УДК 681.3.06

В. Сокирук (м. Вінниця)

ОСОБЛИВОСТІ ПРОЦЕДУРИ РОЗГОРТАННЯ КЛЮЧА БСШ НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ 2^n

Процедура розгортання ключа – важлива складова частина блокового симетричного шифру (БСШ), оскільки недоліки в роботі даної процедури (наявність слабких, еквівалентних, зв'язаних ключів тощо) дозволяють значно спростити криптоаналіз БСШ, навіть якщо алгоритм зашифрування в цілому стійкий до усіх видів криптографічних атак.

Як правило, для отримання необхідної кількості підключів з секретного ключа використовуються спеціальні алгоритми, які діють за принципом генератора псевдовипадкових чисел, однак такий підхід потребує ретельного аналізу стійкості алгоритму розгортання ключа і несе в собі небезпеку, що певні статистичні закономірності можуть бути виявлені вже під час використання БСШ. Більш надійним є використання криптографічних конструкцій, чиї статистичні характеристики добре відомі. Так, в деяких БСШ, таких як Khufu, Blowfish, SEAL та ін., для розгортання ключа використовується хеш-функція. Також можливим підходом є використання процедури зашифрування самого БСШ. Однак на практиці такі підходи використовуються не часто, оскільки до процедури розгортання ключа сучасного БСШ висуваються жорсткі вимоги щодо швидкості та ефективності як програмної, так і апаратної реалізації.

БСШ на основі арифметичних операцій за модулем 2^n (де n – розмір блоку), описаний в попередніх роботах автора, використовує для зашифрування три n-розрядних підключа K_1, K_2 та K_3. Оскільки підключі K_2 та K_3 є множниками в двох операціях множення, виникає небезпека отримання після розгортання ключа таких їх значень, які можуть бути використані для спрощення подальшого криптоаналізу. В попередніх роботах автора показано, що алгоритм зашифрування даного БСШ є статистично безпечним, а його програмна реалізація володіє високою продуктивністю на сучасних мікропроцесорах. Однак використання однакової процедури для створення підключів та зашифрування може призвести до появи «слабких» ключів. Тому в даному випадку для розгортання ключа пропонується використовувати алгоритм зашифрування з меншим розміром

зашифрування з меншим розміром блоку, наприклад $n = 32$, що є більш ефективним, а також дозволяє уникнути залежності між підключами.

Для отримання 3-х n-розрядних підключів необхідно зашифрувати в режимі зчеплення блоків (CBC) блок даних розміром $3 \cdot n$ розрядів за допомогою процедури зашифрування, яка описується виразом:

$$C = \left(\left(\left(\left(M \oplus K_1^I\right) \times K_2^I\right)_{\bmod 2^{32}}\right)^{\leftrightarrow 1} \times K_3^I\right)_{\bmod 2^{32}}, \qquad (1)$$

де K_1^I, K_2^I та K_3^I - фіксовані підключі, значення яких визначаються послідовністю з 96-ти розрядів дробової частини числа π таким чином, щоб K_2^I та K_3^I були непарними.

В загальному випадку процедура розгортання ключа представляється таким чином:

$$K_j = \begin{cases} E(M_j \oplus IV, K_1^I, K_2^I, K_3^I), j = 0 \\ E(M_j \oplus K_{j-1}, K_1^I, K_2^I, K_3^I), j = 1..\dfrac{3 \cdot n}{32} - 1 \end{cases}, \qquad (2)$$

де $E(M, K_1^I, K_2^I, K_3^I)$ - процедура зашифрування j-го 32-розрядного блоку M_j за допомогою виразу (1), IV – нульовий вектор ініціалізації.

Вхідний блок даних M будується на основі секретного ключа K таким чином, щоб на кожній ітерації зашифрування частина ключа K використовувалась в процесі зашифрування. Після виконання всіх кроків процедури розгортання ключа (2), молодші розряди отриманих підключів K_2 та K_3 встановлюються в 1.

Описаний підхід до побудови процедури розгортання ключа є простим, а статистичні характеристики отриманих таким чином підключів відповідають оцінкам, отриманим для БСШ в цілому в попередніх роботах автора. Імовірність знаходження зв'язаних та слабких ключів є низькою.

Важливу роль в алгоритмі відіграє розподіл розрядів секретного ключа при побудові блоку М, розрядність якого перевищує розрядність секретного ключа. Ігнорування даної процедури дозволить підібрати алгоритмічним шляхом такі ключі K, за яких будуть згенеровані потенційно слабкі підключі.