Дослідження можливості проведення invariant subspace атаки на енергоефективний алгоритм Midori

Олексій Наумов[1], Віктор Руженцев[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, м. Харків, пр. Науки, 14, E-mail: oleksii.naumov@nure.ua

2. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, м. Харків, пр. Науки, 14, E-mail: viktor.ruzhentsev@nure.ua

In the past few years, lightweight cryptography has become a popular research discipline with a number of ciphers and hash functions proposed. The designers' focus has been predominantly to minimize the hardware area, while other goals such as low latency have been addressed rather recently only. However, the optimization goal of low energy for block cipher design has not been explicitly addressed so far. At the same time, it is a crucial measure of goodness for an algorithm. Indeed, a cipher optimized with respect to energy has wide applications, especially in constrained environments running on a tight power budget such as Internet of Things.

Midori, lightweight блоковий шифр, AES, слабкі ключі, бітові перестановки, S-box.

I. Вступ

В сучасному світі з кожним роком все більше набуває популярності Інтернет Речей (Internet of Things, IoT). З'являється велика кількість розумних пристроїв вдома, в лікарні, у школі. Виходячи з цього виникає необхідність захисту цих пристроїв від зловмисників. Але через обмеженість в продуктивності, пам'яті чи енергоспоживанні не представляється можливим використання звичайних криптографічних засобів. Рішенням цієї проблеми є легковагова (lightweight) криптографія.

Легковагова криптографія – це розділ криптографії, який спрямований на розробку алгоритмів для використання в пристроях, які не здатні забезпечити виконання більшості існуючих алгоритмів або мають обмежені ресурси (пам'ять, потужність, енергоспоживання). Одним з найбільш енергоефективних та популярних алгоритмів є блочний симетричний шифр Midori.

II. Короткий опис Midori

Midori – це сімейство двох блокових шифрів: Midori64 і Midori128. Вперше було представлено світові на міжнародній конференції ASIACRYPT у 2015 році. Сімейство шифрів відноситься до SPN алгоритмів та має AES – подібну структуру. Обидва шифри приймають 128-бітові ключі і мають різний розмір блоку, 64 біти для Midori64 і 128 біт для Midori128. На виході отримуємо шифротекст тієї ж довжини, що і вхідний блок.

Циклічна функія Midori складається з наступних чотирьох операцій:

1) SubCell - процедура підстановки. Використовується два типи 4-бітних S-боксів, Sb_0 і Sb_1 $\{0, 1\}^4 \rightarrow \{0,1\}^4$ (див. Табл. 1). Sb_0 використовується в Midori64, а Sb_1 – в Midori128.

ТАБЛИЦЯ 1

Таблиця підстановок

S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	C	A	D	3	E	B	F	7	8	9	1	5	0	2	4	6
2	1	0	5	3	E	2	F	7	D	A	9	B	C	8	4	6

Midori128 використовує чотири різних 8-бітових S-бокси SSb_0, SSb_1, SSb_2 і SSb_3, де SSb_0, SSb_1, SSb2, SSb_3: $\{0, 1\}^8 \rightarrow \{0,1\}^8$. Математично, кожен SSb_i складається з вхідних і вихідних бітових перестановок і двох Sb_1, як показано на Рис. 1.

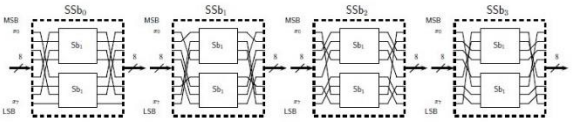

Рисунок 1 – Схема підстановки в Midori128

2) ShuffleCell - процедура циклічного зсуву. Це перетворення виконує розподілення бітів кожного рядка матриці стану серед всієї матриці. Кожна клітинка стану переставляється так:

$$(s_0, s_1, \ldots, s_{15}) \leftarrow (s_0, s_{10}, s_5, s_{15}, s_{14}, s_4, s_{11}, s_1, s_9, s_3, s_{12}, s_6, s_7, s_{13}, s_2, s_8) \quad (1)$$

3) MixColumn виконує множення кожного стовпця стану на матрицю M.

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad (2)$$

Операції множення між матрицею і вектором виконуються над полем $GF(2^m)$.

4) KeyAdd - процедура додавання ключа. Для Midori64 128-бітний секретний ключ K розділяється на два 64-бітні ключі K_0 і K_1. Тоді $WK = K_0 \oplus K_1$.

$$RK_i = K_{(i \bmod 2)} \oplus \alpha_i \quad (3),$$

де $0 \le i \le 14$. Для Midori128, WK = K, $RK_i = K \oplus \beta_i$, де $0 \le i \le 18$.

α_i та β_i - раундові константи, наведені у роботі [1].

Перед першим раундом застосовується додаткова операція KeyAdd, а в останньому раунді операції ShuffleCell та MixColumn відсутні. Загальна кількість циклів для Midori64 та Midori128 – 16 та 20 відповідно.

Загальна процедура зашифрування виглядає наступним чином. Блок вхідного тексту складається з таємним ключем. Потім R - 1 разів, де R – кількість циклів, відбуваються наступні дії: підстановка (SubCell), зсув рядків (ShuffleCell), перемішування стовпців (MixColumn) та додавання циклового ключа. На останньому циклі відбувається лише підстановка та додавання таємного ключа. Схема зашифрування для Midori64 представлена на Рис. 2.

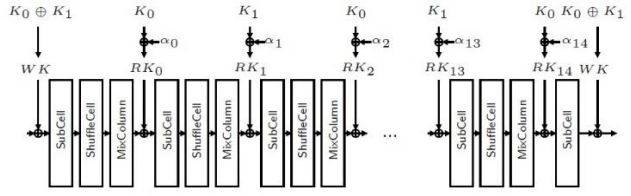

Рисунок 2 - Схема зашифрування Midori64

III. Недоліки Midori

Основним завданням під час розробки будь-якого легковагового блокового симетричного шифру є створення енергоефективного, стійкого та невибагливого до ресурсів алгоритму. Досягти одразу всі три цілі одночасно є досить складним завданням. Розробники сімейства шифрів Midori спробували це зробити. Midori вважається найбільш енергоефективним шифром серед конкурентів. Але окрім цього знайшовся ряд недоліків. До основних з яких відноситься наявність класу слабких ключів розміром 2^{32} [2]. Враховуючи операції, які використовуються в цикловій функції та вищеперераховані особливості можна підібрати відкритий текст, що стає підґрунтям для подальшого проведення атаки invariant subspace. Слід зазначити, що подібна властивість притаманна лише версії шифру з довжиною блоку 64 біти. Її детальний опис наведений нижче.

Нехай ключ складається з напівбайт, які відносяться до множини, що складається з двох елементів 0 та 1. Відкритий текст складається з множини напівбайт елементів 8 та 9. Оскільки ключ належить до множини значень {0, 1}, то і всі циклові ключі будуть відноситись до тієї ж множини значень, дивись (3).

Будь-які операції складання з такими ключами будуть змінювати блок стану, що належить до множини значень {8, 9}, але він і далі буде належати ті й множині, оскільки складання з ключем буде змінювати лише молодший біт кожного напівбайта.

Операція SubCell не спричинить зміни стану, оскільки згідно з Табл.1 після підстановки $8 \rightarrow 8$, а $9 \rightarrow 9$.

Операція ShuffleCell лише перемішує напівбайти між собою, а значить блок стану все ще буде належати множині {8, 9}.

Під час MixColumn виконується перемноження кожного стовпця матриці стану на матрицю (2). Оскільки вона складається лише з 0 та 1, буде справедливим твердження, що блок тексту все ще буде належати множині {8, 9}.

Отже, використання будь-якого слабкого ключа веде до того, що шифротекст буде належати ті й же множині значень, що й відкритий текст. Кількість циклів або порядок операцій не порушують цю властивість [3].

IV. Можливі протидії проведення invariant subspace атаки

Оскільки проведення invariant subspace атаки з відновлення ключа є можливим незалежно від кількості циклів, то лише збільшити їх кількість недостатньо. Отже необхідно змінити саму циклову функцію або механізм генерації циклових ключів. Нижче наведені декілька основних напрямків оптимізації алгоритму.

Перший напрямок це заміна самого S-боксу. Нова таблиця підстановок повинна бути уважно підібрана, без можливості переходу значення напівбайт в себе ж.

Другий напрямок це заміна циклових констат, які беруть участь у генерації циклових ключів. Наприклад, можна змінити один напівбайт в кожній константі на номер циклу.

Останній напрямок це застосування бітових перестановок під час операції SubCell. В Midori вже реалізований подібний механізм для генерації таблиць підстановок для 128-бітової версії шифру (Рис. 1).

Висновки

В цій роботі був досліджений блоковий симетричний шифр Midori. Окрім принципів його побудови був описаний важливий недолік цього шифру, що може слугувати підґрунтям для проведення invariant subspace атаки із відновлення ключа. Були запропоновані шляхи підвищення стійкості алгоритму. Цілями подальших робіт буде практичне застосування цієї атаки, впровадження запропонованих шляхів рішення існуючих проблем та аналіз їх впливу на роботу алгоритму(швидкодію, стійкість).

Перелік посилань

[1] Subhadeep Banik. Midori: A Block Cipher for Low Energy (Extended Version)/ Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita and Francesco Regazzoni – ASIACRYPT-2015, pages 10-14.

[2] Xiaoyang Dong Cryptanalysis of Reduced-Round Midori64 Block Cipher / Xiaoyang Dong, Yanzhao Shen - ISCISC 2017, pages 2-4.

[3] Jian Guo Invariant Subspace Attack Against Full Midori64 / Jian Guo, Jeremy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, Siang Meng Sim - EUROCRYPT 2017, pages 5-7.