7. Лорин Г. Сортировка и системы сортировки / Г. Лорин. – М. : Изд-во "Мир". 1983. – 384 с.
8. Макконелл Дж. Основы современных алгоритмов / Дж. Макконелл. – Изд. 2-ое, [перераб. и доп.]. – М. : Изд-во "Техносфера", 2004. – 368 с.
9. Мельничук А.С. Аналіз методів сортування масиву чисел / А.С. Мельничук, С.П. Луценко, Д.С. Громовий, К.В. Трофимова // Технологический аудит и резервы производства : сб. науч. тр. – 2013. – № 4/1(12). – С. 37-40.
10. Немнюгин С.А. Параллельное программирование для многопроцессорных систем / С.А. Немнюгин, О.Л. Стесик. – СПб. : Изд-во "БХВ-Петербург", 2002. – 400 с.
11. Prots'ko I. Algorithm of efficient computation DST using cyclic convolutions / I. Prots'ko, V. Teslyuk // Wseas transactions on signal processing. – 2014. – Vol. 10. – Pp. 278-288.

Цмоць И.Г., Кись Я.П., Антонив В.Я. **Применение графического процессора для повышения быстродействия сортировки больших массивов данных**

Проанализированы методы и алгоритмы параллельной сортировки массивов данных и особенности архитектуры графических процессоров GPU. Предложено разработку программных средств параллельной сортировки массивов данных с использованием графического процессора GPU и программной модели CUDA осуществлять на основе комплексного подхода, который включает: исследования, разработку методов и алгоритмов параллельной сортировки больших массивов данных; графовые модели алгоритмов параллельной сортировки массивов данных; архитектуру графического процессора GPU и программную модель CUDA. Разработан конкретизированный потоковый граф алгоритма сортировки методом слияния, который обеспечивает обнаружение параллелизма и возможность управлять им. Определены сложность параллельного алгоритма сортировки слиянием и его быстродействие.

Ключевые слова: параллельная сортировка, графический процессор, комплексный подход, потоковый граф, слияние.

Tsmots I.G, Kis Ya.P, Antoniv V.Ya. **Application of Graphic Processor to Improve Sorting Performance of Large Data Sets**

Some methods and algorithms for parallel sorting data sets and architectural features of graphics processor GPU are analysed. We suggest software development for parallel sorting data sets using graphics processor GPU and programming model CUDA based on a comprehensive approach, which includes the following: research and development of methods and algorithms for parallel sorting large data sets; graph models of algorithms for parallel sorting data sets; architecture of graphics processor GPU and programming model CUDA. We have also developed the concretized flow graph of algorithm of merge sort that provides parallelism detection and the ability to manage it. The complexity of algorithm of parallel merge sort and its performance are determined.

Keywords: parallel sorting, graphics processor, comprehensive approach, flow graph, merge.

УДК 681.3.05:004.056.5 ***Проф. Ю.І. Грицюк, д-р техн. наук – НУ "Львівська політехніка"; здобувач П.Ю. Грицюк, магістр – НЛТУ України, м. Львів***

МЕТОДИ І ЗАСОБИ ГЕНЕРУВАННЯ Q_P-МАТРИЦЬ ФІБОНАЧЧІ – КЛЮЧІВ ДЛЯ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Розглядаються особливості ефективного генерування Q_p-матриць Фібоначчі, які можуть використовуватися як ключі (де)шифрування для багатораундової матричної криптографічної системи перетворення інформації. З'ясовано, що основна проблема багатораундової матричної Афінної криптосистеми полягає у генеруванні множини звичайних і обернених матриць – ключів (де)шифрування інформації, елементами яких мають бути цілі числа. Розроблено процедуру генерування множини Q_p-матриць Фібоначчі, яка за відомими значеннями степені матриці (n) та p-чисел Фібоначчі дає змогу отримувати відповідну множину ключів (де)шифрування інформації, здійснювати їхнє розширення для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й створює зручність при передаванні каналами зв'язку.

Ключові слова: захист інформації, шифрування/дешифрування інформації, числа Фібоначчі, Q_p-матриць Фібоначчі, криптографічна система, матричні Афінні перетворення, багатораундова матрична криптографічна система.

Вступ. У роботі **[**3**]** було розглянуто особливості побудови надійної криптосистеми захисту інформації, яка поєднує матричні Афінні перетворення, багатораундові дії з різними ключами, а також перестановні алгоритми, що загалом значно підвищує її криптостійкість до брутальних атак. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної Афінної перестановної криптосистеми з різними ключами шифрування на кожному раунді. Також у цій роботі було зазначено, що, порівняно з іншими методами захисту, класична криптографія гарантує захист інформації тільки за умов, якщо використано ефективний криптографічний алгоритм, а також дотримані умови секретності та цілісності ключів шифрування.

Однак, у матричних Афінних перетвореннях **[**3, розд. 1**]** основна проблема полягає у генеруванні множини матриць $\overline{\overline{A}} = [\overline{A}_i = [a_{ij},\ j = \overline{1,n}], i = \overline{1,n}]$ – ключів шифрування, елементами яких є спеціально підібрані цілі числами з діапазону $1 \le a_{ij} < m$ (де m – кількість символів алфавіту), а також НСД(a, m) = 1, де $a = \det(\overline{\overline{A}}) \bmod m$ – визначник матриці $\overline{\overline{A}}$ за модулем m. Є також деякі питання щодо генерування й стовпців $\overline{B} = [b_i, i = \overline{1,n}]$ – ключів додаткового коригування вже зашифрованого повідомлення, елементами яких є цілі числами з діапазону $1 \le b_i < m$. Водночас, для отримання зворотних матриць $\overline{\overline{A}}' = [\overline{A}_i' = [a_{ij}',\ j = \overline{1,n}], i = \overline{1,n}]$ – ключів дешифрування та зворотних стовпців $\overline{B}' = [b_i', i = \overline{1,n}]$ – ключів коригування потрібно виконати деяку послідовність дій, які детально описано в зазначеній вище роботі.

Якщо ж використовувати багатораундову матричну Афінну криптосистему **[**див. 3, розд. 3**]**, то на кожному раунді криптографічних перетворень (кількість яких може бути від 4 до 16 чи 24) виникає потреба у різних матричних ключах, тобто потрібно вирішувати питання розширення ключів для кожного раунду. Окрім цього, оскільки розмір цих матриць (n) може бути різним (мінімальний 32×32, нормальний 128×128 чи 256×256, надмірний 1048×1048 та більше), а кількість раундів шифрування – великою (32, 48, 64, …), то виникає проблема не тільки у їх зберіганні, але й передачі цих ключів каналами зв'язку з кожним повідомленням. А, як відомо з **[**4, 9**]**, розмір зашифрованого повідомлення практично немає відрізнятися від вхідного повідомлення. Водночас, передані з повідомленням ключі шифрування не мають викликати в криптоаналітиків підозри у цілісності зашифрованого повідомлення.

Отже, основна проблема багатораундової матричної Афінної криптосистеми полягає у генеруванні множини звичайних і обернених матриць – ключів шифрування/дешифрування інформації, елементами яких мають бути цілі числа, розширенні ключів для кожного раунду, а також у ефективній системі їх зберігання та передаванні каналами зв'язку. Для її вирішення пропонуємо використовувати Q_p-матриці, елементами яких є p-числа Фібоначчі [7, 8].

Об'єкт дослідження – матричні ключі (де)шифрування та їх розширення для багатораундової криптографічної системи перетворення інформації.

Предмет дослідження – методи і засоби генерування Q_p-матриць – ключів (де)шифрування та розширення їхньої множини для кожного раунду криптографічних перетворень, елементами яких є *p*-числа Фібоначчі.

Мета роботи полягає в розробленні методів і засобів генерування Q_p-матриць Фібоначчі – ключів (де)шифрування для багатораундової криптографічної системи перетворення інформації та розширення їхньої множини, що дасть змогу не тільки ефективно їх утворювати, але й зберігати та передавати каналами зв'язку.

Для реалізації зазначеної мети потрібно виконати такі основні завдання:

1) з'ясувати основні наслідки модифікування прямокутного трикутника Паскаля, результати якого мали б стати основою ключів (де)шифрування;
2) виявити основні особливості побудови матриць на основі чисел Фібоначчі, які значно полегшать процес їх генерування та розширення потрібної множини для кожного раунду криптографічних перетворень;
3) здійснити реалізацію багатораундової криптосистеми на основі Q_p-матриць Фібоначчі, яка значно підвищує криптостійкість алгоритму шифрування;
4) зробити відповідні теоретичні висновки та надати рекомендації щодо практичного використання.

1. Особливості модифікування прямокутного трикутника Паскаля та його основні наслідки

Як відомо **[2]**, існує багато різних форм подання трикутника Паскаля. В нашому дослідженні використаємо таблицю біноміальних коефіцієнтів (табл. 1.1), яку ще прийнято називати *прямокутним трикутником Паскаля* **[7]**.

Табл. 1.1. Початковий вигляд прямокутного трикутника Паскаля [7]

№\n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1		**1**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2			**1**	3	6	10	15	21	28	36	45	55	66	78	91	105	120	136	153	171	190
3				**1**	4	10	20	35	56	84	120	165	220	286	364	455	560	680	816	969	1140
4					**1**	5	15	35	70	126	210	330	495	715	1001	1365	1820	2380	3060	3876	4845
5						**1**	6	21	56	126	252	462	792	1287	2002	3003	4368	6188	8568	11628	15504
6							**1**	7	28	84	210	462	924	1716	3003	5005	8008	12376	18564	27132	38760
7								**1**	8	36	120	330	792	1716	3432	6435	11440	19448	31824	50388	77520
8									**1**	9	45	165	495	1287	3003	6435	12870	24310	43758	75582	125970
9										**1**	10	55	220	715	2002	5005	11440	24310	48620	92378	167960
10											**1**	11	66	286	1001	3003	8008	19448	43758	92378	184756
11												**1**	12	78	364	1365	4368	12376	31824	75582	167960
12													**1**	13	91	455	1820	6188	18564	50388	125970
13														**1**	14	105	560	2380	8568	27132	77520
14															**1**	15	120	680	3060	11628	38760
15																**1**	16	136	816	3876	15504
16																	**1**	17	153	969	4845
17																		**1**	18	171	1140
18																			**1**	19	190
19																				**1**	20
20																					**1**
Σ	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
pF_0^n	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576

Така таблиця починається з нульового стовпця, який містить єдиний біноміальний коефіцієнт $C_0^0 = 1$, а також з нульового рядка, який містить біноміальні коефіцієнти: $C_0^0 = C_1^0 = C_2^0 = ... = C_n^0 = 1$. "Гіпотенуза" такого прямокутного трикутника складається з таких біноміальних коефіцієнтів: $C_0^0 = C_1^1 = C_2^2 = ... = C_n^n = 1$.

Водночас, у *n*-му стовпці цієї таблиці зверху вниз розміщені такі біноміальні коефіцієнти: C_n^0, C_n^1, C_n^2, …, C_n^j, …, C_n^n. При цьому всі клітини під "гіпотенузою" є порожніми, позаяк всі діагональні коефіцієнти типу C_n^m ($m>n$) тотожно дорівнюють нулю. Якщо ж просумувати значення біноміальних коефіцієнтів *n*-го стовпця прямокутного трикутника Пасскаля, то отримаємо ряд чисел $C_n^0 + C_n^1 + ... + C_n^n = 2^n$, який називається двійковим. Отже, можна стверджувати, що трикутник Паскаля "генерує" двійковий ряд чисел, який можна реалізувати за допомогою такої формули: $pF_0^{n+1} = 2pF_0^n$ при $pF_0^0 = 1$.

Побудова 1-трикутника Паскаля. Спробуємо зсунути кожен рядок початкового трикутника Паскаля (табл. 1.1) на один стовпець вправо відносно попереднього рядка. Внаслідок такого перетворення отримаємо деякий "деформований" трикутник Паскаля **[7]**, який прийнято називати 1-трикутником Паскаля (табл. 1.2).

Табл. 1.2. Вигляд 1-трикутника Паскаля [7]

№\n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1			**1**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2					**1**	3	6	10	15	21	28	36	45	55	66	78	91	105	120	136	153
3							**1**	4	10	20	35	56	84	120	165	220	286	364	455	560	680
4									**1**	5	15	35	70	126	210	330	495	715	1001	1365	1820
5											**1**	6	21	56	126	252	462	792	1287	2002	3003
6													**1**	7	28	84	210	462	924	1716	3003
7															**1**	8	36	120	330	792	1716
8																	**1**	9	45	165	495
9																			**1**	10	55
10																					**1**
Σ	**1**	**1**	**2**	**3**	**5**	**8**	**13**	**21**	**34**	**55**	**89**	**144**	**233**	**377**	**610**	**987**	**1597**	**2584**	**4181**	**6765**	**10946**
pF_1^n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946

Якщо тепер просумувати значення біноміальних коефіцієнтів 1-го трикутника Паскаля в кожному стовпці, то отримаємо ряд чисел 1, 1, 2, 3, 5, 8, 13, …, pF_1^n, які називаються числами Фібоначчі. Задати їх можна за допомогою такого рекурентного співвідношення:

$$pF_1^{n+1} = pF_1^n + pF_1^{n-1} \text{ при } n > 1, pF_1^0 = pF_1^1 = 1. \quad (1.1)$$

Побудова *p*-трикутника Паскаля. А тепер покажемо, що трикутник Паскаля є джерелом нових числових рядів **[7]**, які представляють інтерес для реалізації криптографічних перетворень. Для цього продовжимо наші "маніпуляції" з трикутником Паскаля. Якщо у початковому трикутнику (див. табл. 1.1) зсунути біноміальні коефіцієнти на *p* стовпців (p = 1, 2, 3, …) вправо відносно попереднього рядка, то отримаємо *p*-ий "деформований" трикутник, який при-

йнято називати *p*-трикутником Паскаля. Підсумовуючи значення біноміальних коефіцієнтів у *p*-трикутнику, отримаємо кожного разу новий числовий ряд, який можна задати таким рекурентним співвідношенням:

$$\begin{cases} pF_p^j = 1;\ j = \overline{0, p}; \\ pF_p^{n+1} = pF_p^n + pF_p^{n-p}, \end{cases} \quad \forall n \geq p+1;\ p = 0,1,2,3,...;\ n = 1,2,3,4,.... \tag{1.2}$$

Числові ряди, які задаються рекурентним співвідношенням (1.2), винайдено ще в 1977 р. [6] і названо їх *p*-числами Фібоначчі. У табл. 1.3 наведено найбільш поширені їх числові значення. Також була записана формула, за допомогою якої *p*-числа можна задати через біноміальні коефіцієнти, а саме:

$$pF_p^{n+1} = C_n^0 + C_{n-p}^1 + C_{n-2p}^2 + C_{n-3p}^2 + ...,\ p = \overline{0, n-1}. \tag{1.3}$$

Табл. 1.3. Найпоширеніші p-числа Фібоначчі для різних значень n

p\n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
1	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946
2	1	1	1	2	3	4	6	9	13	19	28	41	60	88	129	189	277	406	595	872	1278
3	1	1	1	1	2	3	4	5	7	10	14	19	26	36	50	69	95	131	181	250	345
4	1	1	1	1	1	2	3	4	5	6	8	11	15	20	26	34	45	60	80	106	140
5	1	1	1	1	1	1	2	3	4	5	6	7	9	12	16	21	27	34	43	55	71
6	1	1	1	1	1	1	1	2	3	4	5	6	7	8	10	13	17	22	28	35	43
7	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	11	14	18	23	29
8	1	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	10	12	15	19
9	1	1	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	10	11	13
10	1	1	1	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	10	11

У роботі [7] автор стверджує, що існують два способи задавання *p*-чисел Фібоначчі: у вигляді рекурентного співвідношення (1.2) і у вигляді формули (1.3), яка їх виражає через біноміальні коефіцієнти.

Однак, формула (1.3) не зручна для використання не тільки через громіздкість виконуваних обчислень, але й через те, що нею, швидше за все, й сам автор ніколи не скористався. Водночас, рекурентне співвідношення (1.2) хоча і досить зручне для використання, проте є одновимірним, тобто значення *p*-чисел Фібоначчі отримуються у вигляді одновимірного масиву. А у алгоритмах реалізації криптографічних перетворень з різних причин прийнято використовувати двовимірні таблиці числових даних [4].

Табл. 1.4. Двовимірне генерування p-чисел Фібоначчі (для p = 4)

i	$pF_p^{i,-1}$	$pF_p^{i,j},\ j = \overline{0, p}$				
		0	1	2	3	4
0		1	1	1	1	1
1	1	2	3	4	5	6
2	6	8	11	15	20	26
3	26	34	**45**	60	80	106
4	106	140	185	245	325	431
5	431	571	756	1001	1326	1757
6	1757	2328	3084	4085	5411	7168
7	7168	9496	12580	16665	22076	29244
8	29244	38740	51320	67985	90061	119305
9	119305	158045	209365	277350	367411	486716
10	486716	644761	854126	1131476	1498887	1985603
11	1985603	2630364	3484490	4615966	6114853	8100456
12	8100456	10730820	14215310	18831276	**24946129**	33046585

З огляду на ці обставини нами розроблено двовимірне рекурентне співвідношення (1.5) для задавання *p*-чисел Фібоначчі. Для розуміння алгоритму генерування таких чисел розглянемо табл. 1.4, в якій кількість стовпців відповідає числу *p*+1 (їх позначено від 0 до *p*). Для встановлення кількості рядків (*k*), потрібно задати число *n*, яке вказує на загальну кількість *p*-чисел Фібоначчі, які потрібно згенерувати. Нехай *n* = 64, тоді за формулою (1.4) знаходимо, що *k* = 12, тобто отримаємо 13 рядків, в т.ч. і 0-ий рядок. В цьому 0-му рядку записуємо числа 1, що відповідає $pF_4^{0,j} = 1,\ j = \overline{0,4}$. У *i*-му рядку і в окремому (лівому) стовпці будемо записувати останнє значення *p*-чисел Фібоначчі з (*i*-1)-го рядка для того, щоб організувати двовимірне рекурентне співвідношення (1.5).

$$k = \text{int}\left(\frac{n}{p+1}\right). \tag{1.4}$$

$$\begin{gathered} pF_p^{i,j} = 1,\ j = \overline{0, p},\ i = 0; \\ pF_p^{i,-1} = pF_p^{i-1,p},\ pF_p^{i,j} = pF_p^{i,j-1} + pF_p^{i-1,j},\ j = \overline{0, p};\ i = \overline{1, k}. \end{gathered} \tag{1.5}$$

Внаслідок виконання таких дій отримаємо двовимірну таблицю *p*-чисел Фібоначчі для *p* = 4 (табл. 1.4), а за потреби можна отримати аналогічні таблиці для різних значень *p*. Водночас, порядкові номери *p*-чисел Фібоначчі наведено в табл. 1.5, а за потреби можна отримати аналогічні таблиці для різних *p*.

Табл. 1.5. Порядкові номери p-чисел Фібоначчі (для p = 4)

i \ *j*	0	1	2	3	4
0	0	1	2	3	4
1	5	6	7	8	9
2	10	11	12	13	14
3	15	**16**	17	18	19
4	20	21	22	23	24
5	25	26	27	28	29
6	30	31	32	33	34
7	35	36	37	38	39
8	40	41	42	43	44
9	45	46	47	48	49
10	50	51	52	53	54
11	55	56	57	58	59
12	60	61	62	**63**	64

Для обчислення порядкових номерів *p*-чисел Фібоначчі використовується така формула:

$$n = i \cdot (p+1) + j,\ j = \overline{0, p};\ i = \overline{0, k}. \tag{1.6}$$

Для знаходження в табл. 1.4 координат (номерів рядка і відповідного стовпця), наприклад, для числа 45, яке відповідає, згідно з табл. 1.5, порядковому номеру *n* = 16, використовуються такі формули:

$$i = 1 + \mathrm{int}\left(\frac{n}{p+1}\right);\ j = (1+n) \bmod (p+1). \qquad (1.7)$$

Отже, внаслідок проведеного дослідження встановлено, що існують не два, а три способи задавання *p*-чисел Фібоначчі: у вигляді одновимірного рекурентного співвідношення (1.2), через біноміальні коефіцієнти у вигляді формули (1.3), а також у вигляді двовимірного рекурентного співвідношення (1.5).

2. Особливості побудови матриць на основі чисел Фібоначчі

Поняття про *Q*-матрицю Фібоначчі. Як відомо з **[**10**]**, існує теорія матриць спеціального типу **[**1**]**, однією з яких є *Q*-матриця **[**8**]**. Найпростішою *Q*-матрицею є квадратна матриця розміром 2×2 такого вигляду:

$$\bar{\bar{Q}} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},\ \det \bar{\bar{Q}} = -1. \qquad (2.1)$$

Однак, яке мають відношення *Q*-матриці до ряду чисел Фібоначчі? Для відповіді на це запитання достатньо піднести *Q*-матрицю до *n*-ої степені, внаслідок чого отримаємо такий набір матриць (звичайних і обернених, а також їхні визначники):

$n=$	0	1	2	3	4	5	6	7	8	9	10
$Q^n=$	1 0 0 1	1 1 1 0	2 1 1 1	3 2 2 1	5 3 3 2	8 5 5 3	13 8 8 5	21 13 13 8	34 21 21 13	55 34 34 21	89 55 55 34
$p=1$											
$\det Q^n=$	1	-1	1	-1	1	-1	1	-1	1	-1	1
$Q^{-n}=$	1 0 0 1	0 1 1 -1	1 -1 -1 2	-1 2 2 -3	2 -3 -3 5	-3 5 5 -8	5 -8 -8 13	-8 13 13 -21	13 -21 -21 34	-21 34 34 -55	34 -55 -55 89
$\det Q^{-n}=$	1	-1	1	-1	1	-1	1	-1	1	-1	1

Отримані матриці можуть використовуватися як ключі шифрування (звичайні Q^n-матриці) та ключі дешифрування (обернені Q^{-n}-матриці) інформації для реалізації матричних Афінних перетворень [3, розд. 1], а також як розширення ключів для реалізації багатораундової криптосистеми [3, розд. 3]. Особливості їхньої реалізації детально розглянуто у розд. 3 цього дослідження.

Розглянувши уважно наведені вище звичайні *Q*-матриці, можна побачити, що їхніми елементами є не що інше, як числа Фібоначчі. Водночас, для певної Q^n-матриці, тобто піднесеної до *n*-ої степені, на головній діагоналі з трьох сусідніх чисел Фібоначчі знаходяться найбільше та найменше з них, а на побічній діагоналі – середнє число. Окрім цього, у звичайній та оберненій матрицях знаходяться одні і ті ж самі числа, тільки в оберненій матриці поміняні місцями числа на головній діагоналі та мають протилежний знак на побічній діагоналі. У загальному випадку *Q*-матриці, піднесені до *n*-ої степені, мають такий математичний запис [8]:

$$\bar{\bar{Q}}^n = \begin{bmatrix} F^{n+1} & F^n \\ F^n & F^{n-1} \end{bmatrix},\ \det \bar{\bar{Q}}^n = (-1)^n, \qquad (2.2)$$

де F^{n-1}, F^n, F^{n+1} – числа Фібоначчі. Задавати *Q*-матриці *n*-го степеня можна за допомогою такого рекурентного співвідношення:

$$\bar{\bar{Q}}^{n+1} = \bar{\bar{Q}}^n + \bar{\bar{Q}}^{n-1},\ n = 2,3,4,..., \qquad (2.3)$$

або за допомогою такого матричного виразу

$$\bar{\bar{Q}}^{n+1} = \bar{\bar{Q}}^n \times \bar{\bar{Q}}^1,\ n = 2,3,4,.... \qquad (2.4)$$

Забігаючи наперед, зазначимо, що матричний вираз (2.4) є більш придатним для використання порівняно з рекурентним співвідношенням (2.3), позаяк має узагальнений характер процесу розрахунку.

Узагальнена Q_p-матриця Фібоначчі. Спробуємо використати ідею побудови *Q*-матриці числами Фібоначчі для отримання узагальнених матриць Фібоначчі. В роботі [11] була введена квадратна матриця спеціального типу, яку названо Q_p-матрицею:

$$\bar{\bar{Q}}_p = \left[\begin{array}{c|cccccc} \mathbf{1} & \mathbf{1} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \mathbf{1} \\ \hline \mathbf{1} & 0 & 0 & 0 & \cdots & 0 & 0 \end{array}\right],\ \det \bar{\bar{Q}}_p = \pm 1,\ p = 0,1,2,3,...., \qquad (2.5)$$

Особливістю будови Q_p-матриці є те, що вона має розміри $(p+1)\times(p+1)$, містить одиничну матрицю розміром $p\times p$, обмежену останнім рядком типу **1** 0 0 … 0 0 і першим стовпцем типу **1** 0 0 … 0 **1**. Якщо $p = 0$, то Q_p-матриця дорівнює $\bar{\bar{Q}}_0 = [1]$, а для p = 1, 2, 3 і 4 – відповідні матриці наведено нижче:

$$\bar{\bar{Q}}_1 = \left[\begin{array}{c|c} 1 & 1 \\ \hline 1 & 0 \end{array}\right],\ \det \bar{\bar{Q}}_1 = -1; \quad \bar{\bar{Q}}_2 = \left[\begin{array}{c|cc} 1 & 1 & 0 \\ \hline 0 & 0 & 1 \\ 1 & 0 & 0 \end{array}\right],\ \det \bar{\bar{Q}}_2 = 1; \quad \bar{\bar{Q}}_3 = \left[\begin{array}{c|ccc} 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{array}\right],\ \det \bar{\bar{Q}}_3 = -1; \quad \bar{\bar{Q}}_4 = \left[\begin{array}{c|cccc} 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{array}\right],\ \det \bar{\bar{Q}}_4 = 1. \qquad (2.6)$$

Як не дивно, але Q_p-матриці також мають безпосереднє відношення до *p*-чисел Фібоначчі. Щоб це зрозуміти, достатньо піднести Q_p-матриці до *n*-ої степені, внаслідок чого для різних значень *p* отримаємо різні набори матриць з різними *p*-числами Фібоначчі. Наприклад, для p = 2 отримаємо набір $\bar{\bar{Q}}_2^n$-матриць, наведений нижче, елементами яких є 2-числа Фібоначчі (див. табл. 1.3).

Набір $\bar{\bar{Q}}_2^n$-матриць Фібоначчі

$n=$	0	1	2	3	4	5	6
$\bar{\bar{Q}}_2^n=$	1 0 0 0 1 0 0 0 1	1 1 0 0 0 1 1 0 0	1 1 1 1 0 0 1 1 0	2 1 1 1 1 0 1 1 1	3 2 1 1 1 1 2 1 1	4 3 2 2 1 1 3 2 1	6 4 3 3 2 1 4 3 2
$\det \bar{\bar{Q}}_2^n=$	1	1	1	1	1	1	1
$\bar{\bar{Q}}_2^{-n}=$	1 0 0 0 1 0 0 0 1	0 0 1 1 0 -1 0 1 0	0 1 0 0 -1 1 1 0 -1	1 0 -1 -1 1 1 0 -1 1	0 -1 1 1 1 -2 -1 1 1	-1 1 1 1 -2 0 1 1 -2	1 1 -2 -2 0 3 1 -2 0
$\det \bar{\bar{Q}}_2^{-n}=$	1	1	1	1	1	1	1

Продовження набору $\bar{\bar{Q}}_2^n$-матриць Фібоначчі

$n=$	7	8	9	10	11	12	13
$\bar{\bar{Q}}_2^n=$	9 6 4 4 3 2 6 4 3	13 9 6 6 4 3 9 6 4	19 13 9 9 6 4 13 9 6	28 19 13 13 9 6 19 13 9	41 28 19 19 13 9 28 19 13	60 41 28 28 19 13 41 28 19	88 60 41 41 28 19 60 41 28
$\det\bar{\bar{Q}}_2^n=$	1	1	1	1	1	1	1
$\bar{\bar{Q}}_2^{-n}=$	1 -2 0 0 3 -2 -2 0 3	-2 0 3 3 -2 -3 0 3 -2	0 3 -2 -2 -3 5 3 -2 -3	3 -2 -3 -3 5 1 -2 -3 5	-2 -3 5 5 1 -8 -3 5 1	-3 5 1 1 -8 4 5 1 -8	5 1 -8 -8 4 9 1 -8 4
$\det\bar{\bar{Q}}_2^{-n}=$	1	1	1	1	1	1	1

Розглянувши уважно звичайні та обернені матриці, можна побачити, що у звичайних матрицях значення елементів набувають тільки додатні 2-числа Фібоначчі, а в обернених – як додатні, так і від'ємні можливо й числа Фібоначчі, однак далеко не з цього самого набору. Водночас, $\bar{\bar{Q}}_2^n$-матриці при $n = \pm1$ та ±2 є бінарними, а вже при $n = \pm3, \pm4, ..., \pm13$ значення елементів набувають наступні 2-числа Фібоначчі. У обернених матрицях більшість значень елементів не відповідають їхнім значенням у звичайних матрицях.

У загальному випадку $\bar{\bar{Q}}_2^n$-матриці мають такий математичний запис:

$$\bar{\bar{Q}}_2^n=\begin{bmatrix} pF_2^{n+1} & pF_2^{n} & pF_2^{n-1} \\ pF_2^{n-1} & pF_2^{n-2} & pF_2^{n-3} \\ pF_2^{n} & pF_2^{n-1} & pF_2^{n-2} \end{bmatrix},\ \det\bar{\bar{Q}}_2^n=(-1)^{2\cdot n},\ n=2,3,4,\ldots, \tag{2.7}$$

де pF_2^{n-1}, pF_2^{n}, pF_2^{n+1} – 2-числа Фібоначчі. Задавати $\bar{\bar{Q}}_2^n$-матриці n-го степеня можна за допомогою такого матричного виразу:

$$\bar{\bar{Q}}_2^{n+1}=\bar{\bar{Q}}_2^n\times\bar{\bar{Q}}_2^1,\ n=2,3,4,\ldots. \tag{2.8}$$

Основний недолік цього виразу в тому, що для отримання $\bar{\bar{Q}}_2^{n+1}$-матриці Фібоначчі потрібно мати при цьому $\bar{\bar{Q}}_2^n$-матрицю, а це означає, що мають бути й усі попередні матриці від 2-го до (n-1)-го степеня.

Для розуміння основних закономірностей процесу побудови $\bar{\bar{Q}}_p^n$-матриць Фібоначчі розглянемо ще один приклад для p = 3. Тоді отриманий набір $\bar{\bar{Q}}_3^n$-матриць (див. нижче), піднесених до n-ої степені, має аналогічні особливості побудови як і $\bar{\bar{Q}}_2^n$-матриці, однак елементами цих матриць вже є 3-числа Фібоначчі (див. табл. 1.3). Звернемо увагу тільки на те, що матрична формула (2.8) є також придатною для задавання $\bar{\bar{Q}}_3^n$-матриці, піднесеної до n-ої степені.

Набір $\bar{\bar{Q}}_3^n$-матриць Фібоначчі

$n=$	0	1	2	3	4	5
$\bar{\bar{Q}}_3^n=$	1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1	1 1 0 0 0 0 1 0 0 0 0 1 1 0 0 0	1 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0	1 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0	2 1 1 1 1 1 0 0 1 1 1 0 1 1 1 1	3 2 1 1 1 1 1 0 1 1 1 1 2 1 1 1
$\det\bar{\bar{Q}}_3^n=$	1	-1	1	-1	1	-1

$\bar{\bar{Q}}_3^{-n}=$	1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1	0 0 0 1 1 0 0 -1 0 1 0 0 0 0 1 0	0 0 1 0 0 0 -1 1 1 0 0 -1 0 1 0 0	0 1 0 0 0 -1 1 0 0 0 -1 1 1 0 0 -1	1 0 0 -1 -1 1 0 1 0 -1 1 0 0 0 -1 1	0 0 -1 1 1 0 1 -2 -1 1 0 1 0 -1 1 0
$\det\bar{\bar{Q}}_3^{-n}=$	1	-1	1	-1	1	-1

Продовження набору $\bar{\bar{Q}}_3^n$-матриць Фібоначчі

$n=$	6	7	8	9	10	11
$\bar{\bar{Q}}_3^n=$	4 3 2 1 1 1 1 1 2 1 1 1 3 2 1 1	5 4 3 2 2 1 1 1 3 2 1 1 4 3 2 1	7 5 4 3 3 2 1 1 4 3 2 1 5 4 3 2	10 7 5 4 4 3 2 1 5 4 3 2 7 5 4 3	14 10 7 5 5 4 3 2 7 5 4 3 10 7 5 4	19 14 10 7 7 5 4 3 10 7 5 4 14 10 7 5
$\det\bar{\bar{Q}}_3^n=$	1	-1	1	-1	1	-1
$\bar{\bar{Q}}_3^{-n}=$	0 -1 1 0 0 1 -2 1 1 0 1 -2 -1 1 0 1	-1 1 0 1 1 -2 1 -1 0 1 -2 1 1 0 1 -2	1 0 1 -2 -2 1 -1 3 1 -2 1 -1 0 1 -2 1	0 1 -2 1 1 -1 3 -3 -2 1 -1 3 1 -2 1 -1	1 -2 1 -1 -1 3 -3 2 1 -1 3 -3 -2 1 -1 3	-2 1 -1 3 3 -3 2 -4 -1 3 -3 2 1 -1 3 -3
$\det\bar{\bar{Q}}_3^{-n}=$	1	-1	1	-1	1	-1

Зрозуміло, що для $\bar{\bar{Q}}_3^n$-матриць Фібоначчі можна вивести й узагальнений математичний запис так, як це показано у виразі (2.7). Однак, основним результатом роботи [11] є наведення для $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-ої степені, такого виразу:

$$\bar{\bar{Q}}_p^n=\begin{bmatrix} pF_p^{n+1} & pF_p^{n} & \cdots & pF_p^{n-p+2} & pF_p^{n-p+1} \\ pF_p^{n-p+1} & pF_p^{n-p} & \cdots & pF_p^{n-2p+2} & pF_p^{n-2p+1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ pF_p^{n-1} & pF_p^{n-2} & \cdots & pF_p^{n-p} & pF_p^{n-p-1} \\ pF_p^{n} & pF_p^{n-1} & \cdots & pF_p^{n-p+1} & pF_p^{n-p} \end{bmatrix}, \tag{2.9}$$

$$\det\bar{\bar{Q}}_p^n=(-1)^{p\cdot n},\ p=1,2,3,\ldots;\ n=\pm2,\pm3,\pm4,\ldots.$$

Елементами цієї $\bar{\bar{Q}}_p^n$-матриці є p-числа Фібоначчі, які можна задати рекурентним співвідношенням (1.2). Зауважимо, що $\bar{\bar{Q}}_p^n$-матриці Фібоначчі для всіх $n \le p$ є бінарними, а при $n > p$ значення елементів набувають наступні p-числа Фібоначчі. Заради святих наукових ідей звернемо увагу й на те, що у виразі (2.9), як на перший погляд, слабо спостерігається закономірність процесу формування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-ої степені, елементами якої є p-числа Фібоначчі. Проте нижче спробуємо виявити таку закономірність, а також замість матричного виразу (2.8) використаємо дещо іншу математичну процедуру побудови $\bar{\bar{Q}}_p^n$-матриць Фібоначчі.

Отже, внаслідок проведеного дослідження встановлено, що існує теорія побудови квадратних матриць спеціального типу [8], які володіють унікальною математичною властивістю, придатною для виконання криптографічних перетворень: наведено алгоритм формування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-ої степені, елементами якої є p-числа Фібоначчі; згідно з (2.9) визначник будь-якої $\bar{\bar{Q}}_p^n$-матриці завжди дорівнює одиниці за абсолютною величиною, а її знак залежить

від добутку двох цілих чисел $p \cdot n$ (p = 1, 2, 3, ...; n = ±2, ±3, ±4, ...). Якщо цей добуток є парним, то визначник матриці (2.9) дорівнює +1, інакше – дорівнює –1. Отримані матриці можуть використовуватися як ключі шифрування (звичайні $\bar{\bar{Q}}_p^n$-матриці) та ключі дешифрування (обернені $\bar{\bar{Q}}_p^{-n}$-матриці) інформації для реалізації матричних криптографічних перетворень, а також як розширення ключів для реалізації багатораундової криптосистеми [3]. Особливості їхньої реалізації детально розглянуто у розд. 3 цього дослідження.

Процедура генерування $\bar{\bar{Q}}_p^n$-матриць Фібоначчі. Для виявлення основних закономірностей процедури генерування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-ої степені, елементами якої є p-числа Фібоначчі, розглянемо такий приклад. За основу візьмемо $\bar{\bar{Q}}_3^n$-матрицю, піднесену до n = ±11, ±12, ..., ±16 степені, внаслідок чого отримаємо їхній набір (див. нижче), елементами яких є 3-числа Фібоначчі (див. табл. 1.3). Спочатку розглянемо елементи $\bar{\bar{Q}}_3^{11}$-матриці, випишемо порядкові номери $u_{ij,3}^{11}$ її елементів і занесемо у відповідну матрицю $\bar{\bar{U}}_3^{11}$. Ці номери, згідно з даними табл. 1.3, відповідають номерам її стовпців, тобто маємо таку послідовність: $u_{1,1,3}^{11} = 11$, $u_{1,2,3}^{11} = u_{4,1,3}^{11} = 10$, $u_{1,3,3}^{11} = u_{3,1,3}^{11} = u_{4,2,3}^{11} = 9$ і т.д.

Продовження набору $\bar{\bar{Q}}_3^n$-матриць Фібоначчі

n=

11	12	13	14	15	16
19 14 10 7 7 5 4 3 10 7 5 4 14 10 7 5	26 19 14 10 10 7 5 4 14 10 7 5 19 14 10 7	36 26 19 14 14 10 7 5 19 14 10 7 26 19 14 10	50 36 26 19 19 14 10 7 26 19 14 10 36 26 19 14	69 50 36 26 26 19 14 10 36 26 19 14 50 36 26 19	95 69 50 36 36 26 19 14 50 36 26 19 69 50 36 26
$\bar{\bar{Q}}_3^n =$					
det $\bar{\bar{Q}}_3^n$ = -1	1	-1	1	-1	1
-2 1 -1 3 3 -3 2 -4 -1 3 -3 2 1 -1 3 -3	1 -1 3 -3 -3 2 -4 6 3 -3 2 -4 -1 3 -3 2	-1 3 -3 2 2 -4 6 -5 -3 2 -4 6 3 -3 2 -4	3 -3 2 -4 -4 6 -5 6 2 -4 6 -5 -3 2 -4 6	-3 2 -4 6 6 -5 6 -10 -4 6 -5 6 2 -4 6 -5	2 -4 6 -5 -5 6 -10 11 6 -5 6 -10 -4 6 -5 6
$\bar{\bar{Q}}_3^{-n}$ =					
det $\bar{\bar{Q}}_3^{-n}$ = -1	1	-1	1	-1	1
11 10 9 8 8 7 6 5 9 8 7 6 10 9 8 7	12 11 10 9 9 8 7 6 10 9 8 7 11 10 9 8	13 12 11 10 10 9 8 7 11 10 9 8 12 11 10 9	14 13 12 11 11 10 9 8 12 11 10 9 13 12 11 10	15 14 13 12 12 11 10 9 13 12 11 10 14 13 12 11	16 15 14 13 13 12 11 10 14 13 12 11 15 14 13 12
$\bar{\bar{U}}_3^n$ =					

n = 11

	1	2	3	4
1	8	7	6	5
2	9	8	7	6
3	10	9	8	7
4	11	10	9	8

12

	1	2	3	4
1	9	8	7	6
2	10	9	8	7
3	11	10	9	8
4	12	11	10	9

13

	1	2	3	4
1	10	9	8	7
2	11	10	9	8
3	12	11	10	9
4	13	12	11	10

14

	1	2	3	4
1	11	10	9	8
2	12	11	10	9
3	13	12	11	10
4	14	13	12	11

15

	1	2	3	4
1	12	11	10	9
2	13	12	11	10
3	14	13	12	11
4	15	14	13	12

16

	1	2	3	4
1	13	12	11	10
2	14	13	12	11
3	15	14	13	12
4	16	15	14	13

$\bar{\bar{D}}_3^n$ =

Проаналізувавши значення елементів матриці $\bar{\bar{U}}_3^{11}$, бачимо, що перший рядок так і "проситься" перенести його вниз матриці, а всі решта рядки потрібно зсунути вверх на одну позицію. Внаслідок такого зсуву рядків матриці $\bar{\bar{U}}_3^{11}$ на одну позицію вверх отримаємо нову матрицю $\bar{\bar{U}}_3'^{11}$. Такі дії можна реалізувати за допомогою такого матричного виразу:

$$\bar{\bar{M}}_3^{+1} \times \bar{\bar{U}}_3^{11} = \bar{\bar{U}}_3'^{11}, \qquad (2.10)$$

де $\bar{\bar{M}}_3^{+1}$ – матриця зсуву рядків матриці на одну позицію вверх. Ця матриця є бінарною, а її елементи формуються так, як це показано нижче. Як виявиться згодом, нам доведеться здійснювати зсув рядків матриці на одну позицію не вверх, а вниз, при цьому матриця зсуву $\bar{\bar{M}}_3^{-1}$ матиме дещо інший порядок розташування елементів (див. нижче). Зрозуміло, що зсув рядків матриці можна організувати не на одну, а на k-ту кількість позицій і, як виявиться потім, це значно вплине на якість виконання криптографічних перетворень, тобто підвищить їхню криптографічну стійкість.

Зсув рядків матриці уверх на 1 позицію

$\bar{\bar{M}}_3^{+1}$

	1	2	3	4
1	0	**1**	0	0
2	0	0	**1**	0
3	0	0	0	**1**
4	**1**	0	0	0

×

$\bar{\bar{U}}_3^{11}$

11	10	9	8
8	7	6	5
9	8	7	6
10	9	8	7

=

$\bar{\bar{U}}_3'^{11}$

8	7	6	5
9	8	7	6
10	9	8	7
11	10	9	8

Зсув рядків матриці вниз на 1 позицію

$\bar{\bar{M}}_3^{-1}$

	1	2	3	4
1	0	0	0	**1**
2	**1**	0	0	0
3	0	**1**	0	0
4	0	0	**1**	0

×

$\bar{\bar{D}}_3^{11}$

8	7	6	5
9	8	7	6
10	9	8	7
11	10	9	8

=

$\bar{\bar{U}}_3'^{11}$

11	10	9	8
8	7	6	5
9	8	7	6
10	9	8	7

Для формування елементів матриці зсуву $\bar{\bar{M}}_p^k$ використовується такий логічний вираз

$$\bar{\bar{M}}_p^k = \left[m_{ij,p}^k = \begin{cases} 1, \text{ якщо } (i+k-j) \bmod (p+1) = 0; \\ 0 - \text{у іншому випадку,} \end{cases} i, j = \overline{1, p+1} \right], \; k \le p, \qquad (2.11)$$

де: $(p+1)$ – розмір бінарної матриці зсуву; k – кількість позицій зсуву ($\pm k$ – зсув відповідно вверх/вниз).

Отже, з новоутвореної матриці $\bar{\bar{U}}_3'^{11}$ видно, що її елементи мають чітке впорядкування: відбувається зменшення їхніх значень з нижнього лівого кута матриці у бік її верхнього правого кута. Для формування елементів такої матриці (назвемо її $\bar{\bar{D}}_p^n$-матрицею), значення яких будуть залежати від p-чисел Фібоначчі та степеня n (до якого потрібно піднести матрицю), використаємо таку формулу

$$\bar{\bar{D}}_p^n = \left[d_{ij,p}^n = n - (p+1-i) - (j-1), \; i, j = \overline{1, p+1} \right]. \qquad (2.12)$$

Ця формула є придатною для формування елементів матриці, якщо нумерація її рядків і стовпців починається з одиниці. Для інших випадків потрібні незначні корективи. Приклади генерування $\bar{\bar{D}}_3^n$-матриць для n = 12, 13, ..., 16 показано вище.

Повертаючись до нашого набору $\bar{\bar{Q}}_3^n$-матриць Фібоначчі для n = 11, 12, ..., 16 (див. вище), бачимо, що, сформувавши $\bar{\bar{D}}_3^{11}$-матрицю, потрібно здійснити зсув її рядків на одну позицію вниз, внаслідок чого отримаємо

$$\bar{\bar{M}}_3^{-1} \times \bar{\bar{D}}_3^{11} = \bar{\bar{U}}_3^{11}. \qquad (2.13)$$

Тепер, за елементами матриці $\bar{\bar{U}}_3^{11}$ можна відновити елементи $\bar{\bar{Q}}_3^{11}$-матриці, значеннями яких будуть 3-числа Фібоначчі (див. табл. 1.3).

Загалом процедура генерування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-ої степені, значеннями елементів яких будуть p-числа Фібоначчі, матиме такий математичний запис:

$$\begin{aligned}
&\bar{\bar{D}}_p^n = \left[d_{ij,p}^n = n - (p+1-i) - (j-1),\ i,j = \overline{1,p+1} \right];\\
&\bar{\bar{M}}_p^k = \left[m_{ij,p}^k = \begin{cases} 1, \text{ якщо } (i+k-j) \bmod (p+1) = 0; \\ 0 - \text{у іншому випадку,} \end{cases} i,j = \overline{1,p+1} \right];\\
&\bar{\bar{U}}_p^n = \left[u_{ij,p}^n = \sum_{l=1}^{p+1} m_{il,p}^{-n} \cdot d_{lj,p}^n,\ i,j = \overline{1,p+1} \right];\\
&\bar{\bar{Q}}_p^n = \left[q_{ij,p}^n = pF_p^{u_{ij,p}^n},\ i,j = \overline{1,p+1} \right],\ p = 1,2,3,\ldots;\ n = 2,3,4,\ldots;\ k = -1,-2,\ldots - p.
\end{aligned} \qquad (2.14)$$

Основною перевагою цієї процедури над матричним виразом (2.8) є те, що для отримання $\bar{\bar{Q}}_p^{n+1}$-матриці зовсім не потрібно мати $\bar{\bar{Q}}_p^n$-матрицю, а це означає, що немає потреби і в будь-яких попередніх матрицях. Єдине що потрібно мати, так це наперед згенеровані p-числа Фібоначчі для різних значень n (див. табл. 1.3). Зазначимо також, що наведені вище $\bar{\bar{Q}}_3^n$-матриці для n = 12, 13, ..., 16 сформовано за допомогою наведеної процедури (2.14), уникнувши при цьому матричний вираз (2.8). При цьому обернені до них матриці отримано звичайним способом, хоча, не виключено, що їх також можна отримати дещо простішим способом. Однак, для цього потрібно провести ще додаткове дослідження з виявлення закономірностей їх побудови.

Продемонструємо використання процедури генерування $\bar{\bar{Q}}_p^n$-матриці Фібоначчі на конкретному прикладі при таких вхідних значеннях: p = 4, n = 16 та k = 2. В цьому випадку, згідно з табл. 1.3, будемо мати справу з такими 4-числа Фібоначчі: 1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 8, 11, 15, 20, 26, 34, 45. Внаслідок виконання математичної процедури (2.14) отримаємо такі результати розрахунку:

$\bar{\bar{D}}_4^{16}$

16	1	2	3	4	5
1	12	11	10	9	8
2	13	12	11	10	9
3	14	13	12	11	10
4	15	14	13	12	11
5	16	15	14	13	12

$\bar{\bar{M}}_4^2$

k=	2				
	0	0	0	1	0
	0	0	0	0	1
	1	0	0	0	0
	0	1	0	0	0
	0	0	1	0	0

$\bar{\bar{U}}_4^{16}$

15	14	13	12	11
16	15	14	13	12
12	11	10	9	8
13	12	11	10	9
14	13	12	11	10

$\bar{\bar{Q}}_4^{16}$

34	26	20	15	11
45	34	26	20	15
15	11	8	6	5
20	15	11	8	6
26	20	15	11	8

$\bar{\bar{Q}}_4^{-16}$

1	0	-1	3	-3
-4	1	1	-4	6
6	-3	1	1	-4
-4	3	-3	1	1
1	-1	3	-3	1

$\det \bar{\bar{Q}}_4^{16} = 1 \qquad \det \bar{\bar{Q}}_4^{-16} = 1$

Отже, внаслідок проведеного дослідження розроблено процедуру генерування множини $\bar{\bar{Q}}_p^n$-матриці Фібоначчі, яка за відомими значеннями степені матриці (n) та p-чисел Фібоначчі дає змогу отримувати відповідні матриці – ключі (де)шифрування, здійснювати їхнє розширення для кожного раунду, що

забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й створює зручність при передаванні каналами зв'язку.

3. Використання узагальнених матриць Фібоначчі для виконання криптографічних перетворень інформації

Виявляється [12], що $\bar{\bar{Q}}_p^n$-матриці Фібоначчі (2.9) можна з успіхом використовувати для шифрування даних. Суть методу шифрування, який базується на використанні цих матриць, полягає у поданні t-го блоку початкового повідомлення у вигляді матриці $\bar{\bar{T}}^{(t)}$ $(\forall t \in T)$ розміром $(p+1)\times(p+1)$ і її множенні на шифрувальну $\bar{\bar{Q}}_p^n$-матрицю Фібоначчі. При цьому процедура дешифрування зводиться до множення t-ої матриці $\bar{\bar{K}}^{(t)}$ $(\forall t \in T)$ розміром $(p+1)\times(p+1)$ зашифрованого повідомлення на дешифрувальну $\bar{\bar{Q}}_p^{-n}$-матрицю. У криптографічних перетвореннях інформації зазначені дії мають такий матричний запис:

шифрування $$\bar{\bar{T}}^{(t)} \underset{m}{\otimes} \bar{\bar{Q}}_p^n = \bar{\bar{K}}^{(t)},\ \forall t \in T; \qquad (3.1)$$

дешифрування $$\bar{\bar{K}}^{(t)} \underset{m}{\otimes} \bar{\bar{Q}}_p^{-n} = \bar{\bar{T}}^{(t)},\ \forall t \in T. \qquad (3.2)$$

У роботі [8] зазначено, що початкова матриця $\bar{\bar{T}}^{(t)}$ пов'язана з зашифрованою матрицею $\bar{\bar{K}}^{(t)}$ деякою властивістю, сутність якої зводиться до такого. Спочатку обчислимо визначник початкової матриці $\bar{\bar{T}}^{(t)}$, який дорівнює числу $\det \bar{\bar{T}}^{(t)}$, а потім знайдемо визначник зашифрованої матриці $\det \bar{\bar{K}}^{(t)}$. Згідно з теорією матриць [1], ці визначники пов'язані між собою таким співвідношенням:

$$\det \bar{\bar{K}}^{(t)} = \det \left(\bar{\bar{T}}^{(t)} \underset{m}{\otimes} \bar{\bar{Q}}_p^n \right) = \det \bar{\bar{T}}^{(t)} \underset{m}{\otimes} \det \bar{\bar{Q}}_p^n. \qquad (3.3)$$

Якщо використати з тотожності (2.9) формулу для обчислення визначника $\bar{\bar{Q}}_p^n$-матриці, то отримаємо нову тотожність, яка пов'язує між собою визначники матриць $\bar{\bar{T}}^{(t)}$ і $\bar{\bar{K}}^{(t)}$, а саме:

$$\det \bar{\bar{K}}^{(t)} = \det \bar{\bar{T}}^{(t)} \underset{m}{\otimes} (-1)^{p \cdot n},\ p = 1,2,3,\ldots;\ n = \pm 2, \pm 3, \pm 4, \ldots. \qquad (3.4)$$

Ця тотожність є "основним контрольним співвідношенням", яке використовується для виявлення та коригування помилок у матриці $\bar{\bar{K}}^{(t)}$, тобто у зашифрованій інформації. Якщо ж не використовувати "основне контрольне співвідношення" (3.4), то криптографічні перетворення (3.1) та (3.2) матимуть дещо простіший матричний запис, а саме:

шифрування $$\bar{\bar{T}} \underset{m}{\otimes} \bar{\bar{Q}}_p^n = \bar{\bar{K}}; \qquad (3.5)$$

дешифрування $$\bar{\bar{K}} \underset{m}{\otimes} \bar{\bar{Q}}_p^{-n} = \bar{\bar{T}}. \qquad (3.6)$$

Продемонструємо особливості застосування розглянутого вище методу (де)шифрування інформації з використанням узагальнених матриць Фібоначчі на конкретному прикладі (див. нижче). У цьому прикладі використана $\bar{\bar{Q}}_p^n$-матриця для p = 3 та n = 11, елементами якої є 3-числа Фібоначчі.

Шифрування вхідного повідомлення

$\bar{\bar{T}}$

1	184	248	143	172
2	125	174	63	199
3	88	242	128	219
4	207	78	55	124
5	82	88	171	123
6	54	167	189	211
7	223	81	75	149
8	238	163	150	224

$\times$ $\bar{\bar{Q}}_3^{11}$

19	14	10	7
7	5	4	3
10	7	5	4
14	10	7	5

-1

$=$ $\bar{\bar{T}} \times \bar{\bar{Q}}_3^{11}$

9070	6537	4751	3464
7009	5051	3654	2644
7712	5528	4021	2949
6765	4913	3525	2523
5606	4015	2888	2137
7039	5024	3630	2690
7640	5542	3972	2849
10299	7437	5350	3875

$\rightarrow$ $\bar{\bar{T}} \times \bar{\bar{Q}}_3^{11} \bmod 256 = \bar{\bar{K}}$

110	137	143	136
97	187	70	84
32	152	181	133
109	49	197	219
230	175	72	89
127	160	46	130
216	166	132	33
59	13	230	35

Дешифрування зашифрованої інформації

$\bar{\bar{K}}$

110	137	143	136
97	187	70	84
32	152	181	133
109	49	197	219
230	175	72	89
127	160	46	130
216	166	132	33
59	13	230	35

$\times$ $\bar{\bar{Q}}_3^{-11}$

-2	1	-1	3
3	-3	2	-4
-1	3	-3	2
1	-1	3	-3

-1

$=$ $\bar{\bar{K}} \times \bar{\bar{Q}}_3^{-11}$

184	-8	143	-340
381	-338	319	-569
344	-14	128	-549
-49	334	55	-132
82	-168	171	-133
310	-345	445	-557
-33	81	-181	149
-274	675	-618	480

$\rightarrow$ $\bar{\bar{K}} \times \bar{\bar{Q}}_3^{-11} \bmod 256 = \bar{\bar{T}}$

184	248	143	172
125	174	63	199
88	242	128	219
207	78	55	124
82	88	171	123
54	167	189	211
223	81	75	149
238	163	150	224

Використання $\bar{\bar{Q}}_p^n$-матриці Фібоначчі для багатораундової криптосистеми. Виявляється, що до матричного виразу (3.5), який дає змогу зашифрувати повідомлення $\bar{\bar{T}}$, можна застосувати R-раундову процедуру шифрування [5], при цьому кожного разу з новими ключами, тобто $\bar{\bar{Q}}_p^n$-матрицями Фібоначчі для $n = r = 1, 2, ..., R$. Водночас, процес дешифрування інформації за виразом (3.6) також повторюватиметься R разів. У цьому випадку узагальнені вирази для реалізації прямого та зворотного криптографічних перетворень матимуть такий вигляд:

$$\bar{\bar{K}} = \underbrace{\bar{\bar{T}} \underset{m}{\otimes} \bar{\bar{Q}}_p^1 \underset{m}{\otimes} \bar{\bar{Q}}_p^2 ... \underset{m}{\otimes} \bar{\bar{Q}}_p^r ... \underset{m}{\otimes} \bar{\bar{Q}}_p^R}_{R\text{раундів}}; \tag{3.7}$$

$$\bar{\bar{T}} = \underbrace{\bar{\bar{K}} \underset{m}{\otimes} \bar{\bar{Q}}_p^{-R} \underset{m}{\otimes} \bar{\bar{Q}}_p^{-(R-1)} ... \underset{m}{\otimes} \bar{\bar{Q}}_p^{-r} ... \underset{m}{\oplus} \bar{\bar{Q}}_p^{-1}}_{R\text{раундів}}. \tag{3.8}$$

Поєднання матричної криптосистеми (3.7) і (3.8) з матричними перестановними алгоритмами [3, розд. 3] дає змогу побудувати багатораундову матричну перестановну криптосистему для захисту інформації, яку загалом можна подавати у вигляді процедури багатораундового (де)шифрування на основі таких матричних виразів:

$$\bar{\bar{K}}_{\text{рс}}^{\text{п}} = \left(\bar{\bar{P}}_{\text{р}}^{\text{п}} \times \bar{\bar{T}} \times \bar{\bar{P}}_{\text{с}}^{\text{п}}\right) \underbrace{\underset{m}{\otimes} \bar{\bar{Q}}_p^1 \underset{m}{\otimes} \bar{\bar{Q}}_p^2 ... \underset{m}{\otimes} \bar{\bar{Q}}_p^r ... \underset{m}{\otimes} \bar{\bar{Q}}_p^R}_{R\text{раундів}}; \tag{3.9}$$

$$\bar{\bar{T}}_{\text{ср}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}'^{\text{п}} \times \left(\underbrace{\bar{\bar{K}}_{\text{рс}}^{\text{п}} \underset{m}{\otimes} \bar{\bar{Q}}_p^{-R} \underset{m}{\otimes} \bar{\bar{Q}}_p^{-(R-1)} ... \underset{m}{\otimes} \bar{\bar{Q}}_p^{-r} ... \underset{m}{\oplus} \bar{\bar{Q}}_p^{-1}}_{R\text{раундів}} \times \bar{\bar{P}}_{\text{с}}'^{\text{п}} \right), \tag{3.10}$$

де: $\bar{\bar{P}}_{\text{р}}^{\text{п}}$, $\bar{\bar{P}}_{\text{р}}'^{\text{п}}$ та $\bar{\bar{P}}_{\text{с}}^{\text{п}}$, $\bar{\bar{P}}_{\text{с}}'^{\text{п}}$ – квадратні перестановні матриці відповідно рядків і стовпців вхідної матриці $\bar{\bar{T}}$ для прямого і зворотного ходів.

Можливі ще й такі матричні вирази для реалізації процедури багатораундового (де)шифрування інформації:

$$\bar{\bar{K}}_{\text{рс}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}^{\text{п}} \times \underbrace{\left(\bar{\bar{T}} \underset{m}{\otimes} \bar{\bar{Q}}_p^1 \underset{m}{\otimes} \bar{\bar{Q}}_p^2 ... \underset{m}{\otimes} \bar{\bar{Q}}_p^r ... \underset{m}{\otimes} \bar{\bar{Q}}_p^R\right)}_{R\text{раундів}} \times \bar{\bar{P}}_{\text{с}}^{\text{п}}; \tag{3.11}$$

$$\bar{\bar{T}}_{\text{ср}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}'^{\text{п}} \times \left(\bar{\bar{K}}_{\text{рс}}^{\text{п}} \times \bar{\bar{P}}_{\text{с}}'^{\text{п}}\right) \underbrace{\underset{m}{\otimes} \bar{\bar{Q}}_p^{-R} \underset{m}{\otimes} \bar{\bar{Q}}_p^{-(R-1)} ... \underset{m}{\otimes} \bar{\bar{Q}}_p^{-r} ... \underset{m}{\oplus} \bar{\bar{Q}}_p^{-1}}_{R\text{раундів}}. \tag{3.12}$$

Отже, внаслідок проведеного дослідження з'ясовано, що $\bar{\bar{Q}}_p^n$-матриці, піднесені до n-ої степені, значеннями елементів яких є p-числа Фібоначчі, можуть ефективно використовуватися для виконання криптографічних перетворень інформації. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної звичайної та перестановної криптосистеми з різними ключами шифрування на кожному раунді, реалізація якого значно підвищує його криптостійкість до брутальних атак.

Висновки

1. З'ясовано, що основна проблема багатораундової матричної Афінної криптосистеми полягає у генеруванні множини звичайних і обернених матриць – ключів (де)шифрування інформації, елементами яких мають бути цілі числа, розширенні ключів для кожного раунду, а також у ефективній системі їх зберігання та передаванні каналами зв'язку. Для її вирішення прийнято рішення використовувати Q_p-матриці Фібоначчі.

2. Виявлено, що існують не два, а три способи задавання p-чисел Фібоначчі: у вигляді одновимірного рекурентного співвідношення, через біноміальні коефіцієнти у вигляді спеціальної формули, а також у вигляді двовимірного рекурентного співвідношення.

3. Наведено алгоритм формування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-ої степені, елементами якої є p-числа Фібоначч. Отримані матриці можуть використовуватися як ключі шифрування (звичайні $\bar{\bar{Q}}_p^n$-матриці) та ключі дешифрування (обернені $\bar{\bar{Q}}_p^{-n}$-матриці) інформації для реалізації матричних перетворень, а також як розширення ключів для реалізації багатораундової криптосистеми.

4. Розроблено процедуру генерування множини $\bar{\bar{Q}}_p^n$-матриці Фібоначчі, яка за відомими значеннями степені матриці (n) та p-чисел Фібоначчі дає змогу отримувати відповідні матриці – ключі (де)шифрування, здійснювати їхнє розширення для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й створює зручність при передаванні каналами зв'язку.

5. З'ясовано, що $\bar{\bar{Q}}_p^n$-матриці Фібоначчі можуть ефективно використовуватися для виконання криптографічних перетворень інформації. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової

матричної звичайної та перестановної криптосистеми з різними ключами шифрування на кожному раунді, реалізація якого значно підвищує його криптостійкість до брутальних атак.

Література

1. Гантмахер Ф.Р. Теория матриц / Ф.Р. Гантмахер. – М. : Изд-во "Физматлит", 2010. – 560 с.
2. Голуб Дж. Матричные вычисления / Дж. Голуб, Ч. ван Лоун. – М. : Изд-во "Мир", 1999. – 548 с.
3. Грицюк П.Ю. Особливості реалізації матричної Афінної криптосистеми захисту інформації / П.Ю. Грицюк, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2015. – Вип. 25.5. – С. 346-356.
4. Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Вид-во БаК, 2003. – 144 с.
5. Красиленко В.Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації: зб. наук. праць. – Харків : Вид-во ХУПС ім. Івана Кожедуба. – 2012. – Вип. 3(101), т. 2. – С. 53-61.
6. Стахов А.П. Введение в алгоритмическую теорию измерения / А.П. Стахов. – М. : Изд-во "Советское Радио", 1977. – 246 с.
7. Стахов А.П. Гармония Мироздания и Золотое Сечение: древнейшая научная парадигма и ее роль в современной науке, математике и образовании / А.П. Стахов. – У 2-ох ч. – Ч. 1. [Электронный ресурс]. – Доступный с http://www.obretenie.info/txt/stahov/harmoni1.htm
8. Стахов А.П. Гармония Мироздания и Золотое Сечение: древнейшая научная парадигма и ее роль в современной науке, математике и образовании / А.П. Стахов. – У 2-ох ч. – Ч. 2. [Электронный ресурс]. – Доступный с http://www.obretenie.info/txt/stahov/harmoni2.htm
9. Хорошко В.О. Методи та засоби захисту інформації : навч. посібн. / В.О. Хорошко, А.О. Четков. – К. : Вид-во "Юніор", 2003. – 502 с.
10. Hoggat, V.E. Fibonacci and Lucas Numbers / V.E. Hoggat. – Houghton-Mifflin, Palo Alto, California, 1969.
11. Stakhov A.P. Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic / A.P. Stakhov // The Computer Journal. – 2002. – Vol. 45, No. 2. – Pp. 222-236.
12. Stakhov A.P. Introduction into Fibonacci Coding and Cryptography / A.P. Stakhov, V. Massingua, A.A. Sluchenkova. – Харьков : Изд-во "Основа" Харьковского университета, 1999 г.

Грыцюк Ю.И., Грыцюк П.Ю. **Методы и средства генерирования Q_p-матриц Фибоначчи – ключей для реализации криптографических преобразований**

Рассматриваются особенности эффективного генерирования Q_p-матриц Фибоначчи, которые могут использоваться как ключи (де)шифрования для многораундовой матричной криптографической системы преобразования информации. Выяснено, что основная проблема многораундовой матричной аффинной криптосистемы заключается в генерировании множества обычных и обратных матриц – ключей (де)шифрования информации, элементами которых должны быть целые числа. Разработана процедура генерирования множества Q_p-матриц Фибоначчи, которая по известным значениям степени матрицы (n) и p-чисел Фибоначчи позволяет получать соответствующее множество ключей (де)шифрования информации, осуществлять их расширения для каждого раунда, что обеспечивает не только эффективный способ их образования и хранения, но и создает удобство при передаче по каналам связи.

Ключевые слова: защита информации, шифрование/дешифрование информации, числа Фибоначчи, Q_p-матрицы Фибоначчи, криптографическая система, матричные Аффинные преобразования, многораундовая матричная криптографическая система.

Gryciuk Yu.I., Grytsyuk P.Yu. **The methods and means of the generation of Fibonacci Q_p-matrices – Keys for the Implementation of Cryptographic Conversion**

The features of effective generation of the Fibonacci Q_p-matrix have been considered. Those matrices are used as decryption/encryption keys for the multi-round matrix cryptographic system of the information transformation. It was found that in multi-round affinity matrix cryptosystem the main problem is to generate a plurality of the conventional and inverse keys-matrices of the information encryption/decryption that must be integers. The procedure for generating a plurality of Fibonacci Q_p-matrix has been developed. This procedure relies on the known degree of matrix values (n) and p-numbers Fibonacci and lets us set of the appropriate information encryption/decryption keys, implement expansion keys for each round. This provides an efficient way of their formation and storage and creates the ease of transmitting channels.

Keywords: information security, encryption/decryption information. Fibonacci numbers, Fibonacci Q_p-matrix, crypto-graphic system, matrix Affine transformation, matrix multi-rounds cryptographic system.

УДК 535.343.2

Проф. З.П. Чорній, д-р фіз.-мат. наук; доц. І.Б. Пірко, канд. фіз.-мат. наук; доц. В.М. Салапак, канд. фіз.-мат. наук; ст. викл. М.В. Дячук; доц. О.Р. Онуфрів, канд. фіз.-мат. наук – НЛТУ України, м. Львів

ГЕНЕРАЦІЯ ЦЕНТРІВ ЗАБАРВЛЕННЯ У КРИСТАЛАХ ФЛЮОРИТІВ З ТЕРМІЧНО НЕРІВНОВАЖНИМИ СТРУКТУРНИМИ ДЕФЕКТАМИ

У моделі лінійного кристала досліджено механізм генерації центрів забарвлення у кристалах CaF_2-Me^+, що містять термічно нерівноважні (Me^+-$V_a^+Me^+V_a^+$)-пари дефектів (Me^+ – іон лужного метала, V_a^+ – вакансія іона фтору). Розраховано імовірність утворення у ґратці кристала ($F_A(1)$-V_K) і ($F_A(1)$-V_{KA})-комплементарних пар при розпаді електронно-діркової пари, кінетику наростання центрів забарвлення та їх граничні концентрації. Досліджено механізм ($F_A(1)$-V_K)→($F_A(1)$-V_{KA}) та ($F_A(1)$-V_K)→(M_A^+-V_{KA})-перетворень. Проаналізовано вплив автолокалізації дірок на радіаційну чутливість кристалів флюоритів.

Ключові слова: кристал, радіація, центри забарвлення.

Вступ. Відомо **[**1-5**]**, що іони лужного металу входять у ґратку кристалів флюоритів у вигляді іонів заміщення: за T<400 K утворюють з аніонними вакансіями домішково-вакансійні диполі $(Me^+)^-(V_a)^+$, де $(Me^+)^-$ – іон лужного металу, а $(V_a)^+$ – вакансія іона фтору. Домішково-вакансійні диполі (ДВД) є ефективними пастками для носіїв електричного заряду. При опроміненні кристалів іонізуючою радіацією внаслідок локалізації електронів і дірок на ДВД у ґратці кристала генеруються ($F_A(1)$-V_K) та ($F_A(1)$-V_{KA})-комплементарні пари:

$$\left(Me^+\right)^-\left(V_a\right)^+ \xrightarrow{R(e^-,e^+)} \begin{matrix}\left(F_A - V_K\right) & (1.1)\\ \left(F_A - V_{KA}\right) & (1.2)\end{matrix}$$

У роботах **[**6-8**]** розроблено методику, яка дає змогу перетворити термічно рівноважні дефекти дипольного типу в термічно нерівноважні електрично заряджені дефекти – в (Me^+-$V_a^+Me^+V_a^+$)$^+$-пари дефектів. Показано **[**6-8**]**, що при опроміненні кристалів з термічно нерівноважними структурними дефектами у ґратці кристала генеруються ($F_A(1)$-V_K) і ($F_A(1)$-V_{KA})-комплементарні пари центрів забарвлення:

$$\left(V_a\right)^+\left(Me^+\right)^-\left(V_a\right)^+ \xrightarrow{R(e^-,e^+)} \begin{matrix}\left(F_A(1) - V_K\right) & (2.1)\\ \left(F_A(1) - V_{KA}\right) & (2.2)\end{matrix}$$

Мета цієї роботи – дослідити ефективність виходу реакцій (2.1) та (2.2).