УДК 004.056.55

ЗАСТОСУВАННЯ БІКЛІК-АНАЛІЗУ ДО ШИФРУ КАЛИНА ТА ЙОГО МОДИФІКАЦІЙ

Ломаченко Ігор

Фізико-технічний інститут, Київський політехнічний інститут імені Ігоря Сікорського

Анотація

В даній роботі буде розглядатись відносно новий метод криптоаналізу, відомий як біклік-аналіз, у застосуванні до українського стандарту шифрування ДСТУ 7624:2014 (шифру Калина).

Для оригінального шифру було обґрунтовано його стійкість до біклік-аналізу. Для модифікацій шифру було одержано чисельні оцінки стійкості та показано захищеність від біклік-атак навіть для послаблених версій шифру.

Abstract

In this work we apply a recent method of cryptanalysis, known as biclique-analysis, to Ukrainian encryption standard DSTU 7624:2014 (Kalyna cipher).

We show that the original cipher is secure against biclique-analysis. For the modifications of the original cipher we estimate the security and show that even weakened version of cipher are secure against biclique-analysis.

Вступ

Не зважаючи на те, що біклік-аналіз виник досить недавно, в останні роки з'явилось багато робіт на цю тематику [1, 3, 4], в яких пропонувались методи вдосконалення самого аналізу, або наводились шляхи його застосування для побудови атак на існуючі шифри. Таким чином, можна сказати, що в даний момент активно розбудовується загальна методика біклік-аналізу та формуються нові підходи, що дадуть опору для нових ідей та відкриттів. Отже, отримання результатів застосування біклік-аналізу до конкретних шифрів є актуальною задачею.

З 2015 року в Україні діє новий національний стандарт шифрування ДСТУ 7624:2014 (шифр Калина) [2]. Дана робота присвячена дослідженню можливості застосування біклік-аналізу до шифру Калина.

Загальні відомості біклік-аналізу

Біклік-аналіз аналіз базується на принципі «Зустріч посередині» (англ. «Meet-in-the-middle»). Шифр *E* розбивається у композицію двох функцій g_1 та g_2: $E = g_2 \circ g_1$.

Аналітик вибирає розбиття простору ключів на групи розміру 2^{2d}, які представляються у вигляді матриць $K[i, j]$ розміру $2^d \times 2^d$. Для деякої пари відкритий текст — шифротекст (P, C), отриманої на невідомому секретному ключі $K_{\text{sec}\,ret}$, аналітик обчислює 2^d значень $\vec{v}$ із *P* за допомогою перетворення g_1 та 2^d значень $\overleftarrow{v}$ з *C*:

$$P \xrightarrow{K[i,\cdot]} \vec{v},$$
$$\overleftarrow{v} \xleftarrow{K[\cdot,j]} C.$$

Пари, для яких $\vec{v} = \overleftarrow{v}$ формують кандидата в ключі $K[i, j]$. Позначимо через *v* одержане однакове проміжне значення.

Очікувана кількість кандидатів в ключі залежить від бітового розміру змінної $|v|$ та отримується за формулою $2^{2d-|v|}$. Для $|v|$, близьких до *d* або більших, атака має

перевагу над атаками повного перебору порядку 2^d, так як вона перевіряє 2^{2d} ключів менш ніж за 2^d викликів шифру.

Базова атака «зустріч посередині» має обмежене застосування у криптоаналізі блокових шифрів, так як внутрішня змінна *v* із зазначеними властивостями може бути знайдена лише для малої кількості раундів шифрування. Саме для подолання цієї перешкоди і застосовується концепція біклік [1].

Нехай f є під шифром, який відображує внутрішній стан S в шифртекст C: $f_K(S) = C$. f пов'язує 2^d внутрішніх станів $\{S_j\}$ з 2^d шифротекстами $\{C_i\}$ із урахуванням 2^{2d} ключів $\{K[i, j]\}$.

Триплет $[\{C_i\},\{S_j\},\{K[i, j]\}]$ називається d-вимірною біклікою, якщо виконується така умова:

$$C_i = f_{K[i,j]}(S_j)$$

для усіх $i, j \in \{0,...,2^d - 1\}$. Інакше кажучи, в бікліці ключ $K[i, j]$ відображає внутрішній стан S_i в шифртекст C_j і навпаки.

Застосування біклік-аналізу до шифру Калина

Національний стандарт шифрування ДСТУ 7624:2014 (шифр Калина) [2] побудовано на основі структури SP-мережі. Він складається з декількох раундів шифрування (від 10 до 18), на кожному з яких виконується нелінійна заміна байтів стану (процедура SubBytes) та лінійне перемішування байтів стану (процедури ShiftRows та MixColumns). Стандарт підтримує різну довжину блоку: 128, 256, 512 бітів; відповідні варіанти алгоритму шифрування ми будемо позначати як Калина-128, Калина-256 та Калина-512.

Для проведення біклік-аналізу в першу чергу необхідно дослідити лавинні ефекти процедури шифрування та схеми генерації раундових ключів. На рисунку 1 схематично зображено зміни у байтах раундових ключів при їх генеруванні у шифрі Калина-512 з двох ключів шифрування, які відрізняються лише значенням першого байту.

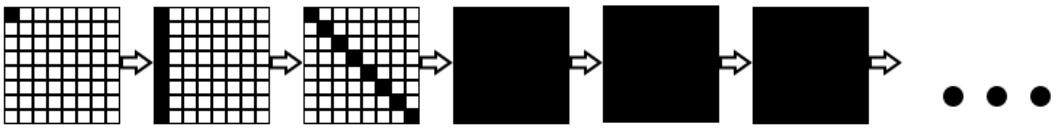

Рисунок 1 — Лавинні ефекти при генеруванні раундових ключів шифру Калина-512

Як видно з рисунку, різниця лише в одному байті ключа шифрування дає непередбачувані зміни у всіх байтах раундових ключів при генеруванні. Аналогічні властивості мають місце для шифрів Калина-128 та Калина-256. З цього випливає, що бікліка, необхідна для здійснення атаки за методикою, наведеною у [1], не може бути побудована. Таким чином, атака на основі біклік на шифр Калина неможлива за рахунок особливостей ключового розкладу.

Застосування біклік-аналізу до модифікованого шифру Калина*

Розглянемо послаблені версії шифру Калина, що будуть містити такі модифікації.

1. Заміна схеми генерування раундових ключів шифру Калина на схему генерування раундових ключів, аналогічну шифру AES. Оскільки Калина є AES-подібним шифром, для неї легко адаптується схема генерування раундових ключів AES.

2. Замішування ключа за допомогою операції XOR. Шифр Калина застосовує для замішування ключа операції XOR та додавання за модулем. Дана модифікація замінює додавання за модулем на XOR, забезпечуючи замішування ключа завжди однією і тією ж

операцією.

3. Вилучення MixColumns з останнього раунду шифрування. Дана модифікація залишає в останньому раунді шифрування, окрім додавання з ключем, лише операції SubBytes та ShiftRows.

Будемо позначати через Калина* шифр Калина із зазначеними модифікаціями.

Для шифру Калина*-512 було побудоване розбиття ключового простору на 2^{496} груп по 2^{16} елементів в кожній. Також була побудована трьохраундова бікліка зі спорідненими ключовими диференціалами (див. [1]). Таким чином, співпадіння перевірялись після 15 раундів шифрування.

Для шифру Калина*-256 було побудоване розбиття ключового простору на 2^{240} груп по 2^{16} елементів в кожній. Була побудована трьохраундова бікліка зі спорідненими ключовими диференціалами. Співпадіння перевірялись після 11 раундів шифрування.

До шифру Калина*-128 навіть після модифікацій не вдалось застосувати атаку на основі біклік в чистому вигляді, так як «вузька» форма матриці (2 стовпчики по 8 байтів) унеможливлює побудуву бікліки, необхідної для проведення атаки.

Оцінки складності побудованих атак на основі біклік для модифікованих шифрів Калина* наведено у таблиці 1.

Таблиця 1 — Оцінки складності атак на розглянуті шифри

Назва шифру	Оцінка складності атаки
Калина*-512	$2^{511.81}$
Калина*-256	$2^{255.7682}$
Калина*-128	Атака неможлива через специфіку форми матриці

Висновки

У даній роботі була досліджена можливість застосування аналізу на основі біклік до національного стандарту шифрування України — шифру Калина. Для оригінального шифру Калина було обґрунтовано неможливість його безпосереднього біклік-аналізу за допомогою існуючих методик. Для модифікацій шифру Калина з різними розмірами блоків було застосовано підходи та методи біклік-аналізу, отримано чисельні оцінки стійкості.

З одержаних результатів випливає, що оригінальний шифр Калина є стійким до атак на основі біклік, так як навіть атаки на послаблені версії шифру мають дуже велику складність. Така стійкість забезпечується перемішуючими властивостями шифру, великою кількістю раундів, специфікою розміру матриці ключів та особливостями схеми генерування ключів.

Список використаних джерел:

1.Bogdanov A. Biclique cryptanalysis of the full AES / A. Bogdanov, D. Khovratovich, C. Rechberger // Proceedings of ASIACRYPT'11. — LSCN. — vol 7073. — Springer, 2011. — P. 344–371.

2.Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Держспоживстандарт України, 2015. – 238 с.

3.Khovratovich D. Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family [електронний ресурс] / D. Khovratovich, C. Rechberger, A. Savelieva. — Режим доступу: http://eprint.iacr.org/2011/286.pdf

4.Mala H. Biclique cryptanalysis of the block cipher Square [електронний ресурс] / H. Mala — Режим доступу: http://eprint.iacr.org/2011/500.pdf