ВИКОРИСТАННЯ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ В ПОСТ-КВАНТОВИЙ ПЕРІОД

Ковтун К. О., Сєвєрінов О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком квантових обчислень та створенням нових квантових комп'ютерів більш гостро постає питання криптографічного захисту інформації. В даний момент теоретично квантовий комп'ютер може зруйнувати більшість класичних алгоритмів, таких як RSA або DSA. Проте деякі класичні криптосистеми, що базуються на обчислювально-складних завданнях, сильно відрізняються від зазначених вище і їх набагато складніше вирішити, їх складність залишається незалежною від появи та розвитку квантових обчислень [1].

Однією із форм захисту конфіденційної інформації є її шифрування. В даний момент існує безліч теоретично стійких шифрів, проте з ростом обчислювальних потужностей такі шифри можуть швидко застаріти. Так, наприклад, для стійкого для свого часу DES найпростіша атака - це перебір ключів, а довжина ключа в 56 бітів дозволяє здійснювати атаку навіть на не досить потужній машині [2].

Таким чином, пост-квантові криптографічні алгоритми повинні бути стійкими для нових більш потужних машин, та не залежати від типу обчислень (специфіки математичної моделі, що використовується для реалізації алгоритму)

Метою доповіді є розгляд сучасних блокових алгоритмів шифрування, їх порівняння та прийняття рішень щодо використання їх для захисту інформації у пост-квантовий період.

В роботі проведений аналіз стійкості блокових симетричних шифрів: Blowfish, Camellia, IDEA, Kalyna, LEA, RC5, SEED, SHACAL-2, SIMECK, Skipjack, SM4, TEA, Threefish, XTEA.

Аналіз показав, що запасом стійкості при використанні в пост-квантовий період володіє блокових алгоритмів шифрування Kalyna, на основі якого побудований национального стандарта шифрування ДСТУ 7624:2014.

Список літератури

1. Рябий М.О., Огляд сучасних методів квантової та пост-квантової криптографії. Безпека інформації, ст. 236-241, 2014

2. Biham, Eli; Dunkelman, Orr; Keller, Nathan. Enhancing Differential-Linear Cryptanalysis. Advances in Cryptology — ASIACRYPT 2002. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. p. 254–266