Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
https://doi.org/10.36930/40350519
Article received 13.09.2025
Article accepted 31.10.2025
UDC 004.[021+023+67+9]:519.6
Correspondence author: P. Yu. Grytsiuk pavlo.y.hrytsiuk@lpnu.ua
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

П. Ю. Грицюк, Ю. І. Грицюк
Національний університет "Львівська політехніка", м. Львів, Україна

ОСОБЛИВОСТІ ШИФРУВАННЯ БЛОКОВИХ ДАНИХ ДВОВАРІАНТНИМИ ПОЛІНОМІАЛЬНИМИ МАТРИЦЯМИ ФІБОНАЧЧІ

Показана можливість вирішення проблеми генерування ключів для шифрування блокових даних у вигляді n-ої послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких є двоваріантні поліноми Фібоначчі не більше (n–1)-го степеня. Отримані матриці Фібоначчі дають змогу знаходити як їхні визначники, так і обернені матриці, придатні для матричного шифрування блокових даних. З'ясовано, що навіть за останнє десятиліття надруковано значну кількість публікацій, в кожній з яких обґрунтовано різні підходи як до генерування послідовностей двоваріантних поліноміальних матриць Фібоначчі, так і доведено доцільність їх використання для шифрування блокових даних. Виявлено, що застосування таких матриць як окремої процедури для захисту блокових даних у теорії та практиці криптографії трапляється вкрай рідко. Розроблено метод генерування послідовності двоваріантних поліноміальних матриць Фібоначчі, який полягає у використанні рекурентного матричного співвідношення, згідно з яким наступну поліноміальну матрицю утворюють шляхом множення змінних x та y послідовно на елементи поточної попередньої матриць відповідно, поелементного додавання утворених матриць та групування схожих доданків у елементах наступної матриці. Наведено механізми утворення послідовності з n=6-ти двоваріантних поліноміальних матриць Фібоначчі від 2-го до 4-го порядків, елементами яких стали двоваріантні поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня, що дало змогу проаналізувати не тільки особливості їхньої побудови, але й усвідомити процедури знаходження їх визначників і обернених матриць. Розроблено ПЗ, яке дає змогу генерувати як послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, так і знаходити їхні визначники та обернені поліноміальні матриці аналогічного порядку. Наведено приклад застосування матричного методу шифрування блокових даних двоваріантною поліноміальною матрицею Фібоначчі, що дає змогу зацікавленому читачу зрозуміти основний принцип шифрування як початкового повідомлення, так і розшифрування зашифрованого повідомлення.

Ключові слова: двоваріантні поліноми Фібоначчі; рекурентне матричне співвідношення; механізм утворення послідовності поліноміальних матриць; обернена поліноміальна матриця Фібоначчі; зашифроване повідомлення; матричний метод шифрування блокових даних.

Вступ / Introduction

Різні дослідження особливостей генерування послідовності поліномів Фібоначчі, а також поліноміальних матриць Фібоначі, елементами яких якраз і є поліноми Фібоначчі, за останні декілька десятиліть хоча й трапляються часто у відкритому друці, позаяк тісно пов'язані між собою [2], однак вони значно менше досліджені через складність процедури їхнього генерування. З розвитком комп'ютерної техніки поліноміальні матриці Фібоначі почали застосовувати в різних областях знань [12], в тому числі й для шифрування блокових даних насамперед матричним методом [20].

Багато науковців у своїх роботах [5, 10, 12, 13, 24, 26, 31] навели результати дослідження властивостей поліномів Фібоначчі та Лукаса і похідних від них. Автори вважають, що такі поліноми є природним розширенням їхніх відповідних послідовностей чисел, тому їм притаманні багато безпосередніх їхніх властивостей. Також вони наводять похідні від цих поліномів у формі відповідних узагальнень, що дало їм змогу сформувати сімейство поліноміальних послідовностей, в тому числі й узагальнених, частковим випадком яких є двоваріантні послідовності поліномів. Ними також наведено багато співвідношень для похідних послідовностей поліномів Фібоначчі та Лукаса [14]. Оскільки такі послідовності поліномів почали часто використовувати в багатьох галузях знань, то авторами наведено відповідні приклади їх застосовування у фізиці високих матерій, криптографії та для шифрування даних [3, 12].

Водночас, чимала кількість досліджень [8, 9, 25, 29, 32, 37] стосується різних підходів до генерування послідовності двоваріантних поліноміальних матриць Фібоначчі, а також їх використання для шифрування блокових даних. Однак, як окрема процедура шифрування блокових даних у практиці їх захисту та передачі каналами зв'язку трапляється вкрай рідко, переважно як складова дещо складнішого алгоритму. Тому виникає потреба проведення додаткових досліджень щодо вико-

Інформація про авторів:
Грицюк Павло Юрійович, магістр, аспірант, кафедра автоматизованих систем управління. **Email:** pavlo.y.hrytsiuk@lpnu.ua; https://orcid.org/0009-0003-5409-2043
Грицюк Юрій Іванович, д-р техн. наук, професор, кафедра програмного забезпечення. **Email:** yurii.i.hrytsiuk@lpnu.ua; https://orcid.org/0000-0001-8183-3466

Цитування за ДСТУ: Грицюк П. Ю., Грицюк Ю. І. Особливості шифрування блокових даних двоваріантними поліноміальними матрицями Фібоначчі. Науковий вісник НЛТУ України. 2025, т. 35, № 5. С. 168–178.
Citation APA: Grytsiuk, P. Yu., & Hrytsiuk, Yu. I. (2025). Features of block data encryption using bivariate Fibonacci polynomial matrices. *Scientific Bulletin of UNFU*, 35(5), 168–178. https://doi.org/10.36930/40350519

ристання наявних і розроблення більш ефективних методів генерування як послідовності двоваріантних поліномів Фібоначчі, так і поліноміальних матриць Фібоначчі, а також встановлення певних особливості їх використання тільки як локального методу для шифрування блокових даних.

Об'єкт дослідження – шифрування блокових даних двоваріантними поліноміальними матрицями Фібоначчі.

Предмет дослідження – методи і засоби шифрування блокових даних двоваріантними поліноміальними матрицями Фібоначчі m-го порядку, матричні операції якого здійснюють за допомогою матричного множення, що призводить до високої продуктивності.

Мета роботи – розробити метод генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких будуть двоваріантні поліноми Фібоначчі не більше (n–1)-го степеня, який дасть можливість знаходити як їхні визначники, так і обернені поліноміальні матриці, які сукупно можна було б застосовувати у матричному методі шифрування блокових даних.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- проаналізувати останні дослідження та публікації, а також з'ясувати складність проблеми генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, які стануть основою для шифрування блокових даних, що дасть змогу здійснювати ефективний їх захист;
- розробити метод генерування n-ої послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких будуть двоваріантні поліноми Фібоначчі не більше (n–1)-го степеня, який дасть можливість знаходити не тільки їхні визначники, але й обернені поліноміальні матриці, які можна застосувати у матричному методі шифрування блокових даних;
- навести механізми утворення послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких будуть двоваріантні поліноми Фібоначчі не більше (n–1)-го степеня ($\forall n \in \{3 \div 6\}$), що дасть змогу проаналізувати не тільки особливості їхньої побудови загалом, але й усвідомити процедури знаходження їх визначників і обернених поліноміальних матриць зокрема;
- навести конкретний приклад застосування матричного методу шифрування блокових даних двоваріантною поліноміальною матрицею Фібоначчі, що дасть змогу зацікавленому читачу зрозуміти основний принцип шифрування як початкового повідомлення, так і розшифрування зашифрованого повідомлення.

Аналіз останніх досліджень та публікацій. Послідовності чисел і матриць Фібоначчі є основою математичного забезпечення процедури шифрування даних [17]. Водночас, різні послідовності поліномів Фібоначчі та поліноміальних матриць Фібоначчі хоча й трапляються інколи в науковій літературі, позаяк тісно пов'язані між собою, однак вони значно менше досліджені. З розвитком комп'ютерної техніки як одно-, так і двоваріантні поліноми та поліноміальні матриці Фібоначчі почали застосовувати для шифрування даних матричним методом [19].

Наприклад, у роботі [11] наведено поліноміальні матриці Фібоначчі–Гессенберга з визначником у вигляді полінома Фібоначчі. Авторами введено поняття двовимірного масиву поліномів Фібоначчі та наведено три класи поліноміальних матриць Фібоначчі–Гессенберга, що задовольняють їхнім властивостям.

У роботі [30] розглянуто узагальнені поліноми Фібоначчі та деякі їхні фундаментальні властивості. Автори вважають, що різні послідовності поліномів під назвами поліномів Фібоначчі та Лукаса трапляються в науковій літературі протягом століття. Узагальнення полінома Фібоначчі зроблено з використанням різних підходів, де зазвичай узагальнення здійснюється шляхом зміни початкових умов. У своєму дослідженні вони вивчають так звані узагальнені поліноми Фібоначчі з будь-яким цілим числом. Далі вони наводять деякі фундаментальні властивості узагальнених поліномів Фібоначчі.

У роботі [6] проаналізовано так звані відстані між елементами узагальнених поліномів Фібоначчі, наведено пряму формулу, твірну функцію та матричні генератори для утворення цих поліномів. Автори також навели графову інтерпретацію цих поліномів, їх зв'язки з трикутником Паскаля та довели деякі тотожності для них.

У роботі [23] наведено відомості про узагальнені $h(x)$-поліноми Фібоначчі та Лукаса, утворені функцією $h(x)$, яка може бути поліномом як з цілими, так і з дійсними коефіцієнтами. Вони наводять $h(x)$-поліноми Фібоначчі, які узагальнюють як поліноми Фібоначчі-Каталона, так і поліноми Фібоначчі-Берда, а також вказують на їхні відповідні властивості. Автори також наводять $h(x)$-поліноми Лукаса, які узагальнюють поліноми Лукаса та вказують на їхні відповідні властивості. Окрім цього, автори навели $Q_h(x)$-матрицю Фібоначчі, елементами якої є поліноми Фібоначчі n-го степеня, що узагальнює Q-матрицю Фібоначчі, породжену відповідними числами.

У роботі [28] наведено інформацію про згорнуті узагальнені поліноми Фібоначчі та Лукаса. Автори визначають згорнуті $h(x)$-поліноми Фібоначчі як розширення класичних чисел Фібоначчі. Також вони наводять декілька комбінаторних формул, що містять $h(x)$-поліноми Фібоначчі та Лукаса. Окрім цього, автори отримали згорнуті $h(x)$-поліноми Фібоначчі з сімейства матриць Гессенберга (англ. *Hessenberg*) та довели їхні відповідні властивості.

У роботі [7] наведено узагальнений поліном Фібоначчі та доведено його властивості. Автори вважають, що поліноми Фібоначчі та Лукаса відомі тим, що володіють чудовими й дивовижними властивостями та відповідними тотожностями. Окрім цього, дослідники визначають деякі рекурентні співвідношення та наводять їх для генерування узагальнених поліномів Фібоначчі.

У роботі [33] наведено інформацію про деякі властивості узагальнених поліномів Фібоначчі та Лукаса, отримані шляхом використання матриць та розкладання Лапласа. Дослідники наводять нові сімейства тридіагональних матриць, послідовні детермінанти яких породжують будь-яку підпослідовність цих поліномів.

У роботі [22] наведено деякі властивості (p,q)-поліномів Фібоначчі та Лукаса. Автори вважають, що масиви Ріордана (англ. *Riordan*) корисні для отримання комбінаторних сум за допомогою генерувальних функцій. Вони стверджують, що багато теорем можна легко довести за допомогою масивів Ріордана. Автори розглядають матрицю Паскаля (англ. *Pascal*) та визначають нове узагальнення поліномів Фібоначчі, які називають (p,q)-поліномами Фібоначчі. За допомогою методу Ріордана вони отримують комбінаторні тотожності, а також здійснюють факторизацію матриці Паскаля, що містить (p,q)-поліноми Фібоначчі.

У роботі [4] запропоновано нову теорію шифрування даних з використанням узагальнених n-крокових поліномів Фібоначчі, на підставі яких визначено новий клас квадратної $M_{h,n}(x)$-матриці n-го порядку ($x \geq 1$) та отримано певні співвідношення між елементами цієї матриці. Проаналізовано достовірність застосування цього методу, де показано, що для $n = 2$ його коригувальна здатність становить 93,33 %, тоді як для $n = 3$ вже становить 99,80 %. Цікавою особливістю розробленого методу шифрування даних є те, що його достовірність не залежить від коефіцієнтів полінома Фібоначчі, за винятком коефіцієнта $h_n(x) = 1$, і зростає зі збільшенням порядку квадратної $M_{h,n}(x)$-матриці.

У роботі [9] наведено деякі формули для утворення двоваріантних поліномів Фібоначчі та Лукаса, а також відповідний набір тотожностей, використовуючи для їхнього виведення матричний підхід. Також сформульовано властивості таких двоваріантних поліномів, де змінні x та y є їхніми складовими, за допомогою яких можна отримати безліч комбінаторних тотожностей.

У роботі [25] наведено узагальнені двоваріантні поліноми, подібні до поліномів Фібоначчі. Автори ввели узагальнену двоваріантну послідовність поліномів типу Фібоначчі, з якої, задаючи початкові умови, отримують двоваріантні поліноми Фібоначчі та Лукаса. Також вони визначили деякі властивості узагальнених двоваріантних поліномів Фібоначчі. У роботі [32] наведено двоваріантні p-поліноми Фібоначчі та Лукаса ($p \geq 0$ є цілим числом), з яких, вказуючи x, y та p, отримують двоваріантні p-поліноми Пелла та Пелля–Лукаса, двоваріантні p-поліноми Якобсталя та Якобсталя-Лукаса, а також двоваріантні поліноми Чебишева першого та другого роду. Після цього вони отримали деякі властивості двоваріантних p-поліномів Фібоначчі та Лукаса.

Отже, за результатами проведеного аналізу останніх досліджень та публікацій стосовно наявних підходів до генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, а також особливостей їх використання для шифрування блокових даних було встановлено, що навіть за останнє десятиліття виконано багато різноманітних досліджень, в кожному з яких тією чи іншою мірою обґрунтовано різні підходи до генерування послідовностей таких поліноміальних матриць, а також доведено доцільність їх використання для шифрування даних. Водночас, застосування двоваріантних поліноміальних матриць Фібоначчі як окремої процедури для захисту відповідно блокових даних у теорії та практиці криптографії трапляється вкрай рідко. Тому проведення додаткового дослідження щодо розроблення ефективного методу генерування n-ої послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких будуть двоваріантні поліноми Фібоначчі не більше (n–1)-го степеня, а також встановлення певних особливості їхнього використання для шифрування блокових даних тільки як локального методу є актуальним завданням, яке й спробуємо частково вирішити в цьому дослідженні.

Результати дослідження та їх обговорення / Research results and their discussion

1. Метод генерування послідовності двоваріантних поліномів Фібоначчі. Для генерування послідовності двоваріантних поліномів Фібоначчі використовують таке рекурентне співвідношення Фібоначчі:

$$\begin{gathered} F^{(n+1)}(x,y) = xF^{(n)}(x,y) + yF^{(n-1)}(x,y), \\ F^{(0)}(x,y) = 0;\ F^{(1)}(x,y) = 1, \end{gathered} \tag{1}$$

де $F^{(n+1)}(x,y)$, $F^{(n)}(x,y)$ і $F^{(n-1)}(x,y)$ – відповідно наступний, поточний та попередній вигляд двоваріантного полінома Фібоначчі. Припускаємо, що $x \neq 0$, $y \neq 0$, $x^2 + 4y \neq 0$. Для $F^{(0)}(x,y) = 0$ та $F^{(1)}(x,y) = 1$ наступний двоваріантний поліном Фібоначчі матиме вигляд $F^{(2)}(x,y) = x \cdot F^{(1)}(x,y) + y \cdot F^{(0)}(x,y) = x \cdot 1 + y \cdot 0 = x$.

Перші декілька двоваріантних поліномів Фібоначчі мають такий вигляд:

$$\begin{aligned} &F^{(0)}(x,y) = 0;\ F^{(1)}(x,y) = 1; \\ &F^{(2)}(x,y) = x; \\ &F^{(3)}(x,y) = x^2 + y; \\ &F^{(4)}(x,y) = x^3 + 2xy; \\ &F^{(5)}(x,y) = x^4 + 3x^2y + y^2; \\ &F^{(6)}(x,y) = x^5 + 4x^3y + 3xy^2; \\ &F^{(7)}(x,y) = x^6 + 5x^4y + 6x^2y^2 + y^3; \\ &F^{(8)}(x,y) = x^7 + 6x^5y + 10x^3y^2 + 4xy^3; \\ &F^{(9)}(x,y) = x^8 + 7x^6y + 15x^4y^2 + 10x^2y^3 + y^4; \\ &F^{(10)}(x,y) = x^9 + 8x^7y + 21x^5y^2 + 20x^3y^3 + 5xy^4. \end{aligned} \tag{2}$$

Метод генерування послідовності двоваріантних поліномів Фібоначчі полягає у використанні рекурентного співвідношення (1), згідно з яким наступний поліном утворюють шляхом множення змінної x на елементи поточного полінома, змінної y на елементи попереднього полінома, після чого групують схожі доданки. Наприклад, за вхідних двоваріантних поліномів $F_6(x,y) = x^5 + 4x^3y + 3xy^2$ і $F_7(x,y) = x^6 + 5x^4y + 6x^2y^2 + y^3$ наступний поліном матиме такий вигляд:

$$\begin{gathered} F_8(x,y) = xF_7(x,y) + yF_6(x,y) = x(x^6 + 5x^4y + 6x^2y^2 + y^3) + \\ y(x^5 + 4x^3y + 3xy^2) = x^7 + 5x^5y + 6x^3y^2 + xy^3 + x^5y + 4x^3y^2 + \\ + 3xy^3 = x^7 + 6x^5y + 10x^3y^2 + 4xy^3. \end{gathered}$$

Отже, послідовності двоваріантних поліномів Фібоначчі є природним розширенням відповідних послідовностей одноваріантних поліномів Фібоначчі [13, 24, 36], тому багато їхніх властивостей допускають пряме доведення.

2. Метод генерування послідовності двоваріантних поліноміальних матриць Фібоначчі. З роботи [34] відомо, що двоваріантна поліноміальна матриця Фібоначчі 2-го порядку має такий вигляд

$$\bar{\bar{B}}_2^{(n)}(x,y) = \begin{bmatrix} F^{(n+1)}(x,y) & F^{(n)}(x,y) \\ F^{(n)}(x,y) & F^{(n-1)}(x,y) \end{bmatrix} \text{ для } \forall n \in \mathbb{Z}, \tag{3}$$

а її визначник отримують за тотожністю Кассіні

$$\begin{gathered} \det\left(\bar{\bar{B}}_2^{(n)}(x,y)\right) = \\ = F^{(n+1)}(x,y)F^{(n-1)}(x,y) - F^{(n)}(x,y)F^{(n)}(x,y) = (-1)^n. \end{gathered} \tag{4}$$

З роботи [37] також відомо, що двоваріантні поліноміальні $\bar{\bar{B}}_m^{(n-1)}(x,y)$ та $\bar{\bar{B}}_m^{(n)}(x,y)$-матриці Фібоначчі від 2-го до 5-го порядків матимуть такий вигляд:

$$\bar{\bar{B}}_2^{(1)}(x,y) = \begin{bmatrix} 1 & 0 \\ 0 & 1/y \end{bmatrix};\ \bar{\bar{B}}_2^{(2)}(x,y) = \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix};\ \bar{\bar{B}}_3^{(1)}(x,y) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1/y \end{bmatrix}; \tag{5}$$

$$\bar{\bar{B}}_3^{(2)}(x,y) = \begin{bmatrix} x & 1 & 0 \\ 0 & x & 1 \\ 0 & 1 & 0 \end{bmatrix};\ \bar{\bar{B}}_4^{(1)}(x,y) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1/y \end{bmatrix};\ \bar{\bar{B}}_4^{(2)}(x,y) = \begin{bmatrix} x & 1 & 0 & 0 \\ 0 & x & 1 & 0 \\ 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix};$$

$$\bar{\bar{B}}_5^{(1)}(x,y) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1/y \end{bmatrix};\ \bar{\bar{B}}_5^{(2)}(x,y) = \begin{bmatrix} x & 1 & 0 & 0 & 0 \\ 0 & x & 1 & 0 & 0 \\ 0 & 0 & x & 1 & 0 \\ 0 & 0 & 0 & x & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Для генерування послідовності двоваріантних поліноміальних матриць Фібоначчі використаємо рекурентне співвідношення Фібоначчі (1), яке в нашому випадку матиме такий матричний вигляд:

$$\overline{\overline{B}}_m^{(n+1)}(x,y) = x\overline{\overline{B}}_m^{(n)}(x,y) + y\overline{\overline{B}}_m^{(n-1)}(x,y), \qquad (6)$$

де $\overline{\overline{B}}_m^{(n+1)}(x,y)$, $\overline{\overline{B}}_m^{(n)}(x,y)$ і $\overline{\overline{B}}_m^{(n-1)}(x,y)$ – відповідно наступний, поточний та попередній вигляд двоваріантних поліноміальних $\overline{\overline{B}}_m^{(\cdot)}(x,y)$-матриць Фібоначчі. Для $\overline{\overline{B}}_2^{(1)}(x,y)$, $\overline{\overline{B}}_2^{(2)}(x,y)$ і $\det(\overline{\overline{B}}_2^{(2)}(x,y)) = x\cdot 0 - 1\cdot 1$ наступна поліноміальна матриця Фібоначчі матиме такий вигляд:

$$\begin{aligned}\overline{\overline{B}}_2^{(3)}(x,y) &= x\overline{\overline{B}}_2^{(2)}(x,y) + y\overline{\overline{B}}_2^{(1)}(x,y) = \\ &= x\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix} + y\begin{bmatrix} 1 & 0 \\ 0 & 1/y \end{bmatrix} = \begin{bmatrix} x^2 & x \\ x & 0 \end{bmatrix} + \begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x^2+y & x \\ x & 1 \end{bmatrix}; \qquad (7) \\ \det(\overline{\overline{B}}_2^{(3)}(x,y)) &= (x^2+y)\cdot 1 - x\cdot x = x^2 + y - x\cdot x = y.\end{aligned}$$

Оскільки двоваріантні поліноміальні $\overline{\overline{B}}_m^{(\cdot)}(x,y)$-матриці Фібоначчі часто використовують для реалізації операцій шифрування даних, то аналогічні оберненні матриці також потрібно мати для зворотнього процесу, тобто розшифрування даних. Інтуїтивно зрозуміло, що ці так звані *обернені двоваріантні поліноміальні* $\overline{\overline{B}}_m^{-(\cdot)}(x,y)$ - *матриці Фібоначчі* мають бути оберненими до матриць шифрування даних. Наприклад, якщо для одноваріантної матриці 2-го порядку $\overline{\overline{B}}_2^{(2)}(x,y) = \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}$ її обернена матриця матиме такий вигляд $\overline{\overline{B}}_2^{-(2)}(x,y) = \begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix}$, то для двоваріантної поліноміальної матриці (7) отримаємо таку обернену двоваріантну поліноміальну матрицю

$$\overline{\overline{B}}_2^{-(3)}(x,y) = \frac{1}{y}\begin{bmatrix} 1 & -x \\ -x & x^2+y \end{bmatrix}.$$

Покажемо, що матричний вираз

$$\overline{\overline{B}}_2^{(n)}(x,y) \times \overline{\overline{B}}_2^{-(n)}(x,y) = \overline{\overline{I}}_{2\times 2}$$

можна виконати для будь-якого значення n, наприклад n=3, де $\overline{\overline{I}}_{2\times 2}$ – одинична матриця m=2-го порядку.

$$\overline{\overline{B}}_2^{(3)}(x,y) \times \overline{\overline{B}}_2^{-(3)}(x,y) = \overline{\overline{I}}_{2\times 2} \Rightarrow \begin{bmatrix} x^2+y & x \\ x & 1 \end{bmatrix} \times \frac{1}{y}\begin{bmatrix} 1 & -x \\ -x & x^2+y \end{bmatrix} =$$

$$= \begin{bmatrix} (x^2+y)\cdot\frac{1}{y} + x\cdot\frac{-x}{y} & (x^2+y)\cdot\frac{-x}{y} + x\cdot\frac{x^2+y}{y} \\ x\cdot\frac{1}{y} + 1\cdot\frac{-x}{y} & x\cdot\frac{-x}{y} + 1\cdot\frac{x^2+y}{y} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Нижче буде наведено декілька послідовностей двоваріантних поліноміальних $\overline{\overline{B}}_m^{(n)}(x,y)$-матриць Фібоначчі від 2-го до 4-го порядків, утворені шляхом використання рекурентного матричного співвідношення (6), елементами яких будуть відповідні двоваріантні поліноми Фібоначчі (2).

Використаний метод дає змогу легко генерувати послідовності двоваріантних поліноміальних матриць Фібоначчі різного порядку. Згенеровані матриці можна аналізувати, зокрема, знаходити їхні визначники та обернені матриці. Отримані матриці як ключі застосовують для шифрування та розшифрування блокових даних, що дає можливість ефективно їх захищати. Процес генерування полягає у послідовному застосуванні рекурентного матричного співвідношення (6) до матриць, елементи яких є поліномами, використовуючи спеціальні матричні методи.

2.1. Механізм генерування послідовності двоваріантних поліноміальних матриць Фібоначчі 2-го порядку. Розглянемо механізм генерування послідовності з 6-ти двоваріантних поліноміальних $\overline{\overline{B}}_2^{(n)}(x,y)$-матриць Фібоначчі 2-го порядку, їхніх визначників та відповідно обернених двоваріантних поліноміальних $\overline{\overline{B}}_2^{-(n)}(x,y)$-матриць Фібоначчі. З наведених матричних виразів видно, що елементами n-ої послідовності двоваріантних поліноміальних $\overline{\overline{B}}_2^{(n)}(x,y)$-матриць Фібоначчі є відповідні двоваріантні $F^{(n)}(x,y)$-поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня.

$$\begin{aligned}
&\overline{\overline{B}}_2^{(n+1)}(x,y) = x\overline{\overline{B}}_2^{(n)}(x,y) + y\overline{\overline{B}}_2^{(n-1)}(x,y);\ \det(\overline{\overline{B}}_2^{(n)}(x,y)) = (-1)^{n-1}y^{n-2};\ \overline{\overline{B}}_2^{(n)}(x,y)\times\overline{\overline{B}}_2^{-(n)}(x,y) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \\
&\overline{\overline{B}}_2^{(0)}(x,y) = \begin{bmatrix} 0 & 1/y \\ 1/y & -x/y^2 \end{bmatrix};\ \overline{\overline{B}}_2^{(1)}(x,y) = \begin{bmatrix} 1 & 0 \\ 0 & 1/y \end{bmatrix};\ \overline{\overline{B}}_2^{(2)}(x,y) = \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix};\ \det(\overline{\overline{B}}_2^{(2)}(x,y)) = -1;\ \overline{\overline{B}}_2^{-(2)}(x,y) = \begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix}; \\
&\overline{\overline{B}}_2^{(3)}(x,y) = x\overline{\overline{B}}_2^{(2)}(x,y) + y\overline{\overline{B}}_2^{(1)}(x,y) = \begin{bmatrix} x^2+y & x \\ x & 1 \end{bmatrix} = \begin{bmatrix} F^{(3)}(x,y) & F^{(2)}(x,y) \\ F^{(2)}(x,y) & F^{(1)}(x,y) \end{bmatrix};\ \det(\overline{\overline{B}}_2^{(3)}(x,y)) = y; \\
&\overline{\overline{B}}_2^{-(3)}(x,y) = \frac{1}{y}\begin{bmatrix} 1 & -x \\ -x & x^2+y \end{bmatrix} = \frac{1}{y}\begin{bmatrix} F^{(1)}(x,y) & -F^{(2)}(x,y) \\ -F^{(2)}(x,y) & F^{(3)}(x,y) \end{bmatrix}; \\
&\overline{\overline{B}}_2^{(4)}(x,y) = x\overline{\overline{B}}_2^{(3)}(x,y) + y\overline{\overline{B}}_2^{(2)}(x,y) = \begin{bmatrix} x^3+2xy & x^2+y \\ x^2+y & x \end{bmatrix} = \begin{bmatrix} F^{(4)}(x,y) & F^{(3)}(x,y) \\ F^{(3)}(x,y) & F^{(2)}(x,y) \end{bmatrix};\ \det(\overline{\overline{B}}_2^{(4)}(x,y)) = -y^2; \\
&\overline{\overline{B}}_2^{-(4)}(x,y) = -\frac{1}{y^2}\begin{bmatrix} x & -(x^2+1) \\ -(x^2+1) & x^3+2x \end{bmatrix} = -\frac{1}{y^2}\begin{bmatrix} F^{(2)}(x,y) & -F^{(3)}(x,y) \\ -F^{(3)}(x,y) & F^{(4)}(x,y) \end{bmatrix}; \\
&\overline{\overline{B}}_2^{(5)}(x,y) = x\overline{\overline{B}}_2^{(4)}(x,y) + y\overline{\overline{B}}_2^{(3)}(x,y) = \begin{bmatrix} x^4+3x^2y+y^2 & x^3+2xy \\ x^3+2xy & x^2+y \end{bmatrix} = \begin{bmatrix} F^{(5)}(x,y) & F^{(4)}(x,y) \\ F^{(4)}(x,y) & F^{(3)}(x,y) \end{bmatrix};\ \det(\overline{\overline{B}}_2^{(5)}(x,y)) = y^3; \\
&\overline{\overline{B}}_2^{-(5)}(x,y) = \frac{1}{y^3}\begin{bmatrix} x^2+y & -(x^3+2xy) \\ -(x^3+2xy) & x^4+3x^2y+y^2 \end{bmatrix} = \frac{1}{y^3}\begin{bmatrix} F^{(3)}(x,y) & -F^{(4)}(x,y) \\ -F^{(4)}(x,y) & F^{(5)}(x,y) \end{bmatrix}; \\
&\overline{\overline{B}}_2^{(6)}(x,y) = x\overline{\overline{B}}_2^{(5)}(x,y) + y\overline{\overline{B}}_2^{(4)}(x,y) = \begin{bmatrix} x^5+4x^3y+3xy^2 & x^4+3x^2y+y^2 \\ x^4+3x^2y+y^2 & x^3+2xy \end{bmatrix} = \begin{bmatrix} F^{(6)}(x,y) & F^{(5)}(x,y) \\ F^{(5)}(x,y) & F^{(4)}(x,y) \end{bmatrix}; \\
&\det(\overline{\overline{B}}_2^{(6)}(x,y)) = -y^4;\ \overline{\overline{B}}_2^{-(6)}(x,y) = -\frac{1}{y^4}\begin{bmatrix} x^3+2xy & -(x^4+3x^2y+y^2) \\ -(x^4+3x^2y+y^2) & x^5+4x^3y+3xy^2 \end{bmatrix} = -\frac{1}{y^4}\begin{bmatrix} F^{(4)}(x,y) & -F^{(5)}(x,y) \\ -F^{(5)}(x,y) & F^{(6)}(x,y) \end{bmatrix}.
\end{aligned} \qquad (8)$$

2.2. Механізм генерування послідовності двоваріантних поліноміальних матриць Фібоначчі 3-го порядку. Розглянемо механізм генерування послідовності з 6-ти двоваріантних поліноміальних $\overline{\overline{B}}_3^{(n)}(x,y)$-матриць

Фібоначчі 3-го порядку, їхніх визначників та відповідно обернених двоваріантних поліноміальних $\overline{\overline{B}}_3^{-(n)}(x,y)$ -матриць Фібоначчі. З наведених матричних виразів видно, що елементами n-ої послідовності двоваріантних поліноміальних $\overline{\overline{B}}_3^{(n)}(x,y)$ -матриць Фібоначчі є відповідні двоваріантні $F^{(n)}(x,y)$ -поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня.

$$\overline{\overline{B}}_3^{(n+1)}(x,y)=x\overline{\overline{B}}_3^{(n)}(x,y)+y\overline{\overline{B}}_3^{(n-1)}(x,y);\ \det(\overline{\overline{B}}_3^{(n)}(x,y))=(-1)^{n-1}y^{n-2}F^{(n)}(x,y);\ \overline{\overline{B}}_3^{(n)}(x,y)\times\overline{\overline{B}}_3^{-(n)}(x,y)=\overline{\overline{I}}_3;$$

$$\overline{\overline{B}}_3^{(0)}(x,y)=\begin{bmatrix}0 & 1/y & 0\\ 0 & 0 & 1/y\\ 0 & 1/y & -x/y^2\end{bmatrix};\ \overline{\overline{B}}_3^{(1)}(x,y)=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1/y\end{bmatrix};\ \overline{\overline{B}}_3^{(2)}(x,y)=\begin{bmatrix}x & 1 & 0\\ 0 & x & 1\\ 0 & 1 & 0\end{bmatrix};\ \overline{\overline{B}}_3^{-(2)}(x,y)=\begin{bmatrix}1/x & 0 & -1/x\\ 0 & 0 & 1\\ 0 & 1 & -x\end{bmatrix};$$

$$\det(\overline{\overline{B}}_3^{(2)}(x,y))=-x=-F^{(2)}(x,y);$$

$$\overline{\overline{B}}_3^{(3)}(x,y)=x\overline{\overline{B}}_3^{(2)}(x,y)+y\overline{\overline{B}}_3^{(1)}(x,y)=\begin{bmatrix}x^2+y & x & 0\\ 0 & x^2+y & x\\ 0 & x & 1\end{bmatrix}=\begin{bmatrix}F^{(3)}(x,y) & F^{(2)}(x,y) & 0\\ 0 & F^{(3)}(x,y) & F^{(2)}(x,y)\\ 0 & F^{(2)}(x,y) & F^{(1)}(x,y)\end{bmatrix};$$

$$\det(\overline{\overline{B}}_3^{(3)}(x,y))=x^2y+y^2=y(x^2+y)=yF^{(3)}(x,y);$$

$$\overline{\overline{B}}_3^{-(3)}(x,y)=\begin{bmatrix}\frac{y}{x^2y+y^2} & \frac{-x}{x^2y+y^2} & \frac{x^2}{x^2y+y^2}\\ 0 & \frac{1}{y} & \frac{-x}{y}\\ 0 & \frac{-x}{y} & \frac{x^2+y}{y}\end{bmatrix}=\begin{bmatrix}\frac{y}{\det(\overline{\overline{B}}_3^{(3)}(x,y))} & \frac{-F^{(2)}(x,y)}{\det(\overline{\overline{B}}_3^{(3)}(x,y))} & \frac{x^2}{\det(\overline{\overline{B}}_3^{(3)}(x,y))}\\ 0 & \frac{F^{(1)}(x,y)}{y} & \frac{-F^{(2)}(x,y)}{y}\\ 0 & \frac{-F^{(2)}(x,y)}{y} & \frac{F^{(3)}(x,y)}{y}\end{bmatrix};$$

$$\overline{\overline{B}}_3^{(4)}(x,y)=x\overline{\overline{B}}_3^{(3)}(x,y)+y\overline{\overline{B}}_3^{(2)}(x,y)=\begin{bmatrix}x^3+2xy & x^2+y & 0\\ 0 & x^3+2xy & x^2+y\\ 0 & x^2+y & x\end{bmatrix}=\begin{bmatrix}F^{(4)}(x,y) & F^{(3)}(x,y) & 0\\ 0 & F^{(4)}(x,y) & F^{(3)}(x,y)\\ 0 & F^{(3)}(x,y) & F^{(2)}(x,y)\end{bmatrix};$$

$$\det(\overline{\overline{B}}_3^{(4)}(x,y))=-(x^3y^2+2xy^3)=-y^2(x^3+2xy)=-y^2F^{(4)}(x,y);$$

$$\overline{\overline{B}}_3^{-(4)}(x,y)=\begin{bmatrix}\frac{y^2}{\det(\overline{\overline{B}}_3^{(4)}(x,y))} & \frac{x^3+xy}{\det(\overline{\overline{B}}_3^{(4)}(x,y))} & \frac{-(x^4+2x^2y+y^2)}{\det(\overline{\overline{B}}_3^{(4)}(x,y))}\\ 0 & \frac{-F^{(2)}(x,y)}{y^2} & \frac{F^{(3)}(x,y)}{y^2}\\ 0 & \frac{F^{(3)}(x,y)}{y^2} & \frac{-F^{(4)}(x,y)}{y^2}\end{bmatrix};$$

$$\overline{\overline{B}}_3^{(5)}(x,y)=x\overline{\overline{B}}_3^{(4)}(x,y)+y\overline{\overline{B}}_3^{(3)}(x,y)=\begin{bmatrix}x^4+3x^2y+y^2 & x^3+2xy & 0\\ 0 & x^4+3x^2y+y^2 & x^3+2xy\\ 0 & x^3+2xy & x^2+y\end{bmatrix}=\begin{bmatrix}F^{(5)}(x,y) & F^{(4)}(x,y) & 0\\ 0 & F^{(5)}(x,y) & F^{(4)}(x,y)\\ 0 & F^{(4)}(x,y) & F^{(3)}(x,y)\end{bmatrix};$$

$$\det(\overline{\overline{B}}_3^{(5)}(x,y))=x^4y^3+3x^2y^4+y^5=y^3(x^4+3x^2y+y^2)=y^3F^{(5)}(x,y);$$

$$\overline{\overline{B}}_3^{-(5)}(x,y)=\begin{bmatrix}\frac{y^3}{\det(\overline{\overline{B}}_3^{(5)}(x,y))} & \frac{-b'_{12}}{\det(\overline{\overline{B}}_3^{(5)}(x,y))} & \frac{b'_{13}}{\det(\overline{\overline{B}}_3^{(5)}(x,y))}\\ 0 & \frac{F^{(3)}(x,y)}{y^3} & \frac{-F^{(4)}(x,y)}{y^3}\\ 0 & \frac{-F^{(4)}(x,y)}{y^3} & \frac{F^{(5)}(x,y)}{y^3}\end{bmatrix},\ \begin{matrix}b'_{12}=x^5+3x^3y+2xy^2,\\ b'_{13}=x^6+4x^4y+4x^2y^2;\end{matrix}$$

$$\overline{\overline{B}}_3^{(6)}(x,y)=x\overline{\overline{B}}_3^{(5)}(x,y)+y\overline{\overline{B}}_3^{(4)}(x,y)=\begin{bmatrix}x^5+4x^3y+3xy^2 & x^4+3x^2y+y^2 & 0\\ 0 & x^5+4x^3y+3xy^2 & x^4+3x^2y+y^2\\ 0 & x^4+3x^2y+y^2 & x^3+2xy\end{bmatrix}=\begin{bmatrix}F^{(6)}(x,y) & F^{(5)}(x,y) & 0\\ 0 & F^{(6)}(x,y) & F^{(5)}(x,y)\\ 0 & F^{(5)}(x,y) & F^{(4)}(x,y)\end{bmatrix};$$

$$\det(\overline{\overline{B}}_3^{(6)}(x,y))=-(x^5y^4+4x^3y^5+3xy^6)=-y^4(x^5+4x^3y+3xy^2)=-y^4F^{(6)}(x,y);\qquad(9)$$

$$\overline{\overline{B}}_3^{-(6)}(x,y)=\begin{bmatrix}\frac{y^4}{\det(\overline{\overline{B}}_3^{(6)}(x,y))} & \frac{b'_{12}}{\det(\overline{\overline{B}}_3^{(6)}(x,y))} & \frac{-b'_{13}}{\det(\overline{\overline{B}}_3^{(6)}(x,y))}\\ 0 & \frac{-F^{(4)}(x,y)}{y^4} & \frac{F^{(5)}(x,y)}{y^4}\\ 0 & \frac{F^{(5)}(x,y)}{y^4} & \frac{-F^{(6)}(x,y)}{y^4}\end{bmatrix},\ \begin{matrix}b'_{12}=x^7+5x^5y+7x^3y^2+2xy^3,\\ b'_{13}=x^8+6x^6y+11x^4y^2+6x^2y^3+y^4.\end{matrix}$$

2.3. Механізм генерування послідовності двоваріантних поліноміальних матриць Фібоначчі 4-го порядку. Розглянемо механізм генерування послідовності з 6-ти двоваріантних поліноміальних $\overline{\overline{B}}_4^{(n)}(x,y)$ -матриць Фібоначчі 4-го порядку, їхніх визначників та відповідно обернених двоваріантних поліноміальних $\overline{\overline{B}}_4^{-(n)}(x,y)$ -матриць Фібоначчі. З наведених матричних виразів видно, що елементами n-ої послідовності двоваріантних поліноміальних $\overline{\overline{B}}_4^{(n)}(x,y)$ -матриць Фібоначчі є відповідні двоваріантні $F^{(n)}(x,y)$ -поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня. Тут використано матричну рекурентна формулу (6), що визначає наступні елементи послідовності через попередні, але з урахуванням поліноміального характеру елементів. Це дає змогу створювати матриці m-го порядку.

$$\overline{\overline{B}}_4^{(n+1)}(x,y)=x\overline{\overline{B}}_4^{(n)}(x,y)+y\overline{\overline{B}}_4^{(n-1)}(x,y);\ \det(\overline{\overline{B}}_4^{(n)}(x,y))=(-1)^{n-1}f^{(n)}(x,y);\ \overline{\overline{B}}_4^{(n)}(x,y)\times\overline{\overline{B}}_4^{-(n)}(x,y)=\overline{\overline{I}}_4;$$

$$\overline{\overline{B}}_4^{(0)}(x,y)=\begin{bmatrix}0&1/y&0&0\\0&0&1/y&0\\0&0&0&1/y\\0&0&1/y&-x/y^2\end{bmatrix};\overline{\overline{B}}_4^{(1)}(x,y)=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1/y\end{bmatrix};\ \overline{\overline{B}}_4^{(2)}(x,y)=\begin{bmatrix}x&1&0&0\\0&x&1&0\\0&0&x&1\\0&0&1&0\end{bmatrix};\ \overline{\overline{B}}_4^{-(2)}(x,y)=\begin{bmatrix}1/x&-1/x^2&0&1/x^2\\0&1/x&0&-1/x\\0&0&0&1\\0&0&1&-x\end{bmatrix};$$

$$\det(\overline{\overline{B}}_4^{(2)}(x,y))=-x^2;$$

$$\overline{\overline{B}}_4^{(3)}(x,y)=x\overline{\overline{B}}_4^{(2)}(x,y)+y\overline{\overline{B}}_4^{(1)}(x,y)=\begin{bmatrix}x^2+y&x&0&0\\0&x^2+y&x&0\\0&0&x^2+y&x\\0&0&x&1\end{bmatrix}=\begin{bmatrix}F^{(3)}(x,y)&F^{(2)}(x,y)&0&0\\0&F^{(3)}(x,y)&F^{(2)}(x,y)&0\\0&0&F^{(3)}(x,y)&F^{(2)}(x,y)\\0&0&F^{(2)}(x,y)&F^{(1)}(x,y)\end{bmatrix};$$

$$\overline{\overline{B}}_4^{-(3)}(x,y)=\begin{bmatrix}\frac{yF^{(3)}(x,y)}{\det(\overline{\overline{B}}_4^{(3)}(x,y))}&\frac{-xy}{\det(\overline{\overline{B}}_4^{(3)}(x,y))}&\frac{x^2}{\det(\overline{\overline{B}}_4^{(3)}(x,y))}&\frac{-x^3}{\det(\overline{\overline{B}}_4^{(3)}(x,y))}\\0&\frac{1}{F^{(3)}(x,y)}&\frac{-F^{(2)}(x,y)}{yF^{(3)}(x,y)}&\frac{x^2}{yF^{(3)}(x,y)}\\0&0&\frac{F^{(1)}(x,y)}{y}&\frac{-F^{(2)}(x,y)}{y}\\0&0&\frac{-F^{(2)}(x,y)}{y}&\frac{F^{(3)}(x,y)}{y}\end{bmatrix};\ \det(\overline{\overline{B}}_4^{(3)}(x,y))=x^4y+2x^2y^2+y^3;$$

$$\overline{\overline{B}}_4^{(4)}(x,y)=x\overline{\overline{B}}_4^{(3)}(x,y)+y\overline{\overline{B}}_4^{(2)}(x,y)=\begin{bmatrix}x^3+2xy&x^2+y&0&0\\0&x^3+2xy&x^2+y&0\\0&0&x^3+2xy&x^2+y\\0&0&x^2+y&x\end{bmatrix}=\begin{bmatrix}F^{(4)}(x,y)&F^{(3)}(x,y)&0&0\\0&F^{(4)}(x,y)&F^{(3)}(x,y)&0\\0&0&F^{(4)}(x,y)&F^{(3)}(x,y)\\0&0&F^{(3)}(x,y)&F^{(2)}(x,y)\end{bmatrix};\qquad(10)$$

$$\overline{\overline{B}}_4^{-(4)}(x,y)=\begin{bmatrix}\frac{-y^2F^{(4)}(x,y)}{\det(\overline{\overline{B}}_4^{(4)}(x,y))}&\frac{y^2F^{(3)}(x,y)}{\det(\overline{\overline{B}}_4^{(4)}(x,y))}&\frac{xb'_{13}}{\det(\overline{\overline{B}}_4^{(4)}(x,y))}&\frac{-b'_{14}}{\det(\overline{\overline{B}}_4^{(4)}(x,y))}\\0&\frac{1}{F^{(4)}(x,y)}&\frac{xF^{(3)}(x,y)}{y^2F^{(4)}(x,y)}&\frac{-b'_{24}}{y^2F^{(4)}(x,y)}\\0&0&\frac{-F^{(2)}(x,y)}{y^2}&\frac{F^{(3)}(x,y)}{y^2}\\0&0&\frac{F^{(3)}(x,y)}{y^2}&\frac{-F^{(4)}(x,y)}{y^2}\end{bmatrix},\begin{array}{l}b'_{13}=b'_{24}=x^4+2x^2y+y^2,\\b'_{14}=x^6+3x^4y+3x^2y^2+y^3;\\\det(\overline{\overline{B}}_4^{(4)}(x,y))=-(x^6y^2+4x^4y^3+4x^2y^4);\end{array}$$

$$\overline{\overline{B}}_4^{(5)}(x,y)=x\overline{\overline{B}}_4^{(4)}(x,y)+y\overline{\overline{B}}_4^{(3)}(x,y)=$$

$$=\begin{bmatrix}x^4+3x^2y+y^2&x^3+2xy&0&0\\0&x^4+3x^2y+y^2&x^3+2xy&0\\0&0&x^4+3x^2y+y^2&x^3+2xy\\0&0&x^3+2xy&x^2+y\end{bmatrix}=\begin{bmatrix}F^{(5)}(x,y)&F^{(4)}(x,y)&0&0\\0&F^{(5)}(x,y)&F^{(4)}(x,y)&0\\0&0&F^{(5)}(x,y)&F^{(4)}(x,y)\\0&0&F^{(4)}(x,y)&F^{(3)}(x,y)\end{bmatrix};$$

$$\det(\overline{\overline{B}}_4^{(5)}(x,y))=x^8y^3+6x^6y^4+11x^4y^5+6x^2y^6+y^7;$$

$$\overline{\overline{B}}_4^{-(5)}(x,y)=\begin{bmatrix}\frac{y^3F^{(5)}(x,y)}{\det(\overline{\overline{B}}_4^{(5)}(x,y))}&\frac{-y^3F^{(4)}(x,y)}{\det(\overline{\overline{B}}_4^{(5)}(x,y))}&\frac{b'_{13}}{\det(\overline{\overline{B}}_4^{(5)}(x,y))}&\frac{-b'_{14}}{\det(\overline{\overline{B}}_4^{(5)}(x,y))}\\0&\frac{1}{F^{(5)}(x,y)}&\frac{-b'_{23}}{y^3F^{(5)}(x,y)}&\frac{b'_{24}}{y^3F^{(5)}(x,y)}\\0&0&\frac{F^{(3)}(x,y)}{y^3}&\frac{-F^{(4)}(x,y)}{y^3}\\0&0&\frac{-F^{(4)}(x,y)}{y^3}&\frac{F^{(5)}(x,y)}{y^3}\end{bmatrix},\begin{array}{l}b'_{13}=x^8+5x^6y+8x^4y^2+4x^2y^3,\\b'_{14}=x^9+6x^7y+12x^5y^2+8x^3y^3,\\b'_{23}=x^5+3x^3y+2xy^2;\\b'_{24}=x^6+4x^4y+4x^2y^2;\end{array}$$

$$\overline{\overline{B}}_4^{(6)}(x,y)=x\overline{\overline{B}}_4^{(5)}(x,y)+y\overline{\overline{B}}_4^{(4)}(x,y)=$$

$$=\begin{bmatrix}x^5+4x^3y+3xy^2&x^4+3x^2y+y^2&0&0\\0&x^5+4x^3y+3xy^2&x^4+3x^2y+y^2&0\\0&0&x^5+4x^3y+3xy^2&x^4+3x^2y+y^2\\0&0&x^4+3x^2y+y^2&x^3+2xy\end{bmatrix}=\begin{bmatrix}F^{(6)}(x,y)&F^{(5)}(x,y)&0&0\\0&F^{(6)}(x,y)&F^{(5)}(x,y)&0\\0&0&F^{(6)}(x,y)&F^{(5)}(x,y)\\0&0&F^{(5)}(x,y)&F^{(4)}(x,y)\end{bmatrix};$$

$$\overline{\overline{B}}_4^{-(6)}(x,y)=\begin{bmatrix}\frac{-y^4F^{(6)}(x,y)}{\det(\overline{\overline{B}}_4^{(6)}(x,y))}&\frac{y^4F^{(5)}(x,y)}{\det(\overline{\overline{B}}_4^{(6)}(x,y))}&\frac{xb'_{13}}{\det(\overline{\overline{B}}_4^{(6)}(x,y))}&\frac{-b'_{14}}{\det(\overline{\overline{B}}_4^{(6)}(x,y))}\\0&\frac{1}{F^{(6)}(x,y)}&\frac{xb'_{23}}{y^4F^{(6)}(x,y)}&\frac{-b'_{24}}{y^4F^{(6)}(x,y)}\\0&0&\frac{-F^{(4)}(x,y)}{y^4}&\frac{F^{(5)}(x,y)}{y^4}\\0&0&\frac{F^{(5)}(x,y)}{y^4}&\frac{-F^{(6)}(x,y)}{y^4}\end{bmatrix},\begin{array}{l}\det(\overline{\overline{B}}_4^{(6)}(x,y))=-(x^{10}y^4+8x^8y^5+22x^6y^6+24x^4y^7+9x^2y^8);\\b'_{13}=x^{10}+8x^8y+23x^6y^2+28x^4y^3+13x^2y^4+2y^5,\\b'_{14}=x^{12}+9x^{10}y+30x^8y^2+45x^6y^3+30x^4y^4+9x^2y^5+y^6,\\b'_{23}=x^6+5x^4y+7x^2y^2+2y^3,\\b'_{24}=x^8+6x^6y+11x^4y^2+6x^2y^3+y^4.\end{array}$$

Отже, розроблено метод генерування послідовності з 6-ти двоваріантних поліноміальних матриць Фібоначчі від 2-го до 4-го порядків, елементами яких є двоваріантні поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня ($\forall n \in \{3 \div 6\}$). Оскільки поліноміальні матриці Фібоначчі часто використовують для реалізації операцій шифрування даних, то для розшифрування даних також наведено аналогічні поліноміальні оберненні матриці. Розроблено ПЗ, яке дає змогу генерувати не тільки послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, але й знаходити їхні визначники та обернені поліноміальні матриці аналогічного порядку.

Під час розроблення ПЗ виникли проблеми чисто математичного характеру. Йдеться про те, що під час генерування 5-ої двоваріантної поліноміальної матриці Фібоначчі 2-го порядку отримуємо двоваріантні поліноми 4-го степеня, утворені внаслідок множення змінної x на 4-ту поліноміальну матрицю, змінної y на 3-ту поліноміальну матрицю, подальшого додавання їхніх елементів, та спрощення отриманих виразів. Для їх правильного подання доводиться спочатку перемножувати відповідні поліноми нижчих степенів, потім отриманий результат треба додати і спростити.

Інша проблема, це обчислення визначників матриць, починаючи з 4-го та вищих порядків, де доводиться використовувати спеціальні математичні методи [15], наприклад алгоритм Барейса (англ. *Bareiss algorithm*). Наступна математична проблема, це обчислення оберненої двоваріантної поліноміальної матриці, для вирішення якої також доводиться використовувати відповідні математичні методи [15], такі як метод Монтанте (англ. *Montante method*), метод елімінації Гауса-Джордана (англ. *Gauss-Jordan elimination*) та за допомогою ад'югованої матриці (англ. *Adjugate matrix*). Всі ці методи та алгоритми детально описано в мережі Інтернет, тому в цьому дослідженні не будемо на них зосереджувати увагу. І остання проблема – уважність запису n-ої двоваріантної поліноміальної матриці Фібоначчі m-го порядку, елементами якої є двоваріантні поліноми Фібоначчі не більше (n–1)-го степеня, насамперед тих, які стосуються матриць вищих порядків і поліномів більших степенів.

2.4. Матричний метод шифрування блокових даних поліноміальними двоваріантними матрицями Фібоначчі. Розглянемо особливості реалізації матричного методу шифрування даних поліноміальними двоваріантними матрицями Фібоначчі m-го порядку [12, 21, 24]. Щоб використовувати цей метод, початкове повідомлення потрібно подати у вигляді квадратної $\overline{\overline{M}}$ -матриці m-го порядку, яку називають *матрицею повідомлення*. Немає обмежень щодо подання такого повідомлення [4], тому користувачеві залишається визначати розташування елементів повідомлення у матриці – рядками чи стовпцями.

Наприклад, деяке вхідне повідомлення "*Cryptographickey*" можна подати матрицею 4-го порядку, заповнюючи її поелементно рядками, після чого потрібно вказати їхні числові значення згідно з таблицею кодів символів ASCII:

$$\overline{\overline{M}} = \begin{bmatrix} C & r & y & p \\ t & o & g & r \\ a & p & h & i \\ c & k & e & y \end{bmatrix} \Rightarrow \begin{bmatrix} 67 & 114 & 121 & 112 \\ 116 & 111 & 103 & 114 \\ 97 & 112 & 104 & 105 \\ 99 & 107 & 101 & 121 \end{bmatrix}.$$

Після узгодження між відправником і одержувачем цілого числа $x \neq 0$ та n-ої поліноміальної двоваріантної матриці Фібоначчі m-го порядку, відповідну матрицю шифрування даних вибирають з виразів (8), (9) чи (10), наведених вище. Потім цю матрицю потрібно помножити справа на матрицю повідомлення , щоб отримати матрицю зашифрованого повідомлення $\overline{\overline{E}}$. Наприклад, для $m = 4$, $n = 4$ з матричного виразу (24) маємо:

$$\overline{\overline{B}}_4^{(4)}(x,y) = \begin{bmatrix} F^{(4)}(x,y) & F^{(3)}(x,y) & 0 & 0 \\ 0 & F^{(4)}(x,y) & F^{(3)}(x,y) & 0 \\ 0 & 0 & F^{(4)}(x,y) & F^{(3)}(x,y) \\ 0 & 0 & F^{(3)}(x,y) & F^{(2)}(x,y) \end{bmatrix}.$$

Тепер, підставивши в цю матрицю значення $x = 5$, $y = 7$ і виконавши відповідні обчислення, отримаємо:

$$F^{(2)}(x,y) = x; \qquad F^{(2)}(5,7) = 5;$$
$$F^{(3)}(x,y) = x^2 + y; \quad F^{(3)}(5,7) = 5^2 + 7 = 32;$$
$$F^{(4)}(x,y) = x^3 + 2xy; F^{(4)}(5,7) = 5^3 + 2 \cdot 5 \cdot 7 = 195;$$
$$\overline{\overline{B}}_4^{(4)}(5,7) = \begin{bmatrix} 195 & 32 & 0 & 0 \\ 0 & 195 & 32 & 0 \\ 0 & 0 & 195 & 32 \\ 0 & 0 & 32 & 5 \end{bmatrix};$$
$$\overline{\overline{E}} = \overline{\overline{B}}_4^{(4)}(5,7) \times \overline{\overline{M}} =$$
$$= \begin{bmatrix} 195 & 32 & 0 & 0 \\ 0 & 195 & 32 & 0 \\ 0 & 0 & 195 & 32 \\ 0 & 0 & 32 & 5 \end{bmatrix} \times \begin{bmatrix} 67 & 114 & 121 & 112 \\ 116 & 111 & 103 & 114 \\ 97 & 112 & 104 & 105 \\ 99 & 107 & 101 & 121 \end{bmatrix} =$$
$$= \begin{bmatrix} 16777 & 25782 & 26891 & 25488 \\ 25724 & 25229 & 23413 & 25590 \\ 22083 & 25264 & 23512 & 24347 \\ 3599 & 4119 & 3833 & 3965 \end{bmatrix}.$$

Елементи матриці зашифрованого $\overline{\overline{M}}$ повідомлення $\overline{\overline{E}}$ надсилають каналом зв'язку рядками в порядку e_1, e_2, ..., e_{16}, за якими слідує окремо значення її визначника

$$\det(\overline{\overline{B}}_4^{(4)}(x,y)) = -(x^6y^2 + 4x^4y^3 + 4x^2y^4);$$
$$\det(\overline{\overline{B}}_4^{(4)}(x,y)) = -(5^6 \cdot 7^2 + 4 \cdot 5^4 \cdot 7^3 + 4 \cdot 5^2 \cdot 7^4) = -1863225.$$

Припускаючи, що передана послідовність чисел отримана без помилок, тоді, шляхом множення оберненої $\overline{\overline{B}}_4^{-(4)}(x,y)$ -матриці Фібоначчі, взятої з матричного виразу (24), на матрицю зашифрованого повідомлення $\overline{\overline{E}}$, наведену вище, отримують початкову матрицю повідомлення, а саме:

$$\overline{\overline{B}}_4^{-(4)}(x,y) =$$
$$= \begin{bmatrix} \dfrac{-y^2F^{(4)}(x,y)}{\det(\overline{\overline{B}}_4^{(4)}(x,y))} & \dfrac{y^2F^{(3)}(x,y)}{\det(\overline{\overline{B}}_4^{(4)}(x,y))} & \dfrac{xb'_{13}}{\det(\overline{\overline{B}}_4^{(4)}(x,y))} & \dfrac{-b'_{14}}{\det(\overline{\overline{B}}_4^{(4)}(x,y))} \\ 0 & \dfrac{1}{F^{(4)}(x,y)} & \dfrac{xF^{(3)}(x,y)}{y^2F^{(4)}(x,y)} & \dfrac{-b'_{24}}{y^2F^{(4)}(x,y)} \\ 0 & 0 & \dfrac{-F^{(2)}(x,y)}{y^2} & \dfrac{F^{(3)}(x,y)}{y^2} \\ 0 & 0 & \dfrac{F^{(3)}(x,y)}{y^2} & \dfrac{-F^{(4)}(x,y)}{y^2} \end{bmatrix},$$

$b'_{13} = b'_{24} = x^4 + 2x^2y + y^2$, $b'_{14} = x^6 + 3x^4y + 3x^2y^2 + y^3$;
$b'_{13} = b'_{24} = x^4 + 2x^2y + y^2 = 5^4 + 2 \cdot 5^2 \cdot 7 + 7^2 = 1024$,
$b'_{14} = x^6 + 3x^4y + 3x^2y^2 + y^3 = 5^6 + 3 \cdot 5^4 \cdot 7 + 3 \cdot 5^2 \cdot 7^2 + 7^3 = 32768$;

$$\overline{\overline{B}}_4^{-(4)}(x,y) = \begin{bmatrix} 0,0005128 & -0,000842 & -0,002748 & 0,017587 \\ 0 & 0,005128 & 0,016745 & -0,107169 \\ 0 & 0 & -0,1020408 & 0,6530612 \\ 0 & 0 & 0,6530612 & -3,9795918 \end{bmatrix};$$

$$\overline{\overline{M}} = \overline{\overline{B}}_4^{-(4)}(5,7) \times \overline{\overline{E}} =$$

$$= \begin{bmatrix} 0,0005128 & -0,000842 & -0,002748 & 0,017587 \\ 0 & 0,005128 & 0,016745 & -0,107169 \\ 0 & 0 & -0,1020408 & 0,6530612 \\ 0 & 0 & 0,6530612 & -3,9795918 \end{bmatrix} \times$$

$$\times \begin{bmatrix} 16777 & 25782 & 26891 & 25488 \\ 25724 & 25229 & 23413 & 25590 \\ 22083 & 25264 & 23512 & 24347 \\ 3599 & 4119 & 3833 & 3965 \end{bmatrix} = \begin{bmatrix} 67 & 114 & 121 & 112 \\ 116 & 111 & 103 & 114 \\ 97 & 112 & 104 & 105 \\ 99 & 107 & 101 & 121 \end{bmatrix}.$$

З огляду на викладене вище, констатуємо факт наведення матричного методу шифрування блокових даних на підставі двоваріантної поліноміальної матриці Фібоначчі, в якому для матриці вхідного повідомлення над алфавітом {0, 1,..., 255} і для цілих чисеа $x = 5$ і $y = 7$ використано $\overline{\overline{B}}_4^{(4)}(x, y)$ -матрицю Фібоначчі 4-го порядку, елементами якої є поліноми Фібоначчі від 1-го до 3-го степеня. Для отримання визначника матриці використано формулу Лейбніца, а для знаходження оберненої матриці застосовано метод Монтанте (англ. *Montante method*).

Отже, показана можливість вирішення проблеми генерування *n*-ої послідовності двоваріантних поліноміальних матриць Фібоначчі *m*-го порядку, які є основою для шифрування блокових даних, що дає можливість здійснювати ефективний їх захист. Розроблено метод генерування *n*-ої послідовності двоваріантних поліноміальних матриць Фібоначчі *m*-го порядку, елементами яких є двоваріантні поліноми Фібоначчі від (*n*–1)-го до (*n*–3)-го степеня, який, на відміну від відомих методів, використовує рекурентне матричне співвідношення, а за отриманими матрицями можна знаходити як їхні визначники, так і обернені поліноміальні матриці відповідного порядку. На конкретному прикладі показана особливість застосування матричного методу шифрування блокових даних з використанням 4-ої послідовності двоваріантної поліноміальної матриці Фібоначчі 4-го порядку.

Обговорення результатів дослідження. У математиці поліноми Фібоначчі – це поліноміальна послідовність, яку розглядають як узагальнення чисел Фібоначчі [12]. Водночас, різні послідовності поліномів під загальною назвою поліноми Фібоначчі трапляються в науковій літературі хоча і давно, позаяк тісно пов'язані між собою, проте вони не так широко досліджені, як відповідні послідовності чисел Фібоначчі. Зазначені одно- та двоваріантні поліноми Фібоначчі, а також матриці Фібоначчі, елементами яких є двоваріантні поліноми Фібоначчі з'являються в різних областях застосування, насамперед для шифрування блокових даних матричним методом.

У роботі [37] наведено деякі нові результати утворення узагальнених двоваріантних поліномів Фібоначчі та Лукаса, а також відповідні нові тотожності, отримані за допомогою цих поліномів. Для таких поліномів досліджено декілька біноміальних підсумків і наведено відповідні формули для отримання як коефіцієнтів поліномів, так і суми їхніх степенів. Також наведено загальні формули для отримання відповідних підсумків, різних твірних функцій та співвідношень між цими поліномами.

У роботі [38] розглянуто спеціальні перетворення узагальнених двоваріантних поліномів Фібоначчі та Лукаса. Результати дослідження стосуються біноміальних перетворень Каталана та Ганкеля щодо таких поліномів. Також наведено деякі корисні результати, такі як генерувальні функції, формули Біне, підсумовування результатів перетворень, визначених за допомогою рекурентних співвідношень для цих поліномів. Окрім цього, деякі важливі співвідношення між цими перетвореннями виведено за допомогою нових формул, отриманих авторами, а також виведено відповідні формули Каталана, Кассіні, Вайди та д'Оканя для цих перетворень.

У роботі [29] розглянуто повні однорідні симетричні функції для поліномів Гаусса-Фібоначчі та двоваріантних поліномів Пелла. Автори ввели симетричну функцію, щоб отримати нові функції, що утворюють двоваріантні поліноми Пелла-Лукаса. Вони визначили повні однорідні симетричні функції та надали генерувальні функції для поліномів Гаусса-Фібоначчі [1], поліномів Гаусса-Лукаса, двоваріантних поліномів Фібоначчі, Лукаса, Якобсталя та Якобсталя-Лукаса.

У роботі [8] розглянуто генерувальні функції для модифікованих чисел Пелла та двоваріантних комплексних поліномів Фібоначчі. Автори ввели поняття оператор, щоб отримати нові функції, що утворюють модифіковані *k*-числа Пелла, а такожмодифіковані числа Пелла за Гауссом. Використовуючи визначений ними оператор, вони надали деякі нові генерувальні функції для двоваріантних комплексних поліномів Фібоначчі та Лукаса, модифікованих поліномів Пелла та Пелла за Гауссом.

У роботі [27] розглянуто особливості реалізації криптографічних перетворень з використанням узагальнених матриць Фібоначчі з Афінним шифром Хілла. Автори запропонували криптографію з відкритим ключем із використанням Афінного шифру Хілла та узагальненої матриці Фібоначчі, яку ще називають матрицею мультиначчі (англ. *Multinacci Matrix*). Також запропоновано схему встановлення ключа (обміну матрицею ключів $K = Q_\lambda^k$ порядку λ×λ для шифрування-дешифрування) за допомогою послідовностей матриць мультиначчі під простим модулем. У цій схемі замість обміну матрицею ключів потрібно обмінятися тільки парою чисел (λ, *k*), що зменшує часову складність передачі даних, а також складність простору обміну ключами та забезпечує великий простір їхнього генерування.

У роботі [35] розглянуто алгоритми симетричного шифрування даних у поліноміальній системі числення залишків. Автори вперше розробили теоретичні положення щодо реалізації симетричних криптографічних алгоритмів на підставі поліноміальної системи числення залишків RNS (англ. *Residue Numeral System*). Основною особливістю запропонованого підходу є те, що при відновленні полінома за методом невизначених коефіцієнтів (англ. *Method of Undetermined Coefficients*) операцію множення виконують не на знайдених базисних числах, а на довільно вибраних поліномах. такі поліноми разом із попарно взаємно простими залишками системи класів залишків (англ. *Residue Class System*) слугують ключами криптографічного алгоритму. Наведено схеми та приклади реалізації розробленого поліноміального симетричного алгоритму шифрування даних. Побудовано аналітичні вирази для оцінювання криптографічної стійкості алгоритму та наведено їх графічну залежність від кількості модулів і степенів полінома. Результати дослідження показують, що криптоаналіз запропонованого алгоритму має комбінаторну складність, що призводить до вирішення NP-повної задачі.

Проаналізовані вище роботи стосовно наявних підходів до генерування послідовності двоваріантних полі-

номіальних матриць Фібоначчі, а також можливості їхнього використання для шифрування блокових даних вказали на те, що навіть за останнє десятиліття виконано багато різноманітних досліджень, в кожному з яких тією чи іншою мірою обґрунтовано різні підходи до їхнього генерування. Проте дослідниками не наведено приклади їхнього конкретного вигляду, однак доведено доцільність їх використання для шифрування блокових даних. Водночас було з'ясовано, що як окрема процедура захисту блокових даних двоваріантними поліноміальними матрицями Фібоначчі в теорії та практиці криптографії трапляється вкрай рідко. Тому проведене нами дослідження щодо розроблення ефективного методу генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, наведення робочих прикладів їхнього конкретного вигляду, а також встановлення певних особливостей їх використання для шифрування блокових даних тільки як локального методу є частковим вирішенням цієї актуальної проблеми, що й було продемонстровано в цьому дослідженні.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – розроблено метод генерування n-ої послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких є двоваріантні поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня, який використовує рекурентне матричне співвідношення, аналогічне рекурентному співвідношенню для генерування двоваріантних поліномів Фібоначі, а за отриманими матрицями Фібоначчі можна знаходити як їхні визначники, так і обернені матриці відповідного порядку.

Практична значущість результатів дослідження – розроблений метод генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких є двоваріантні поліноми Фібоначчі, а також запропоновані методи знаходження їх визначників і обернених матриць можна застосовувати в матричному методі шифрування блокових даних, що загалом дасть можливість ефективно передавати каналами зв'язку блокові повідомлення різної величини.

Висновок / Conclusions

Розроблено метод генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких є двоваріантні поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня, який дає можливість знаходити як їхні визначники, так і обернені поліноміальні матриці, придатні для матричного методу шифрування блокових даних. За результатами виконаного дослідження можна зробити такі основні висновки.

1. Проаналізовано останні дослідження та публікації, внаслідок чого з'ясовано складність проблеми генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку як крипографічних ключів для шифрування блокових даних, що дасть змогу здійснювати ефективний їх захист. З'ясовано, що навіть за останнє десятиліття надруковано значну кількість публікацій, в кожній з яких обґрунтовано різні підходи як до генерування послідовностей таких поліноміальних матриць Фібоначчі, так і доведено доцільність їх використання для шифрування даних. Водночас, застосування поліноміальних матриць Фібоначчі як окремої процедури для захисту відповідно блокових даних у теорії та практиці криптографії трапляється вкрай рідко.
2. Наведено традиційний метод подання двоваріантних поліномів Фібоначчі, що мають багато корисних властивостей, використано тільки ті із них, які можна застосувати для генерування послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку. Для генерування послідовності поліномів Фібоначчі використовують рекурентне співвідношення, згідно з яким наступний поліном утворюють шляхом множення змінної x послідовно на елементи поточного полінома, змінної y послідовно на елементи попереднього полінома, після чого групують схожі доданки двох поліномів у один наступний поліном.
3. Розроблено метод генерування n-ої послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, елементами яких є двоваріантні поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня, який дає можливість знаходити як їхні визначники, так і обернені матриці, які можна застосувати у матричному методі шифрування блокових даних. Встановлено, що метод генерування послідовності двоваріантних поліноміальних матриць Фібоначчі полягає у використанні рекурентного матричного співвідношення, згідно з яким наступну поліноміальну матрицю утворюють шляхом множення змінної x послідовно на елементи поточної матриці, змінної y послідовно на елементи попередньої матриці, якими є відповідні поліноми Фібоначчі, додавання елементів поточної матриці до елементів попередньої матриці, після чого групують схожі доданки у кожному з елементів наступної матриці.
4. Наведено механізми утворення послідовності з 6-ти двоваріантних поліноміальних матриць Фібоначчі від 2-го до 4-го порядків, елементами яких стали двоваріантні поліноми Фібоначчі від (n–3)-го до (n–1)-го степеня ($\forall n \in \{3 \div 6\}$), що дало змогу проаналізувати не тільки особливості їхньої побудови загалом, але й усвідомити процедури знаходження їх визначників і обернених матриць зокрема. Розроблено ПЗ, яке дає змогу генерувати як послідовності двоваріантних поліноміальних матриць Фібоначчі m-го порядку, так і знаходити їхні визначники та обернені поліноміальні матриці аналогічного порядку.
5. Наведено приклад застосування матричного методу шифрування блокових даних двоваріантною поліноміальною матрицею Фібоначчі, що дає змогу зацікавленому читачу зрозуміти основний принцип шифрування як початкового повідомлення, так і розшифрування зашифрованого повідомлення. У наведеному прикладі для матриці вхідного повідомлення над алфавітом {0, 1,..., 255} і для цілих чисел $x = 5$ та $y = 5$ використано 4-ту поліноміальну матрицю Фібоначчі 4-го порядку, елементами якої є двоваріантні поліноми Фібоначчі від (n–3)-го до (n–3)-го степеня. Для отримання визначника матриці використано формулу Лейбніца, а для знаходження оберненої матриці застосовано метод Монтанте (англ. *Montante method*).
6. За результатами виконаного дослідження зроблено висновки та надано відповідні рекомендації щодо їх практичного використання як основи для шифрування блокових даних, що дає змогу ефективно передавати каналами зв'язку відповідні повідомлення різної величини.

References

1. Asci, M., & Gurel, E. (2017). Some properties of k-order Gaussian Fibonacci and Lucas numbers. *Ars Combinatoria*, 135, 345–356. URI: https://hdl.handle.net/11499/23655
2. Asci, M., & Tasci, D. (2007). On Fibonacci, Lucas and special orthogonal polynomials. *Journal of Computational and Applied Mathematics*. https://doi.org/10.1016/J.CAM.2007.01.026
3. Basu, M., & Prasad, B. (2009). The Generalized relations among the code elements for Fibonacci coding theory. *Chaos, Solitons*

and Fractals, vol. 41, issue 5, 2517–2525. https://doi.org/10.1016/j.chaos.2008.09.030
4. Basu, Manjusri, & Das, Monojit. (2017). Coding theory on generalized Fibonacci n-step polynomials. *Journal of Information and Optimization Sciences*, vol. 38, issue 1, 83–131. https://doi.org/10.1080/02522667.2016.1160618
5. Basu, Manjusri, & Prasad, Bandhu. (2011). Coding theory on the (m,t)-extension of the Fibonacci p-numbers. *Discrete Mathematics, Algorithms and Applications*, vol. 3, 259–267. https://doi.org/10.1142/S1793830911001097
6. Bednar, Urszula, & Wołowiec-Musiał, Małgorzata. (2020). Distance Fibonacci Polynomials. *Symmetry* 2020, 12(9), 1540 p. https://doi.org/10.3390/sym12091540
7. Bhatnagar, Shikha, & Sikhwal, Omprakash. (2016, October). Generalized Fibonacci Polynomials and its Propertie. *SCIREA Journal of Mathematics*, vol. 1, issue 1, 161–174. URL: https://article.scirea.org/pdf/11021.pdf
8. Boughaba, Souhila, Boussayoud, Ali, & Boubellouta, Khadidja. (2019, September). Generating Functions of Modified Pell Numbers and Bivariate Complex Fibonacci Polynomials. *Turkish Journal of Analysis and Number Theory*, 7(4), 113–116. https://doi.org/10.12691/tjant-7-4-3
9. Catalani, M. (2004). Some formulae for Bivariate Fibonacci and Lucas polynomials. Arxiv: math/0406323. *Combinatorics*. https://doi.org/10.48550/arXiv.math/0406323; https://www.semanticscholar.org/paper/Some-formulae-for-bivariate-Fibonacci-and-Lucas-Catalani/2db6f60afd636eee90b01ef6dd2ce6768d844a57
10. Chasnov, Jeffrey R. (2008). Fibonacci numbers and the golden ratio. *The Hong Kong University of Science and Technology*, 87 p. URL: https://www.math.hkust.edu.hk/~machas/fibonacci.pdf
11. Esmaeili, M., & Esmaeili, M. (2009). Polynomial Fibonacci-Hessenberg matrices. *Chaos, Solitons and Fractals*, vol. 41, issue 5, 2820–2827. https://doi.org/10.1016/j.chaos.2008.10.012
12. Esmaili, M., & Esmaeili, M. (2010). A Fibonacci-polynomial based coding method with error detection and correction. *Computers and Mathematics with Applications*, vol. 60, issue 10, 2738–2752. https://doi.org/10.1016/j.camwa.2010.08.091
13. Falcon, S., & Plaza, A. (2009). On *k*-Fibonacci sequences and polynomials and their derivatives. *Chaos, Solitons and Fractals*, vol. 39, issue 3, 1005–1019. https://doi.org/10.1016/j.chaos.2007.03.007
14. Filipponi, P., & Horadam, A. F. (1991). Derivative Sequences of Fibonacci and Lucas Polynomials. In: Bergum, G. E., Philippou, A. N., Horadam, A. F. (Eds). *Applications of Fibonacci Numbers*. *Springer, Dordrecht*, (pp. 99–108). https://doi.org/10.1007/978-94-011-3586-3_12
15. Fox, William P., & West, Richard D. (2024, September). Numerical Methods and Analysis with Mathematical Modelling (Textbooks in Mathematics). *Chapman and Hall/CRC*, 424 p. URL: https://www.amazon.com/Numerical-Mathematical-Modelling-Textbooks-Mathematics/dp/1032697237
16. Grytsiuk, P. Y., & Hrytsiuk, Y. I. (2025). Method for generating a sequence of Fibonacci polynomial matrices and their features for use in block data encryption. *Scientific Bulletin of UNFU*, 35(1), 173–191. https://doi.org/10.36930/40350121
17. Grytsiuk, P. Y., Sikora, L. S., & Hrytsiuk, Y. I. (2023). Problems of detecting and correcting errors in messages encoded by Fibonacci matrices. *Scientific Bulletin of UNFU*, 33(2), 45–58. https://doi.org/10.36930/40330407
18. Grytsiuk, P. Yu., & Hrytsiuk, Yu. I. (2025). Features of block data encryption with refined Fibonacci polynomial matrices. *Scientific Bulletin of UNFU*, 35(3), 200–217. https://doi.org/10.36930/40350322
19. Grytsiuk, Pavlo. (2025). Features of Generation Sequences of Refined Fibonacci Polynomial Matrices. *Information Systems and Networks*, vol. 17, 343–365. https://doi.org/10.23939/sisn2025.17.343
20. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci Qp-matrices – keys for implementing cryptographic transformations. *Bulletin of the National University "Lviv Polytechnic". Series: Computer Science and Information Technology*, vol. 843, 251–263. URL: https://vlp.com.ua/node/16094
21. Hoggat, V. E., Bicknell, Marjorie. (1973). Roots of fibonacci polynomials. *The Fibonacci Quarterly*, vol. 11, issue 3, 271–274. https://doi.org/10.1080/00150517.1973.12430825
22. Lee, G. Y., & Asci, M. (2012). Some Properties of the (p,q)-Fibonacci and (p,q)-Lucas Polynomials. *Journal of Applied Mathematics*, vol. 2012, article ID 264842, 18 p. https://doi.org/10.1155/2012/264842
23. Nalli, A Ayse, & Haukkanen, Pentti. (2009, December). On generalized Fibonacci and Lucas polynomials. *Chaos Solitons & Fractals*, vol. 42, issue 5, 3179–3186. https://doi.org/10.1016/J.CHAOS.2009.04.048
24. Özkan, Engin, Taştan, Merve & Aydoğdu, Ali. (2019). Fibonacci Sayılarının Ailesinde 3-Fibonacci Polinomları. *Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi*. Cilt: 12 Sayı: 2, 926–933. https://doi.org/10.18185/erzifbed.512100
25. Panwar, Yashwant K., & Singh, Mamta. (2017). Generalized Bivariate Fibonacci-Like Polynomials. *International journal of pure mathematics*, vol. 1, 8–13. URL: https://www.academia.edu/125691436/Generalized_Bivariate_Fibonacci_Like_Polynomials
26. Perumali, Sundarayya, & Prasad, M. G. Vara. (2019, October). Coding theory on Pell-Lucas p-numbers. *Journal of Physics Conference Series*, 1344(1), article ID 012017. https://doi.org/10.1088/1742-6596/1344/1/012017
27. Prasad, K., & Mahato, H. (2021). Cryptography using generalized Fibonacci matrices with Affine-Hill cipher. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(8), 2341–2352. Corpus ID 14098285. https://doi.org/10.1080/09720529.2020.1838744
28. Ramirez, J. L. (2013). On convolved generalized Fibonacci and Lucas polynomials. *Applied Mathematics and Computation*, 229, 208–213. https://doi.org/10.1016/j.amc.2013.12.049
29. Saba, Nabiha, & Boussayoud, Ali. (2020, June). Complete homogeneous symmetric functions of Gauss Fibonacci polynomials and Bivariate Pell polynomials. *Open Journal of Mathematical Sciences*, 4(1), 179–185. https://doi.org/10.30538/oms2020.0108
30. Sikhwal, Omprakash, & Vyas, Yashwant. (2016, October). Generalized Fibonacci Polynomials and Some Fundamental Properties. *SCIREA Journal of Mathematics*, vol. 1, issue 1, 16–23. URL: https://article.scirea.org/pdf/11002.pdf
31. Singh, B., Sikhwal, O., & Panwar, Y. K. (2009). Generalized Determinantal Identities Involving Lucas Polynomials. *Applied Mathematical Sciences*, 3(8), 377–388. URL: https://www.researchgate.net/publication/228526069_Generalized_Determinantal_Identities_Involving_Lucas_Polynomials
32. Tuglu, Naim, Kocer, E. Gokcen, & Stakhov, Alexey. (2011, August). Bivariate Fibonacci like *p*-polynomials. *Applied Mathematics and Computation*, vol. 217, issue 24, 10239–10246. https://doi.org/10.1016/j.amc.2011.05.022
33. Uçar, S. (2017). On some properties of generalized Fibonacci and Lucas Polynomials. *An International Journal of Optimization and Control: Theories & Applications* (IJOCTA), 7(2), 216–224. https://doi.org/10.11121/IJOCTA.01.2017.00398
34. Urszula Bednar, & Małgorzata Wołowiec-Musiał. (2020). Distance Fibonacci Polynomials. *Symmetry*, 12(7), article ID 1540. https://doi.org/10.3390/sym12091540
35. Yakymenko, I., Karpinski, M., Shevchuk, R., & Kasianchuk, M. (2024, May). Symmetric Encryption Algorithms in a Polynomial Residue Number System. *Journal of Applied Mathematics*. https://doi.org/10.1155/2024/4894415
36. Yang, Jizhen, & Zhang, Zhizheng. (2018, December). Some identities of the generalized Fibonacci and Lucas sequences. *Applied Mathematics and Computation*, vol. 339, 451–458. https://doi.org/10.1016/j.amc.2018.07.054
37. Yilmaz, N. (2024). Some new results for the generalized Bivariate Fibonacci and Lucas polynomials. *Mathematica Moravica*, vol. 28, issue 1, 97–108. https://doi.org/10.5937/matmor2401097y
38. Yılmaz, N., & Aktaş, İ. (2023). Special transforms of the generalized bivariate Fibonacci and Lucas polynomials. *Hacettepe Journal of Mathematics and Statistics*, 52(3), 640–651. https://doi.org/10.15672/hujms.1110311

P. Yu. Grytsiuk, Yu. I. Hrytsiuk
Lviv Polytechnic National University, Lviv, Ukraine

FEATURES OF BLOCK DATA ENCRYPTION USING BIVARIATE POLYNOMIAL MATRICES OF FIBONACCI

The possibility of solving the problem of generating keys for encrypting block data in the form of *n*th sequence of bivariate polynomial matrices of Fibonacci *m*th order, whose elements are bivariate polynomials of Fibonacci no more than (*n*–1)th degree. The obtained Fibonacci matrices make it possible to find both their determinants and inverse matrices suitable for matrix encryption of block data. A method for generating the *n*th sequence of bivariate polynomial Fibonacci matrices of the *m*th order, whose elements are bivariate Fibonacci polynomials of no more than (*n*-1)th power, is developed, which makes it possible to find both their determinants and inverse matrices suitable for the matrix method of encrypting block data. It has been found that even in the last decade, a significant number of publications have been published, each of which substantiates different approaches to generating sequences of bivariate polynomial Fibonacci matrices and proves the feasibility of their use for encrypting block data. At the same time, the use of polynomial Fibonacci matrices as a separate procedure for block data protection in the theory and practice of cryptography is extremely rare. A method for generating a sequence of bivariate polynomial Fibonacci matrices has been developed, which consists in using a recurrence matrix relation, according to which the next polynomial matrix is formed by multiplying the variables *x* and *y* sequentially by the elements of the current and previous matrices, respectively, elementwise adding the resulting matrices and grouping similar terms in the elements of the next matrix. The mechanisms of forming a sequence of *n*=6 bivariate polynomial Fibonacci matrices of the 2nd to 4th orders, the elements of which are bivariate Fibonacci polynomials of (*n*-3)th to (*n*-1)th powers, are presented, which made it possible to analyse not only the peculiarities of their construction, but also to understand the procedures for finding their determinants and inverse matrices. Software has been developed that allows to generate both sequences of bivariate polynomial Fibonacci matrices of the *m*th order and to find their determinants and inverse polynomial matrices of the same order. An example of the application of the matrix method of encrypting block data with a bivariate polynomial Fibonacci matrix is given, which allows the interested reader to understand the basic principle of encrypting both the initial message and decrypting the encrypted message.

Keywords: bivariate Fibonacci polynomials; recurrent matrix ratio; mechanism of formation of a sequence of polynomial matrices; inverse polynomial Fibonacci matrix; encrypted message; matrix method of encrypting block data.