УДК 004.056

ДОСЛІДЖЕННЯ БЕНТ-ФУНКЦІЙ ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ

Шевчук С. В.
Науковий керівник – доц., к. т. н. Семеренко В. П.

При потоковому шифруванні виконується побітове складання по модулю 2 (функція "виключне АБО", XOR) ключової послідовності, що генерується алгоритмом шифрування на основі наперед заданого ключа, і початкового повідомлення. Основною перевагою потокового шифрування є його висока швидкодія, а недоліком – низька криптостійкість.

Причиною недостатньої криптостійкості є лінійність послідовності, що генерується на виході LFSR (лінійного регістру зсуву зі зворотним зв'язком). Для покращення криптостійкості цієї послідовності потрібно зробити її нелінійною.

Міра нелінійності є важливою характеристикою булевої функції. Лінійність і близькі до неї властивості часто свідчать про просту (у певному значенні) структуру цієї функції і, як правило, є багатим джерелом інформації про багато інших її властивостей. Завдання побудови булевих функцій, що мають нелінійні властивості, природним чином виникає в багатьох областях дискретної математики. І часто (що є типовою ситуацією в математиці) найбільший інтерес викликають ті функції, для яких ці властивості екстремальні. Такі булеві функції називаються максимально-нелінійними (або бент-) функціями.Схема криптостійкого генератора псевдо випадкових чисел показана на рис. 1.

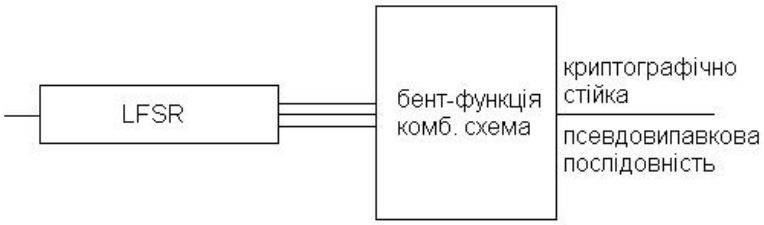

Рис.1 Схема криптостійкого генератора ПВП

Актуальність дослідження бент-функцій підтверджується їх численними теоретичними і практичними використаннями в комбінаториці, алгебрі, теорії кодування, теорії інформації, теорії символьних послідовностей, криптографії і криптоаналізі.