Лабораторна робота №1

з дисципліни «Сучасні проблеми захисту інформації та методи їх рішення»

Конструювання послідовностей де Брейна

Мета роботи: закріпити теоретичні відомості щодо властивостей послідовностей де Брейна та методів їх синтезу. Набути практичні навички синтезу повних класів послідовностей де Брейна, а також синтезу множин економічних S-блоків на їх основі.

Робота в аудиторії

1. Синтезувати повну множину послідовностей де Брейна довжини *N*=32. Порівняти потужність синтезованої множини із теоретичною оцінкою.
2. Виділити у побудованому класі лінійні та нелінійні послідовностей де Брейна.
3. Знайти бітові автокореляційні функції побудованих послідовностей де Брейна та оцінити їх кореляційні властивості по амплітуді бічного пелюстка автокореляційної функції.
4. Побудувати на основі синтезованої множини послідовностей де Брейна множину S-блоків. Знайти для них значення показника криптографічної якості згідно до варіанту (табл. 1.1.) Вибрати серед всіх побудованих S-блоків такі, що у найбільшій степені відповідають заданому показнику криптографічної якості.

Таблиця 1.1. — Варіанти завдань

|  |  |
| --- | --- |
| № | Показник криптографічної якості |
| 1 | Алгебраїчний степінь нелінійності |
| 2 | Відстань нелінійності |
| 3 | Рівномірна мінімізація елементів матриці коефіцієнтів кореляції |
| 4 | Найбільша відповідність суворому лавинному критерію |
| 5 | Найбільша кількість нулів у матриці коефіцієнтів кореляції |

Контрольні запитання

1. Що називається послідовністю де Брейна?
2. Які послідовності де Брейна називаються лінійними, а які — нелінійними?
3. Як визначається кількість послідовностей де Брейна?
4. Наведіть відомі Вам властивості послідовностей де Брейна?
5. Наведіть відомі Вам методи синтезу послідовностей де Брейна.
6. Яким чином на основі послідовностей де Брейна можуть бути синтезовані криптографічні S-блоки?
7. Якими властивостями володіють синтезовані на основі послідовностей де Брейна S-блоки?

Рекомендована література

1. Li C. et al. A class of de Bruijn sequences. IEEE Transactions on Information Theory. 2014. Vol. 60. No. 12. P. 7955-7969.
2. Gabric D., Sawada J. Investigating the discrepancy property of de Bruijn sequences. Discrete Mathematics. 2022. Vol. 345. No. 4. P. 112780.