УДК 003.26

КВАНТОВИЙ КРИПТОАНАЛІЗ СИМЕТРИЧНИХ ШИФРІВ НА ОСНОВІ АЛГОРИТМУ САЙМОНА

О. Т. Шевченко[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В роботі представлено основи криптоаналізу симетричних примітивів у квантовій моделі обчислень. Розглянуто атаки на симетричні криптосистеми на основі квантового алгоритму Саймона. Побудовано атаку на примітив, структура якого є узагальненою мережею Фейстеля з довільним числом підблоків.

Ключові слова: квантовий криптоаналіз, алгоритм Саймона, симетричні криптопримітиви, мережа Фейстеля

Вступ

З появою перших ідей щодо використання квантової моделі обчислень з'явилась можливість використання цієї моделі обчислень для криптоаналізу різних примітивів. Як виявилось, більшість сучасних асиметричних криптосистем є не стійкими у квантовій моделі обчислень. Однак питання стійкості симетричних криптосистем у загальному випадку залишається відкритим. Існуючий квантовий алгоритм Гровера дозволяє скоротити атаки повного перебору вдвічі відносно розміру задачі.

Одним із методів криптоаналізу симетричних криптосистем у квантовій моделі обчислень є використання алгоритму Саймона. На основі цього алгоритму існують атаки на трираундову мережу Фейстеля, схему xor-encrypt-xor, підробки повідомлень в системі аутентифікованого шифрування та значно покращено атаку раундового зсуву.

1. Задача Саймона та її розв'язок у квантовій моделі обчислень

1.1. Задача Саймона

Постановка задачі, а також ефективний квантовий алгоритм її розв'язку було представлено в 1994 році в роботі Саймона[1]. Це був перший квантовий алгоритм (рис. 1), якому достатньо експоненційно меншої кількості запитів до оракула в порівнянні з будь-яким класичним алгоритмом розв'язку.

Задача Саймона[1]. *Нехай задана функція* $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ *за допомогою оракула така, що для довільних значень* $x, y \in \{0,1\}^n$ *виконується рівність* $f(x) = f(y)$ *тоді і тільки тоді, коли* $(x \oplus y) \in \{0, s\}$*, для деякого невідомого фіксованого значення* $s \in \{0,1\}^n$*. Необхідно визначити чи існує ненульове значення* s *та знайти його.*

В класичній моделі така задача розв'язується за щонайменше $\Omega(2^{n/2})$ запитів до оракула, навіть з використанням ймовірнісних алгоритмів. А у квантовій моделі обчислень задачу Саймона можна розв'язати, використовуючи $\mathcal{O}(n)$ запитів до оракула.[1]

Розглянемо алгоритм розв'язку, який наведено в роботі [1], і на який посилаються як на квантовий алгоритм Саймона.

Квантовий алгоритм Саймона

1) Підготувати два регістри розміру n у стані $|0\rangle|0\rangle$.
2) Застосувати перетворення Адамара до першого регістру $(H^{\otimes n} \otimes I_n)|0\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in Z_2^n} |x\rangle|0\rangle$.
3) Використати стандартну модель оракулу, який обчислює значення функції f: $U_f(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$.
4) Зробити вимірювання другого регістру, що переведе перший регістр у стан $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)$ для деякого значення z, де $f(z)$ є результатом вимірювання.
5) Застосувати перетворення Адамара до першого регістру $H^{\otimes n}(\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)) = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_y (-1)^{zy}(1 + (-1)^{sy})|y\rangle$.
6) Зробити вимірювання першого регістру. Результатом вимірювання буде деяке випадкове значення $u \in \{0,1\}^n$ таке, що $u \cdot s = 0$.

Після cn ітерацій алгоритму отримаємо $n-1$ лінійно незалежних векторів, які є ортогональними до вектору s, де $c > 1$ – деяка константа. В результаті отримуємо систему лінійних рівнянь, розв'язавши яку, обчислюємо значення s та перевіряємо чи є воно тривіальним.

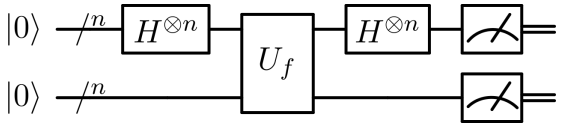

Рис. 1. Схема алгоритму Саймона

[a] alex.shevchenko.ua@gmail.com

1.2. Узагальнена задача Саймона

Постановка задачі Саймона вимагає відсутності додаткових колізій $t \notin \{0, s\}$ таких, що $f(x) = f(x \oplus t)$ для деяких значень x. Проте в роботі [2] було доведено, що квантовий алгоритм Саймона розв'язує задачу Саймона навіть при наявності додаткових колізій. На задачу Саймона з можливістю додаткових колізій функції будемо посилатися, як на узагальнену задачу Саймона.

Нехай $\varepsilon(f, s) = \max_{t \in \{0,1\}^n \setminus \{0, s\}} Pr_x[f(x) = f(x \oplus t)]$ – метрика, яка, пояснюючи неформально, показує, наскільки функція відрізняється від умов оригінальної задачі Саймона.[2]

Теорема (Кеплен, Лорент, Левер'є, Нея-Плесенція) [2]. *Якщо $\varepsilon(f, s) = p < 1$, тоді алгоритм Саймона обчислює значення s, використовуючи cn запитів до стандартної моделі оракула, який обчислює значення функції, з ймовірністю не менше ніж $1 - (2(\frac{1+p}{2})^c)^n$*

Завдяки такому узагальненню, алгоритм Саймона можна застосовувати до класу функцій, які майже задовольняють вимогам оригінальної задачі відповідно до метрики $\varepsilon(f, s)$. Як наслідок, якщо $\varepsilon(f, s) < \frac{1}{2}$, то ймовірність помилки алгоритму можна зробити як завгодно малою, інакше існує диференціал функції f з ймовірністю більшою за $\frac{1}{2}$ (в цьому випадку застосовними є класичні методи диференціального криптоаналізу).[2]

2. Використання алгоритму Саймона для побудови атак на симетричні криптопримітиви

В більшості випадків алгоритм Саймона використовують з метою покращення класичних атак пошуку колізій. Зазвичай, шукане значення s – це значення $s = E_k(\alpha) \oplus E_k(\beta)$ для деякої фіксованої пари значень α, $\beta \in \{0,1\}^n$ та деякого відображення $E_k : \{0,1\}^n \longrightarrow \{0,1\}^n$.

Фактично, шукане значення s є періодом функції. Існують дві основні конструкції для побудови функції з певним періодом, які використовуються в квантовому криптоаналізі:

1) $f_1(x) = S(E_k(x) + E_k(x \oplus s))$
2) $f_2(x, b) = \delta_{b,\,0} E_k(x) + \delta_{b,\,1} E_k(x \oplus s)$

Нескладно перевірити, що період функції f_1 дорівнює s, а період функції f_2 дорівнює $s\|1$. Отже, до функцій такого виду можна застосувати алгоритм Саймона для знаходження невідомого значення періоду.

2.1. Атака на трираундову мережу Фейстеля

Мережа Фейстеля – це класична ітеративна схема для побудови блокових шифрів. Загальновідомо, що трираундова схема Фейстеля (рис. 2) є стійкою псевдовипадковою підстановкою. Проте, в роботах [2] та [3] доведено, що така конструкція не є стійкою у квантовій моделі обчислень.

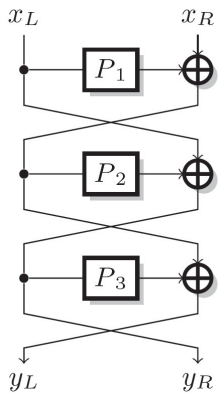

Рис. 2. Трираундова мережа Фейстеля

Атака на 3-раундову мережу Фейстеля. Нехай α_0, $\alpha_1 \in Z_2^{n/2}$ – фіксовані повідомлення, n – довжина блоку шифрування в бітах, $(y_R, y_L) = E(\alpha_b, x)$ – шифруюче перетворення, $b \in \{0, 1\}$.

Визначимо функцію $f(x, b) = y_R \oplus \alpha_b = P_2(x \oplus P_1(\alpha_b))$, де $b \in \{0, 1\}$. Періодом цієї функції є значення $s = P_1(\alpha_0) \oplus P_1(\alpha_1)\|1$, отже, можна застосувати квантовий алгоритм Саймона для знаходження періоду цієї функції, що і буде безпосередньо атакою на таку мережу Фейстеля.

2.2. Атака на схему Івена-Мансура

Схема Івена-Мансура (рис. 3) була побудована в 1991 році для підсилення блокових шифрів. Вона має дуже просту структуру задану за допомогою наступного співвідношення: $E(x, k_1, k_2, k_3) = k_1 \oplus S_{k_2}(x \oplus k_3)$. В класичній моделі обчислень ця схема вважається криптографічно стійкою в загальному випадку, оскільки складність зламу потребує щонайменше $\Theta(2^{n/2})$ запитів до оракула. У квантовій моделі обчислень доведено її вразливість до атак на основі обраного відкритого тексту.[2]

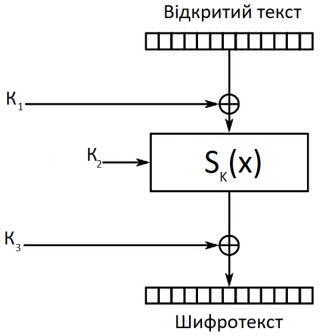

Рис. 3. Схема Івена-Мансура

Атака на схему Івена-Мансура. Визначимо функцію $f(x) = E(x, k_1, k_2) \oplus S(x) = S(x \oplus k_1) \oplus S(x) \oplus k_2$, де $S(x)$ – підстановка задана секретним ключем. Ця функція має період k_1, який можна знайти за допомогою квантового алгоритму Саймона.

2.3. Атака підробки повідомлення на код аутентифікації GMAC

Цей код аутентифікації повідомлень зроблено стандартом NIST в 2007 році. Вхідні повідомлення розглядаються як елементи скінченного поля. В основі коду лежить конструкція Картера-Вегмана, яка забезпечує криптографічну стійкість в класичній моделі обчислень.

Код аутентифікації GMAC. Код аутентифікації GMAC описується двома функціями: $GMAC(N, M) = GHASH(M \| len(M)) \oplus E_k(N\|1)$ та $GHASH(M) = \sum_{i=0}^{len(M)} m_i \cdot H^{len(M)-i+1}$, де $H = E_k(IV)$, k – секретний ключ користувача, N – криптографічний нонс (nonce).

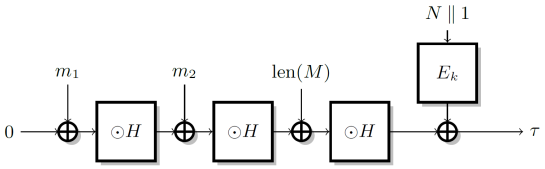

Рис. 4. Схема GMAC

Атака підробки повідомлення з кодом GMAC. Розглянемо повідомлення довжиною в два блоки $M = m_1\|m_2$. Тоді $GMAC(M, N) = \big((m_1 \cdot H) \oplus m_2\big) \cdot H \oplus E_k(N\|1)$. Нехай α_0 та α_1 деякі фіксовані блоки. Для атаки визначимо функцію $f_N(x, b) = GMAC(\alpha_b\|x, N) = \alpha_b \cdot H^2 \oplus x \cdot H \oplus E_k(N\|1)$, де $b \in \{0, 1\}$. Період функції дорівнює $(\alpha_0 \oplus \alpha_1) \cdot H\|1$, отже до неї також можна застосувати квантовий алгоритм Саймона.

Важливо зазначити те, що як $GMAC$ так і f_N залежать від значення нонсу. Алгоритм Саймона на кожній ітерації виконує запит до оракула, який обчислює одну й ту саму функцію, проте окрема ітерація алгоритму повертає вектор, ортогональний вектору $(\alpha_0 \oplus \alpha_1) \cdot H\|1$, який при цьому ніяк не залежить від вибору значення нонсу. Тож атака залишається коректною попри те, що на різних ітераціях алгоритму буде відбуватися запит до функції з різним нонсом.[2]

Код аутентифікації для випадкового фіксованого значення нонсу та довільного двоблокового повідомлення $m_1\|m_2$ буде також коректним для повідомлення $m_1 \oplus 1\|m_2 \oplus H$ з тим самим значенням нонсу N. Ось це повідомлення $m_1 \oplus 1\|m_2 \oplus H$ і буде підробкою оригінального повідомлення $m_1\|m_2$.

2.4. Атака раундового зсуву

Атаки раундового зсуву (англ. *slide attacks*) вперше описані в 1999 в роботі Бірюкова та Вагнера. Вони можуть бути застосовані до класу блокових шифрів з ідентичним раундовим перетворенням $R(x, k) = P(x \oplus k)$, параметризованого одним і тим же ключем, де $P(x)$ – безключова раундова функція.[4]

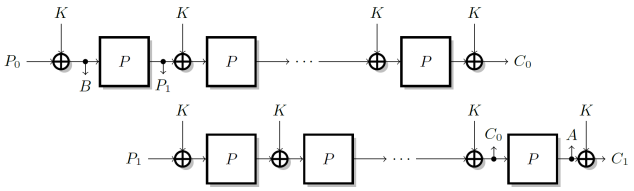

Рис. 5. Схема атаки раундового зсуву

В класичній моделі обчислень ідея атаки полягає в отриманні $\Theta(2^{n/2})$ пар відкритого тексту та шифрованого тексту. З високою ймовірністю серед цих пар знайдеться так звана «пара зсуву» – дві пари відкритого та шифрованого тексту (P_0, C_0) та (P_1, C_1) такі, що $R(P_0) = P_1$. Тоді для класу описаних вище шифрів одразу випливає: якщо пара повідомлень є парою зсуву, то $R(C_0) = C_1$ (рис. 5). В квантовій моделі обчислень можна отримати експоненційне зменшення складності цієї атаки.[2]

Атака раундового зсуву. Нехай $P(x)$ – безключова раундова функція, $E_k(x)$ – повне шифруюче перетворення. Визначимо $f(x, b) = \delta_{b,\,0}(P(E_k(x)) \oplus x) \oplus \delta_{b,\,1}(E_k(P(x)) \oplus x)$. Період функції f дорівнює $k\|1$. Застосувавши алгоритм Саймона до функції $f(x, b)$, ефективно знаходимо значення секретного ключа k.

3. Атака розпізнавання на узагальнену мережу Фейстеля

Як було розглянуто вище, трираундова мережа Фейстеля є вразливою до квантових атак розпізнавання на основі обраного відкритого тексту. Причиною цього є конструктивна особливість: за один раунд шифрування змінюється лише частина блоку, не враховуючи перестановку частин, та те, що об'єднання блоку шифрування та раундового перетворення відбувається за допомогою операції XOR. Ця особливість конструкції присутня у більшості узагальнених схем Фейстеля, що робить їх також вразливими до атак з використанням квантового алгоритму Саймона.

Атака розпізнавання на чотириблокову незбалансовану мережу Фейстеля. Розглянемо узагальнену мережу Фейстеля, в якій блок шифрування розбивається на чотири підблоки. Раунд шифрування описується раундовим перетворенням $Round((x_0, x_1, x_2, x_3), k) = (x_1 \oplus F_k(x_0), x_2, x_3, x_0)$, де $F_k(x)$ – раундова функція (рис. 6).

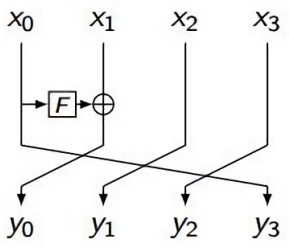

Рис. 6. Раунд узагальненої мережі Фейстеля

За умови, що повне шифруюче перетворення використовує не більше ніж сім раундів шифрування,

побудуємо квантову атаку на основі обраного відкритого тексту.

Атака розпізнавання на 7-раундову узагальнену мережу Фейстеля. Нехай $\alpha_0 = (\alpha_0^{(0)}, \alpha_0^{(1)}, \alpha_0^{(2)})$ та $\alpha_1 = (\alpha_1^{(0)}, \alpha_1^{(1)}, \alpha_1^{(2)})$ – фіксовані повідомлення, $E_k(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$ – шифруюче перетворення.

Визначимо $f(x, b) = y_1 \oplus \alpha_b^{(0)} = \alpha_b^{(0)} \oplus F_4(x \oplus F_3(\alpha_b^{(2)} \oplus F_2(\alpha_b^{(1)} \oplus F_1(\alpha_b^{(0)})))) \oplus \alpha_b^{(0)} = F_4(x \oplus F_3(\alpha_b^{(2)} \oplus F_2(\alpha_b^{(1)} \oplus F_1(\alpha_b^{(0)}))))$, де $b \in \{0, 1\}$.

Позначимо через $G((x_0, x_1, x_2)) = F_3(x_2 \oplus F_2(x_1 \oplus F_1(x_0)))$. Тоді період функції $f(x, b)$ дорівнює $(G(\alpha_0) \oplus G(\alpha_1))\|1$

Розглянувши різні варіації мережі Фейстеля, результат було узагальнено на випадок з довільною кількістю підблоків r, що приводить наступне твердження.

Твердження (атака розпізнавання на узагальнену мережу Фейстеля). *Узагальнена r-блокова мережа Фейстеля з раундом виду $Round((x_0, x_1, x_2, \ldots, x_{r-1}), k) = (x_1 \oplus F_k(x_0), x_2, \ldots, x_{r-1}, x_0)$ та кількістю раундів $n = 2r - 1$ є вразливою до квантових атак розпізнавання на основі обраного відкритого тексту.*

Доведення

Нехай α_0 та α_1 – фіксовані повідомлення, $E_k(x_0, \ldots, x_{r-1}) = (y_0, \ldots, y_{r-1})$ – шифруюче перетворення.

Відповідно до атак розглянутих раніше, визначимо функцію $f(x, b) = y_1 \oplus \alpha_b^{(0)} = \alpha_b^{(0)} \oplus F_r(x \oplus F_{r-1}(\alpha_b^{(r-2)} \oplus \ldots \oplus F_2(\alpha_b^{(1)} \oplus F_1(\alpha_b^{(0)})))) \oplus \alpha_b^{(0)} = F_r(x \oplus F_{r-1}(\alpha_b^{(r-2)} \oplus \ldots \oplus F_2(\alpha_b^{(1)} \oplus F_1(\alpha_b^{(0)}))))$, де $b \in \{0, 1\}$.

Позначимо через $G((x_0, x_1, \ldots, x_{r-2})) = F_{r-1}(x_{r-2} \oplus \ldots \oplus F_2(x_1 \oplus F_1(x_0)))$

Тоді період такої функції $f(x, b)$ дорівнює $(G(\alpha_0) \oplus G(\alpha_1))\|1$. Значення цього періоду знаходиться за допомогою квантового алгоритму Саймона. □

Схожі атаки на узагальнені мережі Фейстеля також досліджено в роботах [5] та [6].

4. Висновки

Алгоритм Саймона є одним з найперспективніших алгоритмів для використання в диференціальному криптоаналізі. Цей алгоритм за $\mathcal{O}(n)$ запитів до оракула розв'язує задачу пошуку періоду функції. Узагальнення формулювання задачі Саймона на випадок функції з додатковими колізіями показує, що алгоритм Саймона може працювати з класом функцій, які майже задовольняють вимогам оригінальної задачі відповідно до метрики $\varepsilon(f, s)$. Наявність додаткових колізій незначним чином впливає на роботу алгоритму, або до даної функції є застосовними методи класичного диференціального криптоаналізу. В роботі розглянуто атаки з використанням алгоритму Саймона на сучасні симетричні криптопримітиви такі як трираундова схема Фейстеля, схема Івена-Мансура, GMAC.

Доведено, що узагальнені мережі Фейстеля є вразливими до атак розпізнавання в квантовій моделі обчислень, які так само використовують алгоритм Саймона, оскільки в їх основі лежить та сама конструкція що й в стандартній мережі Фейстеля. Це свідчить про те, що конструкції схожі на мережу Фейстеля мають значні вразливості до квантових атак на основі обраного відкритого тексту. При цьому доведено, що кількість раундів на які можна побудувати атаку розпізнавання, зростає не повільніше ніж $rounds(r) = 2r - 1$, як функція від кількості підблоків, на які розбивається вхідний блок шифрування. З метою подальшого дослідження слід розглянути блокові шифри малоресурсної криптографії (англ. *lightweight cryptography*), наприклад, шифр Торпа, який є максимально незбалансованою мережею Фейстеля, та інші схожі симетричні криптопримітиви.

Перелік використаних джерел

1. Simon D. R. On the Power of Quantum Computation. — 1994. — P. 116–123. — Access mode: `https://doi.org/10.1109/SFCS.1994.365701`.
2. Breaking Symmetric Cryptosystems using Quantum Period Finding / Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia. — 2016. — 02.
3. Santoli Thomas, Schaffner Christian. Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives. — 2016. — 03. — Vol. 17.
4. Biryukov Alex, Wagner David. Slide Attacks // Fast Software Encryption / Ed. by Lars Knudsen. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1999. — P. 245–259.
5. Dong Xiaoyang, Li Zheng, Wang Xiaoyun. Quantum cryptanalysis on some generalized Feistel schemes // Science China Information Sciences. — 2019. — Jan. — Vol. 62, no. 2. — P. 22501. — Access mode: `https://doi.org/10.1007/s11432-017-9436-7`.
6. Ito Gembu, Iwata Tetsu. Quantum Distinguishing Attacks against Type-1 Generalized Feistel Ciphers // IACR Cryptology ePrint Archive. — 2019. — Vol. 2019. — P. 327.