УДК 621.391:519.2:519.7

Л.В. КОВАЛЬЧУК
Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна,
e-mail: *lusi.kovalchuk@gmail.com.*

І.В. КОРЯКОВ
Товариство з обмеженою відповідальністю «Науково-впроваджувальна фірма Криптон», Київ, Україна,
e-mail: *ikor@i.ua.*

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

KRIP: ВИСОКОШВИДКІСНИЙ АПАРАТНО-ОРІЄНТОВАНИЙ ПОТОКОВИЙ ШИФР, ПОБУДОВАНИЙ НА ОСНОВІ НЕАВТОНОМНОГО НЕЛІНІЙНОГО РЕГІСТРУ ЗСУВУ

Анотація. Запропоновано алгоритм потокового шифрування, побудований на основі неавтономного нелінійного регістру зсуву довжини 2 над алфавітом потужності 2^{256}. Цей регістр функціонує аналогічно шифру Фейстеля з раундовою функцією, що використовується в алгоритмі шифрування Kalyna. Показано, що за стійкості на рівні 2^{256} шифр Krip забезпечує чотирикратний виграш у швидкодії порівняно з прийнятим стандартом потокового шифрування України та майже двадцятикратний порівняно з сучасним алгоритмом шифрування Espresso.

Ключові слова: потоковий алгоритм шифрування, схема Фейстеля, нелінійний регістр зсуву, генератор псевдовипадкових послідовностей, алгебраїчні атаки, кореляційні атаки, Strumok, Espresso, Krip.

ВСТУП

Протягом останніх років спостерігається суттєве поширення сфери застосування потокових шифрів, що зумовлено розвитком інформаційних технологій, засобів передачі даних та помітним прогресом у дослідженні криптографічних властивостей алгоритмів потокового шифрування. Нині потокові шифри використовуються у вбудованих застосунках систем з обмеженою кількістю обчислювальних ресурсів, зокрема у бездротовій телефонії, в системах комутативного зв'язку та платного телебачення (більш докладну інформацію можна знайти, наприклад, в [1]). Окремо зазначимо шифр Strumok [2], який є національним стандартом потокового шифрування України [3].

Попри різноманіття існуючих потокових шифрів, залишається актуальною задача створення апаратно-орієнтованих алгоритмів потокового шифрування, що відповідають підвищеним вимогам до швидкодії та мають прийнятну схемну складність. Як один з можливих підходів до розв'язання сформульованої задачі в цій статті запропоновано алгоритм потокового шифрування Krip, побудований на основі нелінійного регістру зсуву (НРЗ).

На відміну від інших потокових шифрів, побудованих на основі НРЗ, наприклад таких як Grain [4] та Espresso [5], в алгоритмі Krip використовується неавтономний регістр зсуву довжини 2 над алфавітом потужності 2^{256}, який функціонує аналогічно шифру Фейстеля з раундовою функцією, що використовується в алгоритмі шифрування Kalyna [6]. Це надає змогу певною мірою звести проблему стійкості запропонованого шифру стосовно низки атак до аналогічної проблеми стосовно зазначеного шифру Фейстеля.