УДК 004.056.55

ПОБУДОВА КВАНТОВИХ АТАК НА УЗАГАЛЬНЕНУ СХЕМУ ЛАЯ-МЕССІ

М. О. Кривошапова[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі досліджено структуру криптографічної схеми Лая-Мессі, яка є одним із варіантів ітеративної побудови симетричних шифрів. Розглянуто наявні квантові атаки на цю схему. Проаналізовано одне з наявних узагальнень схеми Лая-Мессі. Побудовано атаку відновлення ключа першого раунду для 1-раундової узагальненої схеми Лая-Мессі, а також квантову атаку на відновлення ключа першого раунду для часткового випадку 2-раундової узагальненої схеми Лая-Мессі. Побудовано розпізнавач для часткового випадку 2-раундової та 3-раундової узагальнених схем Лая-Мессі.

Ключові слова: квантові атаки, узагальнена схема Лая-Мессі

Вступ

Схема Лая-Мессі (Lai-Massey) є однією з відомих схем побудови симетричних шифрів. Вона розроблена для забезпечення безпеки в умовах класичних обчислень, однак з розвитком квантових обчислень виникає питання стійкості шифрів, побудованих на цій схемі, до квантових атак. Використання квантових алгоритмів може суттєво знизити рівень безпеки багатьох класичних криптографічних структур, і тому важливо досліджувати їх вплив на наявні криптографічні схеми, зокрема на схему Лая-Мессі.

1. Структура класичної схеми Лая-Мессі та наявні квантові атаки на неї

Схема Лая-Мессі — це криптографічна структура, яка використовується при розробці блокових шифрів, вперше запропонована у 1990 році в шифрі PES (Proposed Encryption Standard) [1]. Після появи лінійного та диференціального криптоаналізу у 1991 році створено модифікований шифр IDEA (International Data Encryption Algorithm) [2, 3] Лаєм, Мессі та Мерфі (Murphy). Водене (Vaudenay) [4] на конференції Asiacrypt'99 узагальнив структуру, прийняту в шифрі IDEA, і назвав її схемою Лая-Мессі. Надалі схему Лая-Мессі використали при побудові шифрів WIDEA [5], MESH [6] та ін.

На основі схеми Лая-Мессі також створено шифр FOX (також відомий як "IDEA NXT"). Шифр FOX використовує операцію XOR замість операцій додавання та віднімання і реалізує ортоморфізм σ на основі одного раунда схеми Фейстеля з ортоморфізмом $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$, де $x_R, x_L \in \{0,1\}^n$ — права та ліва рівні частини вхідного повідомлення, $\oplus$ — операція XOR.

Як і схема Фейстеля, схема Лая-Мессі дозволяє реалізувати інволютивне перетворення, тобто процес розшифрування виконується аналогічно до шифрування, за винятком зворотного порядку раундових ключів.

Однією з ключових переваг схеми Лая-Мессі є те, що вона не вимагає бієктивності раундової функції, що спрощує процес розробки та реалізації. Також ця схема має ітеративну структуру, яка робить її зручною для практичного застосування.

Повідомлення на кожному раунді поділяється на дві частини: L_i — ліва частина, R_i — права частина, де i — номер раунду.

Останній раунд відрізняється від усіх інших раундів тим, що не містить ортоморфізм σ.

Процес шифрування схеми Лая-Мессі з r раундами можна представити так:

1. (L_0, R_0) — початкове повідомлення.
2. Для раунду $i = 1, \dots, r-1$.
   Вхідні дані i-го ранду:
   $$(L_{i-1}, R_{i-1}), \text{ де } L_{i-1}, R_{i-1} \in \{0,1\}^n.$$
   Вихідні дані i-го ранду:
   $$(L_i, R_i), \text{ де}$$
   $$L_i = \sigma(L_{i-1} \oplus F_i(L_{i-1} \oplus R_{i-1}, K_i)),$$
   $$R_i = R_{i-1} \oplus F_i(L_{i-1} \oplus R_{i-1}, K_i).$$
3. Для раунду $i = r$.
   Вхідні дані r-го ранду:
   $$(L_{r-1}, R_{r-1}), \text{ де } L_{r-1}, R_{r-1} \in \{0,1\}^n.$$
   Вихідні дані r-го ранду:
   $$(L_r, R_r), \text{ де}$$
   $$L_r = L_{r-1} \oplus F_r(L_{r-1} \oplus R_{r-1}, K_{r-1}),$$
   $$R_r = R_{r-1} \oplus F_r(L_{r-1} \oplus R_{r-1}, K_{r-1}).$$

4. (L_r, R_r) — зашифроване повідомлення.

При цьому σ — ортоморфізм, відображення F_i — це раундова функція, яка залежить від ключа K_i та забезпечує нелінійність і перемішування.

На рис. 1 представлено і-ий раунд r-раундової схеми Лая-Мессі, де $i \in \{1, ..., r\}$.

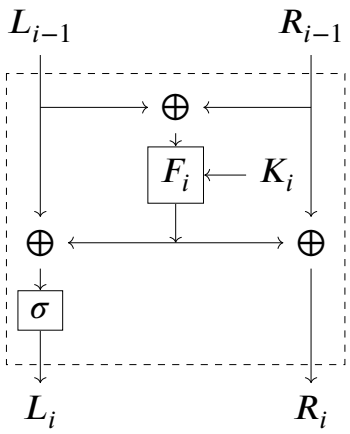

Рис. 1. і-ий раунд схеми Лая-Мессі

Квантові атаки на схему Лая-Мессі використовують особливості квантових алгоритмів, таких як алгоритм Саймона та алгоритм Гровера. Основна увага при дослідженнях зосереджена на атаках, спрямованих на зменшення складності визначення ключа чи розрізнення криптосистеми від випадкової перестановки.

Водене та ін. [4] довели, що 3 - раундові та 4 - раундові схеми Лая-Мессі є захищеними від атак на основі вибраного відкритого тексту (CPA) та атак на основі вибраного шифротексту (CCA). Ло та ін. [7] довели, що 3 раунди (4 раунди) необхідні для CPA-захисту (CCA-захисту). Суй (Sui) та ін. [8] показали, що 4-раундова схема Лая-Мессі є стійкою до CCA-атак навіть за умови доступу зловмисника до двох внутрішніх раундів.

У [9] Ло та ін. показали, що 3-раундова схема Лая-Мессі може протистояти квантовим атакам з використанням алгоритму Саймона, що відрізняє її від схеми Фейстеля.

У 2022 році Мао та інші [10] запропонували квантові атаки на схему Лая-Мессі, використаної в шифрі FOX. Отримані результати показали, що існує квантовий CPA-розпізнавач 3-раундової схеми Лая-Мессі та квантовий CCA-розпізнавач 4-раундової структури Лая-Мессі, який використовує $O(n)$ квантових запитів, де довжина вхідних даних схеми Лая-Мессі становить $2n$ біт.

У статті [10] також побудовано квантову атаку Гровера-Саймона на 4-раундову схему Лая-Мессі, яка використовує $O(n2^{m/2})$ квантових запитів, де $2n$ — довжина входу, а m — довжина ключа K_4 четвертої раундової функції F_4.

Отже, хоча схема Лая-Мессі є відносно стійкою до класичних атак, але з появою квантових методів, таких як алгоритми Саймона та Гровера, з'явились нові можливості для атак, які дозволяють знизити складність криптоаналізу, чим показують її потенційні вразливості в реальних сценаріях.

З урахуванням викликів, які становлять квантові обчислення, необхідно досліджувати нові підходи до модифікацій схеми Лая-Мессі.

2. Структура узагальненої схеми Лая-Мессі

Схема Лая-Мессі була узагальнена в різних напрямах з метою підвищення її стійкості до атак або адаптації до конкретних задач. Одним із підходів до узагальнення є збільшення розміру ключа або розширення простору ключів, застосування нових методів створення раундових ключів, що ускладнює аналіз можливих атак. Деякі узагальнення передбачають використання інших алгебраїчних структур або впровадження додаткових криптографічних примітивів.

У дослідженні [11] проводиться аналіз лінійних, диференціальних і алгебраїчних властивостей узагальненої структури, що використовується в шифрі FLY [12]. І на основі отриманих результатів використану криптографічну структуру назвали узагальненою схемою Лая-Мессі (Generalized Lai-Massey Scheme).

і-ий раунд, $1 \le i \le r$, узагальненої r-раундової схеми Лая-Мессі має вигляд, представлений на рис. 2.

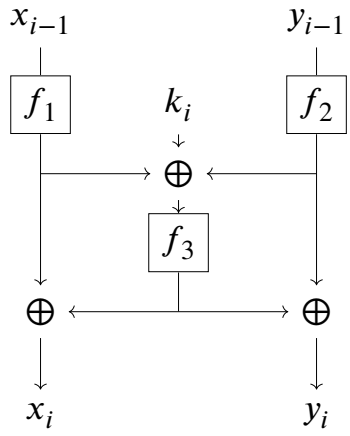

Рис. 2. і-ий раунд узагальненої схеми Лая-Мессі

Розглянемо процес шифрування одного раунду узагальненої схеми Лая-Мессі, зображеної на рис. 2.

1. На вхід подаємо повідомлення $(x_0, y_0) \in \{0,1\}^{2n}$, яке складається з двох рівних частин $x_0, y_0 \in \{0,1\}^n$.
2. Повідомлення на кожному раунді поділяється на дві частини: x_i — ліва частина, y_i — права частина, де i — номер раунду.
   Результат шифрування після проходження і-го раунду:

$$x_i = f_1(x_{i-1}) \oplus f_3(k_i \oplus f_1(x_{i-1}) \oplus f_2(y_{i-1})),$$

$$y_i = f_2(y_{i-1}) \oplus f_3(k_i \oplus f_1(x_{i-1}) \oplus f_2(y_{i-1})).$$

3. Після проходження r раундів, на виході відповідно отримаємо повідомлення $(x_r, y_r) \in \{0,1\}^{2n}$,

яке також складається з двох рівних частин $x_r, y_r \in \{0,1\}^n$.

Відображення f_1, f_2, f_3 — це раундові функції ускладнення (відображення над полем $\mathbb{F}_n^2$), які забезпечують нелінійність і перемішування, f_1 та f_2 мають бути бієктивними.

3. Квантові атаки на узагальнену схему Лая-Мессі

Теорема 1. *Можна ефективно відновити значення раундового ключа k_i i-го раунду r-раундової узагальненої схеми Лая-Мессі, якщо функції f_1, f_2, f_3, вхідні значення i-го раунду x_{i-1}, y_{i-1} та вихідні значення i-го раунду x_i, y_i є відомими.*

Доведення. Так як функції f_1, f_2, f_3, вхідні значення x_{i-1}, y_{i-1} та вихідні значення x_i, y_i відомі, то, виконавши нескладні математичні перетворення, можна виразити ключ k_i. Достатньо навіть знати тільки одну із двох частин вихідного значення. Покажемо на прикладі використання тільки вхідного значення x_{i-1} та вихідного значення x_i.

$$x_i = f_1(x_{i-1}) \oplus f_3(k_i \oplus f_1(x_{i-1}) \oplus f_2(y_{i-1})),$$

$$x_i \oplus f_1(x_{i-1}) = f_3(k_i \oplus f_1(x_{i-1}) \oplus f_2(y_{i-1})),$$

$$f_3^{-1}(x_i \oplus f_1(x_{i-1})) = k_i \oplus f_1(x_{i-1}) \oplus f_2(y_{i-1}),$$

$$f_3^{-1}(y_i \oplus f_1(x_{i-1})) \oplus f_1(x_{i-1}) \oplus f_2(y_{i-1}) = k_i.$$

Аналогічно можна обчислити значення раундового ключа k_i використовуючи тільки вхідне значення y_{i-1} та вихідне значення y_i.

□

Розглянемо 2-раундову узагальнену схему Лая-Мессі.

Позначимо $(x_2, y_2) \in \{0,1\}^{2n}$, де $x_2, y_2 \in \{0,1\}^n$ результат шифрування після проходження двох раундів:

$$x_2 = f_1(x_1) \oplus f_3(k_2 \oplus f_1(x_1) \oplus f_2(y_1)),$$

$$y_2 = f_2(y_1) \oplus f_3(k_2 \oplus f_1(x_1) \oplus f_2(y_1)).$$

Підставимо виведені значення x_1, y_1.

$$x_2 = f_1(f_1(x_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0))) \oplus$$
$$\oplus f_3(k_1 \oplus f_1(f_1(x_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0))) \oplus$$
$$\oplus f_2(f_2(y_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0)))),$$

$$y_2 = f_2(f_2(y_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0))) \oplus$$
$$\oplus f_3(k_1 \oplus f_1(f_1(x_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0))) \oplus$$
$$\oplus f_2(f_2(y_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0)))),$$

Отже,

$$x_2 \oplus y_2 = f_1(f_1(x_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0))) \oplus$$
$$\oplus f_2(f_2(y_0) \oplus f_3(k_1 \oplus f_1(x_0) \oplus f_2(y_0))).$$

Перехресне використання функцій f_1, f_2, f_3 дуже ускладнює пошук періодичної функції і відповідно періоду за допомогою алгоритму Саймона, як було реалізовано в атаках на класичну схему Лая-Мессі. Тому спробуємо використати інші можливості криптоаналізу на основі квантових алгоритмів.

Теорема 2. *Можна відновити значення раундового ключа k_1 1-го раунду для часткового випадку $f_1(x_0) = f_2(y_0) = 0$ 2-раундової узагальненої схеми Лая-Мессі.*

Доведення. Нехай $f_1(x_0) = f_2(y_0) = 0$. Підставляємо в x_2, y_2 і отримуємо фіксовані значення x_2', y_2':

$$x_2' = f_1(f_3(k_1)) \oplus f_3(k_1 \oplus f_1(f_3(k_1)) \oplus f_2(f_3(k_1))),$$

$$y_2' = f_2(f_3(k_1)) \oplus f_3(k_1 \oplus f_1(f_3(k_1)) \oplus f_2(f_3(k_1))),$$

$$x_2' \oplus y_2' = f_1(f_3(k_1)) \oplus f_2(f_3(k_1)).$$

Значення $x_2' \oplus y_2' = s$ можна обчислити, тоді виразимо $f_3(k_1)$.

Для довільного значення $f_3(k_1)$:

$$f_1^{-1}(f_2(f_3(k_1)) \oplus s) = f_3(k_1).$$

Отримали нерухому точку відносно значення $f_3(k_1)$, яку можна знайти за квантовим алгоритмом пошуку нерухомих точок описаним в [13].

З статті [13] також маємо кількість запитів до оракула для реалізації квантового пошуку нерухомої точки — $O(\sqrt{Nlog(1/\varepsilon)})$, де

N — загальна кількість елементів,

ε — допустима похибка (тобто, 1 — ймовірність успіху).

Ймовірність успіху $\geq 1 - \varepsilon$.

Відновивши значення $f_3(k_1) = w$, знайдемо ключ першого раунду $k_1 = f_3^{-1}(w)$.

Але, варто зауважити, що оцінка складності атаки не є поліноміальною, проте є суттєво меншою за повний перебір.

□

Теорема 3. *Якщо накласти додаткову умову $f_1(x) = f_2(x) = f(x)$ для довільного значення $x \in \{0,1\}^n$, то можна побудувати ефективний розпізнавач для 2-раундової узагальненої схеми Лая-Мессі.*

Доведення. Якщо $f_1(x) = f_2(x) = f(x)$ для довільного значення $x \in \{0,1\}^n$, яка доволі часто зустрічається на практиці, то

$$x_2' \oplus y_2' = f(f_3(k_1)) \oplus f(f_3(k_1)) = 0.$$

Отримуємо, якщо $x_2' \oplus y_2' = 0$, то надано 2-раундову узагальнену схему Лая-Мессі, інакше надано випадкову перестановку.

□

Теорема 4. *Для 3-раундової узагальненої схеми Лая-Мессі можна побудувати ефективний розпізнавач, за умов: $f_1(x_0) = f_2(y_0) = 0$ та $f_1(x) = f_2(x) = f(x)$ для довільного значення $x \in \{0,1\}^n$.*

Доведення. Розглянемо 3-раундову узагальнену схему Лая-Мессі. Її вихідні значення $(x_3, y_3) \in \{0,1\}^{2n}$, де $x_3, y_3 \in \{0,1\}^n$ обчислюються за формулами:

$$x_3 = f_1(x_2) \oplus f_3(k_3 \oplus f_1(x_2) \oplus f_2(y_2)),$$

$$y_3 = f_2(y_2) \oplus f_3(k_3 \oplus f_1(x_2) \oplus f_2(y_2)),$$

$$x_3 \oplus y_3 = f_1(x_2) \oplus f_2(y_2).$$

Підставимо виведені значення x_2', y_2' за умови, що $f_1(x_0) = f_2(y_0) = f_1(x_0) \oplus f_2(y_0) = 0$ отримуємо відповідне значення $x_3' \oplus y_3'$.

$$x_3' \oplus y_3' = f_1(x_2') \oplus f_2(y_2') =$$

$$= f_1(f_1(f_3(k_1)) \oplus f_3(k_1 \oplus f_1(f_3(k_1)) \oplus f_2(f_3(k_1)))) \oplus$$

$$\oplus f_2(f_2(f_3(k_1)) \oplus f_3(k_1 \oplus f_1(f_3(k_1)) \oplus f_2(f_3(k_1)))).$$

При накладанні додаткової умови $f_1(x) = f_2(x) = f(x)$ для довільного значення $x \in \{0,1\}^n$, яка часто зустрічається на практиці, отримуємо:

$$x_3' \oplus y_3' = f_1(x_2') \oplus f_2(y_2') =$$

$$= f(f(f_3(k_1)) \oplus f_3(k_1 \oplus f(f_3(k_1)) \oplus f(f_3(k_1)))) \oplus$$

$$\oplus f(f(f_3(k_1)) \oplus f_3(k_1 \oplus f(f_3(k_1)) \oplus f(f_3(k_1)))) = 0.$$

Тобто, для 3-раундової узагальненої схеми Лая-Мессі також можна побудувати розпізнавач, за умов:
$f_1(x_0) = f_2(y_0) = 0$ та $f_1(x) = f_2(x) = f(x)$,
для довільного значення $x \in \{0,1\}^n$.

Якщо $x_3' \oplus y_3' = 0$, то надано 3-раундову узагальнену схему Лая-Мессі, інакше надано випадкову перестановку.

□

Атаку за допомогою алгоритму Саймона складно реалізувати для узагальненої схеми Лая-Мессі, тому що застосування додаткових функції у схемі суттєво ускладнює побудову подібних атак. Але знайдено інші можливості для атак. Наприклад, відновлення ключа першого раунду k_1 для 2-раундової узагальненої схеми Лая-Мессі за допомогою квантового алгоритму пошуку нерухомих точок. Також побудовано розрізнювачі для 2-раундової та 3-раудової узагальненої схеми Лая-Мессі від випадкової перестановки при накладанні додаткових умов.

Висновки

В роботі розглянуті наявні квантові атаки на схему Лая-Мессі. Розглянуті можливості квантового криптоаналізу узагальненої схеми Лая-Мессі, зокрема, атаки відновлення ключа за допомогою квантових алгоритмів та побудови розпізнавача. Виявлено, що при певних умовах, таких як накладення обмежень на вхідні значення та використання нерухомих точок функцій, можна відновити ключ першого раунду k_1 для 2-раундової узагальненої схеми Лая-Мессі. Крім того, побудовано розпізнавачі для 2-раундової та 3-раундової узагальнених схем Лая-Мессі при виконанні додаткових властивостей функцій. Це підкреслює важливість подальшого дослідження стійкості схеми Лая-Мессі в умовах квантових обчислень.

Перелік використаних джерел

1. *Lai X.*, *Massey J. L.* A Proposal for a New Block Encryption Standard // EUROCRYPT 90. — 1991. — С. 389—404.
2. *Lai X.*, *Massey J. L.* A proposal for a new block encryption standard // EUROCRYPT '90, Proceedings. Т. 473. — Springer, 1991. — С. 389—404. — (LNCS). — DOI: 10.1007/3-540-46877-3_35. — URL: https://doi.org/10.1007/3-540-46877-3_35.
3. *Lai X.* On the design and security of block ciphers : дис. ... док. / Lai Xuejia. — Zurich, Switzerland : ETH Zurich, 1992. — URL: https://d-nb.info/920912710.
4. *Vaudenay S.* On the Lai-Massey scheme // ASIACRYPT '99, Proceedings. Т. 1716. — Springer, 1999. — С. 8—19. — (LNCS). — DOI: 10.1007/978-3-540-48000-6_2. — URL: https://doi.org/10.1007/978-3-540-48000-6_2.
5. *Unknown.* The Wide-Lane IDEA Block Cipher. — 2013. — URL: https://www.iacr.org/archive/fse2013/84240037/84240037.pdf ; Presented at FSE 2013.
6. The MESH block ciphers / J. Nakahara, V. Rijmen, B. Preneel, J. Vandewalle // WISA 2003, Proceedings. — 2003. — С. 458—473.
7. *Luo Y.*, *Lai X.*, *Gong Z.* Pseudorandomness analysis of the (extended) Lai-Massey scheme // Information Processing Letters. — 2010. — Т. 111, № 2. — С. 90—96. — DOI: 10.1016/j.ipl.2010.10.012. — URL: https://doi.org/10.1016/j.ipl.2010.10.012.
8. *Sui H.*, *Wu W.*, *Zhang L.* Round security of the Lai-Massey structure (in Chinese) // Journal of Cryptologic Research. — 2014. — Т. 1. — С. 28—40.
9. Study on block cipher structures against Simon's quantum algorithm (in Chinese) / Y. Luo, H. Yan, L. Wang, H. Hu, X. Lai // Journal of Cryptologic Research. — 2019. — Т. 6, № 5. — С. 561—573.
10. Quantum Attacks on Lai-Massey Structure / S. Mao, T. Guo, P. Wang, L. Hu. — 2022. — Available at https://eprint.iacr.org/2022/986.pdf. Cryptology ePrint Archive.
11. *Shamsabad M. R. M.*, *Dehnavi S. M.* Lai-Massey Scheme Revisited. — 2022. — Available at https://eprint.iacr.org/2020/005.pdf. Cryptology ePrint Archive.
12. *Karpman P.* Exercice de style. — 2016. — hal-01263735.
13. *Yoder T. J.*, *Low G. H.*, *Chuang I. L.* Fixed-point quantum search with an optimal number of queries. — 2014. — Available at https://arxiv.org/pdf/1409.3305.