
КРИПТОГРАФІЧНЕ КОДУВАННЯ:
ОБРОБКА ТА ЗАХИСТ
ІНФОРМАЦІЇ
Колективна монографія

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

КРИПТОГРАФІЧНЕ КОДУВАННЯ: ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Колективна монографія

2018

УДК 004.056
К 82

Рецензенти:
Корченко Олександр Григорович, доктор технічних наук, професор, Національний авіаційний університет (м. Київ);
Васіліу Євгеній Вікторович, доктор технічних наук, професор, Одеська національна академія зв'язку ім. О.С. Попова (м. Одеса);
Шостак Ігор Володимирович, доктор технічних наук, професор, Харківський національний університет радіоелектроніки (м. Харків)

Рекомендовано до друку рішенням науково-технічної ради Черкаського державного технологічного університету (протокол № 2 від 26 лютого 2018 року)

К 82 **Криптографічне** кодування: обробка та захист інформації : колективна монографія / під. ред. В. М. Рудницького. – Харків : ТОВ «ДІСА ПЛЮС», 2018. – 139 с.
ISBN 978-617-7645-12-1

Колективна монографія містить матеріали актуальних напрямків криптографічного захисту та обробки інформації, а також соціальної інженерії щодо прогнозування та проведення оцінки якості та ефективності діяльності людства.

Монографія розрахована на наукових та інженерних працівників, викладачів, аспірантів і студентів, які займаються дослідженням в галузі інформаційної безпеки держави.

УДК 004.056

ISBN 978-617-7645-12-1

© Колектив авторів, 2018
© Редакція Рудницького В. М., 2018

ЗМІСТ

ПЕРЕДМОВА

За останні декілька десятиліть відбулися якісні зміни в процесах управління на всіх ієрархічних рівнях за рахунок інтенсивного впровадження сучасних інформаційних технологій (ІТ). Їх швидкий розвиток призвів до зростання цінності інформації як для суспільства взагалі, так і для кожної окремої людини зокрема. Водночас почала зростати небезпека втручання в роботу інформаційних систем для несанкціонованого зчитування інформації. Нині відбувається глобальний перехід до інформаційного суспільства, розвиток якого нерозривно пов'язаний з інтенсифікацією інформаційних процесів, необхідністю збору, обробки і передавання величезних обсягів інформації. Інформатизація торкнулася всіх сфер діяльності людини в цілому: державного управління, фінансів, економіки, освіти, виробництва та ін. Неконтрольоване поширення і застосування програмних засобів призводить до втрати конфіденційності інформаційних ресурсів громадян і держави в цілому. Як наслідок розвиток інформаційних ресурсів нерозривно пов'язаний з їх безпекою та захистом.

Одним із найбільш дієвих засобів захисту інформаційно-телекомунікаційних систем є використання методів та засобів криптографії.

Також з початком формування інформаційного суспільства, стало ясно, що для багатьох управлінських завдань немає достатньо простого математичного апарату, що дозволяє обробляти отримані соціальні дані, визначати найбільш значимі з них, і проводити оцінку ефективності управління соціумом. Тому важливими стали питання дослідження різних математичних методів, в тому числі, питання мінімізації булевих функцій.

Перший розділ монографії присвячено підвищенню ефективності алгоритмів комп'ютерної криптографії за рахунок розробки нових мікрокриптопримітивів на основі використання нових синтезованих операцій криптографічного перетворення інформації.

Таким чином, результати тестування показали відповідність результатів шифрування вимогам до генераторів псевдовипадкових послідовностей і систем шифрування для побудови блочних шифрів.

1.2 Підвищення якості псевдовипадкових послідовностей на основі використання операцій криптографічного перетворення інформації

С.В. Сисоєнко[1], О.Г. Мельник[2], М.О. Пустовіт[2]

[1] Черкаський державний технологічний університет, м. Черкаси

[2] Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля НУЦЗ України, м. Черкаси

1.2.1 Оцінка якості псевдовипадкових послідовностей на основі використання операцій додавання за модулем два

За останні роки опубліковано ряд робіт направлених на створення теорії криптографічного кодування [9, 10]. В даних роботах розглядається можливість розширення кількості операцій для криптографічного перетворення, а також заміни операцій лінійних та нелінійних підстановок елементарними логічними функціями [2]. На даний час розроблено ряд методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення [2, 4, 11]. 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. В роботах [12, 13] проведено дослідження генератора псевдовипадкових чисел на основі використання операції додавання за

модулем деякого числа M двох або більше псевдовипадкових послідовностей (період яких є взаємнопростим), яке показує, що комбінація послідовностей призводить до збільшення періоду та покращення статистичних властивостей результуючої псевдовипадкової послідовності. Перевірено та теоретично обґрунтовано результати даного дослідження на основі використання операцій криптографічного перетворення інформації для модуля 2. При проведенні досліджень обмежимося двохрозрядними операціями криптографічного перетворення інформації. Повна група даних операцій наведена в таблиці 1.2.

Таблиця 1.2

Повна група двохрозрядних операцій криптографічного перетворення інформації

№	операція	№	операція	№	операція	№	операція
1	$F_{0,1}=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	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	$F_{0,2}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	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	$F_{9,12}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

Розглянуто можливість кодування інформації двома випадковими невиродженими операціями криптографічного перетворення інформації (наведеними в табл. 1.2), з подальшим додаванням результатів кодування за модулем 2.

Так як всі двохрозрядні операції криптографічного перетворення інформації можна віднести до матричних операцій криптоперетворення [9],

тому можливість оберненого перетворення оцінювалась на основі невиродженого результуючого перетворення.

Матричні операції криптографічного перетворення, описуються моделлю [10]:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n \oplus b_2 \\ \cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n \oplus b_n \end{pmatrix}, \quad (1.4)$$

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 $\sum_{j=1}^{n} a_{ij} > 0$ чи нульові стовбці $\sum_{i=1}^{n} a_{ij} > 0$;

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

Результат перетворення відповідно до вимоги 1 буде виродженим.

Якщо

$$\vec{F}_{1\oplus 2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{3,5}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \vec{F}_{6,5}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_1 \oplus x_2 \\ x_2 \oplus x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ 0 \end{pmatrix},$$

то результат буде виродженим.

Якщо

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

то результат буде виродженим.

Якщо

$$\vec{F}_{1\oplus 4}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{3,5}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \vec{F}_{5,3}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_1 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus x_2 \end{pmatrix},$$

то результат буде виродженим (вимога 2).

Якщо

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

то результат буде невиродженим.

Якщо

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

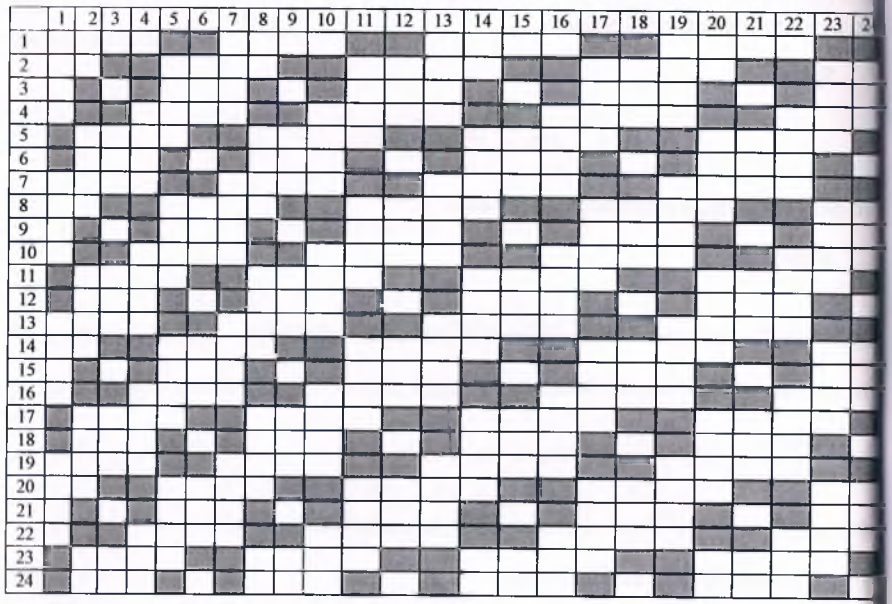
то результат буде невиродженим.

Результати дослідження вродженості результуючої матриці перетворення представлені в таблиці 1.2.

В результаті аналізу 576 результатів сумісного виконання операцій криптографічного перетворення інформації встановлено, що в 192 випадках результуюча операція буде невиродженою, 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 невиродженими. Так як 66,66% операцій перетворення будуть вироджені, то це приводить до покращення статистичних характеристик результуючої псевдовипадкової послідовності.

Таблиця 1.2

Результати дослідження виродженості результуючої матриці перетворення



- результат сумісного виконання операцій вироджений,
- результат сумісного виконання операцій невироджений.

Для практичної оцінки згенерованих послідовностей використано пакет тестів NIST STS [14]. Результати тестування наведені в табл.1.3.

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.

Таблиця 1.3

Наведені 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 %)

Наведені в табл.1.3 результати свідчать, що додавання за модулем два псевдовипадкових послідовностей, підвищує якість результуючої послідовності, оскільки відсутній механізм оберненого перетворення.

1.2.2 Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення

Проведено дослідження сумісного виконання $Q \in \{3;4;5\}$ випадкових операцій криптографічного перетворення інформації з подальшим додаванням отриманих результатів за модулем два. Як і в [15], було взято 24 дворозрядні операції криптографічного перетворення. Оцінку отриманих послідовностей було виконано за методикою, наведеною в [15], для чого визначено долю вироджених операцій перетворення. Під виродженою операцією визначено 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 інформації

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

Проведено 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. 1.8.

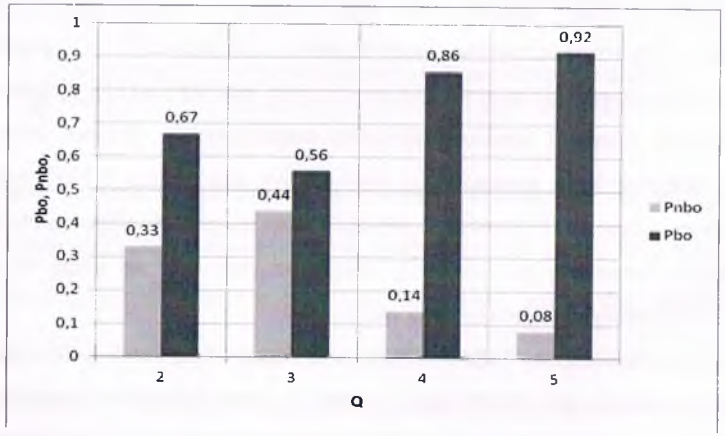


Рис. 1.8 Гістограма ймовірностей вироджених і невироджених результатів експерименту у випадку використання додавання за модулем два

Аналіз представлених на рис. 1.8 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.

Проведено дослідження сумісного виконання $Q \in \{2;3;4;5\}$ 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
730173 (9,17%) випадках результуюча операція є невиродженою, а в 723245
(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. 1.9.

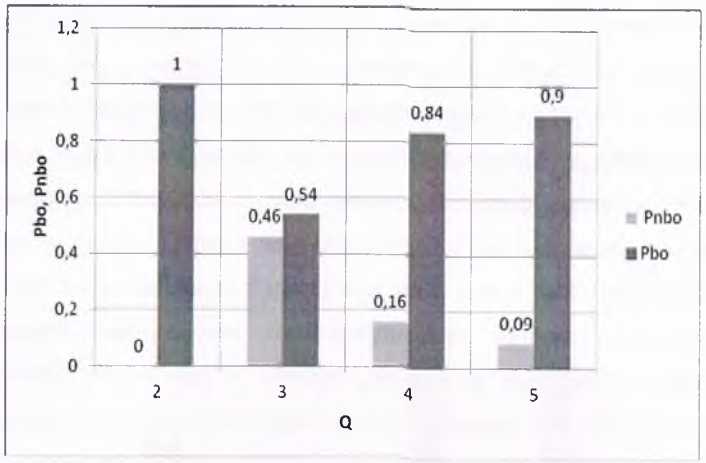


Рис. 1.9 Гістограма ймовірності вироджених і невироджених результатів експерименту у випадку використання додавання за модулем чотири

Аналіз представлених на рис. 1.9 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 характеристиками 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).

1.3.3 Оцінки якості псевдовипадкових послідовностей на основі додавання за модулем

У роботах [13, 16, 18] доведено ефективність комбінаційного генератора псевдовипадкових чисел, що використовує операцію додавання за модулем M декількох первинних псевдовипадкових послідовностей. У роботах [15, 19] цей підхід розширено і доведено можливість підвищення стійкості криптографічних систем за рахунок використання випадкових перетворень операцій криптографічного перетворення інформаційної послідовності замість первинних генераторів. Так, у роботі [15] використано процедуру додавання за модулем два результатів двох випадкових невироджених операцій криптографічного перетворення інформації. У роботі [19] виконано дослідження сумісного виконання трьох, чотирьох і п'яти випадкових операцій криптографічного перетворення інформації з подальшим додаванням отриманих результатів за модулем два та чотири. Разом із тим, у роботах [15, 19] встановлено тільки ймовірність виродженої результуючої операції, за якою визначено найкращі конфігурації перетворення. Як і в [19], під виродженою операцією будемо розуміти результуючу операцію, для якої не існує оберненої операції криптографічного перетворення.

Проведено аналіз імовірностей вироджених і невироджених результуючих операцій перетворення інформації в залежності від кількості первинних операцій криптографічного перетворення інформації, а також часу отримання результуючої псевдовипадкової послідовності.

Для цього введені наступні позначення:

$P_{bo}(M,Q)$ – імовірність виродженої операції під час побудови псевдовипадкової послідовності на основі додавання за модулем M результатів Q операцій криптографічного перетворення;

$P_{bo}(M,Q)=1-P_{nbo}(M,Q)$ – імовірність невиродженої операції;

$t_{pp}(Q)$ – час побудови псевдовипадкової послідовності, який визначається таким чином:

$$t_{pp}(Q)=t_{po}(Q)+t_{+o}(Q), \tag{1.5}$$

де $t_{po}(Q)$ – час виконання Q операцій криптографічного перетворення;

$t_{+o}(Q)$ – час виконання операцій додавання за модулем M під час побудови результуючої псевдовипадкової послідовності.

Якщо допустити, що час, необхідний для кожного з Q перетворень однаковий і дорівнює t_{po1}, то час побудови псевдовипадкової послідовності

$$t_{pp}(Q)=t_{po}(Q)+t_{+o}(Q)=Q\cdot t_{p1}+(Q-1)\cdot t_{+}, \tag{1.6}$$

де t_{+} – час виконання операції додавання за модулем M.

Відносний коефіцієнт якості псевдовипадкової послідовності на основі додавання за модулем M результатів Q операцій криптографічного перетворення інформації будемо визначати наступним чином:

$$k_{kv}(M,Q)=\frac{P_{bo}(M,Q)}{P_{bo}(M,2)}. \tag{1.7}$$

Відносний коефіцієнт часу формування псевдовипадкової послідовності на основі додавання за модулем M результатів Q операцій криптографічного перетворення інформації будемо визначати наступним чином:

$$k_{tv}(M,Q)=\frac{t_{pp}(Q)}{t_{pp}(2)}=\frac{Q\cdot t_{po1}+(Q-1)\cdot t_{+}}{2t_{po1}+t_{+}}. \tag{1.8}$$

Оскільки збільшення коефіцієнта $k_{kv}(M,Q)$ призводить до покращення статистичних характеристик псевдовипадкової послідовності, а збільшення коефіцієнта $k_{tv}(M,Q)$ призводить до збільшення латентності та часу отримання формування послідовності, відносний коефіцієнт якості побудови псевдовипадкової послідовності $k_{pkpv}(M,Q)$ будемо визначати наступним чином:

$$k_{pkpv}(M,Q)=\frac{k_{kv}(M,Q)}{k_{tv}(M,Q)}. \tag{1.9}$$

З урахуванням виразів (1.7) і (1.8) вираз (1.9) можна представити у вигляді

$$k_{pkpv}(M,Q)=\frac{P_{bo}(M,Q)\cdot(2t_{po1}+t_{+})}{P_{bo}(M,2)\cdot(Qt_{po1}+(Q-1)\cdot t_{+})}. \tag{1.10}$$

Враховуючи те, що пристрої цифрової обробки інформації, як правило, працюють синхронно і час їх роботи визначається максимальним часом виконання операції, то максимальний час виконання операції криптографічного перетворення можна представити як час виконання двох операцій додавання за модулем M. Виходячи з цього, вираз (1.10) можна спростити:

$$k_{pkpv}(M,Q)=\frac{P_{bo}(M,Q)\cdot(4t_{+}+t_{+})}{P_{bo}(M,2)\cdot(2Qt_{+}+(Q-1)\cdot t_{+})}=\frac{5P_{bo}(M,Q)}{(3Q-1)\cdot P_{bo}(M,2)}. \tag{1.11}$$

На основі отриманої залежності (2.8) проведено розрахунки відносного коефіцієнта якості побудови псевдовипадкової послідовності у випадку використання двох, трьох, чотирьох та п'яти операцій криптографічного

перетворення інформації з подальшим їх додаванням за модулем два
чотири.

Гістограма залежності відносного коефіцієнта якості побудов
псевдовипадкової послідовності $k_{pkpv}(M,Q)$ від кількості операці
криптографічного перетворення інформації, які використані під час побудов
результуючої псевдовипадкової послідовності на основі додавання
модулем два, представлено на рис. 1.10.

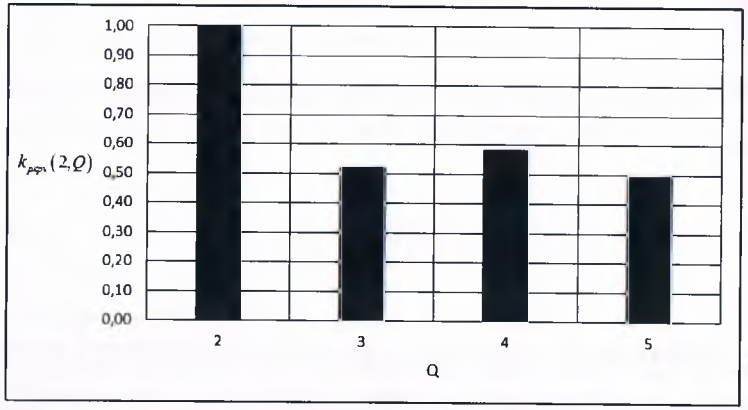


Рис. 1.10 Гістограма залежності відносного коефіцієнта якості побудови псевдовипадкової послідовності від кількості операцій криптографічного перетворення інформації під час використання додавання за модулем 2

Гістограма залежності відносного коефіцієнта якості побудов
псевдовипадкової послідовності $k_{pkpv}(M,Q)$ від кількості операці
криптографічного перетворення інформації, які використані під час побудов
результуючої псевдовипадкової послідовності на основі додавання за
модулем чотири, представлено на рис. 1.11.

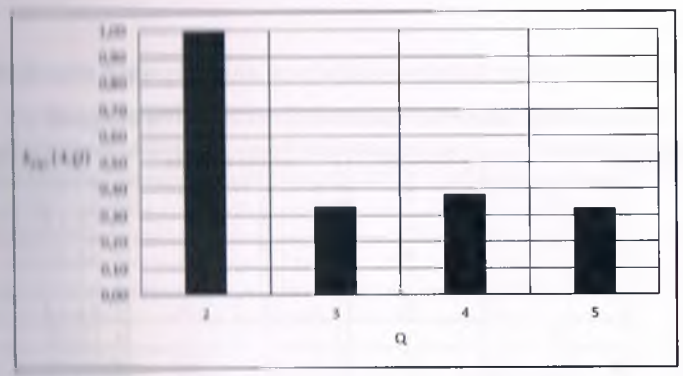


Рис. 1.11 Гістограма залежності відносного коефіцієнта якості побудови псевдовипадкової послідовності від кількості операцій криптографічного перетворення інформації під час використання додавання за модулем 4

Аналіз представлених гістограм свідчить про те, що за визначених умов відносний коефіцієнт якості побудови псевдовипадкової послідовності досягає максимального значення для Q=2 операцій криптографічного перетворення інформації. Разом із тим, варто зауважити, що для $M\in\{2;4\}$ і $Q\in\{3;4;5\}$ відносний коефіцієнт якості побудови псевдовипадкової послідовності досягає максимального значення для Q=2.

1.3 Синтез операцій криптографічного додавання за модулем два з точністю до перестановки результатів виконання операції

В.Г. Бабенко[1], Н.В. Лада[1], С.Г. Козловська[2]
[1] Черкаський державний технологічний університет, м. Черкаси
[2] Східноєвропейський університет економіки і менеджменту, м. Черкаси

1.3.1 Метод синтезу і технологія дослідження операцій додавання за модулем два з точністю до перестановки результатів виконання операції

Наведемо одну з множини операцій $o_1^{\oplus} - o_4^{\oplus}$ в загальному табличному представленні, для цього проведемо заміну цифр на букви. Результати узагальнення операції $o_3^{\oplus}$ наведені в табл. 1.4.