УДК 004.056.55

Є.В. Ланських[1], С.В. Сисоєнко[1], М.О. Пустовіт[2]

[1] *Черкаський державний технологічний університет, Черкаси*
[2] *Черкаський інститут пожежної безпеки імені Героїв Чорнобиля, Черкаси*

ОЦІНКА ЯКОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ВИКОРИСТАННЯ ОПЕРАЦІЙ ДОДАВАННЯ ЗА МОДУЛЕМ ДВА

В статті розглянуто та теоретично обґрунтовано результати дослідження генератора псевдовипадкових чисел на основі використання операції додавання за модулем. Проведено перевірку можливості шифрування інформації двома випадковими не виродженими операціями криптографічного перетворення інформації з подальшим додаванням результатів кодування за модулем 2. В результаті проведеного дослідження було встановлено, що 33,33% результуючих операцій перетворення інформації будуть не виродженими, а 66,66% вироджені, а це в свою чергу не дозволяє використовувати дані перетворення для блокових криптосистем, проте приводить до покращення статистичних характеристик результуючої псевдовипадкової послідовності, яка може використовуватися в потокових шифрах. Отримані результати свідчать, що додавання за модулем два результатів перетворення підвищує якість псевдовипадкових послідовностей оскільки відсутній механізм оберненого перетворення.

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

Вступ

Постановка проблеми. Розвиток інформатики та обчислювальної техніки сумісно з інформаційно-телекомунікаційними системами привів до значного росту цінності інформації. Втрата або несанкціонований доступ до інформації може привести не тільки до матеріальних збитків та економічних втрат, а також може вплинути навіть на здоров'я та самопочуття людей. У наш час мало хто не зустрічався з проблемою захисту особистих даних від несанкціонованого доступу та втручанням у роботу власних комп'ютерних систем.

Паралельно з цим розвивається комп'ютерна злочинність та комп'ютерний тероризм. Одним з найбільш ефективних засобів захисту інформації є використання крипто алгоритмів. Основними характеристиками криптографічних систем є стійкість та швидкість виконання перетворення, які необхідно постійно підвищувати. Необхідно відмітити, що зростання даних показників повинно бути не меншим за зростання продуктивності засобів обчислювальної техніки.

Аналіз останніх досліджень і публікацій. За останні роки опубліковано ряд робіт направлених на створення теорії криптографічного кодування [1, 2]. В даних роботах розглядається можливість розширення кількості операцій для криптографічного перетворення, а також заміни операцій лінійних та нелінійних підстановок елементарними логічними функціями [3]. На даний час розроблено ряд методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення [3 – 5]. Основною перевагою криптографічного перетворення є висока швидкість реалізації крипто алгоритмів. Проте на даний час не вичерпані всі можливості підвищення стійкості криптографічних систем на основі операцій криптографічного перетворення. Тому виникає потреба в проведенні додаткових досліджень направлених на розробку алгоритмів синтезу псевдовипадкових послідовностей на основі використання операцій криптографічного перетворення.

Метою статті є оцінка якості псевдовипадкової послідовності синтезованої на основі операцій криптографічного перетворення інформації та додавання за модулем два.

Основний матеріал

В роботах [6, 7] проведено дослідження генератора псевдовипадкових чисел на основі використання операції додавання за модулем деякого числа M двох або більше псевдовипадкових послідовностей (період яких є взаємно простим), яке показує, що комбінація послідовностей призводить до збільшення періоду та покращення статистичних властивостей результуючої псевдовипадкової послідовності. Перевіримо та теоретично обґрунтуємо результати даного дослідження на основі використання операцій криптографічного перетворення інформації для модуля 2. При проведенні досліджень обмежимося двох розрядними операціями криптографічного перетворення інформації. Повна група даних операцій наведена в табл. 1.

Розглянемо можливість кодування інформації двома випадковими не виродженими операціями криптографічного перетворення інформації (наведеними в табл. 1), з подальшим додаванням результатів кодування за модулем 2.

Таблиця 1

Повна група двох розрядних операцій криптографічного перетворення інформації

№	Операція	№	Операція	№	Операція	№	Операція
1	$F_{3,5}=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	7	$F_{3,10}=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$	13	$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$	19	$F_{12,10}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$
2	$F_{6,5}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	8	$F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$	14	$F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$	20	$F_{9,10}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$
3	$F_{3,6}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	9	$F_{3,9}=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$	15	$F_{12,6}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$	21	$F_{12,9}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
4	$F_{5,3}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	10	$F_{5,12}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	16	$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	22	$F_{10,12}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
5	$F_{5,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	11	$F_{5,9}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	17	$F_{10,6}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	23	$F_{10,9}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
6	$F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	12	$F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	18	$F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	24	$F_{9,12}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

Так як всі двох розрядні операції криптографічного перетворення інформації можна віднести до матричних операцій криптоперетворення [1], тому можливість оберненого перетворення будемо оцінювати на основі не виродженого результуючого перетворення.

Матричні операції криптографічного перетворення, описуються моделлю [2]:

$$\vec{F}=\begin{pmatrix}a_{11}x_1\oplus a_{12}x_2\oplus\ldots\oplus a_{1n}x_n\oplus b_1\\a_{21}x_1\oplus a_{22}x_2\oplus\ldots\oplus a_{2n}x_n\oplus b_2\\\ldots\ldots\ldots\ldots\ldots\ldots\\a_{n1}x_1\oplus a_{n2}x_2\oplus\ldots\oplus a_{n\,n}x_n\oplus b_n\end{pmatrix},\quad(1)$$

де $a_{ij}\in[0,1]$; $b_i\in[0,1]$; $x_1\ldots x_n$ – операнди-розряди відповідно; $\oplus$ – операція «додавання за mod 2» при виконанні наступних вимог:

1. Відсутні нульові рядки, тобто

$$\sum_{j=1}^{n}a_{ij}>0,$$

чи нульові стовбці, тобто

$$\sum_{i=1}^{n}a_{ij}>0;$$

2. Сума за модулем два двох чи декількох рядків не повторює існуючий рядок матриці:

$$\sum_{j=1}^{n}(a_{ij}\oplus a_{lj}\oplus a_{hj}\oplus\ldots\oplus a_{uj})>0.$$

Нехай інформація перетворюється операцією $\vec{F}_{3,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}$ і додаються по модулю результати перетворення. Тоді

$$\vec{F}_{1\oplus1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\vec{F}_{3,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus\vec{F}_{3,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}=$$
$$=\begin{pmatrix}x_1\oplus x_1\\x_2\oplus x_2\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}.$$

Результат перетворення відповідно до вимоги 1 буде виродженим. Якщо

$$\vec{F}_{1\oplus2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\vec{F}_{3,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus\vec{F}_{6,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}=$$
$$=\begin{pmatrix}x_1\oplus x_1\oplus x_2\\x_2\oplus x_2\end{pmatrix}=\begin{pmatrix}x_2\\0\end{pmatrix},$$

то результат буде виродженим. Якщо

$$\vec{F}_{1\oplus3}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\vec{F}_{3,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus\vec{F}_{3,6}\begin{pmatrix}x_1\\x_2\end{pmatrix}=$$
$$=\begin{pmatrix}x_1\oplus x_1\\x_2\oplus x_1\oplus x_2\end{pmatrix}=\begin{pmatrix}0\\x_1\end{pmatrix},$$

то результат буде виродженим. Якщо

$$\vec{F}_{1\oplus4}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\vec{F}_{3,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus\vec{F}_{5,3}\begin{pmatrix}x_1\\x_2\end{pmatrix}=$$
$$=\begin{pmatrix}x_1\oplus x_2\\x_2\oplus x_1\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_1\oplus x_2\end{pmatrix}.$$

то результат буде виродженим (вимога 2). Якщо

$$\vec{F}_{1\oplus5}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\vec{F}_{3,5}\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus\vec{F}_{5,6}\begin{pmatrix}x_1\\x_2\end{pmatrix}=$$
$$=\begin{pmatrix}x_1\oplus x_2\\x_2\oplus x_1\oplus x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_1\end{pmatrix},$$

то результат буде не виродженим. Якщо

$$\vec{F}_{1\oplus 6}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{3,5}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \vec{F}_{6,3}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \\ = \begin{pmatrix} x_1 \oplus x_1 \oplus x_2 \\ x_2 \oplus x_1 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix},$$

то результат буде не виродженим.

Результати дослідження вродженості результуючої матриці перетворення представлені в табл. 2.

В результаті аналізу 576 результатів сумісного виконання операцій криптографічного перетворення інформації було встановлено, що в 192 випадках результуюча операція буде не виродженою, тому що існує обернена операція криптографічного перетворення, а в 384 випадках результуюча операція буде виродженою. Можна констатувати, що в результаті додавання за модулем лише 33.33% результуючих операцій перетворення інформації будуть не виродженими.

Так як 66,66% операцій перетворення будуть вироджені, то це приводить до покращення статистичних характеристик результуючої псевдовипадкової послідовності.

Для практичної оцінки згенерованих послідовностей використаємо пакет тестів NIST STS [8]. Результати тестування наведені в табл. 3.

Таблиця 2

Результати дослідження виродженості результуючої матриці перетворення

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1					■	■					■	■					■	■					■	■
2			■	■					■	■					■	■					■	■		
3		■		■				■		■				■		■				■		■		
4		■	■					■	■					■	■					■	■			
5	■					■	■					■	■					■	■					■
6	■				■		■				■		■				■		■				■	
7					■	■					■	■					■	■					■	■
8			■	■					■	■					■	■					■	■		
9		■		■				■		■				■		■				■		■		
10		■	■					■	■					■	■					■	■			
11	■					■	■					■	■					■	■					■
12	■				■		■				■		■				■		■				■	
13					■	■					■	■					■	■					■	■
14			■	■					■	■					■	■					■	■		
15		■		■				■		■				■		■				■		■		
16		■	■					■	■					■	■					■	■			
17	■					■	■					■	■					■	■					■
18	■				■		■				■		■				■		■				■	
19					■	■					■	■					■	■					■	■
20			■	■					■	■					■	■					■	■		
21		■		■				■		■				■		■				■		■		
22		■	■					■	■					■	■					■	■			
23	■					■	■					■	■					■	■					■
24	■				■		■				■		■				■		■				■	

□ - результат сумісного виконання операцій вироджений,
■ - результат сумісного виконання операцій не вироджений.

Таблиця 3

Зведені результати тестування згенерованих послідовностей

	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Послідовність 1	113 (59,8 %)	183 (96,8 %)
Послідовність 2	150 (79,4 %)	189 (100 %)

Послідовність 1 – послідовність отримана на основі випадкового набору операцій криптографічного перетворення на основі RANDOM. Послідовність 2 – послідовність отримана на основі додавання за модулем 2 результатів перетворення інформації операціями криптографічного перетворення.

Наведені в табл. 3 результати свідчать, що додавання за модулем два псевдовипадкових послідовностей, підвищує якість результуючої послідовності, оскільки відсутній механізм оберненого перетворення.

Висновки

В результаті проведеного дослідження було встановлено, що 33,33% результуючих операцій перетворення інформації будуть не виродженими, а 66,66% вироджені, а це в свою чергу не дозволяє використовувати дані перетворення для блокових криптосистем, проте приводить до покращення статистичних характеристик результуючої псевдовипадкової послідовності, яка може використовуватися в потокових шифрах.

Отримані результати свідчать, що додавання за модулем два результатів перетворення, підвищує якість псевдовипадкових послідовностей оскільки відсутній механізм оберненого перетворення.

Список літератури

1. Криптографическое кодирование: методы и средства реализации: коллективная монография / Под ред. Б.Ф. Мельникова. – Ульяновск, 2013. – 200 с.

2. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В.Н. Рудницкий, В.Я. Мильчевич, В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий, О.Г. Мельник. – Х.: ООО «Щедрая усадьба плюс», 2014. – 224 с.

3. 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.

4. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: коллективная монография / Под ред. В.М. Безрука, В.В. Баранника. – Х. : Компания СМИТ, 2013. – 398 с.

5. Бабенко В.Г. Построение нелинейных операций расширенного матричного криптографического преобразования / В.Г. Бабенко, О.Г. Мельник, Т.А. Стабецька // Криптографическое кодирование : коллективная монография / под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Х.: Изд-во ООО «Щедрая усадьба плюс», 2014. – С. 41-55.

6. 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.

7. 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.

8. Богданов В.В. Навчальний комплекс статистичної оцінки псевдовипадкових і текстових послідовностей / В.В. Богданов, Н.А. Паламарчук // Збірник наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України «Київський політехнічний інститут». – Вип. 3. – К. : ВІТІ НТУУ «КПІ», 2007. – С. 17–26.

Надійшла до редколегії 18.09.2015

Рецензент: д-р техн. наук проф. В.М. Рудницький, Черкаський державний технологічний університет, Черкаси.

ОЦЕНКА КАЧЕСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ОПЕРАЦИЙ СЛОЖЕНИЯ ПО МОДУЛЮ ДВА

Е.В. Ланских, С.В. Сысоенко, М.А. Пустовит

В статье рассмотрены и теоретически обоснованы результаты исследования генератора псевдослучайных чисел на основе использования операции сложения по модулю. Проведена проверка возможности шифрования информации двумя случайными не вырожденными операциям криптографического преобразования информации с последующим сложением результатов кодирования по модулю 2. В результате проведенного исследования было установлено, что 33,33% результирующих операций преобразования информации будут не вырожденными, а 66,66% вырожденные, а это в свою очередь не позволяет использовать данные преобразования для блочных криптосистем, однако приводит к улучшению статистических характеристик результирующей псевдослучайной последовательности, которая может использоваться в потоковых шифрах. Полученные результаты свидетельствуют, что сложение по модулю два результатов преобразования повышает качество псевдослучайных последовательностей поскольку отсутствует механизм обратного преобразования.

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

QUALITY RATING OF PSEUDORANDOM SEQUENCES ON THE BASIS OF CONGRUENCE ADDITION OPERATIONS BY MODUL TWO

Y.V. Lanskykh, S.V. Sysoienko, M.O. Pustovit

The research results pseudorandom number generator, based on the use of congruence addition, are considered and theoretically grounded. A test of the possibility of encoding information in two random not degenerate operations of cryptographic transformation of information, followed by the addition of the results of congruence encoding 2. The study found that 33.33% resulting conversion operations of information will be not degenerate and 66.66%, will be degenerate and this in its turn does not allow using this transformation for block cryptosystems, but leads to improvement of the statistical characteristics of the resulting pseudorandom sequence which can be used in stream code. The results indicate that the congruence addition 2 of the transformation results improves the quality of pseudorandom sequence as inverse transformation mechanism is absent.

Keywords: *pseudorandom sequence, operations of congruence addition 2, degeneration of operation results.*