УДК 003.26.09

КВАНТОВА АТАКА РОЗРІЗНЮВАННЯ НА РОЗШИРЕНУ УЗАГАЛЬНЕНУ МЕРЕЖУ ФЕЙСТЕЛЯ

Б. В. Дигас[1,a]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі проаналізовано розширену узагальнену Фейстель-подібну схему, запропоновану Бергером на ін., та побудовано квантову атаку розрізнювання на дану схему за обраним відкритим текстом з поліноміальною складністю.

Отриманий результат означає, що досліджувана схема не є стійкою в квантовій моделі обчислень як мінімум до зазначеного типу атак.

Ключові слова: Фейстель-подібні схеми, квантова атака розрізнювання, алгоритм Саймона

Вступ

У 1997 році Даніель Саймон сформулював задачу Саймона, а також сформулював алгоритм її розв'язку за поліноміальний час в квантовій моделі обчислень [1]. Потім, в 2010 році, Кувакадо та Морі використали цей алгоритм і побудували атаку розрізнювання на класичну трьохраундову схему Фейстеля за поліноміальний час, а саме побудували функцію від шифротексту, виділили в ній період та звели атаку розрізнювання до задачі Саймона [2].

З тих пір досліджувались схожі атаки на узагальнені мережі Фейстеля запропоновані, Гоангом та Рогевеєм в 2010 році [3]. Прикладами таких атак є атаки на GFN Type 1, Type 2 [4], [5] та Type 3 [6].

В 2013 році Бергер та Мін'є ввели новий спосіб представлення узагальнених мереж Фейстеля у вигляді матриць та на його основі створили нову схему шифрування, яка отримала назву розширена узагальнена мережа Фейстеля або EGFN (з англ. Extended Generalized Feistel Network). Використовуючи EGFN, вони подали нову схему, для якої після 4 раундів шифрування шифротекст досягає повного розсіювання [7]. Для зручності в даній роботі називатимемо цю схему схемою Бергера.

Метою роботи є побудова квантової атаки розрізнювання на схему Бергера.

1. Опис розширених узагальнених мереж Фейстеля та схеми Бергера

У роботі [7] Бергер запропонував матричний спосіб представлення різноманітних узагальнених мереж Фейстеля (з англ. General Feistel Network). Основна ідея ґрунтується в розділенні схеми на два етапи, для кожного з яких визначається матриця: етап раундового шифрування $\mathscr{F}$ та етап перестановки $\mathscr{P}$. Кожна матриця задає свій етап шифрування, а їхній добуток $\mathscr{M} = \mathscr{F} \times \mathscr{P}$ задає всю схему.

Це дозволило аналізувати властивості схеми ґрунтуючись виключно на властивостях матриць. Тоді Бергер, не знайшовши оптимальнішої GFN схеми за наявні, додав ще один етап до шифрування – лінійний, з матрицею $\mathscr{L}$, і назвав цей тип матриць **EGFN**: $\mathscr{M} = \mathscr{F} \times \mathscr{L} \times \mathscr{P}$. Приклад матриць та схеми, яку вони задають, наведено на рисунках 1 та 2 відповідно. Зауважимо, що в матрицях $\mathscr{L}$ та $\mathscr{F}$, формальні параметри I та F на позиції (i, j) позначають раундову функцію чи лінійне з'єднання від x_j до x_i.

$$\mathscr{M} = \begin{pmatrix} I & F & 1 & \\ F & I & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix} \quad \mathscr{P} = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}$$

$$\mathscr{L} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ I & & 1 & \\ & I & & 1 \end{pmatrix} \quad \mathscr{F} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & F & 1 & \\ F & & & 1 \end{pmatrix}$$

Рис. 1. Приклад матриці EGFN

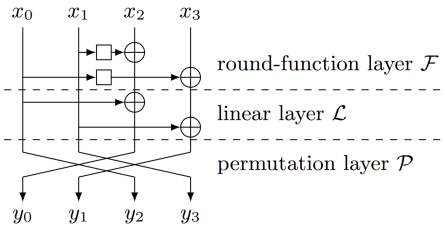

Рис. 2. Приклад схеми EGFN

Використовуючи EGFN, була створена схема Бергера, що задається схемою на рисунку 3 та матрицею $\mathscr{M}$ для $k = 2^i, i \in \mathbb{N}$:

$$\mathscr{M} = \begin{pmatrix} (0) & & & F & 1 & & \\ & \ddots & & I & & \ddots & \\ & & (0) & \vdots & & & \\ F & I & \dots & I & & & 1 \\ 1 & & & & & & \\ & \ddots & & & & (0) & \\ & & & 1 & & & \end{pmatrix}.$$

[a] bogddygas-ipt24@lll.kpi.ua

Також доведено, що ця схема досягає повного розсіювання за 4 раунди для $k \geq 4$ і з меншою обчислювальною складністю [7, теорема 7].

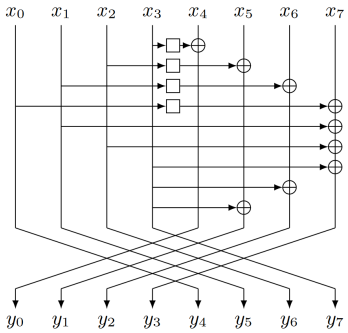

Рис. 3. Схема Бергера для $k = 8$

2. Опис квантового алгоритму Саймона

Алгоритм Саймона вирішує задачу Саймона [1]:

Задача 1 (Саймона). *Нехай $f : \{0,1\}^n \to \{0,1\}^n$ – функція, що для всіх $x, y \in \{0,1\}^n$ і $x \neq y$, $f(x) = f(y)$ тоді й тільки тоді, коли $x = y \oplus s$. За умови, що можливо робити запити до оракула O_f функції f, знайдіть s.*

Тотожність 1 також називають умовою Саймона:

$$\forall x, y : x \neq y, f(x) = f(y) \Leftrightarrow x = y \oplus s. \qquad (1)$$

Розглянемо роботу алгоритма Саймона:

Алгоритм 1. Алгоритм Саймона.

Вхід: $n, O_f : |x\rangle|0\rangle \to |x\rangle|f(x)\rangle$.
Вихід: y, де $y \cdot s = 0, y \in \{0,1\}^n$.

1. Ініціалізуємо два n-кубітних регістра $|\psi_0\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes n}$ і застосовуємо вентиль Адамара до першого регістру, отримуємо:
$$|\psi_1\rangle = H^{\otimes n}(|0\rangle)|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle.$$
2. Виконуємо квантовий запит до оракулу O_f, після цього отримуємо стан:
$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle.$$
3. Вимірюємо другий регістр, отримуємо $f(z)$, де $z \in \{0,1\}^n$. Перший регістр змінюється при цьому в стан:
$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}}(|z\rangle + |z \oplus s\rangle).$$
4. Застосовуємо вентиль Адамара до першого регістру, в ньому отримуємо стан:
$$|\psi_4\rangle = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{y \cdot z}(1 + (-1)^{y \cdot s})|y\rangle.$$
5. Після вимірювання стану отримуємо y, яке відповідає умові $y \cdot s = 0$.

Очевидно, що після $\mathcal{O}(n)$ виконань алгоритму 1 та розв'язання отриманої системи лінійних рівнянь, буде знайдено період s.

Схема квантового алгоритму Саймона наведена на рисунку 4.

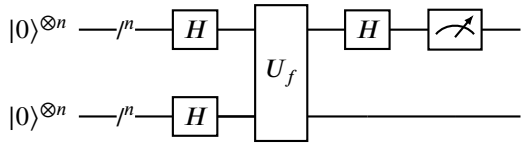

Рис. 4. Схема квантового алгоритму Саймона

3. Побудова квантової атаки розрізнювання на схему Бергера

Розглянемо схему Бергера для $k = 4$ на рисунку 5, і обчислимо результати кожного виходу після чотирьох раундів. Нехай вхідне повідомлення це $4n$-бітний вектор розбитий на 4 рівні частини:

$$x = x_1 \| x_2 \| x_3 \| x_4, \text{ де } x_1, x_2, x_3, x_4 \in \{0,1\}^n.$$

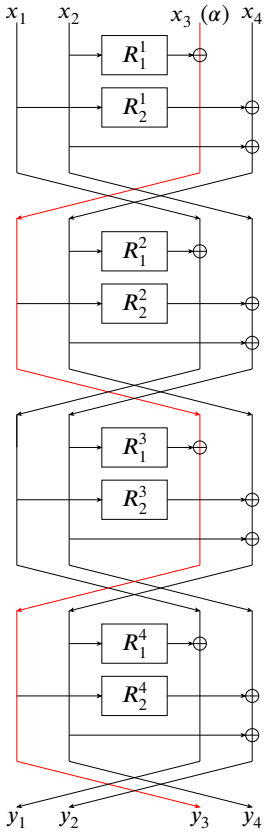

Рис. 5. 4-раундова схема Бергера для $k = 4$

Нехай R_j^i – раундова функція, яка отримує n-бітний секретний ключ k_j^i, де i це номер раунду, а j – номер раундової функції. Третій блок y_3 в четвертому раунді набуває наступного значення:

$$W(x) = W(x_1 \| x_2 \| x_3 \| x_4) =$$
$$= R_1^3(R_2^2(R_1^1(x_2) \oplus x_3) \oplus R_2^1(x_1) \oplus x_4) \oplus R_1^1(x_2) \oplus x_3.$$

Визначимо функцію $f : \{0,1\}\times\{0,1\}^n \to \{0,1\}^n$:

$$f(b \parallel x_4) = \begin{cases} W(x_1 \parallel x_2 \parallel \alpha \parallel x_4) \oplus \beta, & \text{якщо } b = 0 \\ W(x_1 \parallel x_2 \parallel \beta \parallel x_4) \oplus \alpha, & \text{якщо } b = 1 \end{cases},$$

де α і β – випадкові n-бітні вектори, а x_1, x_2 – фіксовані вхідні n-бітні вектори.

Твердження 3.1. *$f(b \parallel x_4) = f(b \oplus 1 \parallel x_4 \oplus h_\alpha \oplus h_\beta)$ тоді й тільки тоді, коли функція f має період $s = 1 \parallel h_\alpha \oplus h_\beta$.*

Доведення. Доведемо, що:

$$f(b \parallel x_4) = f(b' \parallel x_4') \Leftrightarrow b' = b \oplus 1 \;\&\; x_4' = x_4 \oplus h_\alpha \oplus h_\beta,$$

де $h_\alpha = R_2^2(R_1^1(x_2) \oplus \alpha)$, $h_\beta = R_2^2(R_1^1(x_2) \oplus \beta)$.

- $(\Rightarrow)$:
  - ▶ Нехай $b = b' = 0$, тоді:

$$f(b \parallel x_4) = W(x_1 \parallel x_2 \parallel \alpha \parallel x_4) \oplus \beta =$$
$$= \underline{R_1^3(h_\alpha \oplus R_2^1(x_1) \oplus x_4) \oplus R_1^1(x_2) \oplus \alpha \oplus \beta.}$$
$$f(b' \parallel x_4') = W(x_1 \parallel x_2 \parallel \alpha \parallel x_4') \oplus \beta =$$
$$= \underline{R_1^3(h_\alpha \oplus R_2^1(x_1) \oplus x_4') \oplus R_1^1(x_2) \oplus \alpha \oplus \beta.}$$

    Оскільки $f(b \parallel x_4) = f(b' \parallel x_4')$, звідси випливає, що $x_4 = x_4'$ – тривіальний випадок.
  - ▶ Нехай $b = 0$, а $b' = 1$:

$$f(b \parallel x_4) = W(x_1 \parallel x_2 \parallel \alpha \parallel x_4) \oplus \beta =$$
$$= \underline{R_1^3(h_\alpha \oplus R_2^1(x_1) \oplus x_4) \oplus R_1^1(x_2) \oplus \alpha \oplus \beta.}$$
$$f(b' \parallel x_4') = W(x_1 \parallel x_2 \parallel \beta \parallel x_4') \oplus \alpha =$$
$$= \underline{R_1^3(h_\beta \oplus R_2^1(x_1) \oplus x_4') \oplus R_1^1(x_2) \oplus \beta \oplus \alpha.}$$

    Оскільки $f(b \parallel x_4) = f(b' \parallel x_4')$, отримуємо:

$$x_4' = x_4 \oplus h_\alpha \oplus h_\beta.$$

  - ▶ Доведення аналогічні для $(b = 1,\ b' = 0)$ та $(b = b' = 1)$.
- $(\Leftarrow)$: Обчислимо результат напряму:
  - ▶ Нехай $b = 0$, тоді $b' = 1$:

$$\underline{f(0 \parallel x_4)} = W(x_1 \parallel x_2 \parallel \alpha \parallel x_4) \oplus \beta =$$
$$= R_1^3(h_\alpha \oplus R_2^1(x_1) \oplus x_4) \oplus R_1^1(x_2) \oplus \alpha \oplus \beta =$$
$$(x_4' = x_4 \oplus h_\alpha \oplus h_\beta)$$
$$= R_1^3(R_2^1(x_1) \oplus x_4' \oplus h_\beta) \oplus R_1^1(x_2) \oplus \beta \oplus \alpha =$$
$$= \underline{f(1 \parallel x_4')}.$$

□

Теорема 3.1. *Шифротекст, отриманий в результаті 4 раундів схеми Бергера, можна відрізнити від випадкового тексту за поліноміальну кількість запитів до квантового оракула.*

Доведення. З твердження 3.1 випливає, що функція f задовільняє умову Саймона (1). Отже, застосувавши алгоритм Саймона, можна знайти період функції за поліноміальну кількість запитів до квантового оракула, що дозволяє відрізнити випадковий набір бітів від тексту зашифрованого схемою, адже для випадкового тексту умова Саймона виконуватись буде лише з ймовірністю 2^{-n}, де n – довжина вхідного повідомлення [2]. □

Висновки

У роботі побудовано квантову атаку розрізнювання з поліноміальною складністю за обраним відкритим текстом на схему Бергера. Отриманий результат означає, що ця схема не є стійкою в квантовій моделі обчислень, як мінімум до цього типу атак. В подальшому планується дослідити квантову атаку розрізнювання за обраним шифротекстом та атаку відновлення раундових ключів на схему Бергера, та дослідити можливість побудови цих атак на розширені та звичайні узагальнені мережі Фейстеля.

Перелік використаних джерел

1. *Simon D. R.* On the Power of Quantum Computation // SIAM Journal on Computing. — 1997. — Т. 26, № 5. — С. 1474—1483. — DOI: 10.1137/S0097539796298637.
2. *Kuwakado H., Morii M.* Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation //. — 06.2010. — С. 2682—2685. — DOI: 10.1109/ISIT.2010.5513654.
3. *Hoang T., Rogaway P.* On Generalized Feistel Networks //. Т. 2010. — 08.2010. — С. 613—630. — ISBN 978-3-642-14622-0. — DOI: 10.1007/978-3-642-14623-7_33.
4. *Cui J., Guo J., Ding S.* Applications of Simon's algorithm in quantum attacks on Feistel variants // Quantum Information Processing. — 2021. — Бер. — Т. 20. — DOI: 10.1007/s11128-021-03027-x.
5. *Dong X., Li Z., Wang X.* Quantum cryptanalysis on some generalized feistel schemes // Science China Information Sciences. — 2019. — Т. 62, вип. 2. — DOI: 10.1007/s11432-017-9436-7.
6. Quantum Attacks on Type-3 Generalized Feistel Scheme and Unbalanced Feistel Scheme with Expanding Functions / Z. Zhang, W. Wu, H. Sui, B. Wang // Chinese Journal of Electronics. — 2023. — Т. 32, № 2. — С. 209—216. — DOI: 10.23919/cje.2021.00.294.
7. *Berger T. P., Minier M., Thomas G.* Extended Generalized Feistel Networks using Matrix Representation // Selected Areas in Cryptography 2013. Т. 7707 / за ред. Knudsen, L. R., Wu, Huapeng. — Burnaby, British Columbia, Canada : Springer, 08.2013. — С. 355—371. — (Lecture Notes in Computer Science). — URL: https://hal.science/hal-00913881.