УДК 004.056.55

КОНЦЕПЦІЯ ПОТОКОВОГО ШИФРУВАННЯ НА ОСНОВІ ДВОХ КВАЗІГРУП

THE CONCEPT OF STREAM ENCRYPTION BASED ON TWO QUASIGROUPS

Галина Крайнічук, Богдан Загирняк, Богдан Микитченко

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна

Abstract. *The article proposes the new approach to streaming encryption based on a recursive pseudorandom sequence generator constructed from two binary quasigroups. The encryption/decryption algorithm is presented.*

В процесі свого розвитку суспільство сьогодення переходить на повну цифровізацію. Це спричинює потребу захисту інформації від несанкціонованого доступу. Захист інформації базується в основному на криптографічних методах, яких є безліч і всі вони ґрунтуються на різних математичних операціях. Пошук нових методів та підходів до шифрування інформації триває й досі. Однією із можливих концепцій є використання квазігруп, латинських квадратів, кубів та гіперкубів для побудови шифрів. Подібні підходи застосовані у блоковому шифрі IDEA [1], потоковому шифрі Edon80 [2], у сімействі геш-функцій Edon-R [3] та інших. Алгоритми на основі квазігруп, можуть бути ефективно реалізовані на апаратному і програмному рівнях. Квазігрупи дозволяють створювати різні криптографічні схеми, які можуть бути адаптовані до специфічних вимог інформаційної безпеки.

Ідея концепції алгоритму потокового шифрування базується на побудові генератора псевдовипадкових послідовностей (ПВП) в поєднанні з рекурсією, елементами якої є значення, взяті з перетину стовпчика і рядка відповідних двох латинських квадратів. Опис побудови ПВП на основі двох квазігруп 4-го порядку подано в [4].

Алгоритм потокового шифрування на основі квазігруп має два режими зашифрування та розшифрування повідомлення. Процес зашифрування / розшифрування має такі кроки:

Крок 1. Введення вхідних даних *M* (шифротексту *C*) та ключа *K*.

Крок 2. Генерування псевдовипадкової послідовності *S* на основі ключа *K*.

Крок 3. Передавання повідомлення *M (C),* ключа *K*, та ПВП *S* на вхід операційного блоку.

Крок 4. Виконання головної операції операційного блоку із квазігрупою Q_1. (Q_1^{-1})

Крок 5. Запис результату операційного блоку в шифротекст *C (M).*

Крок 6. Зсув послідовностей *M (C), K* та *S* на основі регістра зсуву.

Крок 7. Генерування наступного значення ключа K на основі квазігрупи Q_0 (Q_0^{-1}) та *M (C)* і так до передавання даних всього повідомлення (шифротексту) до завершення процесу.

Апаратна реалізація такого алгоритму відповідає граничним вимогам складності засобів LW-криптографії.

Бібліографія

1. John Carl Villanueva Stream Ciphers vs. Block Ciphers. 2015. URL: https://www.jscape.com/blog/stream-cipher-vs-block-cipher (дата звернення: 04.06.2024).
2. Gligoroski D., Markovski S., Kocarev L., Gusev M. Edon80. 2007. URL: http://www.ecrypt.eu.org/stream/edon80p3.html (дата звернення: 04.06.2024).
3. Gligoroski D. et al. Cryptographic Hash Function Edon-R. Proc. IWSCN. Trondheim, 2009. 54p.
4. Микитченко Б.В. Загирняк Б.Д. Крайнічук Г.В. Побудова псевдовипадкових послідовностей на основі двох латинських квадратів. ВНТУ, 20-22 березня. Вінниця. 2024. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2024/paper/view/20722/17125 (дата звернення: 04.06.2024).