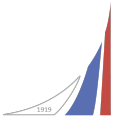
Сложность решения систем полиномиальных уравнений с помощью квантового алгоритма Гровера на примере блочного алгоритма шифрования КБ-256

Коренева А.М.[1,2], Поляков М.В.[1,3]

[1]ООО «Код Безопасности»
[2]Финансовый университет при Правительстве РФ
[3]МГТУ им. Н.Э. Баумана

20 марта 2025



Описание КБ-256

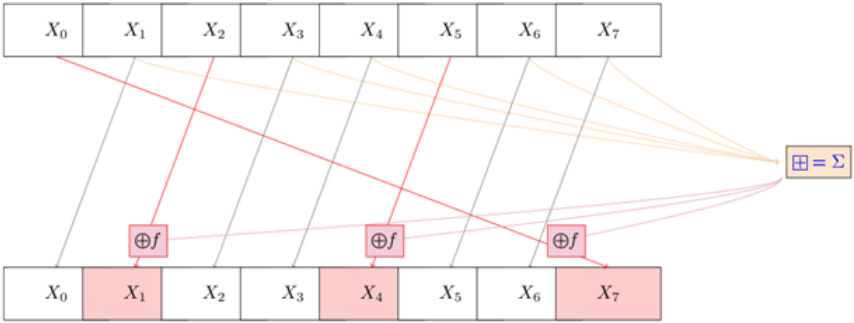
- Обобщенная сеть Фейстеля на 8 регистрах;
- Длина блока – 256 бит, длина ключа – 256 бит;
- Раундовая функция $\mathbb{Z}_2^{256} \times \mathbb{Z}_2^{96} \to \mathbb{Z}_2^{256}$:

$$\overline{X} = (X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7) \to$$
$$\left(X_1, X_2 \oplus f\left(\Sigma\left(\overline{X}\right) \boxplus b_0^{(i)}\right), X_3, X_4, X_5 \oplus f\left(\Sigma\left(\overline{X}\right) \boxplus b_1^{(i)}\right), X_6, X_7, X_0 \oplus f\left(\Sigma\left(\overline{X}\right) \boxplus b_2^{(i)}\right)\right)$$

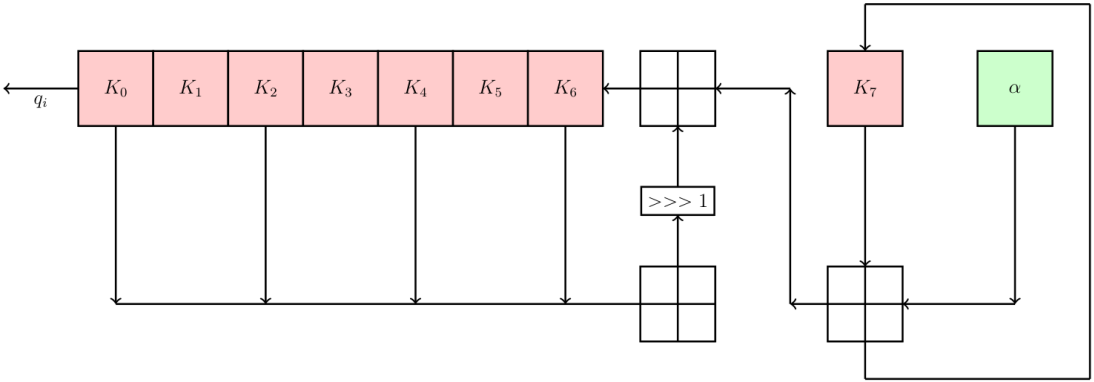
где

- $\Sigma(X_0, X_1, \ldots, X_7) = X_1 \boxplus X_3 \boxplus X_4 \boxplus X_6 \boxplus X_7$, $X_i \in \mathbb{Z}_2^{32}$;
- $f\left(X_0, X_1, \ldots, X_7\right) = (\pi_0(X_0), \pi_1(X_1), \ldots, \pi_7(X_7)) <<< 19$, $\pi_i \in S\left(\mathbb{Z}_2^4\right)$ – подстановки из ГОСТ 34.12 – 2018 «Магма».

Раундовая функция КБ-256



Ключевая развертка



$$X_{i+7} = ((X_i \boxplus X_{i+2} \boxplus X_{i+4} \boxplus X_{i+6}) >>> 1) \boxplus K_i \boxplus \alpha$$

Алгоритм Гровера для КБ-256. Сложность

- Наличие 1 пары открытого/шифрованного текстов;
- Схемная сложность оракула:
  - 865 кубитов;
  - Реализация S-блоков: 240 гейтов;
  - 5 узлов суммирования в кольце $\mathbb{Z}_{2^{32}}$: 1080 гейтов;
  - В ключевом расписании: $112 \cdot 7 \cdot 216 = 169344$ гейта;
  - Итого с экономией кубитов $\frac{\pi}{4} \cdot 2^{128} \cdot (2 \cdot 18 \cdot 2832 + 169344) = \frac{\pi}{4} \cdot 2^{128} \cdot 271296$.

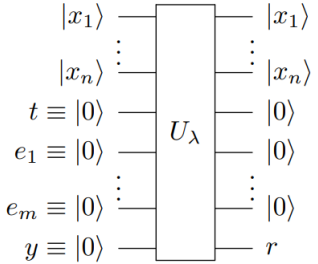
Система полиномиальных уравнений с PolyBori

- Строится программное описание шифра
- По данному описанию строится система полиномиальных уравнений над полем $\mathbb{Z}_2$:
  - Уравнения строятся также по 1 паре открытого и шифрованного текстов;
  - Учет ключевого расписания добавляет промежуточные переменные в системе;

```
sage: F
Polynomial Sequence with 2640 Polynomials in 1520 Variables
sage: F.part(2)
(w020000 + k010000 + x010000 + x010001 + x010003 + x010501 + x010502 + x011000 + x011002 + x011003 + x011500 + x011502 + x011503,
 w020001 + k010001 + x010000 + x010001 + x010002 + x010502 + x010503 + x011000 + x011001 + x011003 + x011500 + x011501 + x011503 + 1,
 w020002 + k010002 + x010000 + x010001 + x010502 + x011000 + x011001 + x011002 + x011500 + x011501 + x011502 + 1,
 w020003 + k010003 + x010000 + x010002 + x010003 + x010500 + x010501 + x011001 + x011002 + x011003 + x011501 + x011502 + x011503,
 w020100 + k010100 + x010000 + x010002 + x010003 + x010500 + x010501 + x010503 + x011001 + x011002 + x011500 + x011502 + x011503,
 w020101 + k010101 + x010000 + x010001 + x010003 + x010500 + x010501 + x010502 + x011002 + x011003 + x011500 + x011501 + x011503 + 1,
 w020102 + k010102 + x010000 + x010001 + x010002 + x010500 + x010501 + x011002 + x011500 + x011501 + x011502 + 1,
 w020103 + k010103 + x010001 + x010002 + x010003 + x010500 + x010502 + x010503 + x011000 + x011001 + x011501 + x011502 + x011503,
 w020200 + k010200 + x010000 + x010002 + x010003 + x010500 + x010502 + x010503 + x011000 + x011001 + x011003 + x011501 + x011502,
 w020201 + k010201 + x010000 + x010001 + x010003 + x010500 + x010501 + x010503 + x011000 + x011001 + x011002 + x011502 + x011503 + 1,
 w020202 + k010202 + x010000 + x010001 + x010002 + x010500 + x010501 + x010502 + x011000 + x011001 + x011502 + 1,
 w020203 + k010203 + x010001 + x010002 + x010003 + x010501 + x010502 + x010503 + x011000 + x011002 + x011003 + x011500 + x011501,
 w020300 + k010300 + x010001 + x010002 + x010500 + x010502 + x010503 + x011000 + x011002 + x011003 + x011500 + x011501 + x011503,
 w020301 + k010301 + x010002 + x010003 + x010500 + x010501 + x010503 + x011000 + x011001 + x011003 + x011500 + x011501 + x011502 + 1,
 w020302 + k010302 + x010002 + x010500 + x010501 + x010502 + x011000 + x011001 + x011002 + x011500 + x011501 + 1,
 w020303 + k010303 + x010000 + x010001 + x010501 + x010502 + x010503 + x011001 + x011002 + x011003 + x011500 + x011502 + x011503,
 w020400 + k010400 + x010300 + x010302 + x010303 + x010400 + x010401 + x010403 + x010901 + x010902 + x011400 + x011402 + x011403,
 w020401 + k010401 + x010300 + x010301 + x010303 + x010400 + x010401 + x010402 + x010902 + x010903 + x011400 + x011401 + x011403 + 1,
 w020402 + k010402 + x010300 + x010301 + x010302 + x010400 + x010401 + x010902 + x011400 + x011401 + x011402 + 1,
 w020403 + k010403 + x010301 + x010302 + x010303 + x010400 + x010402 + x010403 + x010900 + x010901 + x011401 + x011402 + x011403,
 w020500 + k010500 + x010300 + x010302 + x010303 + x010400 + x010402 + x010403 + x010900 + x010901 + x010903 + x011401 + x011402,
 w020501 + k010501 + x010300 + x010301 + x010303 + x010400 + x010401 + x010403 + x010900 + x010901 + x010902 + x011402 + x011403 + 1,
 w020502 + k010502 + x010300 + x010301 + x010302 + x010400 + x010401 + x010402 + x010900 + x010901 + x011402 + 1,
 w020503 + k010503 + x010301 + x010302 + x010303 + x010401 + x010402 + x010403 + x010900 + x010902 + x010903 + x011400 + x011401,
 w020600 + k010600 + x010301 + x010302 + x010400 + x010402 + x010403 + x010900 + x010902 + x010903 + x011400 + x011401 + x011403,
 w020601 + k010601 + x010302 + x010303 + x010400 + x010401 + x010403 + x010900 + x010901 + x010903 + x011400 + x011401 + x011402 + 1,
 w020602 + k010602 + x010302 + x010400 + x010401 + x010402 + x010900 + x010901 + x010902 + x011400 + x011401 + 1,
```

Квантовый оракул для системы

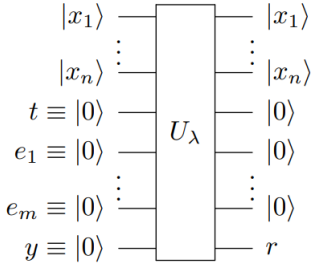
- Для решения системы можно также применять алгоритм Гровера с оракулом вида[1]



[1] P. Schwabe and B. Westerbaan. Solving binary MQ with Grover's algorithm.

Квантовый оракул для системы

- Для решения системы можно также применять алгоритм Гровера с оракулом вида[1]



- Регистры $|x_1\rangle, \ldots, |x_n\rangle$ – неизвестные переменные системы (биты ключа);
- Регистры $|e_1\rangle, \ldots, |e_m\rangle$ – для уравнений системы;
- Регистры $|t\rangle, |y\rangle$ – вспомогательные ($|y\rangle$ будет равен 1 при найденном решении системы).

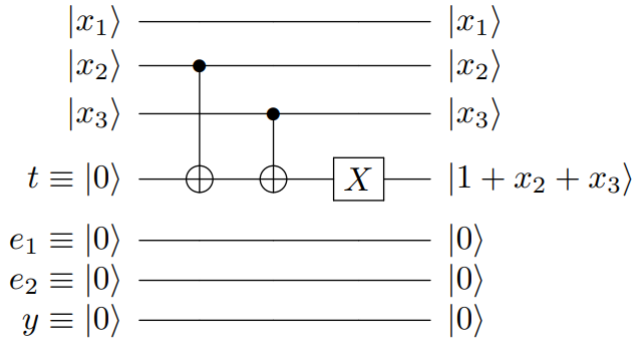
[1] P. Schwabe and B. Westerbaan. Solving binary MQ with Grover's algorithm.

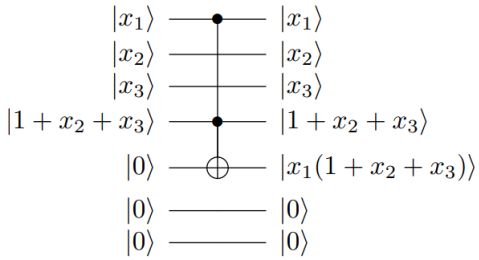
Квантовый оракул для системы

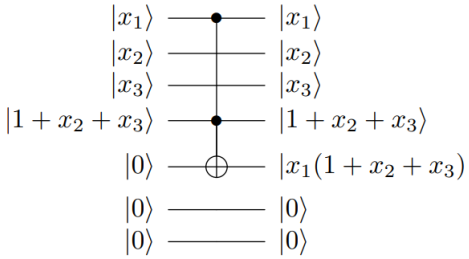
- Пусть имеется два уравнения

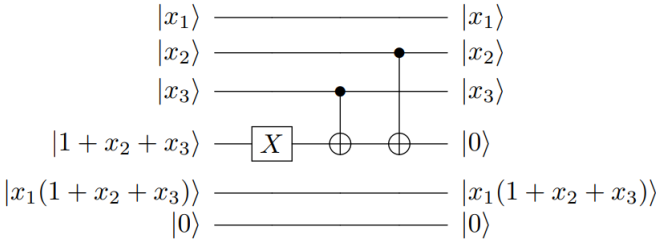
$$x_1(x_2 \oplus x_3 \oplus 1) + \ x_2x_3 = 1,$$
$$x_2(1 \oplus x_3) = 1$$

оракул можно построить следующим образом:




$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|1 + x_2 + x_3\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|1 + x_2 + x_3\rangle$
$|x_1(1 + x_2 + x_3)\rangle$
$|0\rangle$
$|0\rangle$


$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|1 + x_2 + x_3\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|1 + x_2 + x_3\rangle$
$|x_1(1 + x_2 + x_3)$
$|0\rangle$
$|0\rangle$


$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|1 + x_2 + x_3\rangle$
$|x_1(1 + x_2 + x_3)\rangle$
$|0\rangle$
X
$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|0\rangle$
$|x_1(1 + x_2 + x_3)\rangle$
$|0\rangle$

Квантовый оракул для системы. Сложность

- Потребуется $1008 + 7488 + 2 = 8498$ кубитов;
- Квантовых гейтов для системы (с экономией кубитов): 31207681.

Спасибо за внимание!