infotecs

Квантово-усиленный симметричный криптоалализ S-AES

Алексей Моисеевский

Квантовый криптоанализ

infotecs

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

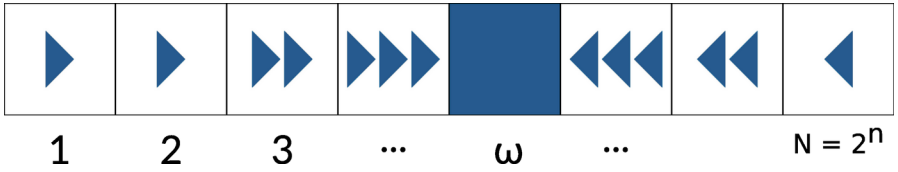
Квантовый алгоритм Гровера – алгоритм ускоренного поиска по неструктурированной базе данных

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»

Квантовый алгоритм Гровера



infotecs

Неструктурированный поиск

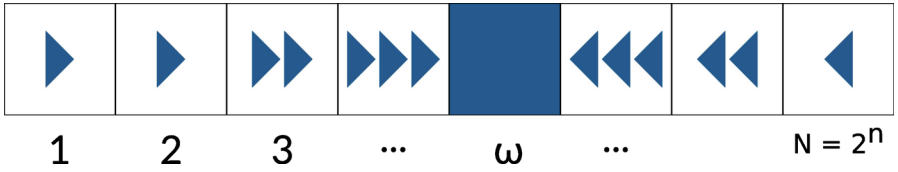
Задача оракула – распознать решение

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

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



infotecs

Неструктурированный поиск

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

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

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

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

Квантовый алгоритм Гровера

R – число повторений

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

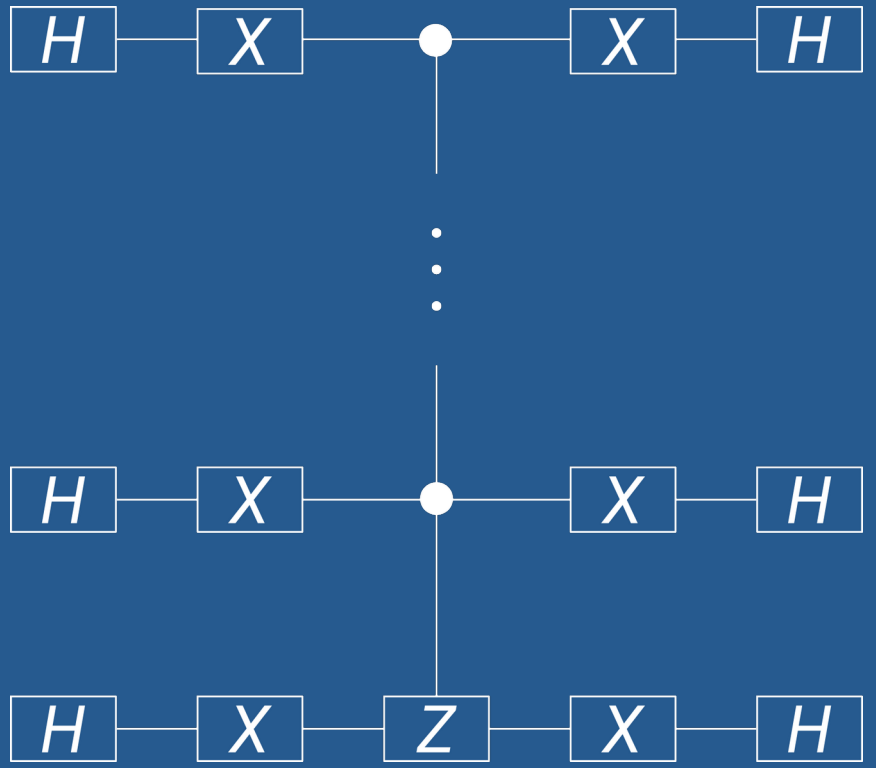
N – размер базы

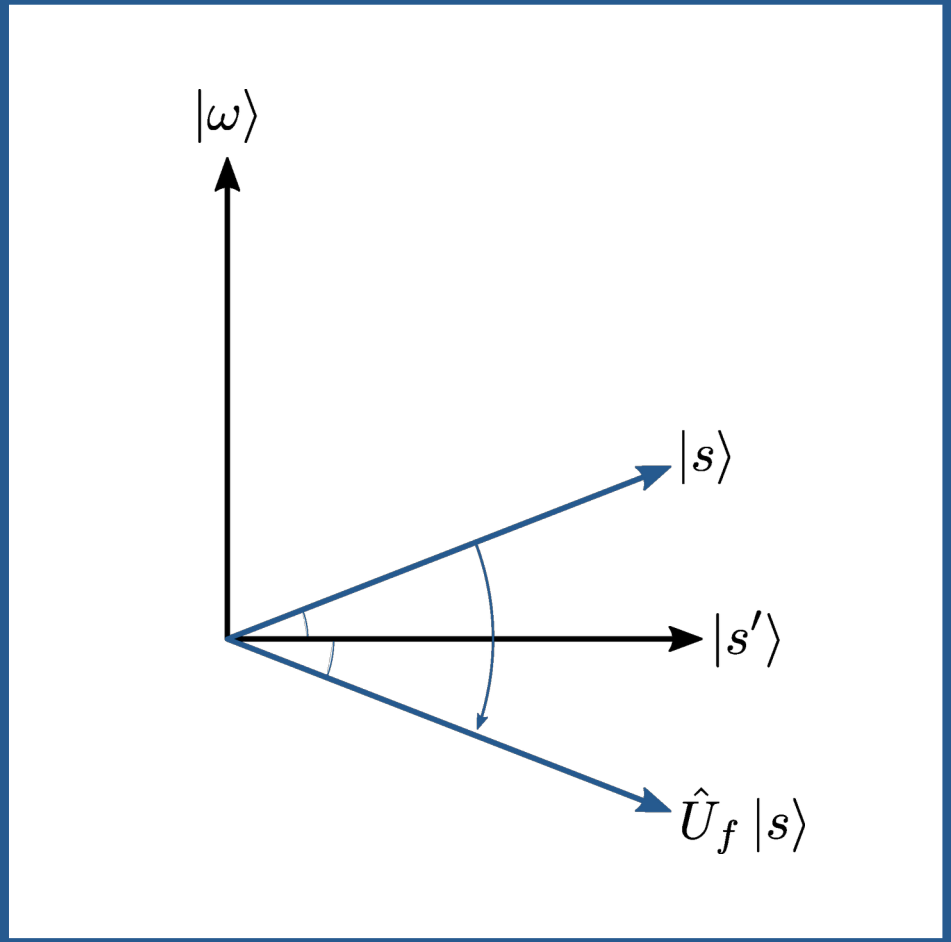
M – число решений

Квантовый алгоритм Гровера

infotecs

Усиление амплитуды





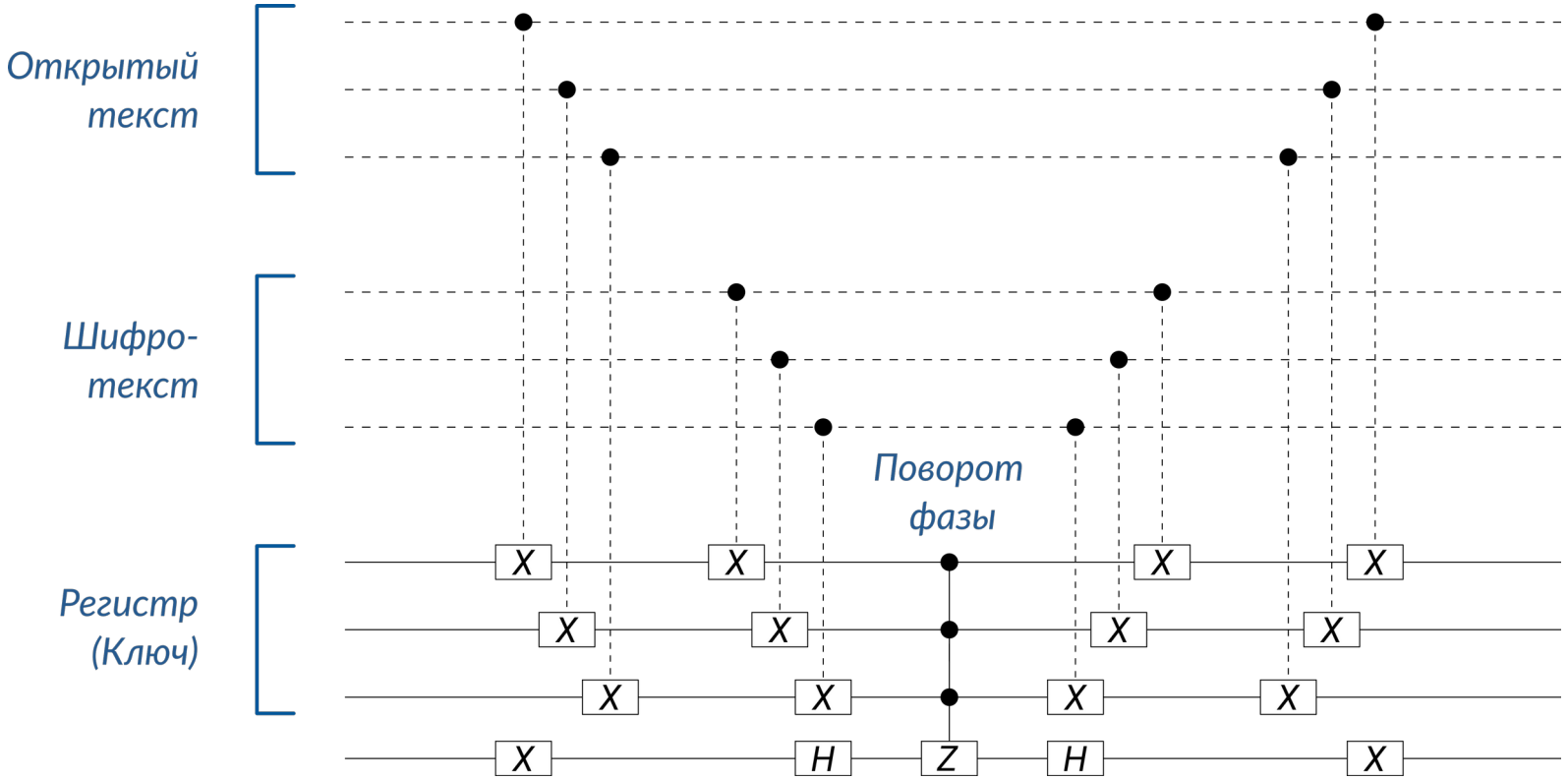
Задача оракула

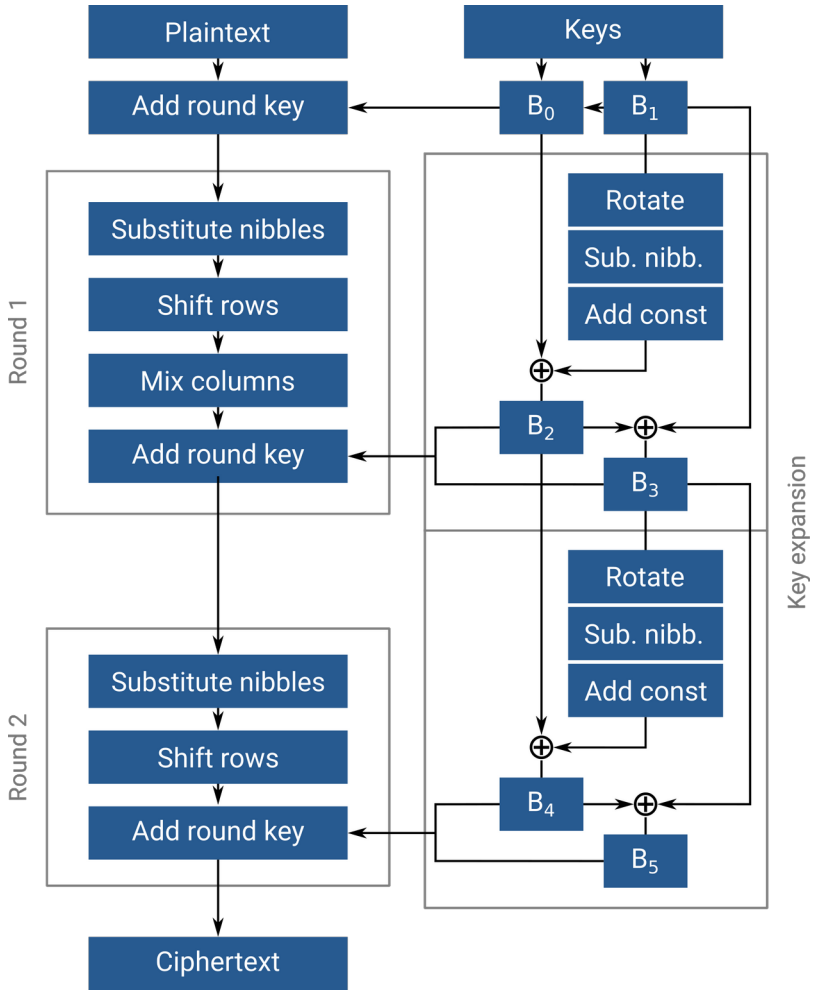
Дан открытый текст и зашифрованный текст

Требуется найти ключ

Работа оракула — повернуть фазу для нужного ключа

Простейший оракул





infotecs

Simplified-AES

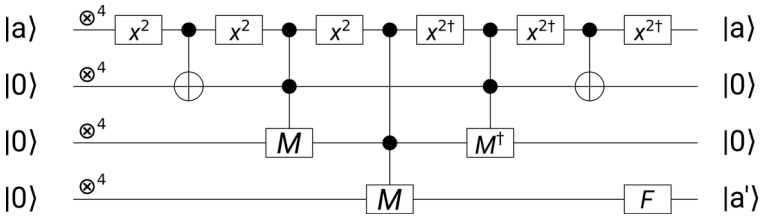
16 битов
2 раунда

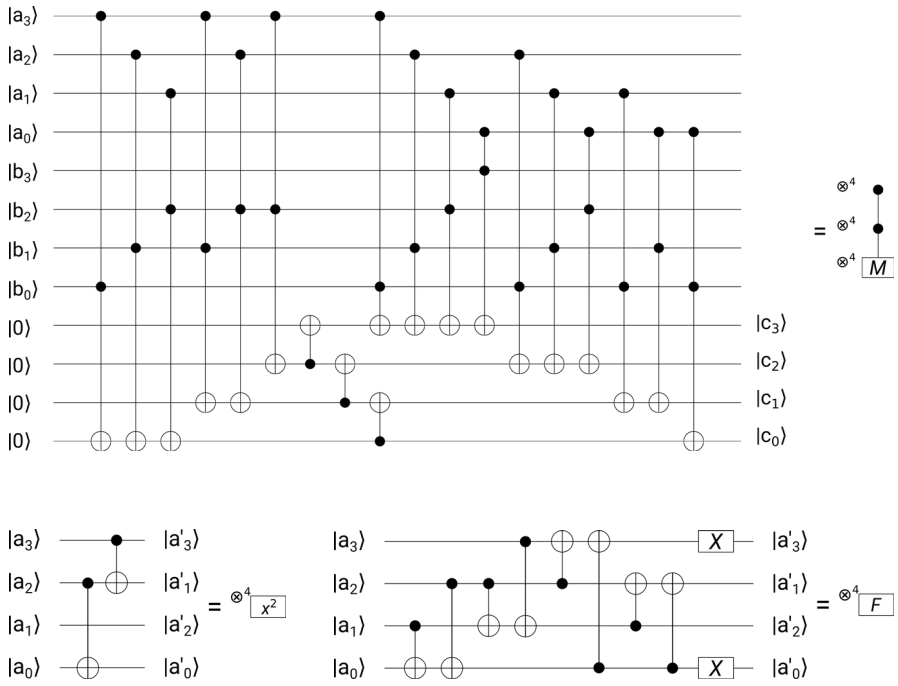
Базовые элементы:
1) S-Box
2)Сдвиг строк
3)Смешение колонок
4)Добавление ключа

S-box на основе алгебры

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

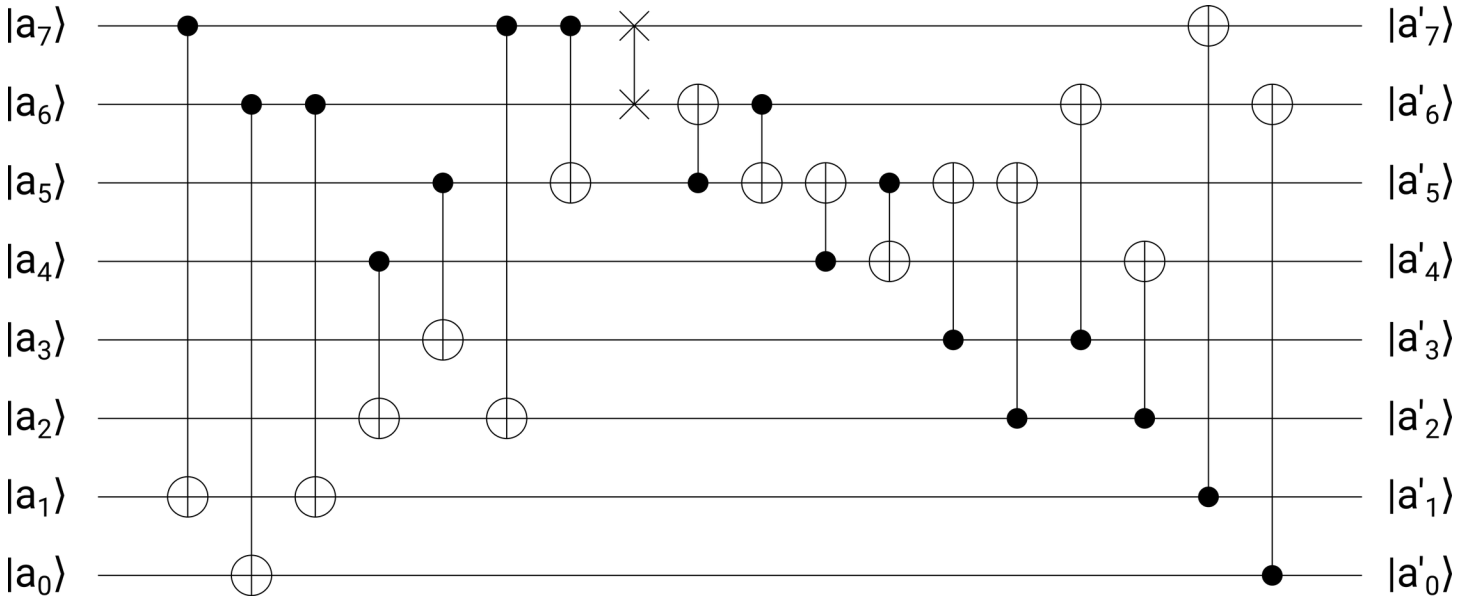
$$a^{-1} = a^{14} = a^2 * (a^2)^2 * ((a^2)^2)^2$$





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

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

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

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

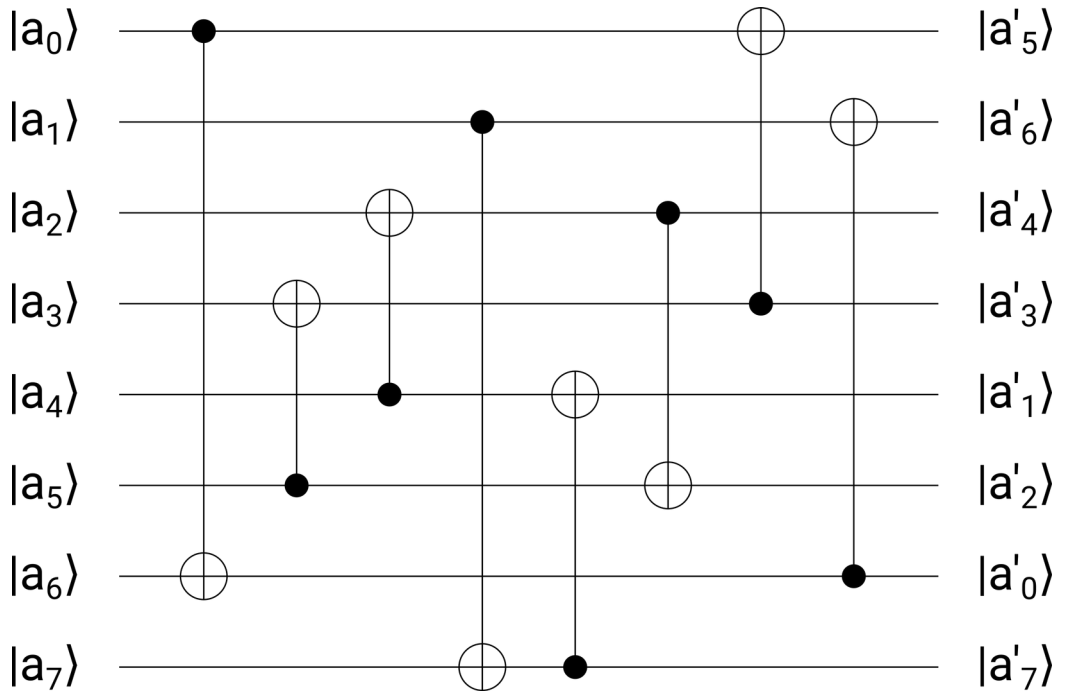
$$a'_3 = a_3 \oplus a_5$$

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

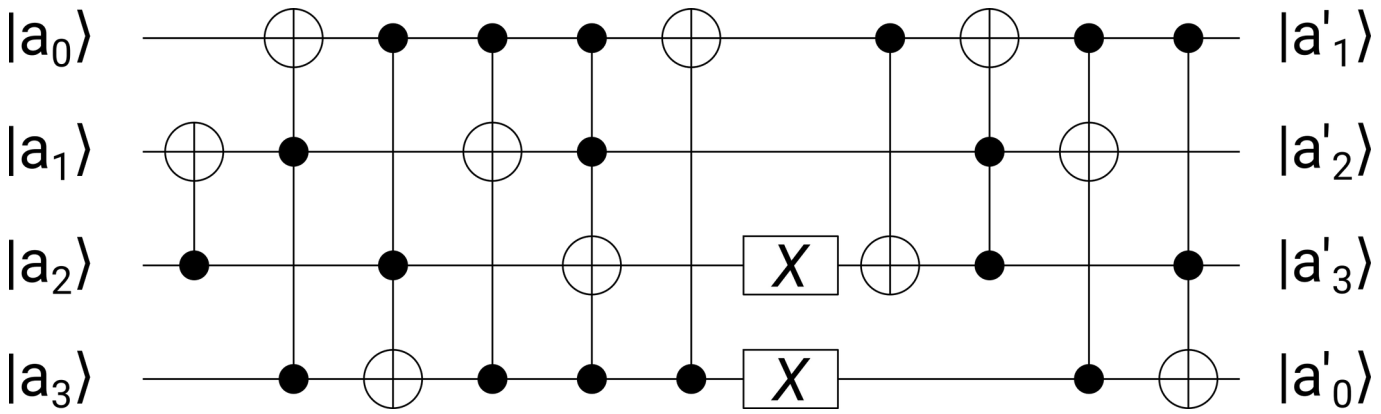
$$a'_5 = a_5 \oplus a_3 \oplus a_0$$

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

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



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)

Раунд квантового S-AES

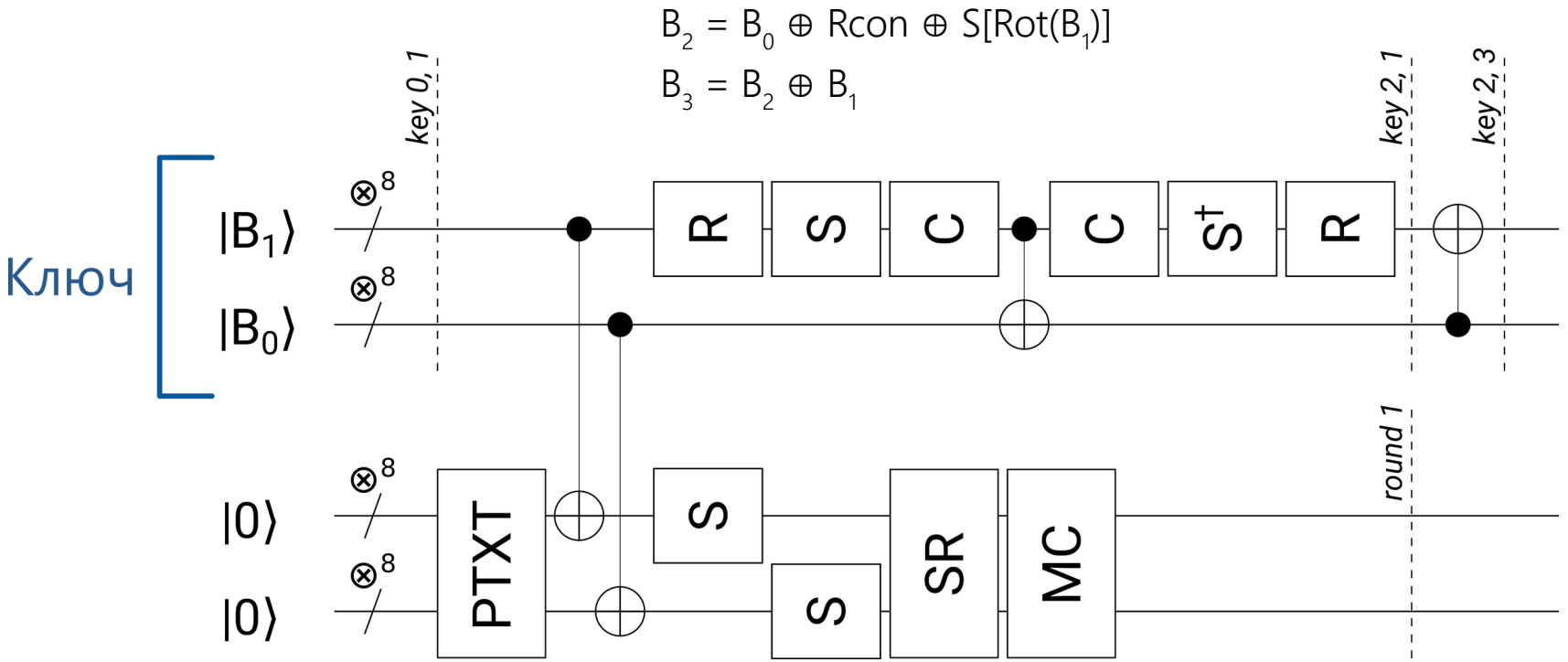
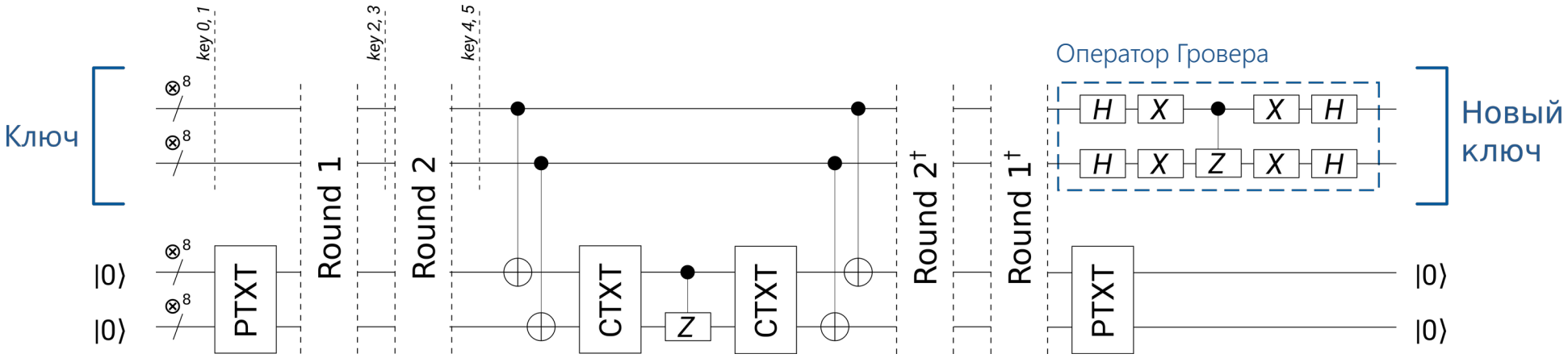
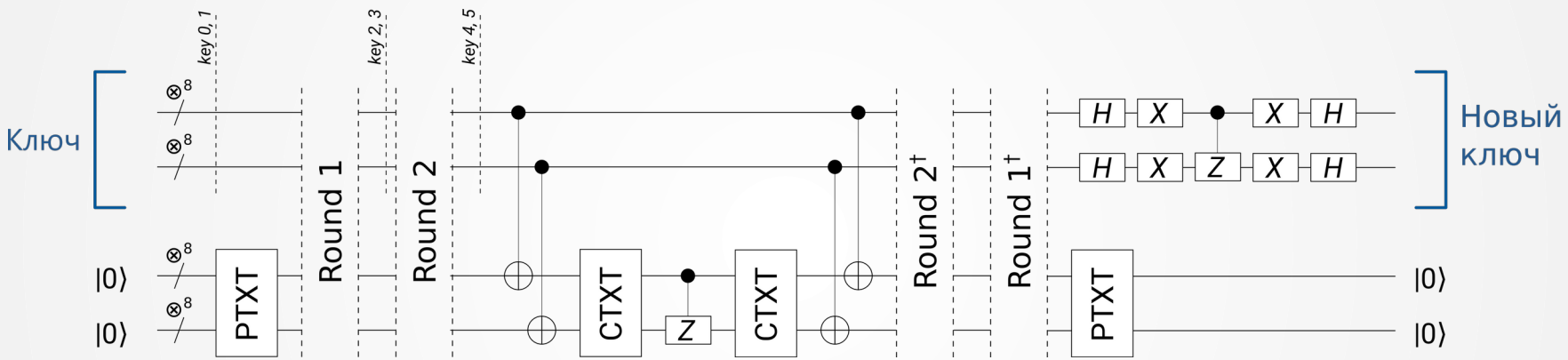


Схема квантовой атаки S-AES



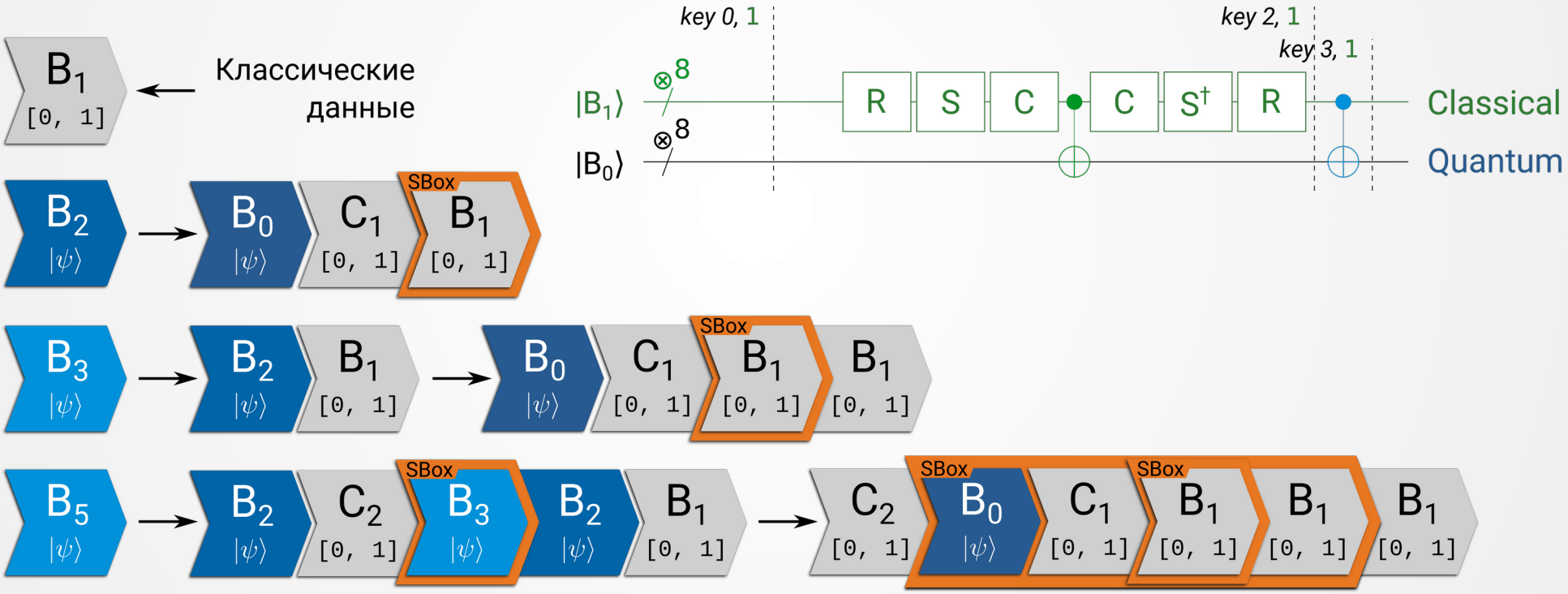
Оптимизация оракула

Полная атака на S-AES

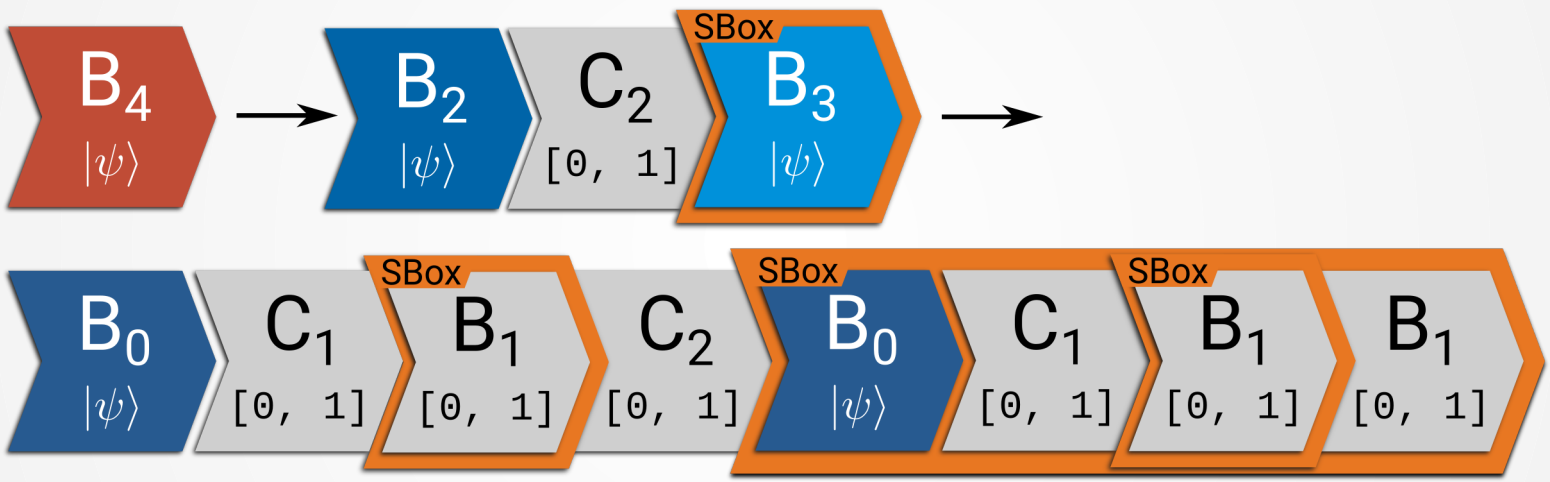


Требуется 32 кубита
Возможности моделирования GPU с 32Гб VRAM – 29 кубитов
Предлагается исследовать возможности оптимизации за счёт утечки

Атака ключей раунда с утечкой



Проблема ключа B_4



Генерация B_4 необратима, неунитарна и не может быть выполнена квантовой схемой

Анализ f = x⊕Sbox[x]

infotecs

Случаи с вырождением

```
0010
0011  ──►  0000
1011
1111

0000
0100  ──►  0001

0110
1000  ──►  0110
```

Нормальные случаи

```
0001 – 1101
0101 – 1100
0111 – 1010
1001 – 0011
1010 – 1010
1100 – 1000
1101 – 1011
1110 – 1001
```

Исключённые случаи

```
X 0100
X 0101
X 0111
X 1110
X 1111
```

Анализ f = x⊕Sbox[x]

infotecs

Случаи с вырождением

0010		+ 00
0011	→ 0000	+ 01
1011		+ 11
1111		+ 10
0000	→ 0001	+ 00
0100		+ 01
0110	→ 0110	+ 01
1000		+ 10

Дополнение: N[0], N[1]⊕N[3]

Требует два дополнительных кубита

Произвол №1: вариативность дополнения

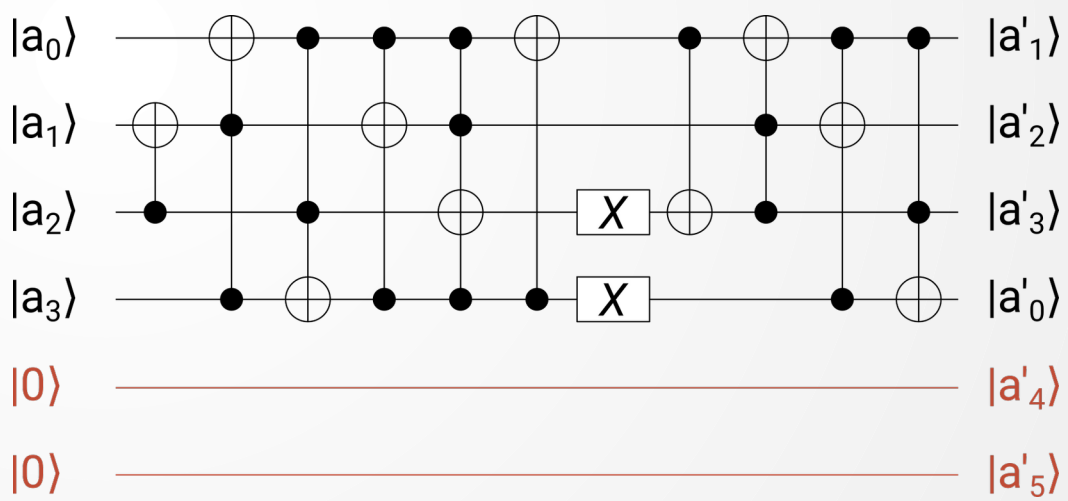
Анализ f = x⊕Sbox[x]

infotecs

Случаи с вырождением

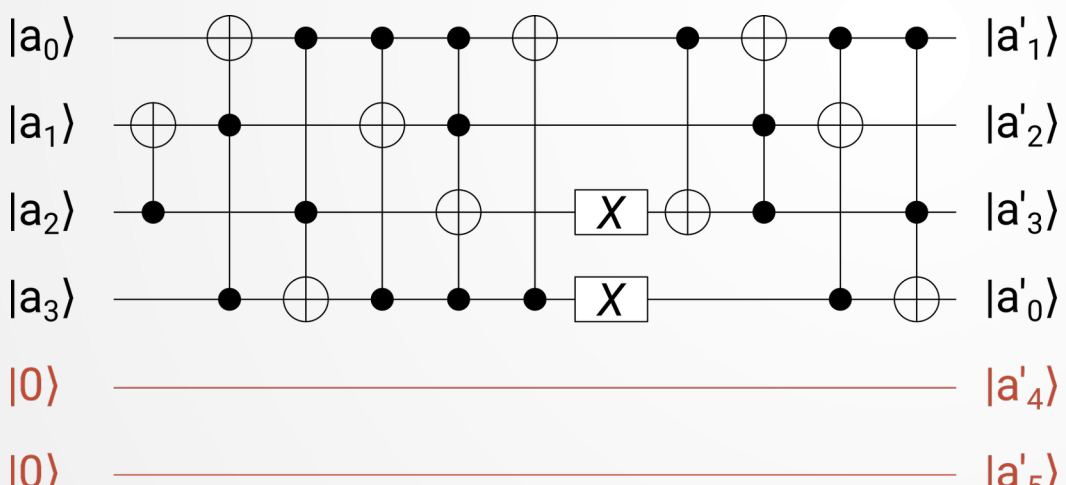
```
0010          + 00
0011  ──►0000 + 01
1011          + 11
1111          + 10

0000  ──►0001 + 00
0100          + 01

0110  ──►0110 + 01
1000          + 10
```

Произвол №2: вариативность действия при ненулевых анциллах



Анализ f = x⊕Sbox[x]

Произвол №2: вариативность действия при ненулевых анциллах



Решение 1:
Перебор алгебраических конфигураций

Решение 2:
Перебор конфигураций матрицы преобразования

Анализ конфигураций схемы

Создано вспомогательное ПО для анализа корреляций преобразования

Дополнение $N_0 \oplus N_2$, $N_1 \oplus N_3$

Исчезнувшие строки

001001	101011
001101	101100
001110	101111
011000	111010
011100	111101
011111	111110

Дублирующиеся строки

000001	100001
000011	100011
001010	101000
010000	110000
010010	110010
011011	111001

Решение проблемы четвёртого ключа

infotecs

Путь 1:

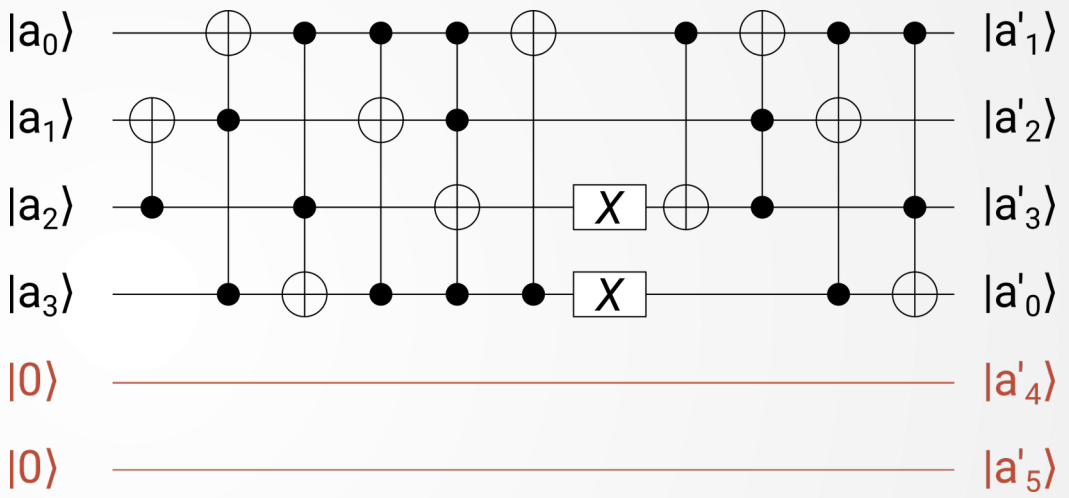
Расширять схему Sbox

Путь доказано тупиковый

Путь 2:

Составлять матрицу U и раскладывать на гейты

Путь крайне трудоёмкий

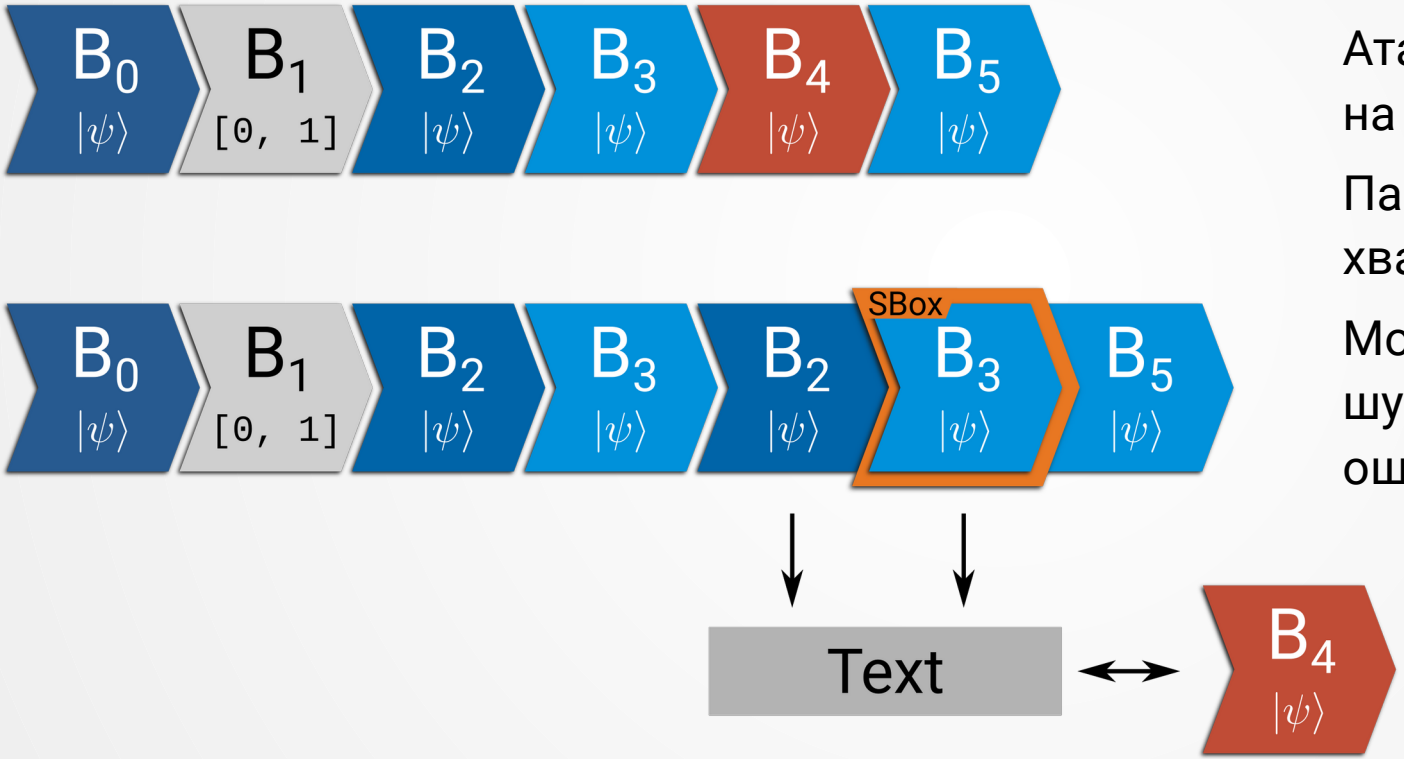


Путь 3 – корректное решение:

Сменить постановку задачи,

Включать кубиты текста в процесс генерации

Решение проблемы четвёртого ключа



Атака с утечкой возможна на 24 кубитах

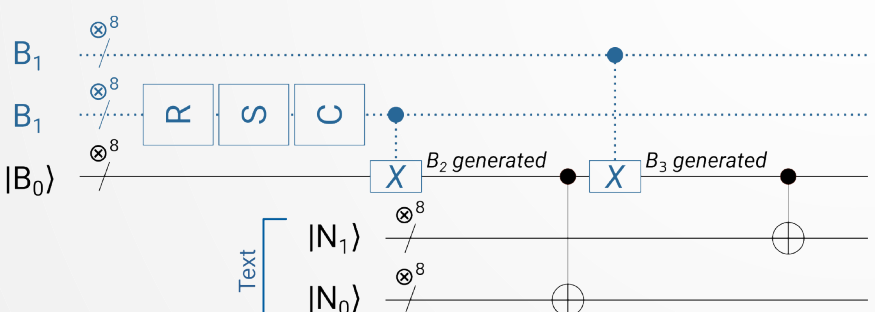
Памяти Nvidia Tesla A100 хватает для атаки

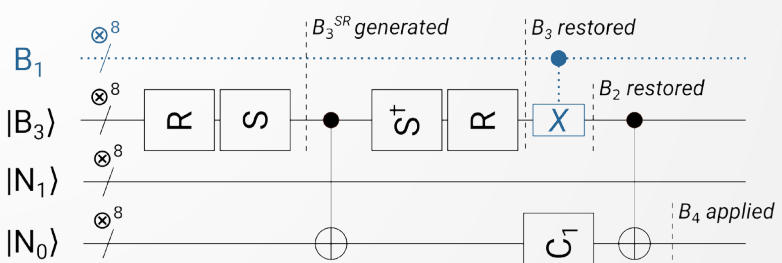
Можно моделировать с шумами и подавлением ошибки

Построение масштабируемой атаки

Генерация ключей S-AES

$$B_0 = B_0 \qquad B_3 = B_1 B_2 = C_0 B_0 B_1 B_1^{SR}$$
$$B_1 = B_1 \qquad B_4 = C_1 B_2 B_3{}^{SR} = C_0 C_1 B_0 B_1^{SR} [C_0 B_0 B_1 B_1^{SR}]^{SR}$$
$$B_2 = C_0 B_0 B_1^{SR} \qquad B_5 = B_3 B_4 = C_1 B_1 B_2 B_2 B_3{}^{SR} = C_1 B_1 B_3{}^{SR}$$





Прямая атака на утечку B_1

24 кубита

Из-за проблемы необратимости X Sbox[X] алгоритм не универсален

Action	Key		Text			
Init	$\boldsymbol{B_0}$	B_1	N_0	N_1	N_2	N_3
Add key	$\boldsymbol{B_0}$	B_1	$\boldsymbol{B_0 N_0}$	$\boldsymbol{B_0 N_1}$	$B_1 N_2$	$B_1 N_3$
Round 1						
S	$\boldsymbol{B_0}$	B_1	$\boldsymbol{B_0 N_0^S}$	$\boldsymbol{B_0 N_1^S}$	$B_1 N_2^S$	$B_1 N_3^S$
SR	$\boldsymbol{B_0}$	B_1	$\boldsymbol{B_0 N_0^S}$	$B_1 N_3^S$	$B_1 N_2^S$	$\boldsymbol{B_0 N_1^S}$
MC	$\boldsymbol{B_0}$	B_1	$\boldsymbol{N_0^*}$	$\boldsymbol{N_1^*}$	$\boldsymbol{N_2^*}$	$\boldsymbol{N_3^*}$
Add key	$\boldsymbol{B_2}$	B_1	$\boldsymbol{B_2 N_0^*}$	$\boldsymbol{B_2 N_1^*}$	$\boldsymbol{N_2^*}$	$\boldsymbol{N_3^*}$
	$\boldsymbol{B_3}$	B_1	$\boldsymbol{B_2 N_0^*}$	$\boldsymbol{B_2 N_1^*}$	$\boldsymbol{B_3 N_2^*}$	$\boldsymbol{B_3 N_3^*}$
Round 2						
S	$\boldsymbol{B_3}$	B_1	$\boldsymbol{N_0'^S}$	$\boldsymbol{N_1'^S}$	$\boldsymbol{N_2'^S}$	$\boldsymbol{N_3'^S}$
SR	$\boldsymbol{B_3}$	B_1	$\boldsymbol{N_0'^S}$	$\boldsymbol{N_3'^S}$	$\boldsymbol{N_2'^S}$	$\boldsymbol{N_1'^S}$
Add key	$\boldsymbol{B_3^{RSC}}$	B_1	$\boldsymbol{B_3^{RSC} N_0^{**}}$	$\boldsymbol{B_3^{RSC} N_1^{**}}$	$\boldsymbol{B_3^{RSC} N_2^{**}}$	$\boldsymbol{B_3^{RSC} N_3^{**}}$
	$\boldsymbol{B_2}$	B_1	$\boldsymbol{B_4 N_0^{**}}$	$\boldsymbol{B_4 N_1^{**}}$	$\boldsymbol{B_5 N_2^{**}}$	$\boldsymbol{B_5 N_3^{**}}$

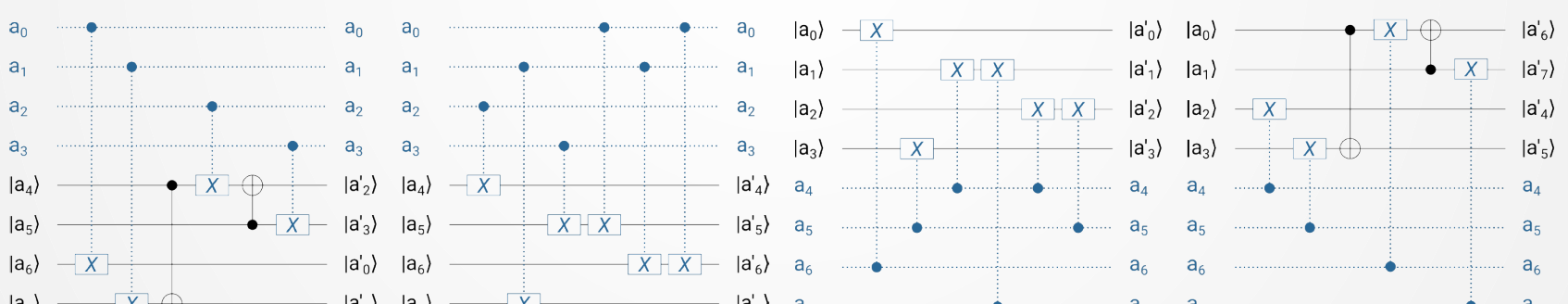
Сплит-атака на утечку B_0

25 кубитов

Добавляется атака на преобразование MC, генерирующая половину результата

Идея – разделить используемый объём кубитов во времени

SR	$\boldsymbol{B_0}$	B_1	$\boldsymbol{B_0 N_0}^S$	$B_1 N_3{}^S$	$B_1 N_2{}^S$	$\boldsymbol{B_0 N_1}^S$
MC	$\boldsymbol{B_0}$	B_1	$\boldsymbol{N_0^*}$	$\boldsymbol{N_1^*}$	$\boldsymbol{N_2^*}$	$\boldsymbol{N_3^*}$



(a) MC_0^0 (b) MC_0^1 (c) MC_1^0 (d) MC_1^1

Сплит-атака на утечку B_0

Action	Key	Text				Ancilla
Init	B_0, $\boldsymbol{B_1}$	N_0	N_1	N_2	N_3	
Add key	B_0, $\boldsymbol{B_1}$	B_0N_0	B_0N_1	$\boldsymbol{B_1N_2}$	$\boldsymbol{B_1N_3}$	
Round 1						
S, SR	B_0, $\boldsymbol{B_1}$	$B_0N_0^S$	$\boldsymbol{B_1N_3^S}$	$\boldsymbol{B_1N_2^S}$	$B_0N_1^S$	
MC_0^0, MC_1^1	B_0, $\boldsymbol{B_1}$	$\boldsymbol{N_0^*}$		$\boldsymbol{N_3^*}$		
Add key	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3}$	$\boldsymbol{B_2N_0^*}$		$\boldsymbol{B_3N_3^*}$		
Round 2.1						
S, SR	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3^{RSC}}$	$\boldsymbol{N_0'^S}$	$\boldsymbol{N_3'^S}$	-	-	
Add key	B_0, $\boldsymbol{B_4}$ $\boldsymbol{B_3^{RSC}}$	$\boldsymbol{B_4N_0'^S}$	$\boldsymbol{B_4N_3'^S}$	-	-	$\boldsymbol{X_0}$
Data recovery						
Add key†	B_0, $\boldsymbol{B_4}$ $\boldsymbol{B_3^{RSC}}$	$\boldsymbol{N_0'^S}$	$\boldsymbol{N_1'^S}$	-	-	$\boldsymbol{X_0}$
SR†, S†	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3^{RSC}}$	$\boldsymbol{N_0'}$	-	$\boldsymbol{N_3'}$	-	$\boldsymbol{X_0}$
Add key†	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3}$	$\boldsymbol{N_0^*}$		$\boldsymbol{N_3^*}$		$\boldsymbol{X_0}$
$MC_0^{0\dagger}$, $MC_1^{1\dagger}$	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3}$	$B_0N_0^S$	$\boldsymbol{B_1N_3^S}$	$\boldsymbol{B_1N_2^S}$	$B_0N_1^S$	
Round 2.2						
MC_0^1, MC_1^0	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3}$	$\boldsymbol{N_1^*}$		$\boldsymbol{N_2^*}$		$\boldsymbol{X_0}$
Add key	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3}$	$\boldsymbol{B_2N_1^*}$		$\boldsymbol{B_3N_2^*}$		$\boldsymbol{X_0}$
S, SR	B_0, $\boldsymbol{B_2}$, $\boldsymbol{B_3^{RSC}}$	-	-	$\boldsymbol{N_2'^S}$	$\boldsymbol{N_1'^S}$	$\boldsymbol{X_0}$
Add key	B_0, $\boldsymbol{B_4}$ $\boldsymbol{B_3}$	-	-	$\boldsymbol{B_4N_2'^S}$	$\boldsymbol{B_5N_1'^S}$	$\boldsymbol{X_0}$

25 кубитов при утечке B_0

17 кубитов при утечке B_1

Возникает понятие “промежуточного раунда”

Если получилось разделить данные по 8 бит,
можно ли разделить их по 4?

Двойная сплит-атака на утечку B_0^0

infotecs

Action	Key	Text	Ancilla
Init	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$N_0,\ N_1,\ N_2,\ N_3$	
Round 1.1			
AddTxt, S, SR	$\underline{(B_0^0 N_0)^S, (\boldsymbol{B_1^1 N_3})^{\boldsymbol{S}}},\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0}$		
$MC_0^0,\ S^\dagger$, AddTxt	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_0^*}$	
Add key	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ (\boldsymbol{B_1^1})^{\boldsymbol{SC}}$	$\boldsymbol{N_0' = B_2^0 N_0^* = B_0^0 (B_1^1)^{SC} N_0^*}$	
Round 2.1			
S, SR, AddKey	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_0'' = B_4^0 (N_0')^S = = B_0^0 (B_1^1)^{SC} (B_1^1 B_0^1 (B_1^0)^{SC})^{SC} (N_0')^S}$	$\boldsymbol{X_0}$
Round 1.2			
Data recovery	$\underline{(B_0^0 N_0)^S, (\boldsymbol{B_1^1 N_3})^{\boldsymbol{S}}},\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0}$		$\boldsymbol{X_0}$
$MC_0^1,\ S^\dagger$, AddTxt	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_1^*}$	$\boldsymbol{X_0}$
Add key	$B_0^0,\ \boldsymbol{B_0^1},\ (\boldsymbol{B_1^0})^{\boldsymbol{SC}},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_1' = B_2^1 N_1^* = B_0^1 (B_1^0)^{SC} N_0^*}$	$\boldsymbol{X_0}$
Round 2.2			
S, SR, AddKey	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_3'' = B_5^1 (N_1')^S = = B_1^1 (B_1^0 B_1^1 B_0^0 (B_1^1)^{SC})^{SC} (N_1')^S}$	$\boldsymbol{X_0, X_3}$

Двойная сплит-атака на утечку B_0^0

Round 1.3			
Data recovery, AddTxt, S, SR	$B_0^0,\ \boldsymbol{B_1^1},\ \underline{(\boldsymbol{B_1^0 N_2})^S, (\boldsymbol{B_0^1 N_1})^S}$		$\boldsymbol{X_0, X_3}$
MC_0^0, $S^\dagger$, AddTxt	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_2^*}$	$\boldsymbol{X_0, X_3}$
Add key	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ (\boldsymbol{B_1^1})^{SC}$	$\boldsymbol{N_2' = B_3^0 N_2^* = B_1^0 B_0^0 (B_1^1)^{SC} N_2^*}$	$\boldsymbol{X_0, X_3}$
Round 2.3			
S, SR, AddKey	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_2'' = B_5^0 (N_2')^S = B_1^0 (B_3^1)^{SC} (N_2')^S = = B_1^0 (B_1^1 B_0^1 (B_1^0)^{SC})^{SC} (N_2')^S}$	$\boldsymbol{X_0, X_2 X_3}$
Round 1.4			
Data recovery	$B_0^0,\ \boldsymbol{B_1^1},\ \underline{(\boldsymbol{B_1^0 N_2})^S, (\boldsymbol{B_0^1 N_1})^S}$		$\boldsymbol{X_0, X_2 X_3}$
MC_0^1, $S^\dagger$, AddTxt	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_3^*}$	$\boldsymbol{X_0, X_2 X_3}$
Add key	$B_0^0,\ \boldsymbol{B_0^1},\ (\boldsymbol{B_1^0})^{SC},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_3' = B_3^1 N_3^* = B_1^1 B_0^1 (B_1^0)^{SC} N_3^*}$	$\boldsymbol{X_0, X_2 X_3}$
Round 2.4			
S, SR, AddKey	$B_0^0,\ \boldsymbol{B_0^1},\ \boldsymbol{B_1^0},\ \boldsymbol{B_1^1}$	$\boldsymbol{N_1'' = B_4^0 (N_3')^S = B_2^0 (B_3^1)^{SC} (N_1')^S = = B_2^0 (B_1^1 B_0^1 (B_1^0)^{SC})^{SC} (N_1')^S}$	$\boldsymbol{X_0, X_2 X_3}$

Выводы: сплит-атака

Атака “в стойке”

- 19 или 17 кубитов для утечки одного полубайта
  15 кубитов для утечки пары полубайтов
  11 кубитов для утечки трёх полубайтов
- 23 кубита для атаки в общем случае
  Новый рекорд
  Кубитов меньше, чем битов в тексте с ключом
- Универсальность и масштабируемость
  Атаки в стойке и на GPU
  Возможность экстраполяции до полного AES

Что дальше?

- AES
- Априорное распределение
- Инвертированный оракул
- Специфичное шумоподавление
- Оптимизированная атака VQE

infotecs

Благодарю за внимание!

Алексей Моисеевский

+7 968 016 97 32

Aleksey.Moiseevsky@infotecs.ru
amoiseevskiy@gmail.com