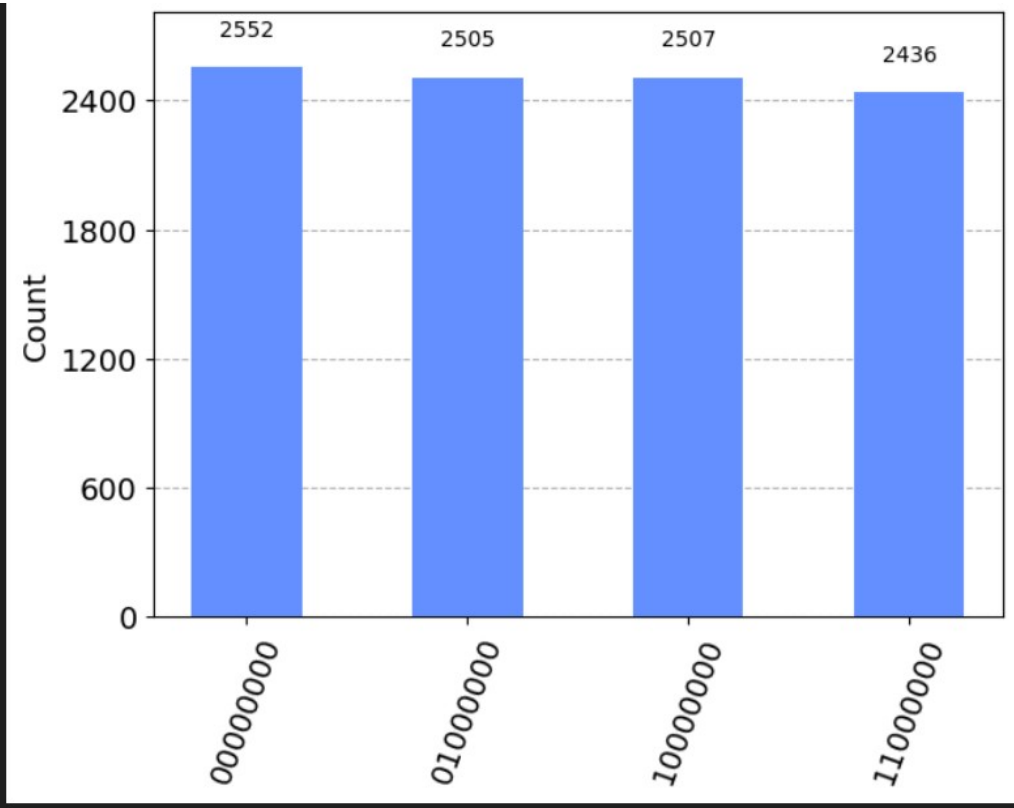
N	n	Длина вектора состояния
15	4	2^{18}
21	5	2^{22}
35	6	2^{26}

Рассмотрим подробно работу алгоритма Шора для разложения числа $N = 15$ и покажем корректность выполнения. Выбираем случайное число $x = 2$, $\text{НОД}(x, N) = 1$.Выбираем $M = 2^{2 \cdot 4} = 256$.

Наибольшим общим делителем полученных чисел будет $\text{НОД}\,(0,\ 64,\ 128,\ 192) = 64$. Число $M/g = 4$ чётно. $\text{НОД}\left(N,\ x^{\frac{M}{2g}} + 1\right) = 5$ - искомый делитель числа $N = 15$.

Демонстрация алгоритма Шора для N=15

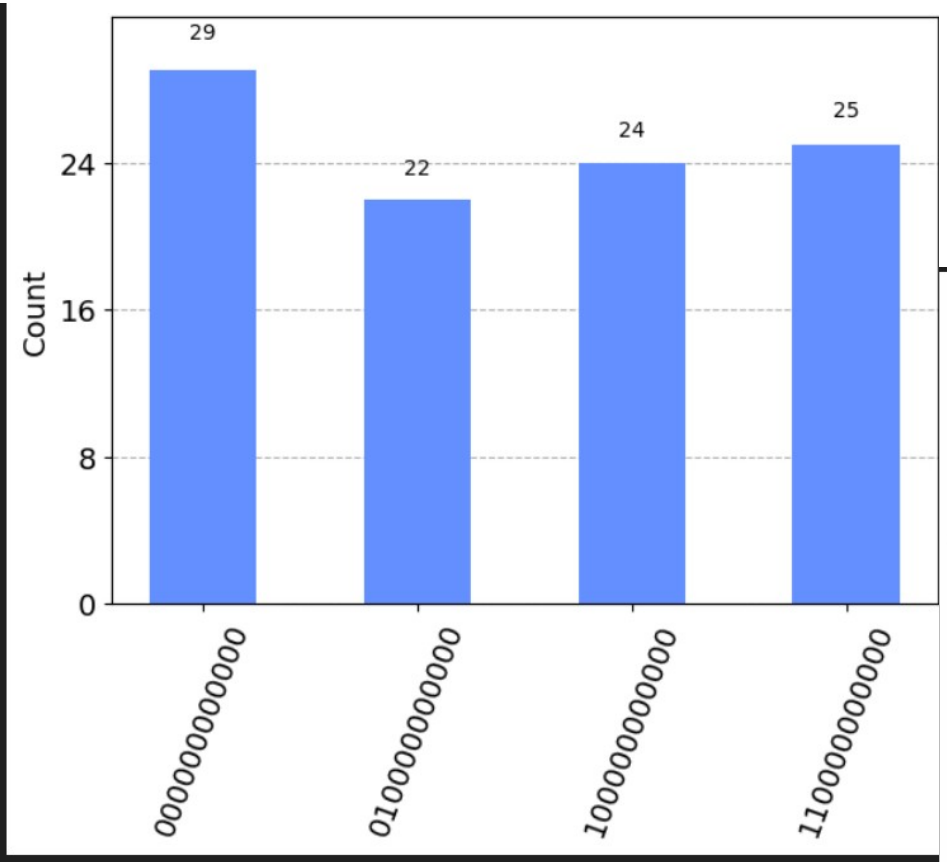





```
classical_shor(N, a, counts)
```

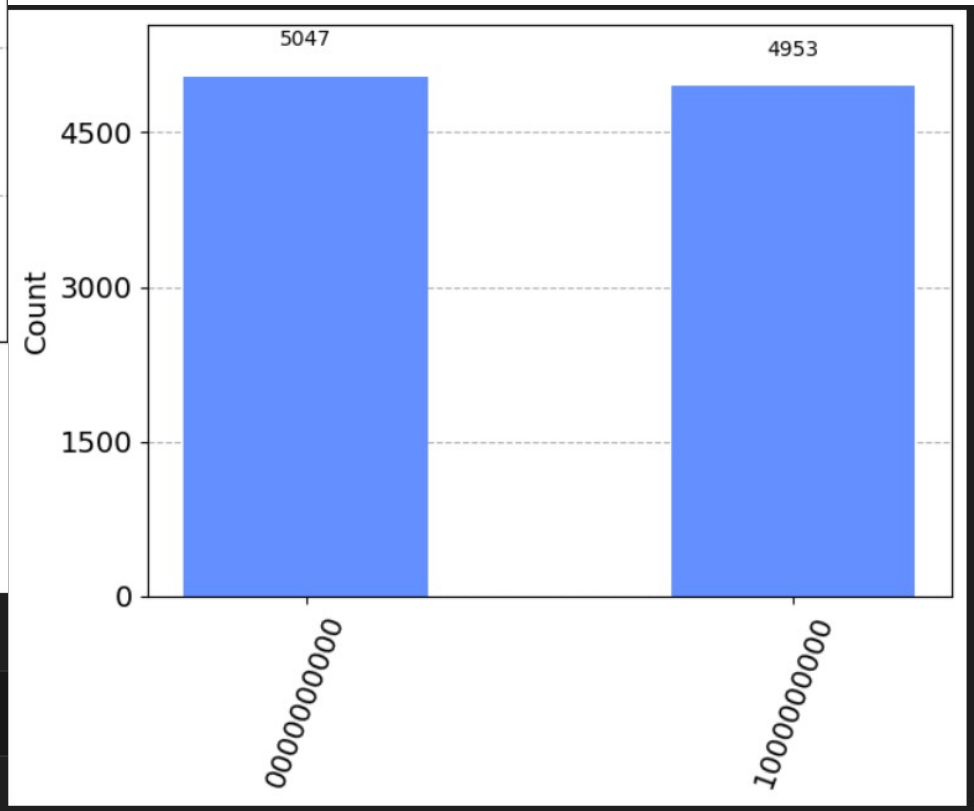
```
Найденный порядок: 4
Множители числа 15 (a = 2): 3 * 5
```

Демонстрация алгоритма Шора для N=35, N=21




```
classical_shor(N, a, counts)
```

```
Найденный порядок: 4
Множители числа 35 (a = 13): 7 * 5
```




```
classical_shor(N, a, counts)
```

```
Найденный порядок: 2
Множители числа 21 (a = 13): 3 * 7
```

Оценка сложности симуляции

Из проведенных экспериментов видно, что как глубина квантовой схемы, так и время выполнения значительно растут с увеличением числа бит в двоичном представлении числа N. Графики демонстрируют экспоненциальный рост сложности симуляции, что можно объяснить природой квантового алгоритма и необходимыми ресурсами для его симуляции на классическом компьютере.