УДК 681.32

# ШВИДКІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ СИСТЕМ АЛГЕБРАЇЧНИХ ПОРІВНЯНЬ

**В.А. Лужецький, д.т.н., професор,**
**М.Л. Гаєвський, магістр з ІБ**
**Вінницький національний технічний університет**

Останнім часом багато вчених відходять від стандартних методів побудови блокових шифрів. Основою багатьох таких методів є використання різних теоретико числових перетворень.

Основна ідея запропонованого способу шифрування полягає у виконанні обчислень з використанням матриці Уолша:

$$\mathbf{C} \equiv (\mathbf{H} \times \mathbf{M}) \bmod m,$$

$$\mathbf{M} \equiv (\mathbf{H} \times \mathbf{C}) \bmod m,$$

де **H** – матриця Уолша порядку N;

**M** – вектор відкритого повідомлення;

m – модуль;

**C** – вектор зашифрованого повідомлення.

Вектор відкритого повідомлення **M** складається з блоків даних розрядністю L = var:

$$\mathbf{M} = \{m_1, m_2, ..., m_g\},$$

У запропонованому способі існують два змінних параметри перетворення, які залежать від секретного ключа K: N – розмірність перетворень, яка визначається функцією $f_1(K)$, і n – розрядність даних, яка визначається функцією $f_2(K)$.

$$N = f_1(K)$$

$$n = f_2(K)$$

Розрядність блоку даних L дорівнює добутку розмірності перетворення та розрядності даних.

$$L = N \cdot n$$

Таким чином, розрядність блоку L також змінна величина.

Для забезпечення оптимального рівня крипостійкості та швидкості шифрування даних рекомендується виконувати 12 раундів перетворень. Розшифрування повідомлення виконується в зворотному до зашифрування порядку.

Для визначення змінних параметрів перетворення пропонується використовувати регістр зсуву з лінійним зворотнім зв'язком. Початковий стан регістра представляє собою секретний ключ. Оскільки стандартом AES рекомендується використовувати секретний ключ розміром не менше 128 розрядів, пропонується використовувати такий поліном для побудови лінійного регістра зсуву зі зворотнім зв'язком:

$$f(x) = x^{128} + x^7 + x^2 + x + 1$$

Такий генератор випадкових чисел буде мати максимальний період:

$$T = 2^{128} - 1$$

Вихідна послідовність псевдовипадкових чисел ділиться на послідовності по 5 біт, 3 з яких визначають розмірність перетворень, а 2 – розрядність даних. Можливі варіанти розмірності перетворень такі:

2, 4, 8, 16, 32, 64, 128, 256.

Можливі варіанти розрядності даних:

8, 16, 32, 64

Перевагою швидкого перетворення Уолша є те, що його реалізація вимагає тільки операцій додавання і віднімання в кількості $N \cdot \log_2 N$, що забезпечує достатньо високу швидкість шифрування інформації. Отримано оцінку середньої швидкості шифрування (2,4 оп./біт), що свідчить про покращення значення цього критерію порівняно з іншими блоковими шифрами.