КІБЕРНЕТИКА

УДК 519.8

С.М. НІКОЛАЄВ
Науково-дослідний інститут воєнної розвідки, Київ, Україна,
e-mail: *divan24@i.ua.*

УДОСКОНАЛЕНИЙ МЕТОД БЕРЛЕКЕМПА–МЕССІ ЯК ОСНОВА ПОШУКУ ПЕРІОДИЧНОСТЕЙ У БІТОВИХ ПОТОКАХ

Анотація. Запропоновано вдосконалення методу Берлекемпа–Мессі у разі його застосування для пошуку періодичностей у бітових потоках з помилками. Суть удосконалення полягає в інакшому розбитті бітового потоку на блоки, використанні послідовного побітового зсуву перед кожним обчисленням параметрів, а також у прийнятті рішення про довжину регістра і значення полінома зворотного зв'язку на основі запропонованого математичного виразу.

Ключові слова: регістр зсуву з лінійним зворотним зв'язком, довжина регістра, поліном зворотного зв'язку, бітовий потік, метод Берлекемпа–Мессі.

ВСТУП

Розвиток криптології, кібернетики та радіотехніки тісно пов'язаний із застосуванням псевдовипадкових послідовностей, які будуються, зокрема, регістрами зсуву із лінійним зворотним зв'язком (LFSR) [1–3]. Значна кількість досліджень і відповідних публікацій щодо псевдовипадкових послідовностей присвячена аналізу їхніх властивостей та можливості й ефективності застосування в системах захисту інформації [4]. Досі нерозв'язаними проблемами є такі:

— методологія оцінювання ефективності криптогенераторів і відповідних криптомасивів (під криптомасивом будемо розуміти сформований криптогенератором на основі вхідних даних бітовий потік, що використовується для закриття інформації [5–7]; основними вимогами до криптомасиву (гамми) є якнайбільший період без повторень, неможливість передбачення поточного значення біта на основі аналізу попередніх його значень [8], висока лінійна складність, відповідність статистичним критеріям, складне правило перетворення бітів ключа в біти криптомасиву тощо);

— універсальні методи оцінювання лінійної складності послідовностей [9], а також складності максимального порядку (для нелінійних послідовностей) [10], складності Лемпеля–Зіва, Маурера тощо;

— ефективні способи ідентифікації ознак використання криптогенераторів та регістрів зсуву з нелінійним зворотним зв'язком у бітових потоках;

— ефективні методи криптоаналізу [11];

— методологія аналізу бітових потоків, які мають неперіодичну структуру, але не є криптомасивами і застосовуються в підсистемах кібернетичних або радіотехнічних засобів.