УДК 004.056.55

Е.В. Фауре, С.В. Сисоєнко, Т.В. Миронюк

Черкаський державний технологічний університет, Черкаси

СИНТЕЗ І АНАЛІЗ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

У статті розглянуто та теоретично обґрунтовано результати дослідження синтезу псевдовипадкових послідовностей на основі використання операції додавання за модулем два та чотири результатів двох, трьох, чотирьох і п'яти випадкових дворозрядних операцій криптографічного перетворення інформації. Побудовано гістограми ймовірностей вироджених і невироджених результатів експерименту в залежності від кількості результатів криптографічного перетворення, які використані для побудови результуючої псевдовипадкової послідовності. Визначено конфігурації перетворення, які дозволяють отримати найбільшу долю вироджених результуючих операцій.

***Ключові слова**: псевдовипадкова послідовність, операції додавання за модулем, виродженість результатів операцій.*

Вступ

Постановка проблеми. Інформація сьогодні розглядається як стратегічний продукт. Якісно зріс обсяг інформаційних потоків, які циркулюють у суспільстві. Ухвалення важливих рішень у промисловості, фінансовій і державній сферах уже неможливе без обробки гігантських масивів інформації. Здатність суспільства та його інституцій збирати, обробляти, аналізувати, систематизувати та накопичувати інформацію, забезпечувати свободу інформаційного обміну є важливою передумовою соціального та технологічного прогресу, чинником національної безпеки, однією з основ успішної внутрішньої та зовнішньої політики. Інформаційна сфера має системотворчий характер і впливає практично на всі галузі суспільних відносин [1].

Таким чином, актуальність проблеми забезпечення захисту інформації в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо) служить підставою для створення нових розробок у сфері інформаційної безпеки та вважається одним із перспективних напрямків наукових досліджень.

Аналіз останніх досліджень і публікацій. За останній час можна виділити роботи, спрямовані на створення і розвиток теорії криптографічного кодування інформації [2, 3, 4]. Зокрема, для цієї теорії розроблено методи синтезу операцій прямого, оберненого та взаємного криптографічного перетворення (див., наприклад, [4, 5]). Разом з тим, у роботі [6] доведено можливість підвищення стійкості криптографічних систем за рахунок розробки алгоритмів синтезу псевдовипадкових послідовностей на основі використання операцій криптографічного перетворення. Для цього використано процедуру додавання за модулем два результатів двох випадкових невироджених операцій криптографічного перетворення інформації. Зауважимо, що процедура додавання за модулем деякого числа M двох або більше псевдовипадкових послідовностей лежить в основі побудови комбінаційного генератора [7], а його ефективність доведена в роботах [8 – 10].

Ця робота продовжує почате в [6] дослідження та збільшує кількість незалежних криптографічних перетворень і модуль M.

Метою роботи є синтез псевдовипадкових послідовностей на основі додавання за модулем M (Mϵ{2;4}) результатів Q (Qϵ{2;3;4;5}) операцій криптографічного перетворення інформації, а також аналіз отриманих послідовностей для теоретичного обґрунтування причин зміни їх якості.

Основний матеріал

Проведемо дослідження сумісного виконання Qϵ{3;4;5} випадкових операцій криптографічного перетворення інформації з подальшим додаванням отриманих результатів за модулем два. Як і в [6], в цій роботі обмежимося 24 дворозрядними операціями криптографічного перетворення. Оцінку отриманих послідовностей будемо виконувати за методикою, наведеною в [6], для чого визначимо долю вироджених операцій перетворення. Під виродженою операцією будемо розуміти результуючу операцію, для якої не існує оберненої операції криптографічного перетворення.

У результаті аналізу 13824 псевдовипадкових послідовностей, отриманих шляхом сумісного виконання трьох операцій криптографічного перетворення інформації з подальшим додаванням результатів кодування за модулем два, встановлено, що в 6144 випадках результуюча операція буде невиродженою, а в 7680 – виродженою. Таким чином, у результаті додавання за модулем два результатів трьох операцій криптографічного перетворення ін-

формації 44,44% результуючих операцій перетворення інформації будуть невиродженими, а 55,55% операцій – вироджені.

Провівши аналіз 331776 результатів криптографічного перетворення інформації, отриманих на основі додавання за модулем два результатів чотирьох операцій, встановлено, що результуюча операція є невиродженою в 47411 (14,29%) випадках. Відповідно, результуюча операція є виродженою в 284365 (85,71%) випадках.

На основі аналізу 7962624 результатів перетворення інформації, отриманих шляхом додавання за модулем два результатів п'яти криптографічних операцій, визначено, що 623473 (7,83%) операцій є невиродженими, а 7339151 (92,17%) операцій – вироджені.

Гістограма ймовірностей вироджених (Pbo) і невироджених (Pnbo) результатів експерименту в залежності від кількості Q операцій криптографічного перетворення, які використані для побудови результуючої псевдовипадкової послідовності за допомогою додавання за модулем два, представлено на рис. 1.

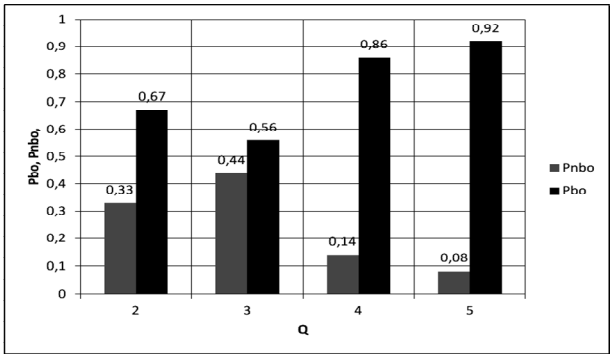

Рис. 1. Гістограма ймовірностей вироджених і невироджених результатів експерименту у випадку використання додавання за модулем два

Аналіз представлених на рис. 1 даних свідчить про те, що псевдовипадкова послідовність, отримана шляхом криптографічного перетворення вхідної інформації паралельно трьома операціями криптоперетворення з наступним додаванням результатів за модулем два, за своїми статистичними характеристиками гірша за аналогічну послідовність, побудовану на основі використання двох операцій. Це пояснюється тим, що в першому випадку використовується 55,55% вироджених операцій, а в другому – 66,66%.

Разом із тим, наступне збільшення кількості операцій криптоперетворення до чотирьох і п'яти призводить до збільшення долі вироджених результуючих операцій та, відповідно, до покращення статистичних характеристик отриманих псевдовипадкових послідовностей.

Проведемо дослідження сумісного виконання Qє{2;3;4;5} випадкових операцій криптографічного перетворення інформації з подальшим додаванням отриманих результатів за модулем чотири.

Перевірка 576 результатів сумісного виконання двох випадкових невироджених операцій криптографічного перетворення інформації з подальшим додаванням за модулем чотири їх результатів, свідчить, що жодна з операцій не є невиродженою.

Таким чином, можна констатувати, що в результаті додавання за модулем чотири 100% операцій вироджені.

Перетворюючи інформацію трьома випадковими невиродженими операціями з наступним додаванням отриманих результатів за модулем чотири, отримано 13824 послідовностей. Встановлено, що в 6394 (46,25%) випадках результуюча операція є невиродженою, а в 7430 (53,75%) випадках – виродженою.

Провівши аналіз 331776 послідовностей, отриманих на основі додавання за модулем чотири результатів чотирьох операцій криптоперетворення інформації, встановлено, що 54212 (16,34%) результатів є невиродженими, а 277564 (83,66%) – вироджені.

Проаналізувавши 7962624 послідовності, отримані на основі додавання за модулем чотири результатів п'яти операцій криптографічного перетворення інформації, визначено, що в 730173 (9,17%) випадках результуюча операція є невиродженою, а в 7232451 (90,83%) випадках – виродженою.

Гістограма ймовірностей вироджених (Pbo) і невироджених (Pnbo) результатів експерименту в залежності від кількості Q операцій криптографічного перетворення, які використані для побудови результуючої псевдовипадкової послідовності за допомогою додавання за модулем чотири, представлено на рис. 2.

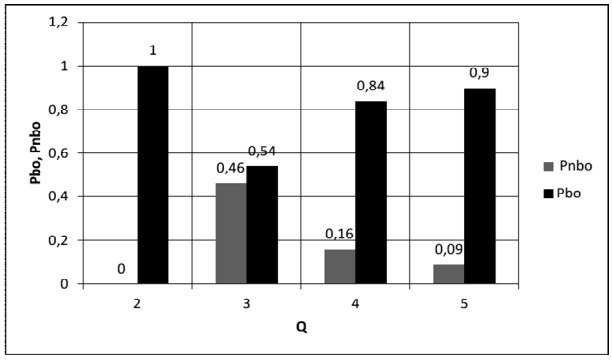

Рис. 2. Гістограма ймовірності вироджених і невироджених результатів експерименту у випадку використання додавання за модулем чотири

Аналіз представлених на рис. 2 даних свідчить про те, що псевдовипадкова послідовність, отримана шляхом криптографічного перетворення вхідної інформації паралельно двома операціями криптоперетворення з наступним додаванням результатів за модулем чотири, за своїми статистичними характерис-

тиками є найкращою, оскільки усі можливі результуючі операції є виродженими. Збільшення кількості операцій криптоперетворення призводить до стрибкоподібного суттєвого зменшення долі вироджених результуючих операцій (для Q=3) з наступним поступовим збільшенням цієї долі (для Q=4 і Q=5).

Висновки

У результаті проведеного обчислювального експерименту встановлено, що якість псевдовипадкової послідовності чисел, отриманої шляхом криптографічного перетворення вхідної інформації паралельно $Q \geq 2$ операціями криптоперетворення з наступним додаванням результатів за модулем M, відрізняються за своїми статистичними характеристиками.

Отримані результати ймовірностей вироджених і невироджених результатів експерименту в залежності від M і Q свідчать про те, що для M$\in${2;4} і Q$\in${2;3;4;5} за своїми статистичними характеристиками є найкращими наступні конфігурації перетворення: для M=2 – Q=5 (найгірша – Q=3); для M=4 – Q=2 (найгірша – Q=3).

Список літератури

1. *Стратегії розвитку України: теорія і практика / За ред. О. С. Власюка. — К. : НІСД, 2002. — 864 с.*
2. *Рудницький В.М. Алгебраїчна структура множини логічних операцій кодування / В.М. Рудницький, В.Г. Бабенко, Д.А. Жиляєв // Наука і техніка Повітряних Сил Збройних Сил України». – Х.: ХУПС. – 2011. – № 2(6). – С. 112-114.*
3. *Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного перекодування інформації / В.М. Рудницький, В. . Бабенко, С.В. Рудницький // Захист інформації : наук.-практ. журн. – № 3 (56). – К. : НАУ, 2012. – С. 50–56.*
4. *Рудницький В.М. Узагальнений метод синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення / В.М. Рудницький, В.Г. Бабенко, Т.А. Стабецька // Системи обробки інформації. – 2013. – Вип. 6(122). – С. 118-121.*
5. *Наукоемкие технологии в инфокоммуникациях:обработка и защита информации: коллективная монография / Под ред. В.М. Безрука, В.В. Баранника. – Х. : Компания СМИТ, 2013. – 398 с.*
6. *Ланських Є.В. / Оцінка якості псевдовипадкових послідовностей на основі використання операцій додавання за модулем два / Є.В. Ланських, С.В. Сисоєнко, М.О. Пустовіт // Наука і техніка Повітряних Сил Збройних Сил України. – Х.: ХУПС, 2014. – №4 (21). – С. 122-125.*
7. *Лавданский А.А. Комбинационный метод формирования последовательности псевдослучайных чисел [Електронний ресурс] / А.А. Лавданский, Э.В. Фауре // Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014р. / ННК «ІПСА» НТУУ «КПІ». – К.: ННК «ІПСА» НТУУ «КПІ», 2014. – С. 403-404. – Режим доступу: http://sait.kpi.ua/books/sait2014.ebook.pdf/view.*
8. *Лавданский А.А. Оценка статистических свойств последовательностей на выходе комбинационного генератора с помощью графических тестов / А.А. Лавданский, Э.В. Фауре // Системні дослідження та інформаційні технології. -Київ, 2015. №2 - С.39-50.*
9. *Фауре Э.В. Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором / Э.В. Фауре, А.И. Щерба, А.А. Лавданский // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2015. – № 18. – С. 165-171.*
10. *Фауре Э.В. Анализ корреляционных свойств последовательностей (псевдо) случайных чисел [Електронний ресурс] / Э.В. Фауре, А.И. Щерба, А.А. Лавданский // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – №1(18) – С. 142-150. – Режим доступу: http://nbuv.gov.ua/j-pdf/Nitps_2015_1_32.pdf.*

Надійшла до редколегії 16.09.2015

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

СИНТЕЗ И АНАЛИЗ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

Э.В. Фауре, С.В. Сысоенко, Т.В. Миронюк

В статье рассмотрены и теоретически обоснованы результаты исследования синтеза псевдослучайных последовательностей на основе использования операции сложения по модулю два и четыре результатов двух, трех, четырех и пяти случайных двухразрядных операций криптографического преобразования информации. Построены гистограммы вероятностей вырожденных и невырожденных результатов эксперимента в зависимости от количества результатов криптографического преобразования, которые использованы для построения результирующей псевдослучайной последовательности. Определены конфигурации преобразования, которые позволяют получить наибольшую долю вырожденных результирующих операций.

Ключевые слова: *псевдослучайная последовательность, операции сложения по модулю, вырожденность результатов операций.*

SYNTHESIS AND ANALYSIS OF PSEUDORANDOM SEQUENCES BASED ON CRYPTOGRAPHIC TRANSFORMATION OPERATIONS

E.V. Faure , S.V. Sysoienko, T.V. Mironiuk

In the article the research results of synthesis of pseudorandom sequences based on the use of operation of addition modulo two and four of the results of two, three, four and five random two-digit operations of information cryptographic transformation are considered and theoretically proved. Histograms of probabilities of degenerate and nondegenerate experimental results are built depending on the number of cryptographic transformation results used to construct the resulting pseudorandom sequence. The transformation configurations that allow to obtain the largest share of degenerate resulting operations are defined.

Key words: *pseudorandom sequence, operation of addition modulo, degeneration of operation results.*