УДК 004.056.55:512.6+519.24

ПОБУДОВА ДИФЕРЕНЦІАЛЬНОЇ АТАКИ ЗБОЇВ НА МОДИФІКОВАНИЙ ШИФР QALQAN

М. А. Недождій[1,a], С. В. Яковлєв[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У даній роботі досліджується застосування диференціальних атак збоїв (DFA) на модифікований шифр Qalqan, що є кандидатом у національний стандарт Республіки Казахстан. Описано шифр і його модифікацію, з якою буде йти робота. Показано принцип застосування атак на останній і передостанній раунди шифру. Пояснена різниця у застосуванні збоїв на діагональний і не діагональний елемент матриці байтів ключа. Наведено рівняння для пошуку кандидатів у байти ключа за збитим і звичайним шифротекстами і пояснено процес цього пошуку. Наведено оцінки складності пошуку кандидатів у байти ключа.

Ключові слова: атака, збій, диференційний аналіз

Вступ

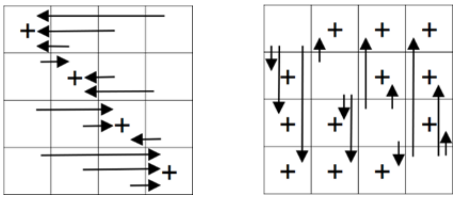
На сьогодні активно розвивається розділ криптографії під назвою легка криптографія. Суть цього розділу полягає у розробці криптосистем, які працюють якомога швидше і використовують якомога менше ресурсів при цьому. Таким криптосистемам дозволяється понижена стійкість до класичних атак, в порівнянні з традиційними криптосистемами, через меншу кількість ресурсів. Однак такі криптосистеми мають бути стійкими до певної низки інших атак, які можна реалізувати використовуючи мінімальні обчислювальні ресурси. До таких атак відносять атаки за сторонніми каналами, зокрема дифереціальні атаки збоїв (DFA). Концепт атак збоїв з'явився у 2001 році і швидко став одним з важливих критеріїв при побудові симетричних криптосистем у сфері легкої криптографії через свою простоту у реалізації і ефективність. На певну кількість сучасних шифрів було побудовано практичні атаки використовуючи цей підхід [1, 2].

У даній роботі буде побудована диференціальна атака збоїв на останній і передостанній раунди шифру Qalqan [3] і надана попередня оцінка складності атаки.

1. Структура шифру Qalqan

Симетричний блоковий шифр Qalqan було запропоновано у 2021 році як кандидат на національний стандарт шифрування Республіки Казахстан [3]. Даний шифр є орієнтованим на байтову архітектуру. Розмір блоку складає 128 бітів, довжина ключа може варіюватись від 256 до 1024 бітів з кроком у 128 бітів. В залежності від довжини ключа, схема шифрування містить від 17 до 23 раундів.

[a] fi.03maksimnedozhdii@gmail.com



(а) фаза «всмоктування» (б) фаза «розповсюдження»

Рис. 1. Схема роботи лінійного перетворення L

Шифр Qalqan побудовано на основі архітектури SP-мережі. Кожен раунд, окрім останнього, складається з трьох операцій: накладання раундового ключа, застосування нелінійного перетворення (S-блоку) та лінійного перетворення L, яке має унікальну структуру; останній раунд містить тільки операцію накладання ключа. У лінійному перетворенні шифру використовується побайтове додавання $\boxplus$ (тобто додавання за модулем 256 з переносом без виходу за межі байту). Ключі на усіх раундах, окрім першого і останнього, накладаються додаванням за модулем 2^{128}; у першому та останньому раундах накладання ключа відбувається побітовим додаванням $\oplus$.

Усі блоки відкритого тексту, проміжні шифротексти та раундові ключі представляються матрицями розміру 4×4. Лінійне перетворення $L : V_{128} \to V_{128}$ складається з фаз «всмоктування» і «розповсюдження». Схему обчислення перетворення L наведено на рис. 1.

Попередній аналіз криптографічної стійкості шифру Qalqan наведено у [4, 5]. Зокрема, у [5] було показано, що структура шифру має уразливості до диференціальних та лінійних атак, головними з яких

є низьке значення індексу розгалуження лінійного перетворення L та велика кількість його нерухомих точок.

У даній роботі розглядається модифікована версія шифру Qalqan із 17 раундами шифрування та довжиною ключа 256 бітів. Окрім першого і останнього раундів ключі будуть накладатись — як у модифікації запропонованій [5] — побайтовим додаванням $\boxplus$ без переносу за межі байту (тобто так, як додаються у перетворенні L). Відповідно, структура модифікованого шифру Qalqan стає повністю байт-орієнтованою, тому доцільно розглядати усі збої як випадкові спотворення на рівні окремих байтів проміжних шифротекстів.

2. Атака збоїв на модифікований шифр Qalqan

Для отримання кандидатів у байти ключа використовуються диференціальні атаки збоїв — атаки на реалізацію криптосистеми у певному обчислювальному середовищі. Основним інструментом таких атак є внесення збоїв у виконання криптографічних операцій для одержання інформації про ключі шифрування на основі відмінностей між коректним та збитим шифротекстами. Для цього збої (випадкові спотворення) вносяться у біти (у цій роботі байти) проміжних шифротекстів перед певною операцією раундової функції; аналітику при цьому доступні тільки результати шифрування, тобто фінальні шифротексти, обчислені правильно та зі збоями. Застосування декількох збоїв означає внесення іншого збою у текст і отримання іншого шифротексту, який можна використати для додаткового аналізу.

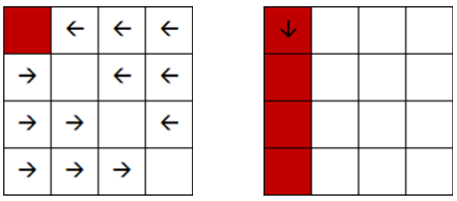
У наступних розділах 2.1, 2.2 буде описано процес побудови атак збоїв на останній і передостанній раунди модифікованої версії шифру Qalqan.

2.1. Атака збоїв на останній раунд шифру Qalqan

Атака на останній раунд шифрування визначається такою послідовністю дій:

- внесення збою у певний байт матриці;
- накладання ключа $K^{(r-1)}$ побайтовим додаванням $\boxplus$;
- застосування нелінійного перетворення — шару S-блоків;
- застосування лінійного перетворення L;
- накладання ключа $K^{(r)}$ побітовим додаванням $\oplus$ (фінальне маскування).

У цій атаці збій буде вноситись у діагональний елемент матриці. Розповсюдження цих збоїв є важливим параметром у атаці збоїв, на яке не впливають накладання ключа побайтовим додаванням, S-блок та маскування. Відповідно лавинний ефект виникає лише при застосуванні лінійного перетворення L. При цьому значення збою поширюється на цілий стовпчик матриці і усі байти стовпчика спотворюються однаковим чином. Дію лавинного ефекту можна побачити на рис. 2.



(а) збій у одному елементі (б) поширення на увесь стовпчик

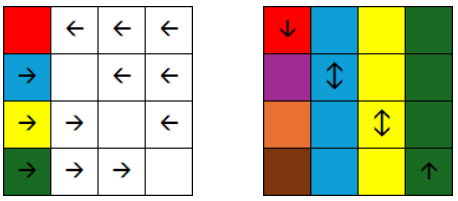
Рис. 2. Лавинний ефект на останньому раунді при збитті байту $a_{1,1}$

Байтову різницю між збитим і звичайним шифротекстом позначимо як β. Позначимо лівий стовпчик нормального шифротексту через y_1, y_2, y_3, y_4, тоді лівий стовпчик збитого шифротексту виражається через $y'_i = y_i \boxplus \beta$. Застосувавши перебір усіх можливих значень байтів пари ключів (2^{16}) можна знайти усі значення, для яких виконується рівність

$$(y_1 \oplus K_1^{(r)}) - (y'_1 \oplus K_1^{(r)}) = (y_2 \oplus K_2^{(r)}) - (y'_2 \oplus K_2^{(r)}).$$

Якщо зафіксувати ці значення і повторити пошук з y_3, y'_3, y_4, y'_4, аналогічно отримуємо кандидати на байти пари ключів $K_3^{(r)}, K_4^{(r)}$. Якщо виявиться, що існує декілька кандидатів у потенційні байти пар ключів, перевіряємо рівність на інших четвірках. Кожне рівняння такого вигляду залишає декілька варіантів на значення байтової різниці, з якого можна отримати в середньому $2^8 - 2^{10}$ кандидатів у байти ключа, з максимальним значенням близько 2^{15} варіантів. Внесенням збоїв у кожен діагональний елемент можна досягти значного зменшення кількості кандидатів усіх байтів останнього раундового ключа з 2^{128} до приблизно $2^{64} - 2^{120}$. Ці значення можна зменшити за рахунок крос-валідації, яка полягає у обрахунку декількох різних рівнянь, що використовують однакові пари елементів (наприклад, окремо обчислити y_1, y'_1, y_2, y'_2, а потім y_1, y'_1, y_3, y'_3). Збиття одного і того ж тексту двома різними збоями майже напевно дозволить отримати точне значення байту ключа.

Необхідно зазначити, що збої можна вносити і не у діагональні елементи матриці ключа. Внесення збою такого характеру дозволяє отримати, окрім основного активного стовпчику (такого, у якому є ненульова відмінність між збитим і звичайним шифротекстами), у який розповсюдиться збій з діагонального елементу на одному рядку з обраним, також активний не діагональний елемент, обраний нами. Цей варіант, коли збій вноситься у не діагональний байт ключа, призводить до виникнення п'яти замість чотирьох активних байтів, що дозволяє одразу отримати п'ять кандидатів у байти ключа. Відповідно, внесення збою у три не діагональні елементи дозволяє суттєво зменшити кількість кандидатів у байти ключа для п'ятнадцяти з шістнадцяти байтів ключа. Це може бути суттєво для випадку, коли з точки зору реалізації чи зовнішніх чинників кількість збоїв, доступна зловмиснику, є обмеженою.



(а) зміна збоїв у першому стовпчику

(б) поширення на усю матрицю

Рис. 3. Лавинний ефект на останньому раунді при збитті байту $a_{1,1}$ на передостанньому раунді

2.2. Атака збоїв на передостанній раунд шифру Qalqan

Ідея атаки на усі попередні раунди є аналогічною до атаки на останній раунд. У елемент вноситься збій, який розповсюджується на інші елементи матриці. Відмінністю є безпосередньо значення збою, адже додаткові застосування S-блоку та інших операцій повністю змінюють значення збою на деяке інше, яке аналітик не здатен передбачити. Додаткове застосування перетворення L розповсюджує збій на усі клітинки матриці. Припустимо, що на передостанньому раунді було внесено збій, аналогічно до рис. 2. Дію лавинного ефекту на останньому раунді для такого випадку зображено на рис. 3

Позначимо збої у клітинках першого стовпчика матриці на рис. 3(а), як α, β, γ, δ. В результаті застосування другого перетворення L отримаємо диференціал між звичайним і збитим шифротекстом:

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha \boxplus \beta & \beta & \gamma & \delta \\ \alpha \boxplus \gamma & \beta & \gamma & \delta \\ \alpha \boxplus \delta & \beta & \gamma & \delta \end{pmatrix}$$

Повторюючи схему атаки, описану у розділі 2.1, можна відновити кандидати у байти ключа. Далі, на основі одержаних кандидатів у байти ключа, можна по відомих звичайному і збитому шифротексту відновити значення збоїв β, γ, δ. Підставивши ці значення у перший стовпчик, отримуємо систему співвідношень, пов'язаних однаковим диференціалом α, що дозволить ще раз застосувати техніку, описану у розділі 2.1. Таким чином, атака на передостанній раунд дозволяє отримати кандидати у правильні байти ключа для усієї матриці. Як було зазначено у розділі 2.1, в середньому буде отримано $2^8 - 2^{10}$ кандидатів на кожен стовпчик ключа.

Внесення збою у не діагональний елемент для атаки на передостанній раунд призводить до ускладнення пошуку кандидата через збільшення кількості рівнянь, які потрібно розв'язати. Як було зазначено, навіть внесення збою у діагональний елемент призводить до змін в усіх байтах матриці, а з додаткових перетворень отримується більше інформації. Завдяки цьому, внесення збою у не діагональний елемент матриці дозволяє утворити більше залежностей за допомогою більшої кількості рівнянь, а їх обчислення дозволяє провести кращу крос-валідацію для отриманих кандидатів, що дозволить уточнити отримані результати.

Висновки

У даній роботі було розглянуто шифр Qalqan і запропоновано диференціальні атаки збоїв (DFA) на передостанній і останній раунди модифікованої версії цього шифру. Показано, що складність пошуку кандидату у байти ключа складає від $8 \cdot 2^8$ до $8 \cdot 2^{15}$, що дає складність пошуку самого ключа від 2^{64} до 2^{120}, і може бути суттєво зменшена, якщо використовувати усі можливі комбінації одержаних співвідношень для крос-валідації. В подальшому планується розглянути атаки збоїв на центральні раунди шифрування з використанням статистичних методів.

Перелік використаних джерел

1. *Piret G., Quisquater J. J.* A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad // CHES 2003. — 2003. — С. 77—88.
2. *Яковлєв С.* Атаки збоїв на шифр ДСТУ ГОСТ 28147:2009 // Інформаційна безпека людини, суспільства, держави. — 2015. — №2(18). — С. 124—136.
3. Алгоритм шифрования Qalqan / L. Gorlov, R. Ibrayev, G. Ospanov, R. Itemirov, I. Kiyashko // Proceedings of VI International Scientific Conference "Computer Science and Applied Mathematics". — 2021. — 29 жовт. — С. 458—463. — URL: https://conf.iict.kz/wp-content/uploads/2021/11/6th_csam.29.09-02.10.21_sbornik.pdf.
4. About Cryptographic Properties of the Qalqan Encryption Algorithm / N. Seilova, A. Kungozhin, R. Ibrayev, L. Gorlov, Z. Ospanov, R. Itemirov, I. Kiyashko // CEUR Workshop Proceedings "Cybersecurity Providing in Information and Telecommunication Systems II". —: — CPITS-II'2021. — С. 206—215. — URL: https://ceur-ws.org/Vol-3187/paper19.pdf.
5. *Yakovliev S., Stolovych M.* On the Security of Qalqan Cipher against Differential Cryptanalysis // Theoretical And Applied Cybersecurity. — 2022. — Т. 4, № 1. — URL: https://doi.org/10.20535/tacs.2664-29132022.1.274112.