АНАЛІЗ СХЕМ РОЗГОРТАННЯ КЛЮЧІВ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Горбенко І.Д., Шапочка Н.В.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Леніна, 14, каф. БІТ, тел. (057) 702-14-25
E-mail: natali_shap@mail.ru

Key expansion scheme is carried out in this work. Cryptographic analysis methods concerned to key expansion scheme are considered. Projects of block symmetric ciphers are presented and requirements to key expansion schemes are studied. Because of serious deficiency the national algorithm "Kalina" is studied and requirements to its key expansion scheme are proposed.

Одним з найважливіших етапів створення сучасного блокового симетричного шифру (БСШ) є здатність шифру протистояти найпотужнішим на сьогоднішній день методам лінійного і диференціального криптоаналізу, які відносяться до атак на циклову функцію. Проте останнім часом одержали розвиток методи криптоаналізу, які відносяться до атак на схеми розгортання ключів. Проведений аналіз сучасних БСШ показав, що багато сучасних криптографічних алгоритмів, що володіють цикловою функцією, здатною протистояти атакам на основі лінійного і диференціального криптоаналізів, виявляються вразливими до атак на схеми розгортання ключів.

На початку 90-х років критика алгоритмів БСШ почала підсилюватися. У відкритій закордонній пресі з'явився ряд фундаментальних робіт, що були присвячені вирішенню завдань криптоаналізу БСШ. У першу чергу це лінійний криптоаналіз Матсуі і диференціальний криптоаналіз Біхама й Шаміра, а також розширення зазначених атак. У вказаних роботах критиці піддається схема формування циклових підключів БСШ DES. Далі критиці була піддана простота схеми розгортання ключів, описано існування 4 слабких і 12 наполовину слабких ключів, а також властивість інвертування, що дозволяє скоротити пряме перебирання усіх ключів з 2^{55} до 2^{54}. В процесі розгляду алгоритму DES та його модифікації DEA було виявлено слабкі й наполовину слабкі ключі, для чого було використано поняття двоїстих ключів.

В подальшому проводився ряд робіт по аналізу схем розгортання ключів у БСШ. Фундаментальною роботою можна вважати публікацію Біхама [1]. В цій роботі вперше описана атака на схему розгортання ключів типу «зв'язані ключі», яка могла бути застосованою до БСШ DES і LOKI. Однак цей метод криптоаналізу з атакою на схему розгортання ключів мав більше теоретичну, чим практичну цінність, і не представляв у порівнянні з диференціальним та лінійним криптоаналізом циклової функції шифру реальної погрози для БСШ.

У зв'язку із вказаним пошук нових рішень торкнувся вдосконалювання криптографічних перетворень циклової функції. З'явився ряд нових криптографічних алгоритмів. Найбільшої уваги з них заслуговує алгоритм PES, що став основою при розробленні Європейського стандарту IDEA, а також алгоритми RC5 та SAFER. Особливістю вказаних шифрів є те, що схеми розгортання ключів нових БСШ формують циклові підключі аналогічно БСШ DES, по суті вони являють собою алгоритми вибору певних біт із секретного ключа. В подальшому на названі шифри були розроблені ефективні методи криптоаналізу через схеми розгортання ключів.

В результаті аналізу схеми розгортання ключів алгоритму IDEA було виявлено кілька класів слабких ключів. Найбільший із цих слабких класів становить множину 2^{51} ключів. Причому приналежність ключа. що застосовується, до цього класу, може бути перевірена двома шифруваннями й виконанням невеликої кількості додаткових обчислень. Якщо ключ належить цьому класу, то він може бути відновлений після 16 зашифрувань відкритих текстів з підібраною різницею, а також порядку 2^{16} групових операцій і 2^{17} шифрувань перевірки ключа.

Схема розгортання ключів БСШ SAFER K-64 виявилася уразливою до атаки на зв'язані ключі, що запропонована Біхамом. Це пояснюється тим, що схема розгортання ключів має недостатній лавино утворюючий ефект і генерує всі циклові ключі за однаковим алгоритмом. Запропонована оригінальна схема криптоалгоритму продовжила свій розвиток у криптоалгоритмах SAFER SK-128, SAFER+ і SAFER++.

Також буда знайдена диференціальна атака на RC5, а також визначено безліч слабких ключів, для яких ця атака стає ще ефективнішою. Криптоалгоритм одержав свій розвиток в RC6 зі змінами в схемі розгортання ключів.

В подальшому до кінця 90-х років з'являється ряд нових ефективних методів криптоаналізу схем розгортання ключів БСШ, які засновані на використанні як диференціального, так і лінійного методів криптоаналізу. Принципово необхідно виділити диференціальний криптоаналіз на зв'язаних ключах, атаку ковзання і її розширення. Особливістю таких атак, у порівнянні з атаками на циклову функцію БСШ (наприклад, диференціальним і лінійним криптоаналізом), є більша ефективність, що полягає в слабкій залежності від кількості ітерацій що використаються в шифрі.

Загальною рекомендацією є пропозиція уникати лінійних алгоритмів при формуванні циклових підключів, а також щоб процес вироблення підключів був важко оборотним. При цьому існуючий між цикловими підключами зв'язок повинен бути складним з точки складності аналізу.

В проекті AES уперше була зібрана воєдино безліч різних криптографічних алгоритмів з різною архітектурою й піддані цілеспрямованому, детальному аналізу. В процесі проведення конкурсу були визначені нові вимоги до схем розгортання ключів. У представлених на конкурс БСШ схеми розгортання ключів суттєво відрізняються від DES-подібних. Крім того, відсутність основоположних принципів проектування схем розгортання ключів привела до того, що розроблювачі шифрів керувалися суб'єктивним розумінням побудови схем розгортання ключів. У підсумку більша частина шифрів виявилися уразливими до атак на схеми розгортання ключів. Так, у проекті AES брали участь БСШ Deal, Rijndael, SAFER+, DFC, MAGENTA, CRYPTON, HPC, LOKI97, MARS, RC6, Serpent, Twofish, CAST, E2, FROG. Але більшість із названих БСШ були уразливі до атак на схеми розгортання ключів, в тому числі: SAFER+, CRYPTON, DFC, FROG, HPC, MAGENTA. Для інших БСШ атаки на схеми розгортання ключів були реалізовані на неповну кількість ітерацій, але виявилися найбільш ефективними в порівнянні з атаками на циклову функцію алгоритму. Так прикладом може служити БСШ Rijndael, для якого знайдено 9 циклова атака на зв'язаних ключах (версія алгоритму з довжиною ключа $l_k = 128$ й кількістю ітерацій $r = 12$) Фергусоном і розширена Square-атака С. Люка на 7-ми цикловий варіант алгоритму.

Наш аналіз БСШ Rijndael [2] зводився до пошуку схованих аномалій у розгорнутому ключі. Було підтверджене існування сильних лінійних зв'язків між бітами циклових підключів, однак було виявлено, що використання циклової функції з високими криптографічними властивостями дозволяє компенсувати ці вади вже після чотирьох ітерацій. Було показано, що в БСШ із «криптографічно слабкою» схемою розгортання ключів (на яку існує атака), необхідно використовувати підвищену кількість ітерацій. Крім того необхідно приділяти особливу увагу розробці циклової функції, що задовольняє вимогам високої криптостійкості. В процесі аналізу також підтверджено, що використання схеми формування циклових підключів з високими криптографічними властивостями дозволить знизити рівень витрат на проектування циклової функції й зменшити кількість ітерацій [3]. Також показано, що криптографічно сильна схема розгортання ключів підвищує стійкість до лінійного й диференціальному криптоаналізу.

В процесі аналізу було визначено наступні недоліки схеми вироблення підключів Rijndael:

- можливість відновлення майстер-ключа по одному підключу;

- досить прості залежності між підключами (вразливість до атак на зв'язаних ключах);
- перший з підключів – майстер-ключ;
- слабкий вплив змін бітів майстер-ключа на біти перших підключів (задовільні результати – тільки 5-7-й підключі);
- використання в схемі розгортання іншої конструкції, відмінної від циклової функції;

різна складність генерації послідовності підключів для зашифрування та розшифрування.

У зв'язку з наявністю істотних недоліків на національному рівні ЗАТ «Інститут інформаційних технологій» було розроблено алгоритм «Калина», в якому було прийнято використовувати принципово нову схему розгортання ключів.

Вимоги до схеми розгортання ключів алгоритму «Калина»:

- нелінійна залежність кожного біта кожного підключа від кожного біта майстер-ключа, відповідно забезпечення всіх необхідних лавинних властивостей і відсутність «проміжних точок»;
- забезпечення стійкості до всіх відомих атак на схеми вироблення підключів;
- відсутність слабких ключів, на яких може відбутися погіршення криптографічних властивостей шифру;
- неможливість (висока обчислювальна складність) відновлення майстер-ключа по одному або декількох підключам;
- простота реалізації, використання циклового перетворення шифру;
- обчислювальна складність генерації всіх підключів не перевищує складності однієї операції шифрування;
- можливість генерації підключів у будь-якому порядку (як для зашифрування, так і для розшифрування).

Дана схема являється стійкою, має низьку обчислювальну складність, проста в реалізації та зручна у використанні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. E. Biham New types of cryptanalytic attacks using related keys //Advances in Cryptology.– Proceedings Eurocrypt'93.– LNCS 765.– 1993.– P. 398-409.
2. Бондаренко М.Ф., Лепеха А.Н. Исследование статистических свойств схемы разворачивания ключей FIPS-197 //Радиотехника: Всеукр межвед. науч.-техн. сб.– 2004. Вып. 136. С.101–107.
3. L. R. Knudsen, J. Mathiassen On The Role Of Key Schedules In Iterated Block Ciphers //LNCS'2004.– 2004.– P 322-334.