УДК 681.32

БЛОКОВИЙ ШИФР НА ОСНОВІ НЕДЕРМІНОВАНОГО АЛГОРИТМУ

В. А. Лужецький, д. т. н., професор
А. В. Остапенко, магістрант
Вінницький національний технічний університет
asja87@gmail.com

Постійно зростаючі вимоги до шифрів, врахування ними особливості сучасної елементної бази обумовлює потребу у створенні нових підходів до реалізації блокових шифрів. Пропонується будувати блоковий шифр на основі використання недетермінованих алгоритмів. Ідея цього підходу полягає в тому, що перетворення на кожному із раундів складається з елементарних перетворень набір і послідовність виконання яких визначаються певними ознаками, що формуються з ключової інформації.

З точки зору секретних систем за Шеноном даний блоковий шифр можна представити як комбінацію «взваженої суми» та «добутку», тобто :

$$S=\prod_{i=1}^{n}\ (\sum_{j=1}^{m} p_{ij}\cdot T_{ij}),\ \sum_{j=1}^{m} p_{ij}=1,$$

де T_{ij} – *ij*-а секретна система;

p_{ij} – ймовірність вибору *ij*-ї секретної системи.

Основними аспектами розробки даного підходу є реалізація механізму формування ознак та створення множини базових мікроопераций. Тобто для нього буде введена множина яка буде характеризувати вигляд функції перетворення F на певному етапі алгоритму. Тоді:

$$P_r=F_q\,(C_k,\ K_k),\ P=\{F_1,\ F_{2,\ldots},F_L\},$$

де F_l – множина різних за виглядом функцій перетворення визначених ознакою q, $(i=1\ldots L)$, P_r – раундові перетворення, r – кількість раундів.

В такому випадку залежно від ознаки q на базі використання множини мікрооперацій буде формуватися певний вигляд функції перетворення F та алгоритму шифрування в цілому.

Для побудови недетермінованих алгоритмів пропонується система базових мікрооперацій в якій виділяються два основних вида мікрооперацій:

- одноопераднді (циклічний зсув на k біт (вліво, вправо), інвертування);
- двоопераднді(додавання за модулем 2 та 2^n).

На основі визначених видів базових мікрооперацій можна побудувати базові структури операцій та описати графічно і мнемонічно можливі реалізації різноманітних раундових перетворень, що забезпечить достатню кількість варіантів для оперування у блоковому шифрі.

Множина ознак включає три вида ознак серед яких:

- ознака визначення виду перетворення (256 варіантів);
- ознака визначення кількості оброблюваних підблоків (2,3,4,5);
- ознака визначення розрядності підблоку (8, 16,32, 64 біт).

З використанням вищеописаних ознак може бути побудовано $4 \cdot 4 \cdot 256 = 4096$ різних алгоритмів для одного раунду перетворення.

Запропонований набір базових мікрооперацій та видів ознак дозволяє створювати високошвидкісні блокові шифри з достатньо простою програмною та апаратною реалізацією.