УДК 004.056.55

ВИКОРИСТАННЯ ОПЕРАЦІЇ МНОЖЕННЯ ЗА СЕКРЕТНИМ ЗНАЧЕННЯМ МОДУЛЯ

О.В. Дмитришин, аспірант
Вінницький національний технічний університет
olexanderdm@gmail.com

В криптографії, під час розробки криптографічних засобів захисту використовують різні криптопримітиви. Зокрема, операцію множення за модулем, яка нелінійним чином зв'язує переважну більшість бітів вихідного блоку даних від вхідного. На сьогоднішній день розробники шифрів використовують операцію множення за відкритим модулем 2^n, $2^n \pm 1$, оскільки використання фіксованого модуля спрощує реалізацію операції множення та пошуку взаємно простих чисел, обернено мультиплікативних за заданим модулем.

Так, наприклад, в симетричних блокових шифрах операцію множення використовують як:

- деяку модифіковану операцію інверсії, оскільки відомі значення множника та модуля;
- допоміжну операцію для зав'язки підблоків даних, при цьому не вимагається пошук обернено мультиплікативних елементів;
- безпосередній криптопримітив, для того, щоб перетворення було зворотне, необхідно знаходити обернено мультиплікативні елементи.

Проте, встановлено, що доцільно використовувати різні значення модулів, оскільки в такому випадку для двох послідовних множень буде отримано дві групи несумісних

операцій множення за різними модулями, які не задовольнятимуть асоціативному закону:

$$a\cdot(b\cdot c)\neq(a\cdot b)\cdot c.$$

Операцію множення n-бітних чисел достатньо ефективно реалізують сучасні процесорах, проте множення за змінним модулем, вимагає, щоб модуль не був більшим за 2^n.

Для вирішення даної проблеми та з метою усунення залежностей між модулями пропонується використовувати таке множення за секретним значенням модуля:

$$X\times A \bmod m=\begin{cases} X\cdot A' \bmod m', \text{якщо } X<m', \\ (X-m')\cdot A'' \bmod m''+m', \text{якщо } X\geq m', \end{cases} \quad (1)$$

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

A', A'' – взаємно прості числа з m' і m'' відповідно.

Використання таких двох послідовних множень за різними модулями утворює групи несумісних операцій. Окрім того, оскільки значення модуля залишається невідомим, то це дозволяє протидіяти криптоаналізу на основі мультиплікативних диференціалів.

Якщо замість операції множення «×» в формулу (1) підставити операцію додавання «+», то отримаємо:

$$[X+A] \bmod m=\begin{cases} [X+A'] \bmod m', \text{якщо } X<m', \\ [(X-m')+A''] \bmod m''+m', \text{якщо } X\geq m', \end{cases} \quad (2)$$

де A', A'' – n-бітні доданки, $A'<m'$ і $A''<m''$.

Послідовне використання операції додавання згідно (2) дозволяє отримувати групи несумісних операцій, які не задовольнятимуть асоціативному закону:

$$a+(b+c)\neq(a+b)+c.$$