УДК 004.056:519.2

А.М. ОЛЕКСІЙЧУК
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *alex-dtn@ukr.net.*

А.А. МАТІЙКО
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *alexm1710@ukr.net*.

АНАЛІТИЧНИЙ ВИРАЗ ІМОВІРНОСТІ ЗБІГУ СУСІДНІХ ЗНАКІВ ВИХІДНОЇ ПОСЛІДОВНОСТІ КОМБІНУВАЛЬНОГО ГЕНЕРАТОРА ГАМИ, ПОБУДОВАНОГО НА БАЗІ РЕГІСТРІВ ЗСУВУ, ЩО РУХАЮТЬСЯ З ПРОСТОЮВАННЯМ

Анотація. Доведено теорему, яка встановлює явний вираз імовірності збігу двох сусідніх знаків вихідної послідовності довільного комбінувального генератора гами, побудованого на базі лінійних регістрів зсуву, кожен з яких або простоює, або зсувається на один крок у кожному такті. Отриманий результат надає змогу обчислювати цю ймовірність безпосередньо за відомими законом руху лінійних регістрів зсуву генератора та перетворенням Уолша-Адамара його комбінувальної функції.

Ключові слова: потоковий шифр, комбінувальний генератор гами з нерівномірним рухом, кореляційна атака, перетворення Уолша–Адамара, A5/1, Alpha1.

Комбінувальні генератори гами з нерівномірним рухом (clock-controlled keystream combination generators) використовують як основу для побудови синхронних потокових шифрів принаймні з 90-х років минулого століття. Найвідомішими прикладами таких шифрів є A5/1 [1] та Alpha1 [2], які не є стійкими, зокрема, відносно кореляційних атак.

Першу таку атаку на шифр A5/1 запропоновано у [3] та підсилено й узагальнено в [4–8] на інші комбінувальні генератори гами з нерівномірним рухом. У [9] досліджено кореляційні властивості вихідних послідовностей генератора гами шифру Alpha1, які (поряд з деякими іншими слабкостями) використано в [10, 11] для побудови ефективних атак на нього. Відзначимо також нещодавню роботу [12], присвячену новітнім атакам на шифр A5/1.

Через велику кількість атак на відомі генератори гами з нерівномірним рухом виникає природне запитання: чи існують взагалі (ефективні з практичного погляду) генератори гами такого типу, що є стійкими відносно усіх відомих атак? Нижче зроблено крок до відповіді на це запитання, який полягає в обґрунтуванні певної необхідної умови стійкості.

Метою цієї статті є доведення теореми, яка встановлює явний вираз імовірності збігу двох сусідніх знаків вихідної послідовності довільного комбінувального генератора гами, побудованого на основі лінійних регістрів зсуву (ЛРЗ), кожен з яких або простоює, або зсувається на один крок у кожному такті. Зауважимо, що генератори гами шифрів A5/1 та Alpha1 належать цьому класу. При цьому використано традиційну ймовірнісну модель генератора гами з нерівномірним рухом [3, 5, 8]. Отриманий результат надає змогу обчислювати зазначену ймовірність безпосередньо за відомими законом руху лінійних регістрів зсуву генератора та перетворенням Уолша-Адамара його комбінувальної функції. Окрім того, підсилено та узагальнено окремі результати роботи [9].

Розглянемо комбінувальний генератор гами з нерівномірним рухом (рис. 1), який складається з n лінійних регістрів зсуву з примітивними (над полем з двох елементів) поліномами зворотного зв'язку степенів $m_1, \ldots, m_n$ відповідно, збалансованої комбінувальної Булевої функції $f = f(z, \ldots, z_n)$ та блоку керування рухом, який виробляє послідовності невід'ємних цілочисельних векторів