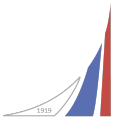
О стойкости алгоритма блочного шифрования КБ-256 к атакам с использованием квантовых алгоритмов

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

21 марта 2024



Описание КБ-256

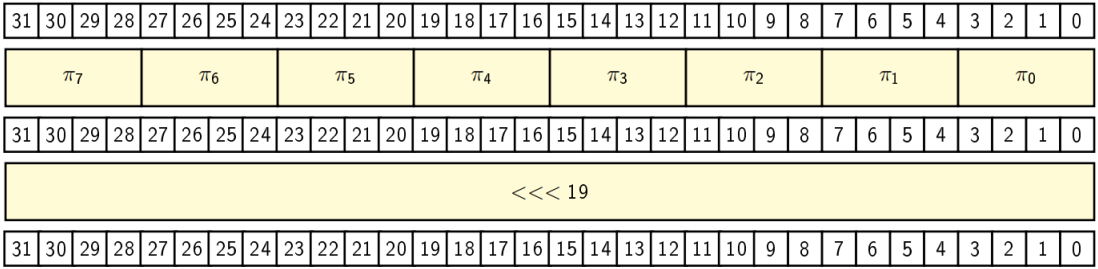
- Обобщенная сеть Фейстеля на 8 регистрах;
- Длина блока – 256 бит, длина ключа – 256 бит;
- Раундовая функция $\mathbb{Z}_2^{256} \times \mathbb{Z}_2^{96} \to \mathbb{Z}_2^{256}$:

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

где

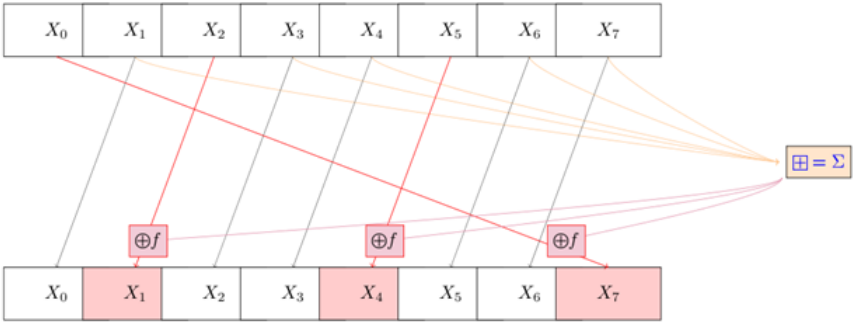
- $\Sigma(X_0, X_1, \ldots, X_7) = X_1 \boxplus X_3 \boxplus X_4 \boxplus X_6 \boxplus X_7,\ X_i \in \mathbb{Z}_2^{32}$;
- $f\left(X_0, X_1, \ldots, X_7\right) = (\pi_0(X_0), \pi_1(X_1), \ldots, \pi_7(X_7)) <<< 19,\ \pi_i \in\ S\left(\mathbb{Z}_2^4\right)$ – подстановки из ГОСТ 34.12 – 2018 «Магма».

Раундовое преобразование f



Схематичное изображение раундового преобразования f

Раундовая функция КБ-256

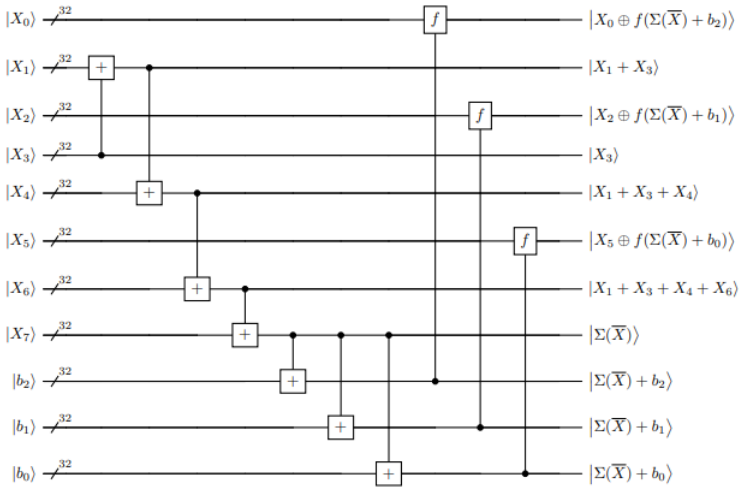


Квантовая схема одного раунда

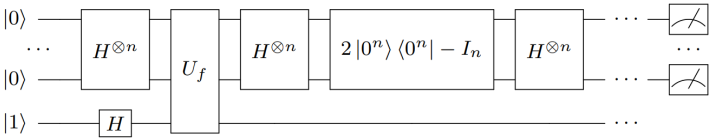
Для реализации одного раунда КБ-256 в виде квантовой схемы потребуется:

- 3 раза реализовать подстановки из ГОСТ 34.12 – 2018 «Магма»;
- 7 раз реализовать узел суммирования по модулю 2^{32};
- 8 квантовых регистров для состояний $|X_0\rangle, \ldots, |X_7\rangle$;
- 3 квантовых регистра для раундовых ключей $\left|b_0^{(i)}\right\rangle, \left|b_1^{(i)}\right\rangle, \left|b_2^{(i)}\right\rangle$.

Квантовая схема одного раунда



Алгоритм Гровера. Алгоритм Саймона



Алгоритм Гровера. Для функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ находит такие x, что $f(x) = 1$ за $\left[\frac{\pi}{4}\sqrt{\frac{2^n}{m}}\right]$ итераций.

Алгоритм Саймона. Для функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ находит такой $a \in \mathbb{Z}_2^n \setminus \{0\}$, что

$$F(x) \oplus F(x \oplus a) = 0$$

за $O(n)$ итераций схемы с квантовым оракулом U_F.

Сложность схемной реализации

- 11 квантовых регистров – 352 кубита;
- Количество квантовых вентилей – 1752:
  - Сложность одного оператора суммирования: $(7n - 8)$. Получаем $7 \cdot (7n - 8) = 1512$ [1];
  - Реализация подстановок – 240 вентилей [2]
- В алгоритме КБ-256 18 раундов. При реализации с экономией кубитов получаем
  - $2 \cdot 18 \cdot 1752 = 63072$ гейтов;
  - 352 кубита.

[1] Yasuhiro T. et al. Quantum Addition Circuits and Unbounded Fan-Out

[2] Dasu V. A. et al. LIGHTER-R: Optimized Reversible Circuit Implementation For SBoxes

Алгоритм Гровера для КБ-256. Сложность

- По расстоянию единственности

$$n \geqslant \left\lceil \frac{256}{256} \right\rceil = 1,$$

  т.е. потребуется 1 пара открытого/шифрованного текстов.
- В схеме алгоритма Гровера с КБ-256 в качестве оракула потребуется:
  - $352 + 1 \cdot 256 + 1 = 865$ кубитов.
- Количество гейтов: $\frac{\pi}{4} \cdot 2^{128} \cdot 64103$.

Построение квантового различителя

Для раундового преобразования $f^{(i)}$ сети Фейстеля на d регистрах:

$$f^{(d-1)}\left(f^{(d-2)}\left(\dots f^{(3)}\left(f^{(2)}\left(f^{(1)}\left(X_0^{(0)}\right)\oplus X_1^{(0)}\right)\oplus X_2^{(0)}\right)\dots\oplus X_{d-2}^{(0)}\right)\oplus X_{d-1}^{(0)}\right)\oplus X_d^{(0)}.$$

Фиксируем $X_1^{(0)},\dots,X_d^{(0)}$, а $X_0^{(0)}=\gamma_b$, $b\in\mathbb{Z}_2$. Тогда, если у функции

$$g(b,x)=f^{(d)}\left(h(\gamma_b)\oplus x\right)$$

существует период вида

$$(1,h\left(\gamma_0\right)\oplus h\left(\gamma_1\right)),$$

то можно построить различитель на $2d-1$ раундов такой сети Фейстеля[3].

[3] Dong X.Y, et al. Quantum Key-Recovery Attack on Feistel Structures

Наличие нетривиального периода

- Обозначим входной блок о.т.

$$\overline{X}^{(0)} = \left(X_0^{(0)}, X_1^{(0)}, \ldots, X_7^{(0)}\right);$$

- $f\left(\alpha^{(i)}, b_j^{(i)}\right)$ – раундовое преобразование f на i-м раунде, $b_j^{(i)}$ – раундовый ключ ($j = 0, 1, 2$);
- $\alpha^{(i)} = \Sigma\left(X_0^{(i)}, X_1^{(i)}, \ldots, X_7^{(i)}\right)$

$$
\begin{aligned}
X_0^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus X_4^{(0)}, \\
X_1^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_1^{(1)}\right) \oplus X_5^{(0)}, \\
X_2^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_2^{(3)}\right) \oplus X_6^{(0)}, \\
X_3^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_1^{(3)}\right) \oplus X_7^{(0)}, \\
X_4^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_1^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_2^{(1)}\right) \oplus X_0^{(0)}, \\
X_5^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_1^{(3)}\right) \oplus X_1^{(0)}, \\
X_6^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_0^{(1)}\right) \oplus X_2^{(0)}, \\
X_7^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus f^{(2)}\left(\alpha^{(2)}, b_0^{(2)}\right) \oplus X_4^{(0)}.
\end{aligned}
$$

Наличие нетривиального периода

Из выписанных уравнений можно заметить, что:

- $X_1^{(4)} = f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_1^{(1)}\right) \oplus X_5^{(0)}$
- $X_4^{(4)} = f^{(3)}\left(\alpha^{(3)}, b_1^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_2^{(1)}\right) \oplus X_0^{(0)}$

Т.е. мы имеем соотношения, связывающие входной блок о.т. с выходом 4-го раунда. А теперь, если расписать функцию $f^{(i)}(\alpha^{(i)}, b_j^{(i)})$:

- $f^{(1)}\left(\alpha^{(1)}, b_1^{(1)}\right) = S\left(\Sigma\left(\overline{X}^{(0)}\right) \boxplus b_1^{(1)}\right) <<< 19$

Наличие нетривиального периода

- Получается, что перемешивающие свойства преобразований $\Sigma\left(\overline{X}^{(i)}\right)$ и $f^{(i)}\left(\alpha^{(i)}, b_j^{(i)}\right)$ не позволяют в явном виде выписать уравнение периодической функции для алгоритма Саймона.

Спасибо за внимание!