УДК 004.056.55

О.В. Дмитришин

Вінницький національний технічний університет, Вінниця

ОПЕРАЦІЯ МНОЖЕННЯ ЯК БАЗОВИЙ КРИПТОГРАФІЧНИЙ ПРИМІТИВ В СИМЕТРИЧНИХ БЛОКОВИХ ШИФРАХ

В симетричних блокових шифрах, наприклад IDEA, RC6, Nimbus тощо, множення за модулем є одним із базових примітивів, яке є зручним під час розробки програмних та апаратних засобів, оскільки множення є вбудованою командою в більшості процесорів. Популярність операції множення пояснюється тим, що вона є достатньо цікавим оператором перемішування бітів, яку можна використовувати як альтернативу операціям перестановки та заміни.

Проте, одним з недоліків шифрів, таких як XMX, Nimbus, MultiSwap тощо, які зокрема використовують операцію множення за відомим модулем є їхня нестійкість до диференційного криптоаналізу із використанням мультиплікативних диференціалів, сам принцип описаний в [1]. Мультиплікативні диференціали розраховуються на підставі відомого значення модуля, який проходить через перестановки, додавання за модулем 2^n, операцію виключного-АБО і дозволяє відновити раундові ключі.

В роботі [2], проаналізовано можливі варіанти комбінацій секретних модулів та множників і встановлено, що доцільно використовувати різні значення модулів на кожному раунді. До недоліків розглянутих методів шифрування можна віднести те, що значення модуля на наступному раунді шифрування мало бути більшим за попереднє, що зменшувало крипостійкість шифрування із урахуванням використовуваних процедур розширення ключів описаних в [3]. Окрім того, розрядність модулів була більша за розрядність процесора, що ускладнювало програмну реалізацію та висувалися доволі складні вимоги до формування підключів шифрування, складовими яких є модуль та множник.

В якості вирішення проблеми надлишковості вихідного блоку даних та з метою усунення залежностей між модулями пропонується використовувати таке модульне множення:

$$X \circ A \bmod m = \begin{cases} X \cdot f(m') \bmod m', \text{ якщо } X < m'; \\ (X\text{-}m') \cdot f(m'') \bmod m'' + m', \text{ інакше,} \end{cases}$$

де X – n-бітний вхідний блок даних;

m′, m″ – n-бітні модулі, $m''=2^n-m'$, $m'=\overline{2^{n-2};3\cdot 2^{n-2}}$;

f(m′), f(m″) – n-бітні множники, які визначаються за такою функцією ($m = m_{n-1}m_{n-2}\ldots m_1m_0$):

$$f(m) = \begin{cases} (m \pm 1) >> 1, \text{якщо } m_0 = 1; \\ (m \pm 2) >> \text{,якщо } m_0 = 0 \text{ і } m_1 = 0; \\ (m+4) >> 1, \text{якщо } m_0 = 0 \text{ і } m_1 = 1. \end{cases}$$

Обернено мультиплікативні f(m′) і f(m″) відповідно за модулями m′ і m″ знаходяться таким чином:

$$f^{-1}(m) = 2, \text{ якщо } f(m) = (m+1) >> 1 \text{ і } m_0 = 1;$$

$$f^{-1}(m) = m-2, \text{якщо } f(m) = (m-1) >> 1 \text{ і } m_0 = 1;$$

$$f^{-1}(m) = (m \pm 2) >> 1, \text{якщо } m_0 = 0 \text{ і } m_1 = 0;$$

$$f^{-1}(m) = (m+4) >> 2, \text{якщо } f(m) = (m+4) >> 1, \; m_0 = 0 \text{ і } m_1 = 1;$$

$$f^{-1}(m) = (m + f(m)) >> 1, \text{якщо } f(m) = (m+4) >> 1, \; m_0 = 0 \text{ і } m_1 = m_2 = 1;$$

$$f^{-1}(m) = (m - f(m)) >> 1-1, \text{ якщо } f(m) = (m\text{-}4) >> 1, \; m_0 = 0 \text{ і } m_1 = m_2 = 1.$$

Застосування вище розглянутого модульного множення та функцій знаходження взаємно простих чисел дозволяють будувати процедури розширення ключів «на льоту».

В роботі [1], для модульного множення з відомим модулем рекомендується використовувати як мінімум дві групи несумісних операцій. Проте, для модульного множення із невідомим модулем, яке протидіє визначенню мультиплікативних диференціалів можна використовувати як одну, так і більше несумісних груп операцій.

Список літератури

1. Multiplicative differentials / N. Borisov, M. Chew, R. Johnson, D. Wagner // Fast Software Encryption: 9th International Workshop on table of contents. – 2002. – Vol. 2365. – P. 17-33.

2. Лужецький В.А. Блокові шифри для режиму роботи ECB / В.А. Лужецький, О.В. Дмитришин // Інформаційні технології та комп'ютерна інженерія. – В.: ВНТУ, 2008. – № 1 (11). – С. 154-158.

3. Лужецький В.А. Процедури розгортання ключів для блокових шифрів на основі арифметичних операцій за модулем / В.А. Лужецький, О.В. Дмитришин // Інформаційні технології та комп'ютерна інженерія. – В.: ВНТУ, 2009. – № 2 (15). – С. 69-74.