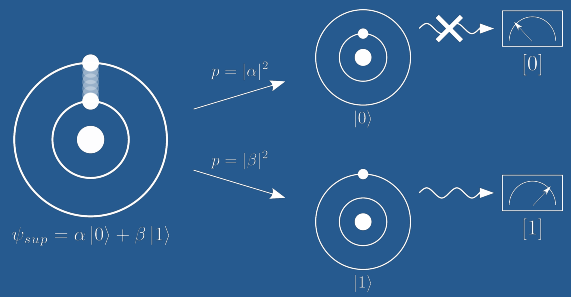
infotecs

Подходы к моделированию атаки на упрощённый алгоритм AES при помощи квантового алгоритма Гровера

Алексей Моисеевский



Квантовые вычисления

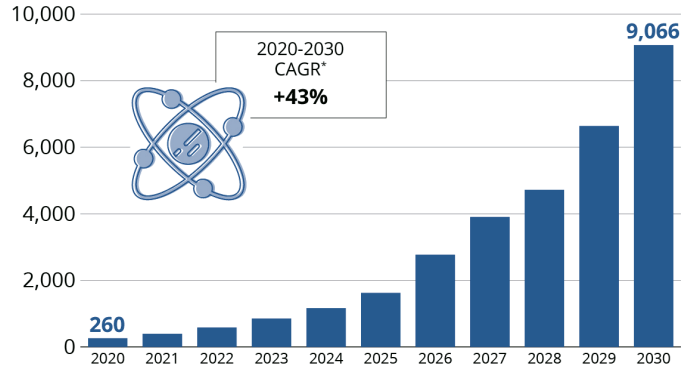
Почему квантовые вычисления?

infotecs

Hilbert space is a big place!
Квантовая память открывает
новые масштабы моделирования

Решение задач ускоряется
Минимум квадратично
В ряде случаев – экспоненциально

Упрощается криптоанализ
Гарантия безопасности потребует
увеличения длины ключей



Прогноз роста объёма мирового рынка квантовых вычислений в миллионах $

Statista Digital Economy Compass 2021

Квантовые алгоритмы

infotecs

Алгоритмы оптимизации

VQE, QAOA

Система представляется кубитами непосредственно

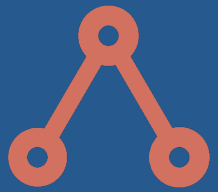
Уже имеют реальные приложения

Обобщённый поиск

Алгоритм Гровера

Квадратичное ускорение перебора симметричных ключей

O(log M) кубитов



Задача факторизации

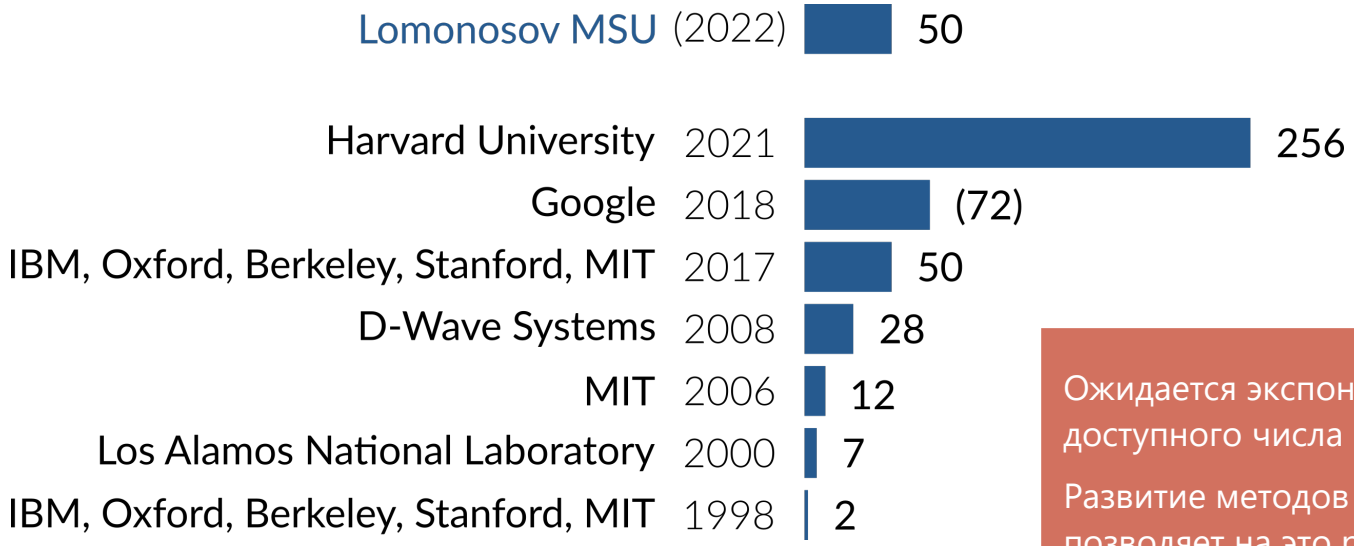
Алгоритм Шора

Экспоненциальное ускорение взлома асимметричных шифров

O(log M) кубитов

Доступное число кубитов

infotecs



Ожидается экспоненциальный рост доступного числа кубитов

Развитие методов подавления шумов позволяет на это рассчитывать

Что это даёт для криптографии?

infotecs

	Сложность классической атаки	Сложность квантовой атаки
Асимметричная криптография	Субэкспоненциальная Дискретное логарифмирование Факторизация целых чисел	Полиномиальная Алгоритм Шора
Симметричная криптография	Экспоненциальная Перебор ключей $O(2^n)$	Экспоненциальная Алгоритм Гровера $O(2^{n/2})$
Хэш-функции	Экспоненциальная *Перебор прообразов* $O(2^n)$	Экспоненциальная Алгоритм Гровера $O(2^{n/2})$

Что это даёт для криптографии?

infotecs

$n = 128$

$N_{Classic} \sim 2^{n}$ (операций)

$N_{Quantum} \sim 2^{n/2}$ (операций)

$V_{classic} \sim 10^{17}$ (операций / с)

$V_{quantum} \sim 10^{3}$ (операций / с)

$T_{Classic} \sim 2^{n} / V_{Classic} \sim 2^{77}$ с

$T_{Quantum} \sim 2^{n/2} / V_{Quantum} \sim 2^{35}$ с

Что это даёт для криптографии?

infotecs

n = 128

$N_{Classic}$ ~ 2^{n} (операций)

$N_{Quantum}$ ~ $2^{n/2}$ (операций)

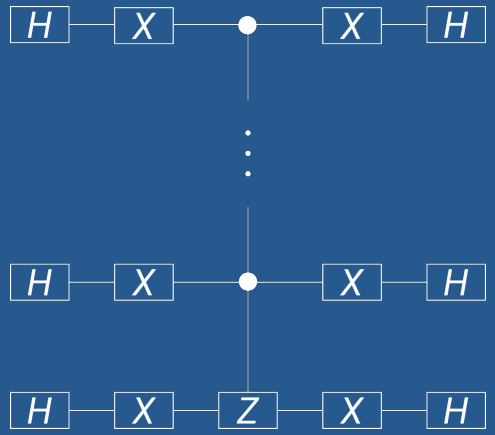
$V_{classic}$ ~ 10^{17} (операций / с)

$V_{quantum}$ ~ 10^{3} (операций / с)

$T_{Classic} \sim 2^{n} / V_{Classic} \sim 2^{77}$ с

$T_{Quantum} \sim 2^{n/2} / V_{Quantum} \sim 2^{35}$ с

Ускориться на пять порядков?
Не исключено. Y. Chew, K. Ohmori et al.,
Ultrafast energy exchange between two single Rydberg atoms on the nanosecond timescale (2021)



Алгоритм Гровера

Квантовый алгоритм Гровера

infotecs

Сложность O(√N)

Алгоритм требует меньше действий, чем простое обращение ко всем элементам

Обобщённый поиск

Единственное требование к данным – возможность распознавания решения

Универсальное решение

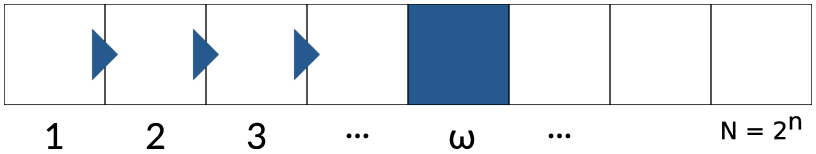
В общем случае алгоритм применим для ускорения решения любой NP задачи

Квантовый алгоритм Гровера – алгоритм ускоренного поиска по неструктурированной базе данных

М. Нильсен, И. Чанг

«Квантовые вычисления и квантовая информация», 2001

«В высшей степени удивительно, что существует квантовый алгоритм, позволяющий существенно ускорить метод поиска простым перебором»



Неструктурированный поиск

Классический подход

Перебрать все элементы

O(N / 2) в среднем

O(N – 1) в худшем случае

Неструктурированный поиск

Алгоритм Гровера

1) Начать с суперпозиции
2) Отметить решение фазой
3) Усилить амплитуду по отметке
4) Считать усиленную компоненту

O(√N) почти всегда

Квантовый алгоритм Гровера

infotecs

infotecs

Неструктурированный поиск

Задача оракула – распознать решение

Это проще, чем отыскать его

$$f(x) = \begin{cases} 1 & \text{if } x = \omega \\ 0 & \text{if } x \neq \omega \end{cases}$$

Квантовый оракул должен записывать результат в дополнительный кубит

$$\hat{U}_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$$

Неструктурированный поиск

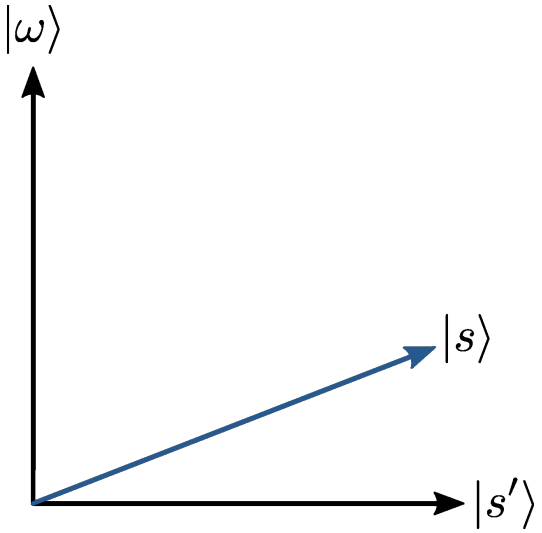
$$\hat{U}_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$$

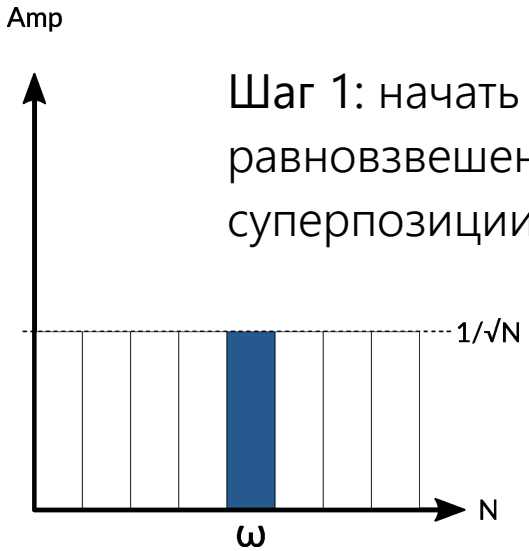
Возьмём $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = -\left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right)$

$$\hat{U}_f|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\hat{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$$

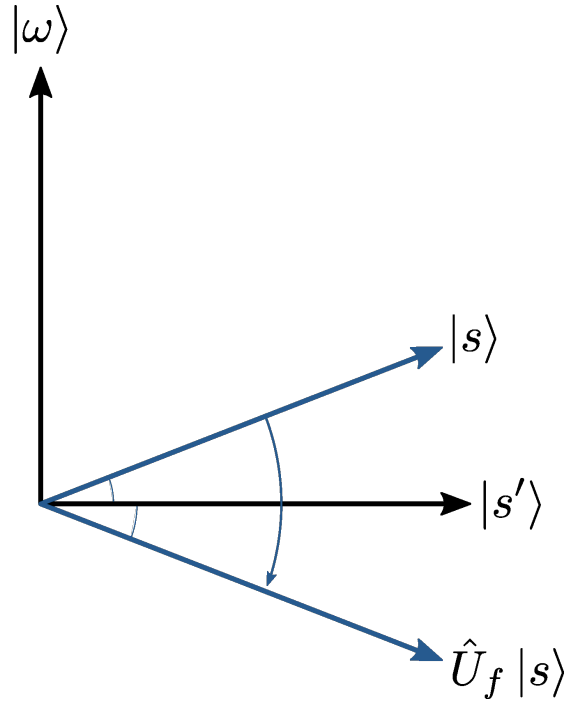
Алгоритм Гровера

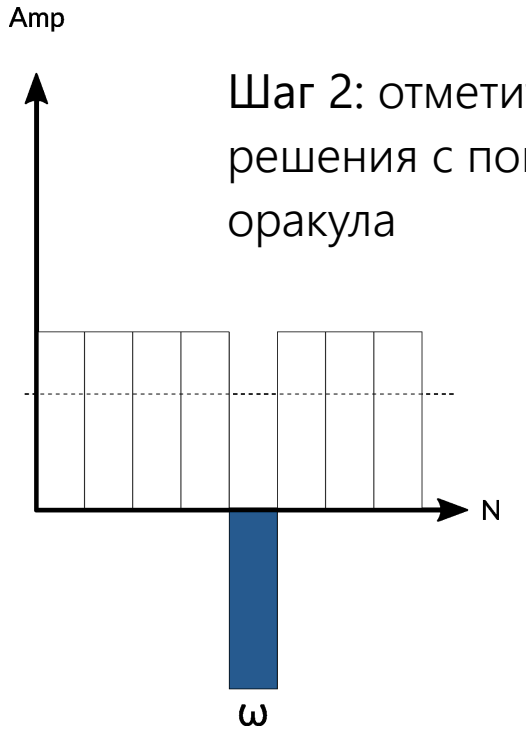




Шаг 1: начать с равновзвешенной суперпозиции *s*

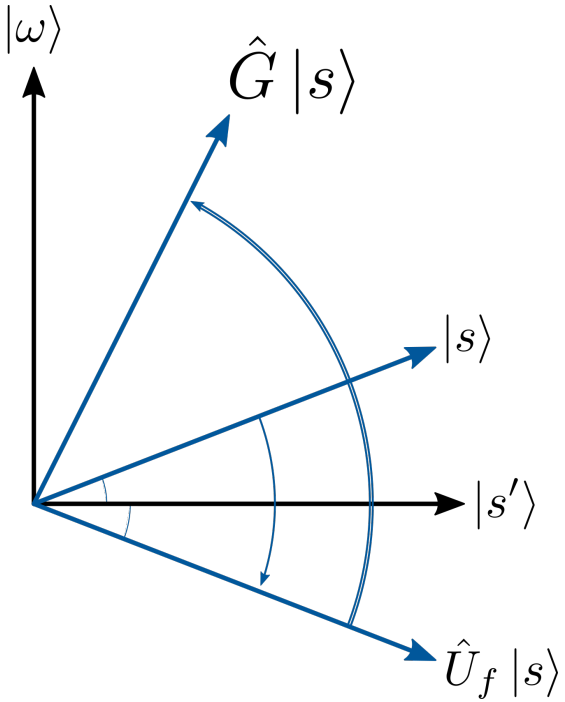
Алгоритм Гровера

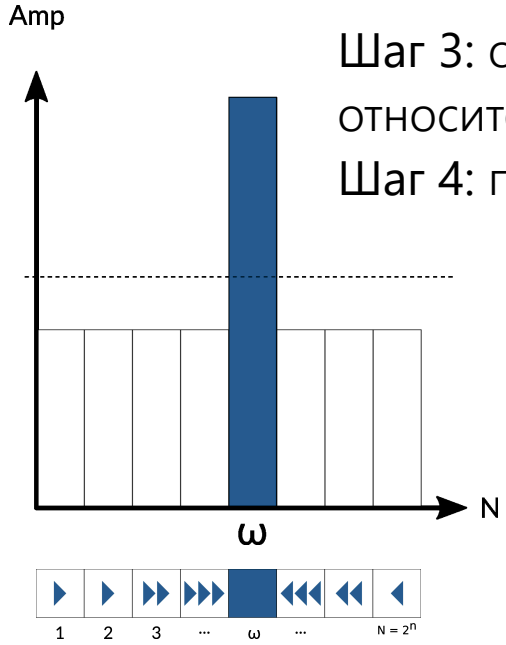




Шаг 2: отметить фазу решения с помощью оракула

Алгоритм Гровера





Шаг 3: отразить относительно S

Шаг 4: повторить

Квантовый алгоритм Гровера

R – число повторений

$$R = \left\lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rfloor$$

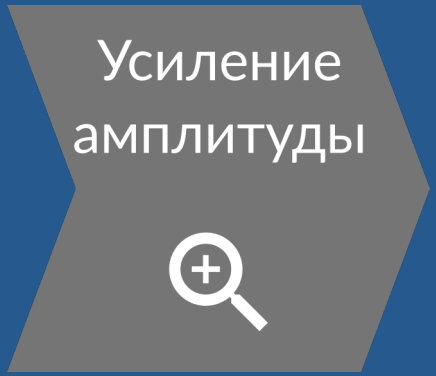
N – размер базы

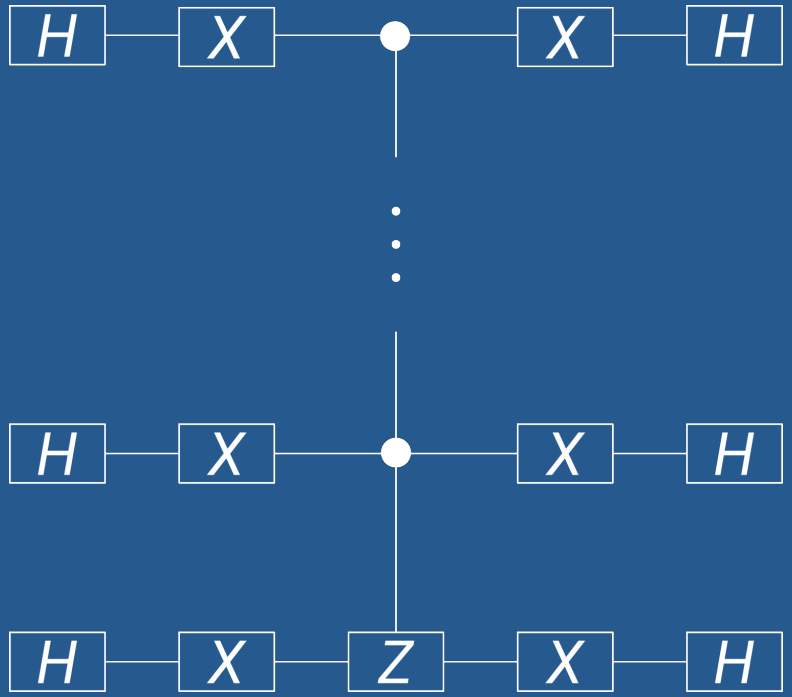
M – число решений

Квантовый алгоритм Гровера

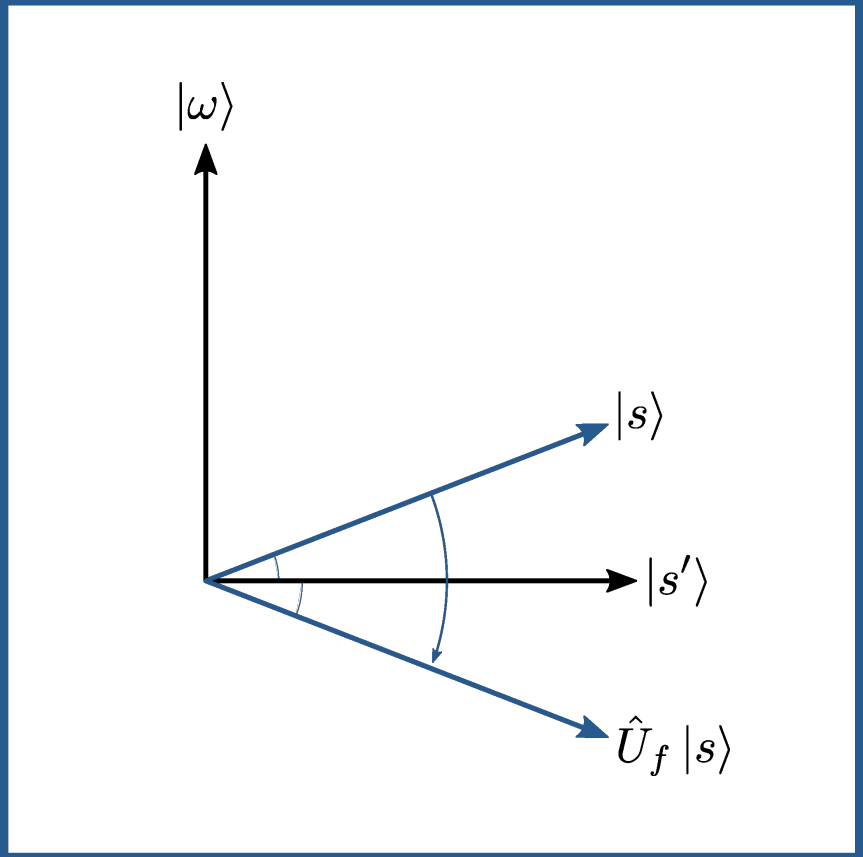
infotecs

Усиление амплитуды





Крипто-Оракул



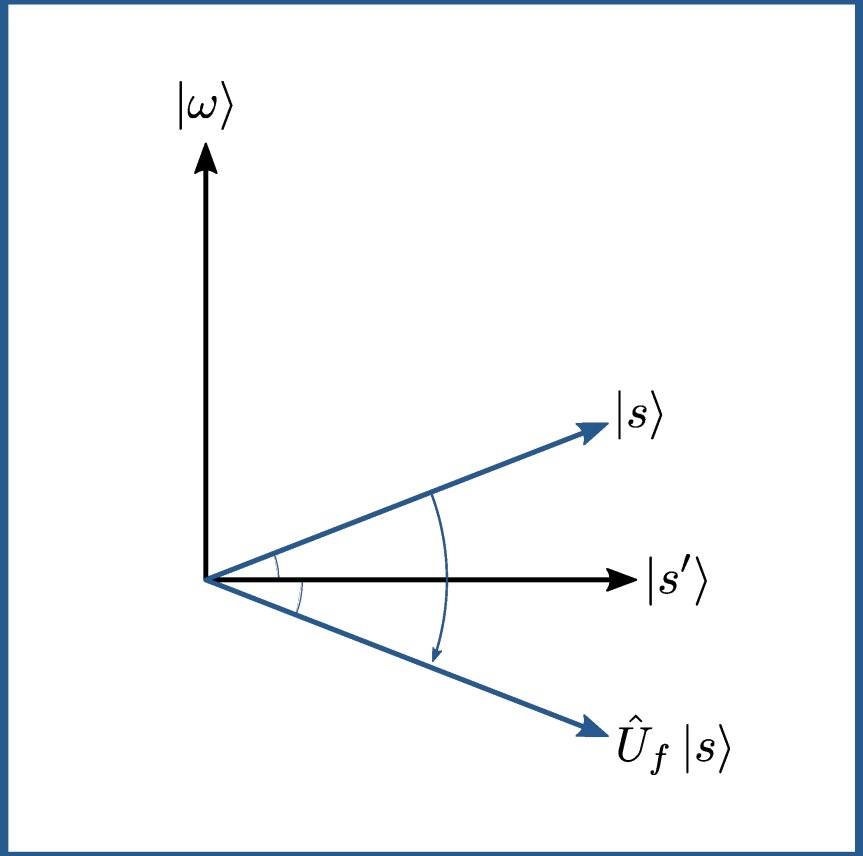
Задача оракула

$$\hat{U}_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$$

Возьмём $|q\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} = -\left(\dfrac{|1\rangle - |0\rangle}{\sqrt{2}}\right)$

$$\hat{U}_f|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\hat{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$$



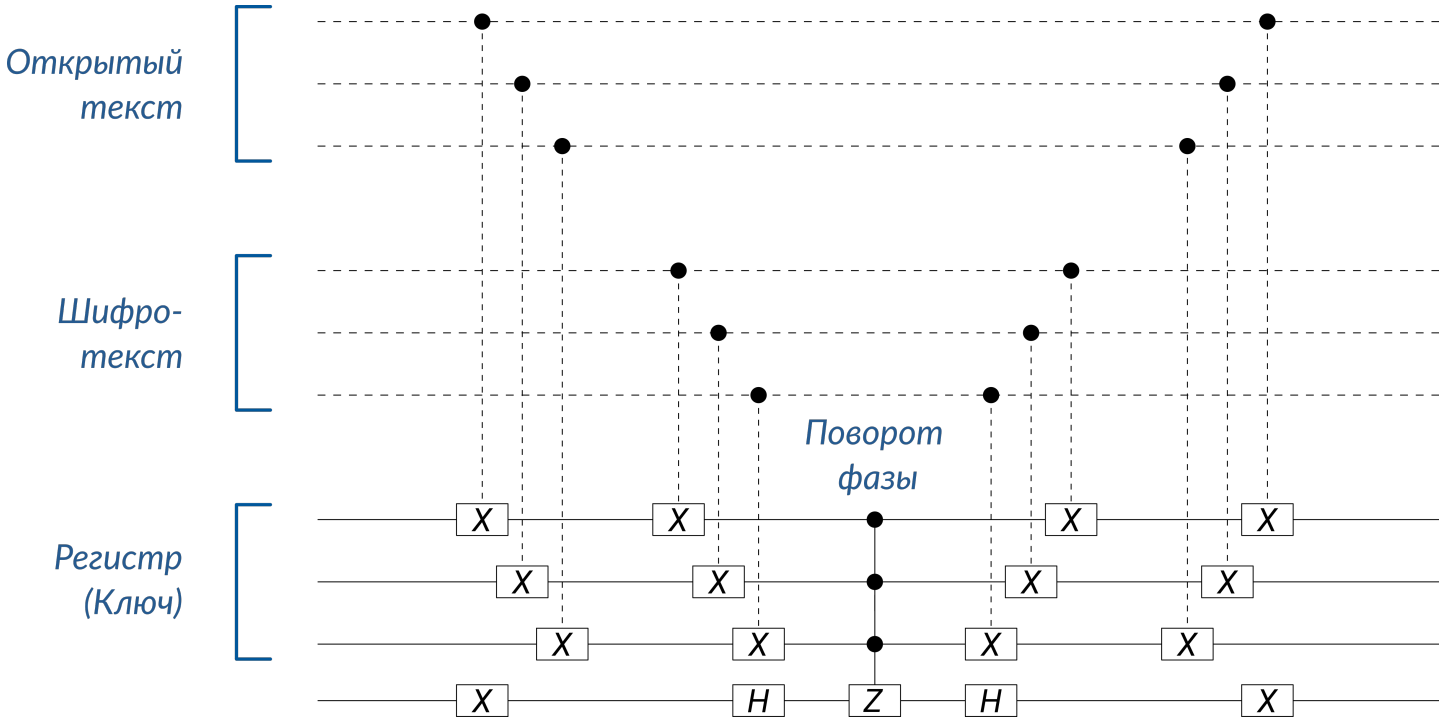
Задача оракула

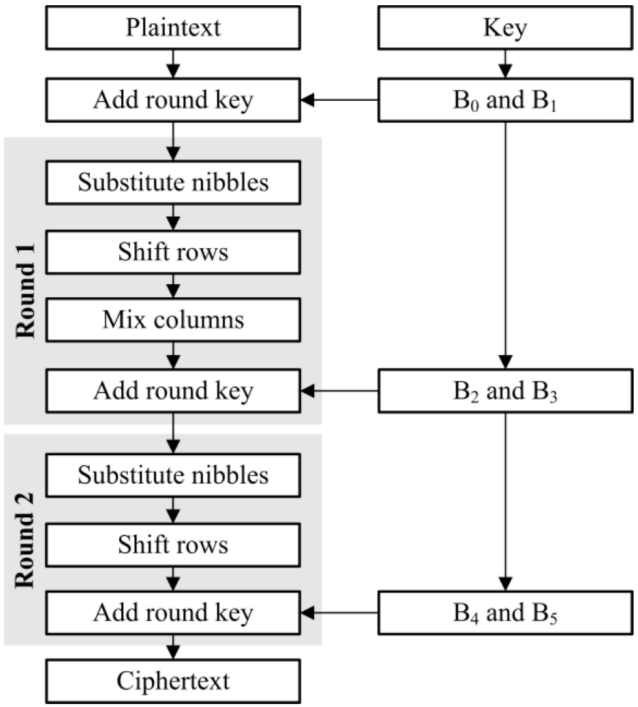
Дан открытый текст и зашифрованный текст

Требуется найти ключ

Работа оракула — проверять ключи

Простейший оракул





Simplified-AES

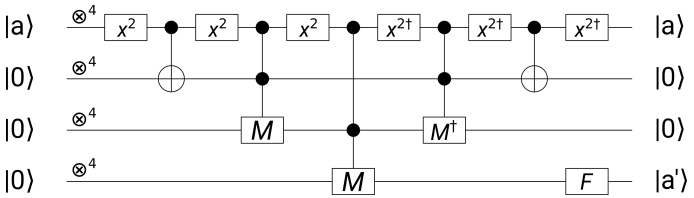
16 битов
2 раунда

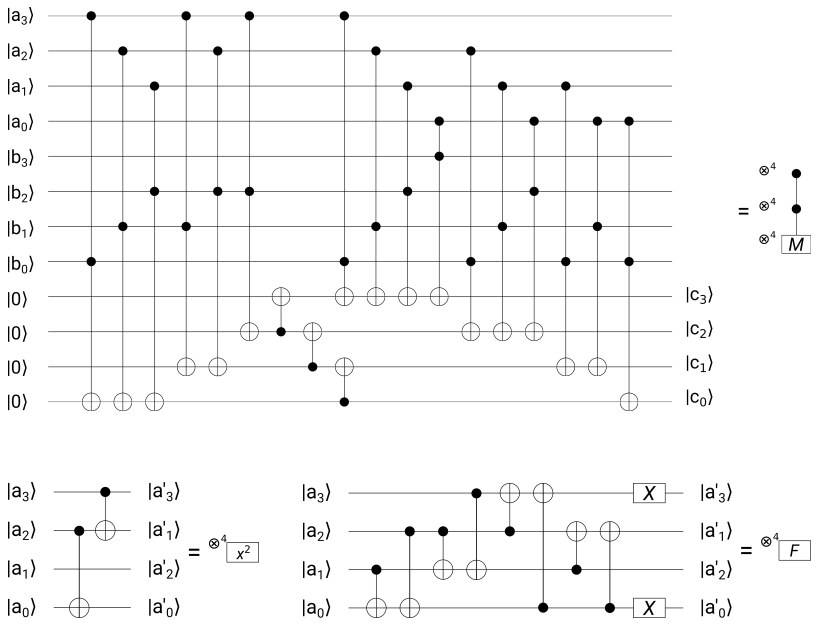
S-Box
Сдвиг строк
Смешение колонок
Добавление ключа

S-box на основе алгебры

GF(2)[y]/(y^4 + 1)

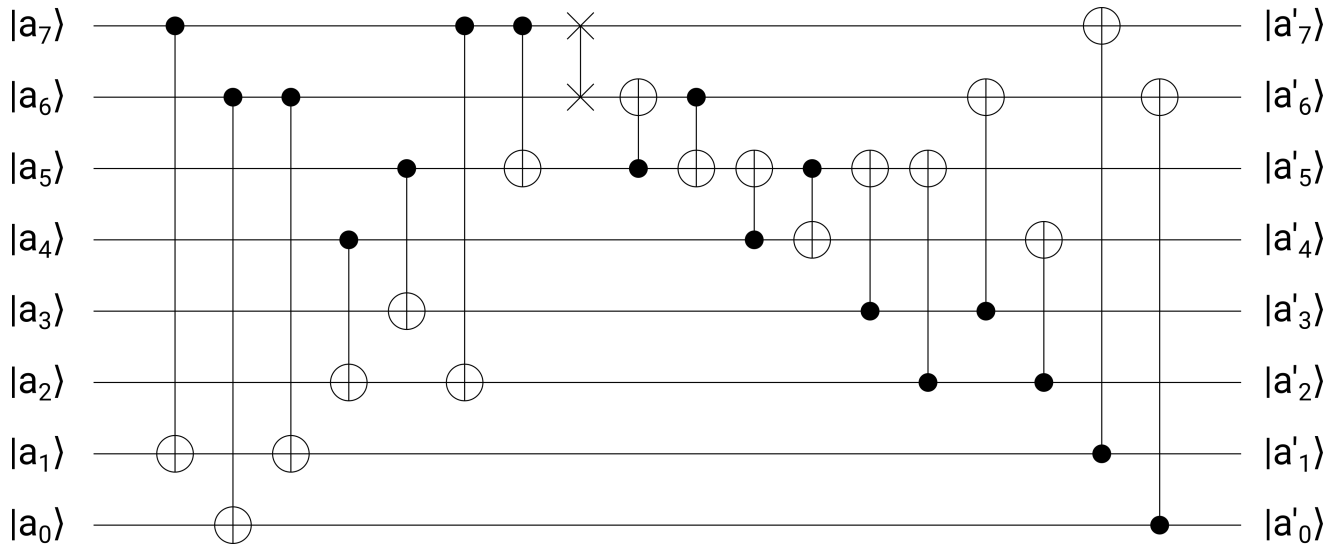
$a^{-1} = a^{14} = a^2 * (a^2)^2 * ((a^2)^2)^2$





Almazrooie M., Mutter K. et al. Quantum Grover Attack on the Simplified-AES,
ICSCA 2018: Proceedings of the 2018 7th International Conference on Software and Computer Applications (2018)

Mix Column из матричного представления



Almazrooie M., Mutter K. et al. Quantum Grover Attack on the Simplified-AES,
ICSCA 2018: Proceedings of the 2018 7th International Conference on Software and Computer Applications (2018)

Mix Column из явного преобразования битов

infotecs

$$a'_0 = a_0 \oplus a_6$$

$$a'_1 = a_1 \oplus a_4 \oplus a_7$$

$$a'_2 = a_2 \oplus a_4 \oplus a_5$$

$$a'_3 = a_3 \oplus a_5$$

$$a'_4 = a_4 \oplus a_2$$

$$a'_5 = a_5 \oplus a_3 \oplus a_0$$

$$a'_6 = a_6 \oplus a_1 \oplus a_0$$

$$a'_7 = a_7 \oplus a_1$$

Mix Column из явного преобразования битов

infotecs

$$a'_0 = a_0 \oplus a_6$$

$$a'_1 = a_1 \oplus a_4 \oplus a_7$$

$$a'_2 = a_2 \oplus a_4 \oplus a_5$$

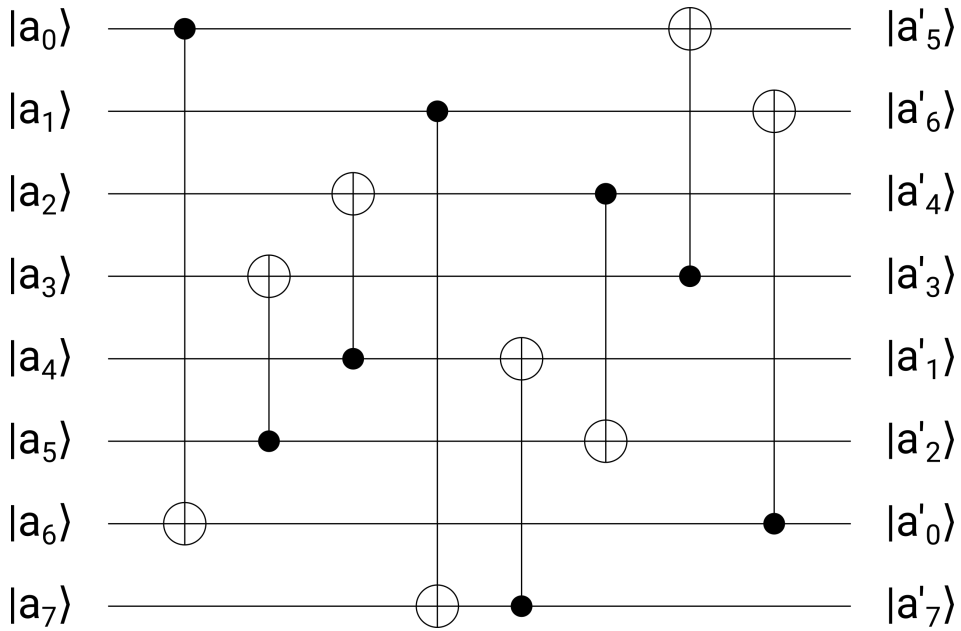
$$a'_3 = a_3 \oplus a_5$$

$$a'_4 = a_4 \oplus a_2$$

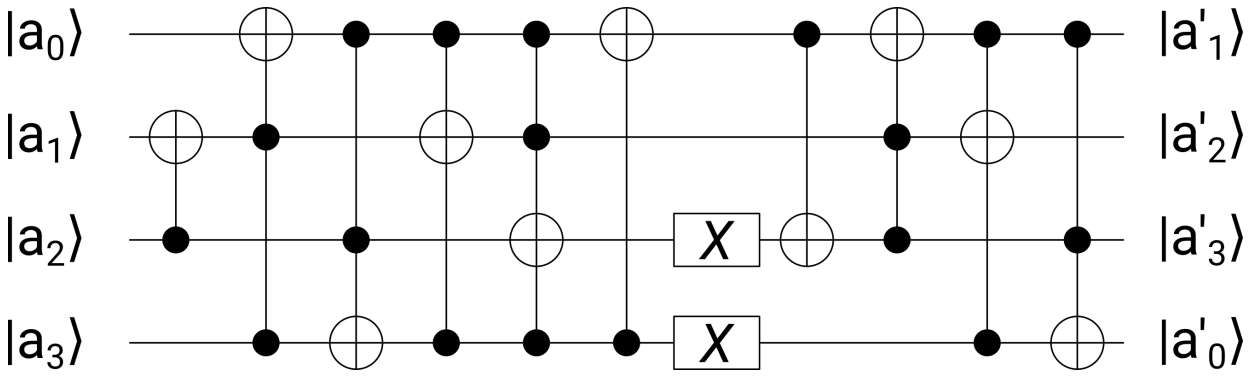
$$a'_5 = a_5 \oplus a_3 \oplus a_0$$

$$a'_6 = a_6 \oplus a_1 \oplus a_0$$

$$a'_7 = a_7 \oplus a_1$$



S-box из таблицы соответствия при помощи LighterR



Kyung-Bae Jang et. al., Grover on Simplified AES,
2021 IEEE International Conference on Consumer Electronics-Asia, ICCE-Asia (2021)

Требования оракула

infotecs

Kyung-Bae Jang et. al.
(2021)

32 кубита

144 CNOT

96 C^2NOT

16 C^3NOT

Almazrooie et. al.
(2018)

72 кубита

1080 CNOT

576 C^2NOT

Раунд квантового S-AES

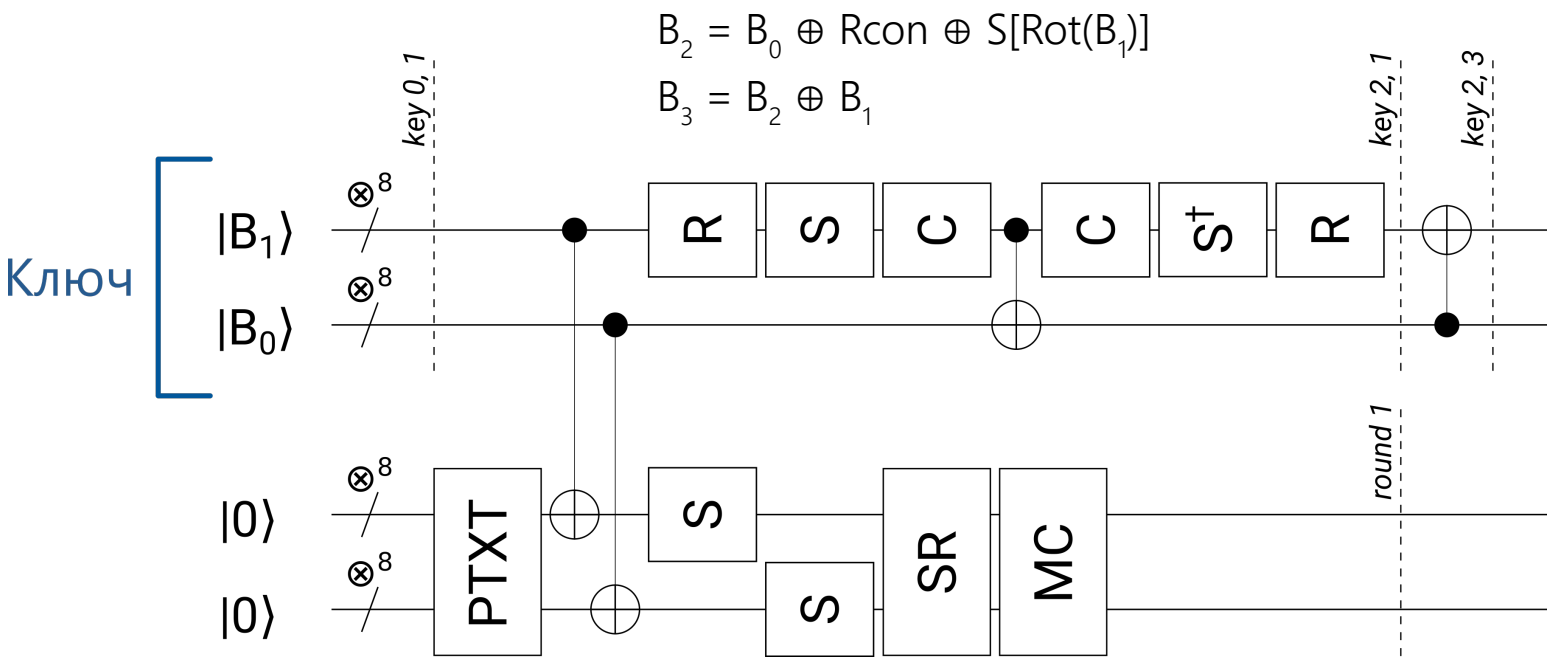


Схема квантовой атаки S-AES

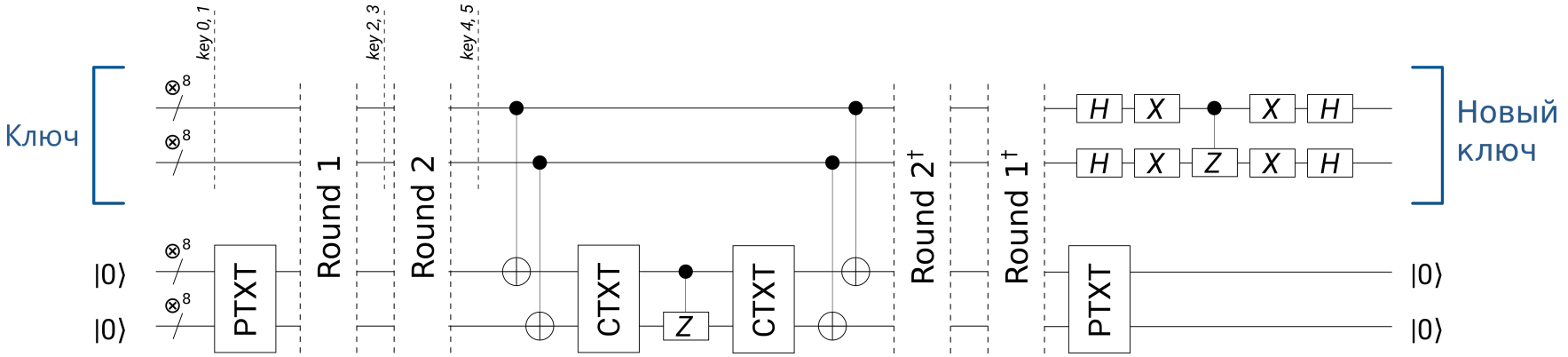


Схема квантовой атаки S-AES

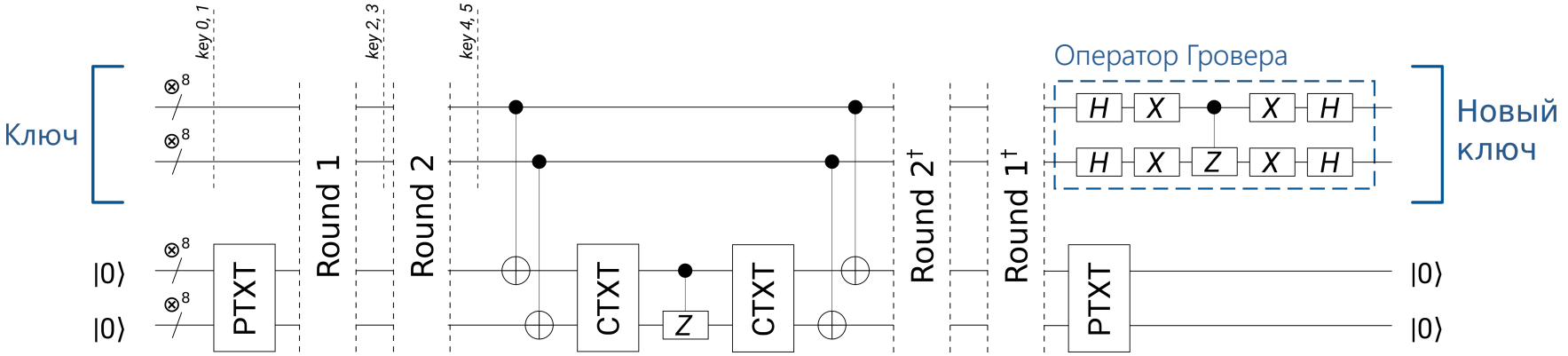
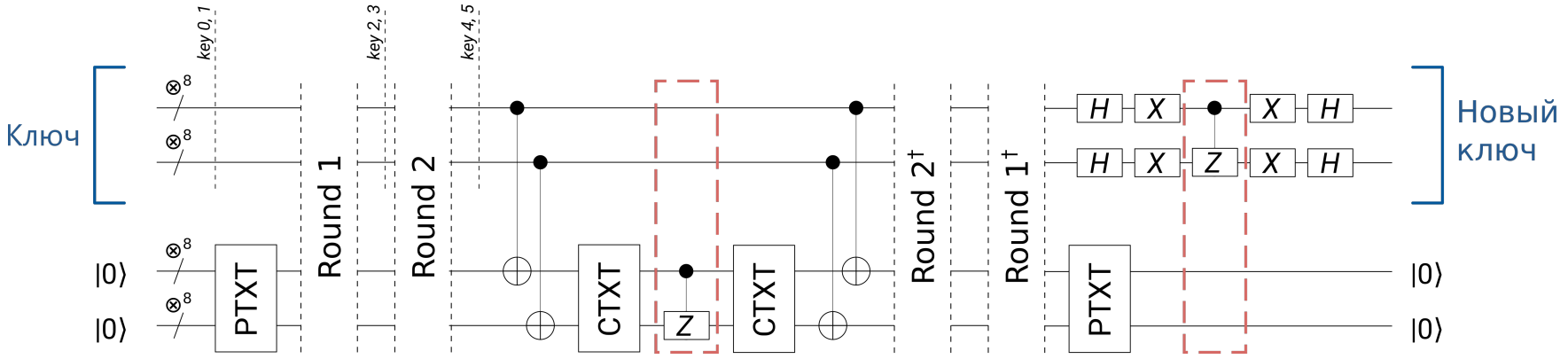
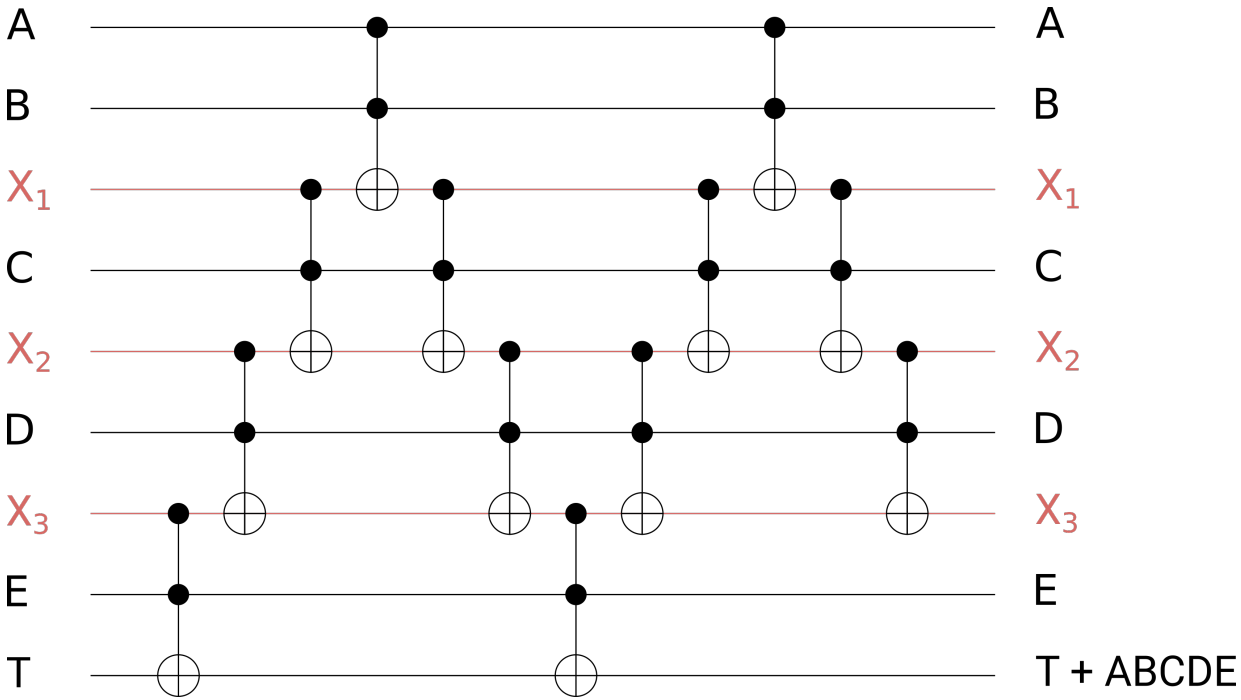


Схема квантовой атаки S-AES



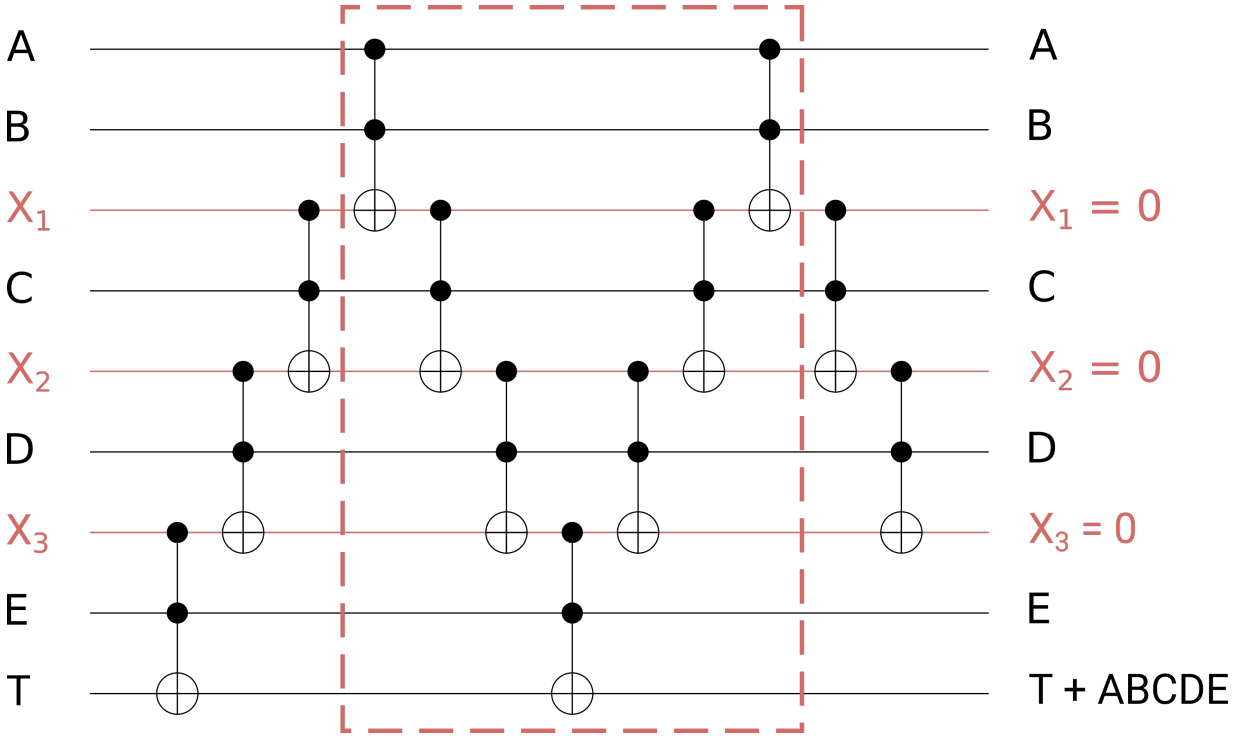
Мультиконтрольный гейт

infotecs

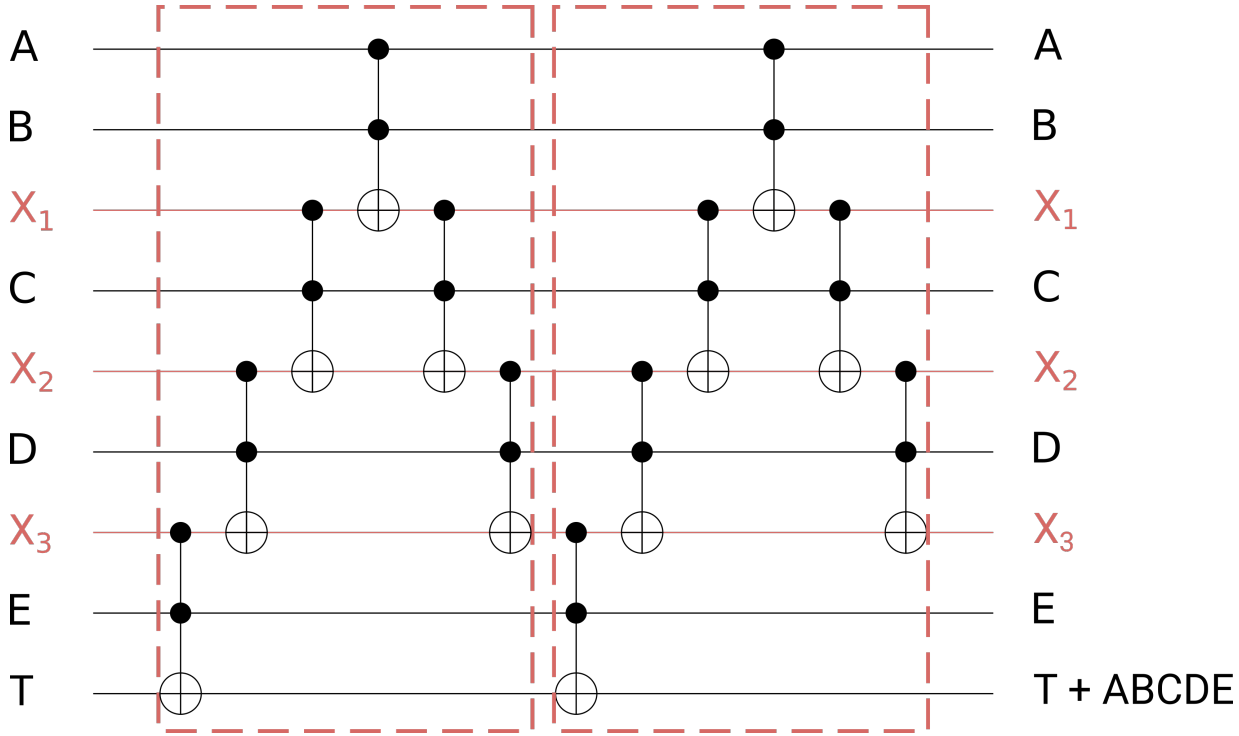


Мультиконтрольный гейт

infotecs



Мультиконтрольный гейт



Результаты на сегодняшний день

Полная готовность провести моделирование атаки
S-AES в квантово-вычислительной системе
Центра Квантовых Технологий МГУ

Все составляющие элементы алгоритма
протестированы, в том числе с реалистичным шумом

Перспективы работы

infotecs

Моделирование атаки с помощью
тензорного симулятора

Исследование возможностей оптимизации алгоритма
атаки за счёт доступа к побочной информации

Внедрение алгоритмов подавления ошибки

Исследование возможностей использования
квантового отжига

infotecs

Благодарю за внимание!

Алексей Моисеевский
+7 968 016 97 32
Aleksey.Moiseevsky@infotecs.ru