Усиление квантовой угрозы на примере оптимизированной атаки Гровера для S-AES

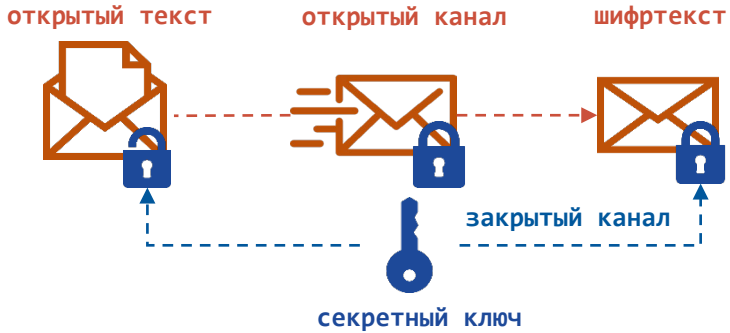
Манько Софья

Исследователь, Центр научных исследований и перспективных разработок ИнфоТеКС

infotecs

Введение

Симметричное шифрование



Классическая атака
Полный перебор ключей ($O(N)$)

Квантовая атака
Алгоритм Гровера ($O(\sqrt{N})$)

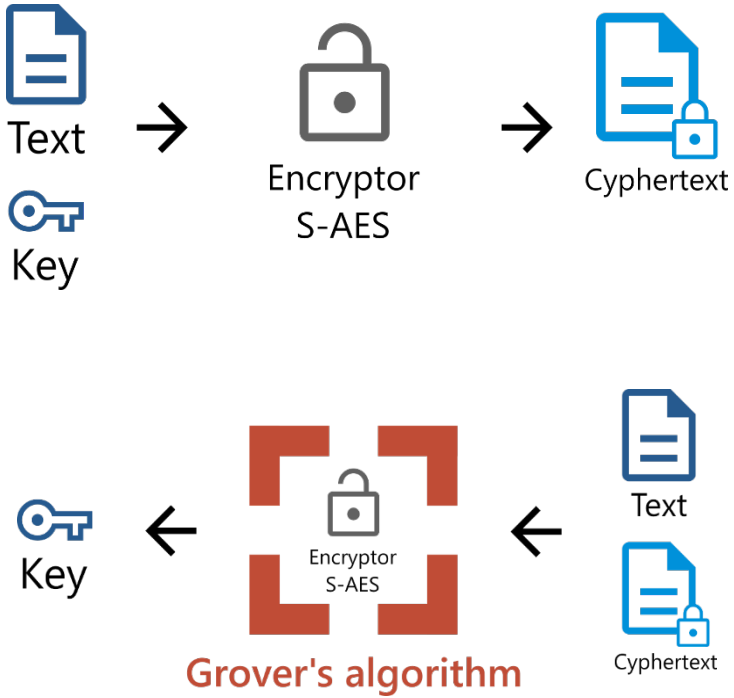
Длина ключа AES: от n=128 бит (симметричный шифр)

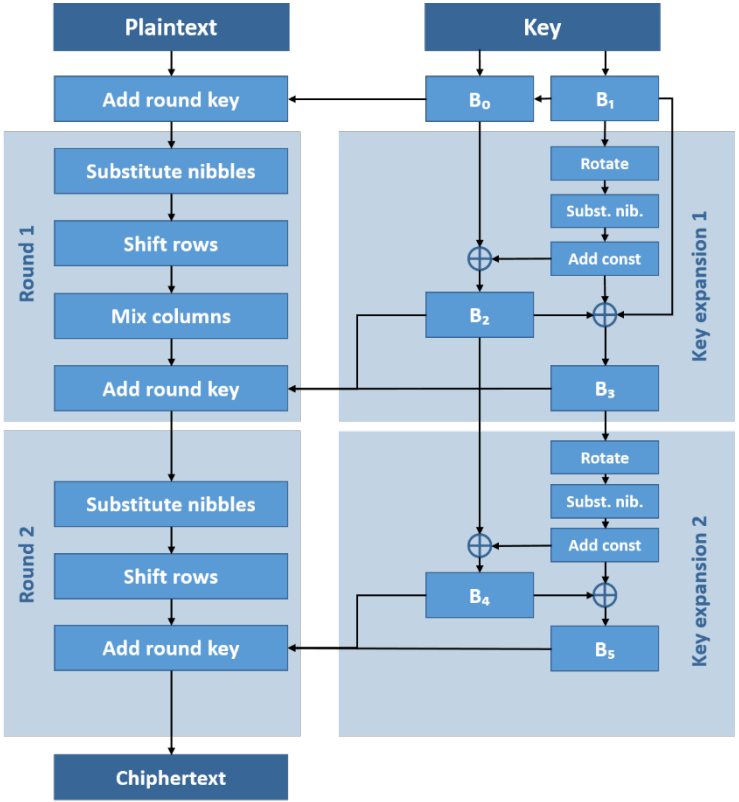
Длина ключа RSA: от n=1024 бит (асимметричный шифр)

Атака требует $O(n)$ кубитов

Квантовая схема атаки Гровера на S-AES

Квантовая атака





S-AES

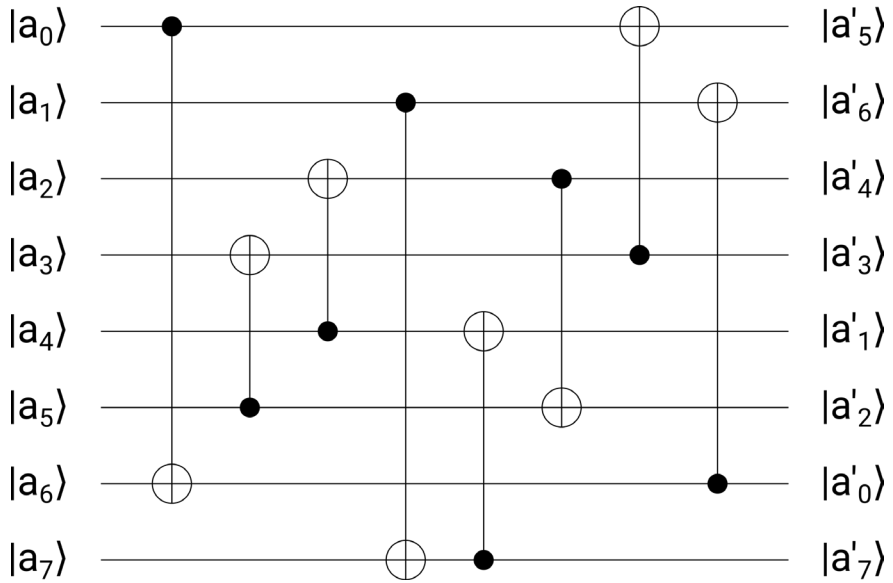
16 битов ключа
16 битов блока

2 раунда

Базовые элементы:

- S-Box
- Shift rows
- Mix columns
- Add key

Mix columns (MC)



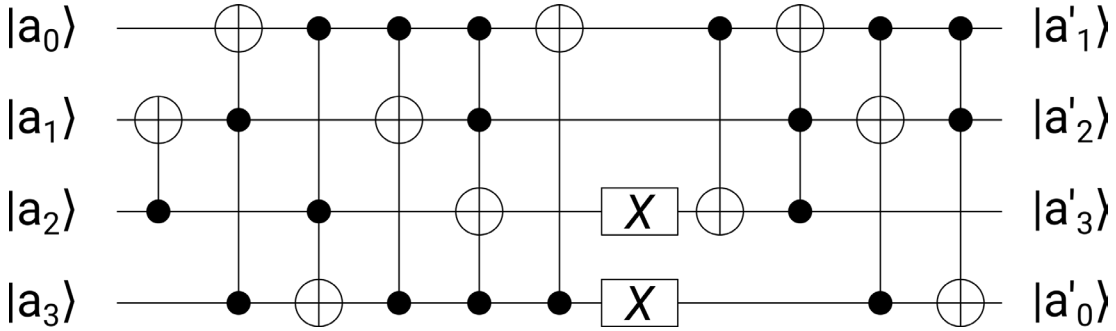
$$a'_0 = a_0 \oplus a_6$$
$$a'_1 = a_1 \oplus a_4 \oplus a_7$$
$$a'_2 = a_2 \oplus a_4 \oplus a_5$$
$$a'_3 = a_3 \oplus a_5$$
$$a'_4 = a_4 \oplus a_2$$
$$a'_5 = a_5 \oplus a_3 \oplus a_0$$
$$a'_6 = a_6 \oplus a_1 \oplus a_0$$
$$a'_7 = a_7 \oplus a_1$$

CNOT

Ввод	Вывод
$\|0\rangle\otimes\|0\rangle$	$\|0\rangle\otimes\|0\rangle$
$\|0\rangle\otimes\|1\rangle$	$\|0\rangle\otimes\|1\rangle$
$\|1\rangle\otimes\|0\rangle$	$\|1\rangle\otimes\|1\rangle$
$\|1\rangle\otimes\|1\rangle$	$\|1\rangle\otimes\|0\rangle$

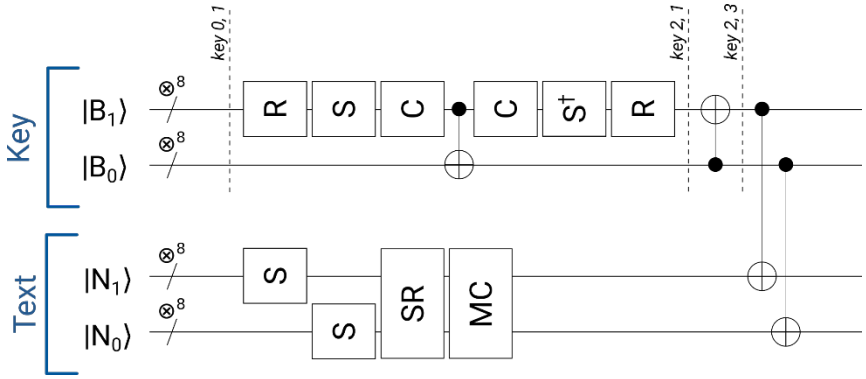
K. Jang, G. Song, H. Kim et al. Grover on Simplified AES // IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia) (2021)

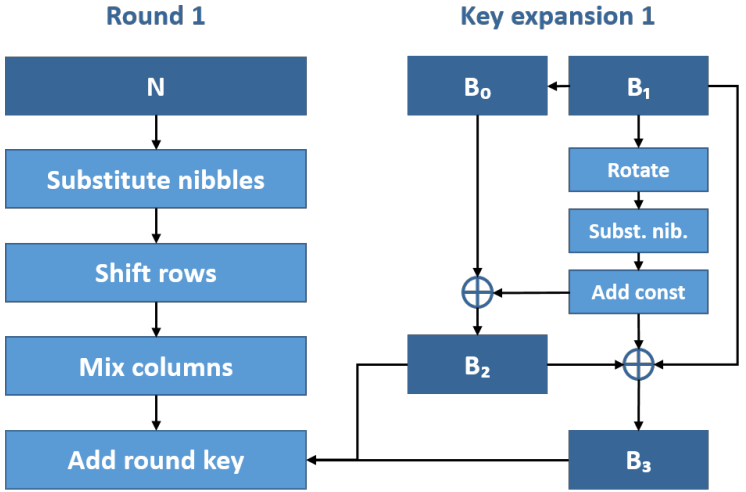
Substitute nibbles (S-box)



K. Jang, G. Song, H. Kim et al. Grover on Simplified AES // IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia) (2021)

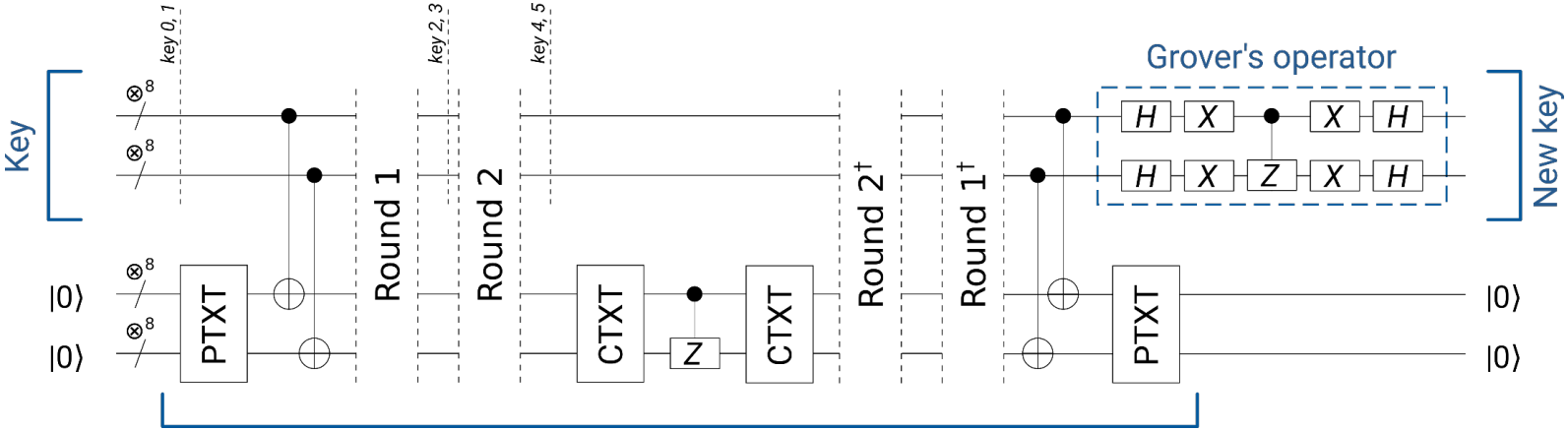
Первый раунд





$$B_2 = C_0 B_0 (B_1)^{RS}$$
$$B_3 = B_1 B_2$$

Одна итерация алгоритма Гровера

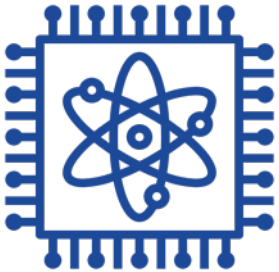


$$|x\rangle \to (-1)^{f(x)}|x\rangle$$

$$\begin{cases} f(x) = 0, x \ - \text{не решение} \\ f(x) = 1, x \ - \text{решение} \end{cases}$$
$$x \in [0, N-1], \qquad N = 2^n$$

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

Проблема

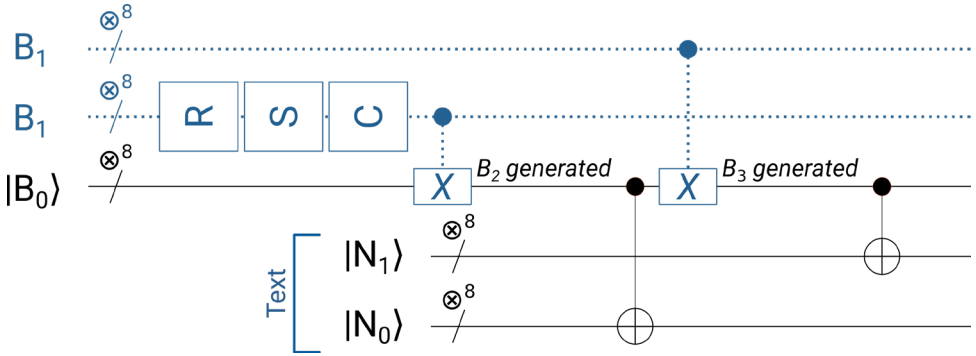


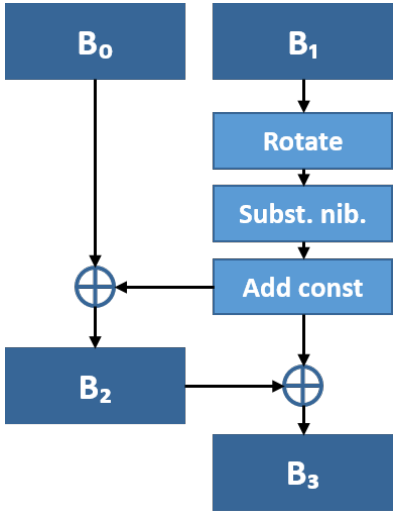
Для такой атаки необходимо 32 кубита
Это затрудняет исследования, поскольку моделирование требует много памяти и времени

480 часов на вычислительном кластере ЦКТ МГУ (4 процессора по 24 ядра, 2.1 ГГц, 24 модуля 64Гб RAM 2933МГц) при использовании CPU, либо недостижимые 128Гб памяти при использовании GPU

Атака с утечкой B1

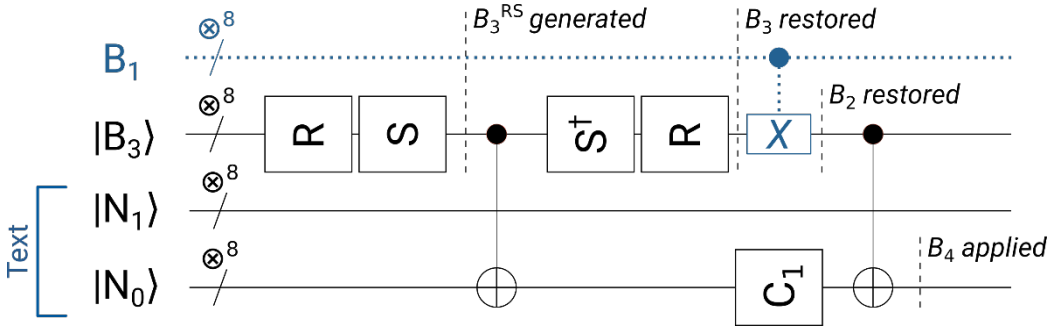
Генерация B2 и B3

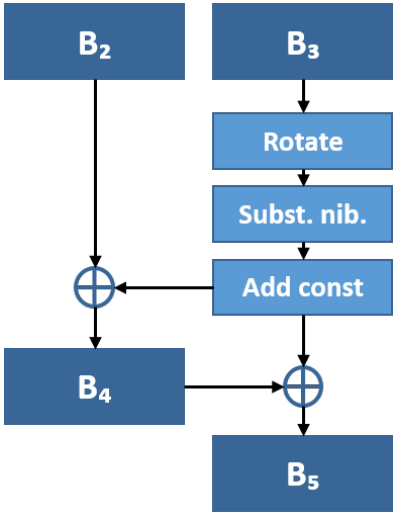




$$B_2 = C_0 B_0 (B_1)^{RS}$$
$$B_3 = B_1 B_2 = C_0 B_0 B_1 (B_1)^{RS}$$

Генерация B4 и B5

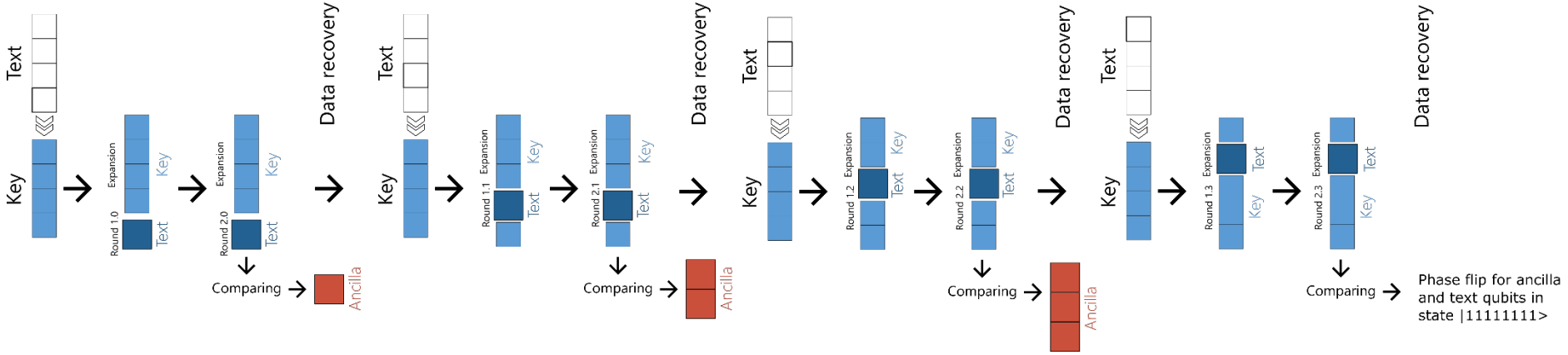




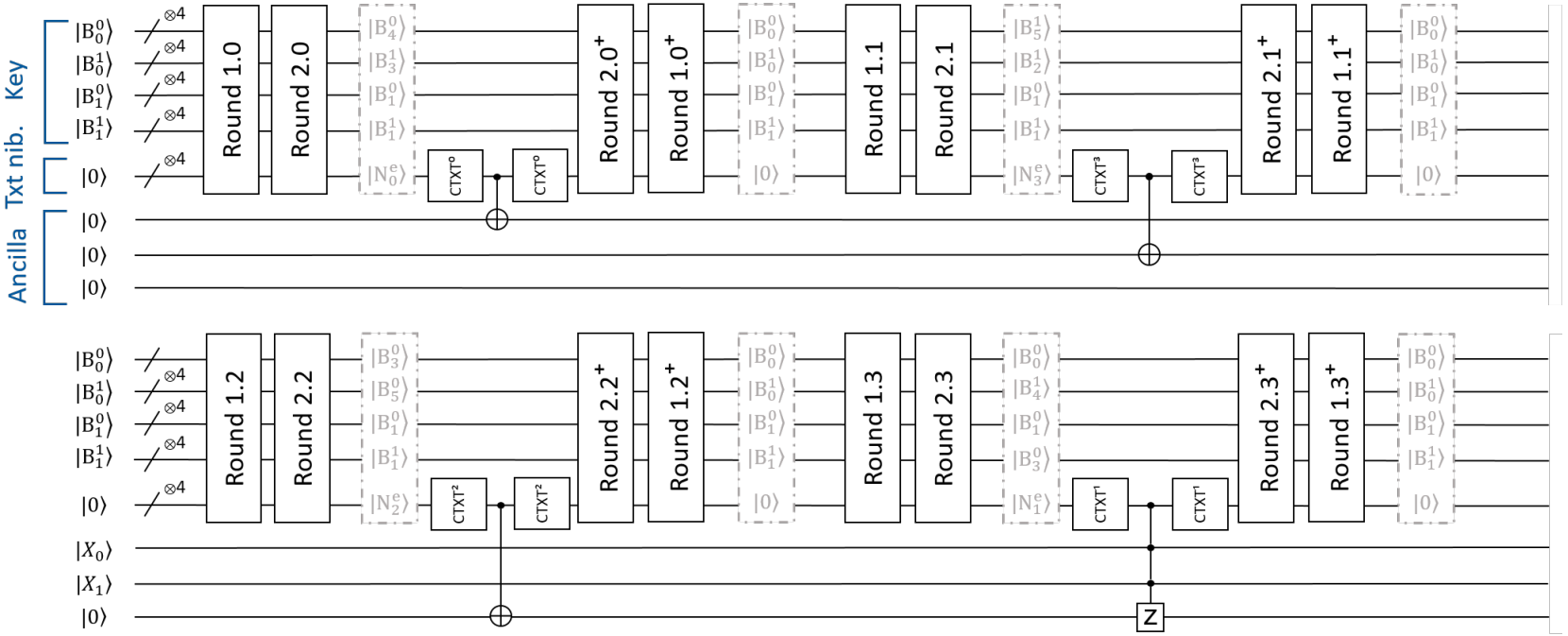
$$B_4 = C_1 B_2 (B_3)^{RS}$$
$$B_5 = B_3 B_4 = C_1 B_1 B_2 B_2 (B_3)^{RS} = C_1 B_1 (B_3)^{RS}$$

Атака с разделением

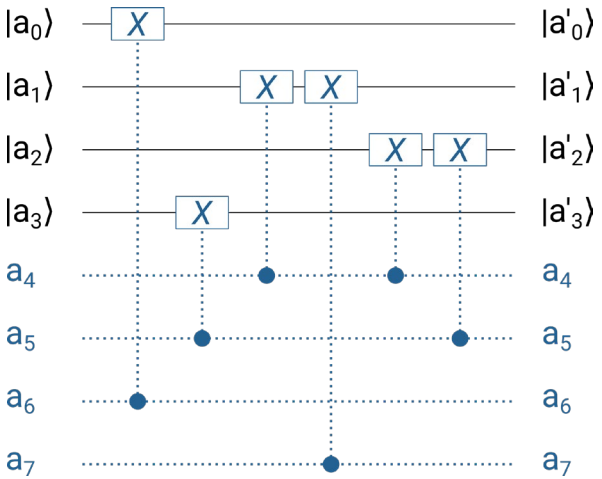
Концептуальная схема

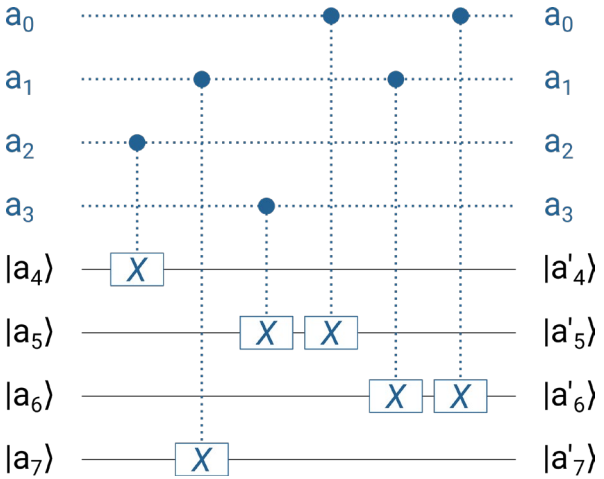


Квантовая схема



МС для одного полубайта





$$
\begin{aligned}
a'_0 &= a_0 \oplus a_6 \\
a'_1 &= a_1 \oplus a_4 \oplus a_7 \\
a'_2 &= a_2 \oplus a_4 \oplus a_5 \\
a'_3 &= a_3 \oplus a_5 \\
a'_4 &= a_4 \oplus a_2 \\
a'_5 &= a_5 \oplus a_3 \oplus a_0 \\
a'_6 &= a_6 \oplus a_1 \oplus a_0 \\
a'_7 &= a_7 \oplus a_1
\end{aligned}
$$

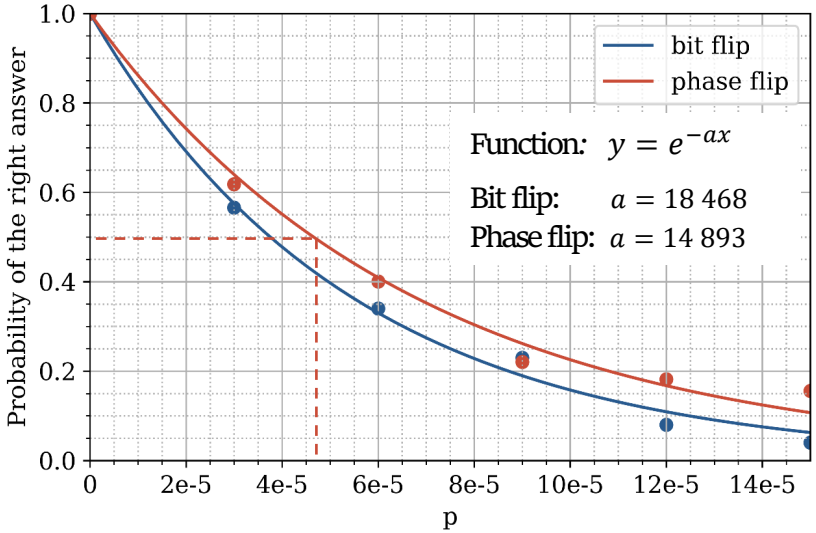
Результаты моделирования

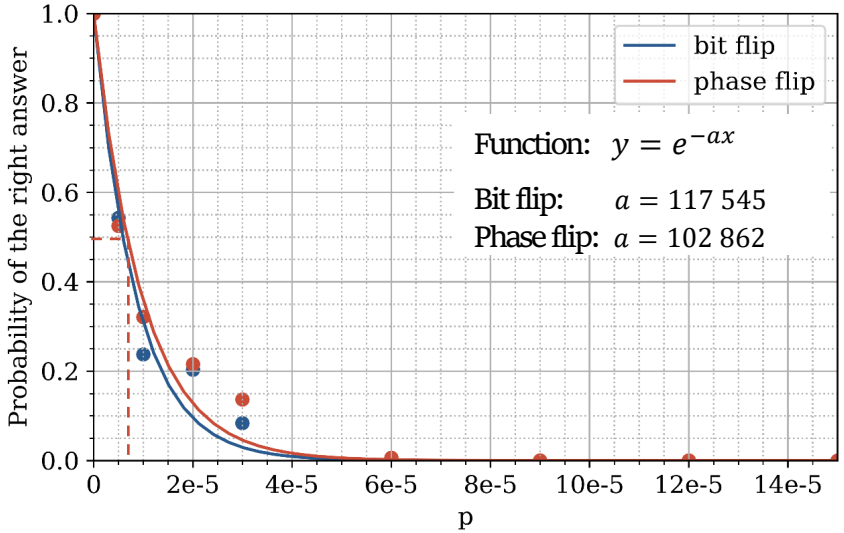
Результаты моделирования

infotecs

Тип оракула в алгоритме Гровера (вид утечки ключа)	Число кубитов		Одна итерация алгоритма Гровера		Необходимое число итераций	Время моделирования атаки	Успех при p_{Z-flip}
	Всего в атаке	Из них в регистре ключа	Глубина схемы	Число гейтов CNOT			
Прямой	32	16	3 236 ± 1	2 380	201 (142)	100+ часов	-
Прямой (B_1)	24	8	2 016 ± 1	1 586	12	1 минута	<4.65e-5
С разделением	23	16	11 998 ± 9	10 924	201 (142)	18 минут	-
С разделением (1 nibb.)	19	12	9 277 ± 9	7 860	50 (35)	30 секунд	<1.29e-6
С разделением (2 nibb.)	15	8	6 136 ± 9	4 912	12	5 секунд	<6.74e-6
С разделением (3 nibb.)	11	4	4 853 ± 10	2 860	3	1 секунда	<4.64e-5

Результаты моделирования





Тип оракула	Прямой	С разделением
Полный	100+ часов	18 минут
Утечка B1	1 минута	5 секунд
Необходимый уровень ошибки	$< 5 \cdot 10^{-5}$	$< 0.7 \cdot 10^{-5}$

Заключение

- Предложенные атаки с уменьшенными требованиями по числу кубитов были смоделированы
- Оценены параметры схем (число кубитов, глубина, число запутывающих гейтов, классические ресурсы для симуляции)
- Проведен анализ устойчивости квантовых схем атак к шумам и получены зависимости вероятности успешного выполнения от уровня элементарных шумов
- Анализ шумовых зависимостей позволил оценить минимальные требования для квантового устройства, при достижении которых алгоритм атаки на S-AES сможет быть продемонстрирован экспериментально хотя бы при частичной утечке ключа - необходимо снизить уровень шума до 10^{-5}
- Такой подход может быть потенциально расширен на атаку AES, что позволит существенно сократить число необходимых кубитов и приблизить момент практического применения квантовых вычислений в криптоанализе

Спасибо за внимание!

Манько Софья
Исследователь, Центр научных исследований и перспективных разработок ИнфоТеКС

e-mail:
Sofia.Manko@infotecs.ru

Моисеевский Алексей
Исследователь, Центр научных исследований и перспективных разработок ИнфоТеКС

e-mail:
Aleksey.Moiseevsky@infotecs.ru

Прямая экстраполяция на AES-128