Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)
https://doi.org/10.36930/40350322
Article received 19.02.2025
Article accepted 11.03.2025
UDC 004.[021+023+67+9]:519.6
Correspondence author: P. Yu. Grytsiuk pavlo.y.hrytsiuk@lpnu.ua

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

ОСОБЛИВОСТІ ШИФРУВАННЯ БЛОКОВИХ ДАНИХ УТОЧНЕНИМИ ПОЛІНОМІАЛЬНИМИ МАТРИЦЯМИ ФІБОНАЧЧІ

Показана можливість вирішення проблеми генерування ключів для шифрування блокових даних у вигляді n-ої послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, елементами яких є поліноми Фібоначчі з номерами від $(n–2)$-го до $(m+n–2)$-го. 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 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. Проаналізовано послідовності поліноміальних матриць Фібоначчі від 2-го до 5-го, згідно з яким виявлено недоліки у традиційному підході до формування структури елементів таких матриць, насамперед кількості (k) різних її елементів, якими є поліноми Фібоначчі не вище $(n–1)$-го степеня. Встановлено, що для матриць Фібоначчі будь-якого порядку (m) таких різних поліномів Фібоначчі буде всього $k = 3$, структура яких залежатиме тільки від номера (n) послідовності поліноміальної матриці Фібоначчі. Така незначна їх кількість є не тільки малоінформативною та прозорою для криптоаналітика, але й не стійкою щодо криптоаналізу. Уточнено структуру елементів поліноміальних матриць Фібоначчі, кількість яких вже залежить від порядку матриці (m) і становить $k = m+1$. Розроблено метод генерування послідовності уточнених поліноміальних матриць Фібоначчі, який полягає у використанні рекурентного матричного співвідношення, згідно з яким наступну поліноміальну матрицю утворюють шляхом множення змінної x послідовно на елементи поточної матриці, здійснюють додавання елементів утвореної матриці до елементів попередньої матриці, після чого в утворених елементах групують усі схожі доданки. Виявлено, що запропонована структура елементів n-ої послідовності поліноміальних матриць Фібоначчі m-го порядку має цікаву властивість, згідно з якою можна уникнути використання рекурентного матричного співвідношення, а генерувати відповідні поліноміальні матриці Фібоначчі тільки за номерами $(m+n–2–j)$-ої послідовності поліномів Фібоначчі, конкретні значення яких залежать від місця їхнього розташування в матриці та номера її стовпця, а саме $\forall j \in [0 \div (m–1)]$. Наведено механізми утворення послідовності з 8-ми поліноміальних уточнених матриць Фібоначчі від 2-го до 5-го порядків, елементами яких стали поліноми Фібоначчі не вище $(m+n–2)$-го степеня, що дало змогу проаналізувати не тільки особливості їхньої побудови, але й усвідомити відповідні процедури знаходження їхніх визначників і обернених матриць. Розроблено ПЗ, яке дає змогу генерувати як послідовності уточнених 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 уточненою поліноміальною матрицею Фібоначчі, що дає змогу зацікавленому читачу зрозуміти основний принцип шифрування як початкового повідомлення, так і розшифрування зашифрованого повідомлення.

Ключові слова: послідовність поліномів Фібоначчі; рекурентне матричне співвідношення; механізм утворення послідовності; обернена поліноміальна матриця Фібоначчі; зашифроване повідомлення; матричний метод шифрування даних.

Вступ / Introduction

Прогрес інформаційних технологій посприяв тому, що поліноміальні матриці Фібоначчі та різноманітні їхні модифікації почали застосовувати в різних областях знань [67], враховуючи й шифрування блокових даних насамперед матричним методом [36]. Чимала кількість досліджень щодо особливостей генерування відповідних ключів для шифрування блокових даних у вигляді послідовності поліноміальних матриць Фібоначчі, елементами яких є поліноми Фібоначчі та їхні різноманітні аналоги, за останні дедекілька десятиліть хоча й трапляються час від часу у відкритому друці, однак вони значно менше досліджені, ніж так звані матриці Фібоначчі, елементами яких є різноманітні числа Фібоначчі. Наприклад, у роботі [22] розроблено $\bar{\bar{Q}}_m^n$-матрицю Фібоначчі розміром $m \times m$, елементами якої є поліноми Фібоначчі $(n–1)$-го степеня і менше, а також досліджено основні її властивості. У роботі [43] автори навели $Q_h(x)$-матрицю Фібоначчі, елементами якої є поліноми Фібоначчі n-го степеня, що узагальнюють Q-матрицю Фібоначчі, породжену відповідними числами. Автори роботи [41] розглядають матрицю Паскаля та визнача-

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 уточненими поліноміальними матрицями Фібоначчі. Науковий вісник НЛТУ України. 2025, т. 35, № 3. С. 200–217.
Citation APA: 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

ють нове узагальнення поліномів Фібоначчі, які було названо (p,q)-поліномами Фібоначчі. У роботі [29] наведено метод генерування послідовності поліноміальних матриць Фібоначчі m-го порядку, елементами яких є поліноми Фібоначчі не більше (n–1)-го степеня, який дає можливість знаходити як їхні визначники, так і обернені матриці, придатні для матричного методу шифрування блокових даних.

Чимала кількість досліджень стосується різних підходів до генерування послідовності поліноміальних матриць Фібоначчі, а також особливостей їхнього використання для шифрування блокових даних. Наприклад, у роботі [51] розроблено новий клас квадратних $Q_{pm}^{n}(x)$ - матриць Фібоначчі (n–1)-го степеня та pm-го порядку для шифрування даних, елементами яких є поліноми Фібоначчі. У роботі [8] 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 та отримано певні співвідношення між елементами цієї матриці. Однак, автори цих і багатьох інших досліджень вважають, що як окрему процедуру шифрування даних за допомогою послідовностей поліноміальних матриць Фібоначчі для передачі їх каналами зв'язку застосовувати недоцільно через малу кількість різних елементів таких матриць, а також незначну криптостійкість алгоритму шифрування [5].

У кожному з вказаних вище та багатьох інших дослідженнях тією чи іншою мірою обґрунтовано різні підходи щодо генерування послідовності поліноміальних матриць Фібоначчі, проте не наведено приклади їхнього конкретного вигляду, однак доведено доцільність їх використання для шифрування блокових даних як складової дещо складніших алгоритмів. Тільки у роботі [29] розроблено метод генерування n-ої послідовності поліноміальних матриць Фібоначчі m-го порядку, елементами яких є поліноми Фібоначчі не вище (n–1)-го степеня. Цей метод використовує матричне рекурентне співвідношення, аналогічне рекурентному співвідношенню для генерування чисел Фібоначчі, в якому було застосовано загальновідому структуру елементів таких матриць [62]. Однак, навіть поверхневий аналіз послідовності поліноміальних матриць Фібоначчі від 2-го до 5-го порядків, наведених у дослідженні [29], показує, що застосування традиційної структури елементів таких матриць є недоцільним через незначну кількість (k) різних поліномів Фібоначчі не вище (n–1)-го степеня. Наприклад, для матриць Фібоначчі будь-якого порядку (m) таких різних поліномів Фібоначчі буде всього k = 3, степінь яких залежатиме тільки від номера (n) послідовності поліноміальної матриці Фібоначчі, а саме від (n–3)-го до (n–1)-го степеня. Така мала кількість різних елементів матриць Фібоначчі та незначне варіювання степенів відповідних поліномів Фібоначчі є інформативною та прозорою для криптоаналітика, а також слабкою для криптоаналізу відповідного алгоритму [30]. Тому виникає потреба проведення додаткового дослідження щодо особливостей генерування послідовностей поліноміальних матриць Фібоначчі та уточнення структури їхніх елементів так, щоб за отриманими матрицями була можливість знаходити як їхні визначники, так і обернені матриці, а також була можливість встановлення певних особливостей їхнього використання тільки як локального методу шифрування блокових даних.

Об'єкт дослідження – генерування послідовності уточнених поліноміальних матриць Фібоначчі.

Предмет дослідження – методи та алгоритми генерування послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку як ключів для шифрування блокових даних, що дасть можливість здійснювати ефективний їх захист.

Мета роботи – розробити метод генерування ключів для шифрування блокових даних у вигляді послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, структура елементів яких міститиме значну кількість поліномів Фібоначчі відповідних номерів, а отримані матриці дадуть можливість знаходити як їхні визначники, так і обернені матриці, що сукупно уможливить їхнє застосування 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 поліноміальних матриць Фібоначчі, які стануть ключами для шифрування блокових даних, що дасть змогу здійснювати ефективний їх захист;
- розробити метод генерування n-ої послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, елементами яких будуть поліноми Фібоначчі відповідних номерів, який дасть можливість знаходити як їхні визначники, так і обернені матриці, які можна застосовувати у матричному методі шифрування блокових даних;
- навести алгоритми утворення деякої послідовності уточнених поліноміальних матриць Фібоначчі від 2-го до 5-го порядків, елементами яких будуть поліноми Фібоначчі відповідних номерів, що дасть змогу проаналізувати не тільки особливості їхньої побудови загалом, але й усвідомити процедури знаходження їхніх визначників і обернених матриць зокрема;
- навести конкретний приклад застосування матричного методу шифрування блокових даних уточненою поліноміальною матрицею Фібоначчі, що дасть змогу зацікавленому читачу зрозуміти основний принцип шифрування як початкового повідомлення, так і розшифрування зашифрованих даних;
- зробити висновки за результатами виконаного дослідження та надати відповідні рекомендації щодо їх практичного використання.

Аналіз останніх досліджень та публікацій. У роботі [60] проаналізовано поліноми Фібоначчі та детерміновані тотожності, пов'язані з ними. Авторами встановлено, що поліноми Фібоначчі та поліноми Лукаса володіють чудовими та дивовижними властивостями, а також відповідними детермінованими тотожностями, які було детально описано. Записи детермінованих тотожностей задовольняють рекурентним співвідношенням утворення поліномів Фібоначчі та поліномів Лукаса.

У роботі [43] 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 узагальнюють Q-матрицю Фібоначчі, породжену відповідними числами.

У роботі [55] наведено інформацію про згорнуті узагальнені поліноми Фібоначчі та Лукаса. Автори визначають згорнуті $h(x)$-поліноми Фібоначчі як розширення класичних чисел Фібоначчі. Також вони наводять дедекілька 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 [65] 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 [41] 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 [51] наведено обнадійливі, як на перший погляд, показники надійності теорії шифрування даних поліномами Фібоначчі. Розроблено новий клас квадратних $Q_{pm}^{n}(x)$ -матриць Фібоначчі $(n–1)$-го степеня та pm-го порядку для шифрування даних, де $p \geq 3$, $m \geq 1$, $n \geq 1$, $x \geq 1$, елементами яких є поліноми Фібоначчі. Запропонований метод дешифрування даних випливає з можливості отримання відповідних обернених $Q_{pm}^{-n}(x)$ -матриць Фібоначчі, визначник яких становить ±1. При цьому відзначено як незначні тривалості виконання таких процедур, так і надійність зашифрованих повідомлень, стійких до криптографічних атак [30].

У роботі [22] розроблено метод шифрування будь-яких повідомлень на підставі поліномів Фібоначчі. Для цілих чисел $m \geq 2$, $x \geq 1$ і $n \geq 1$ було розроблено Q_{m}^{n} -матрицю Фібоначчі розміром $m \times m$, елементами якої є поліноми Фібоначчі $(n–1)$-го степеня, а визначник матриці становить ±1. Для розшифрування даних автори ввели обернену $Q_{m}^{-n}(x)$ -матрицю, елементи якої є оберненими поліноми Фібоначчі n-го степеня.

У роботі [8] 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 [5] розглянуто підхід до реалізації криптосистеми з використанням поліномів і чисел Лукаса. Автори навели інноваційний підхід до реалізації криптосистеми, яка використовує поліноми та числа Лукаса. Числа Лукаса, послідовність яких подібна до чисел Фібоначчі, мають унікальні властивості, які часто використовують для шифрування та дешифрування даних. Запропонована поліноміальна криптосистема Лукаса описує процеси генерування ключів, шифрування та дешифрування, вказуючи на питання безпеки та особливості управління ключами. Стійкість системи залежить від складності розкладання великих простих чисел і виклику щодо отримання секретного ключа з відкритого ключа. У своєму дослідженні автори забезпечують всебічне розуміння криптосистеми та досліджують її потенційні можливості застосування в безпечному зв'язку та захисті даних. Також проведено широкий аналіз і криптоаналіз, щоб оцінити безпеку та ефективність запропонованої системи, що робить її перспективним доповненням до криптографічного середовища.

У роботі [10] наведено узагальнену теорію шифрування даних на (m,t)-розширенні поліномів p-числами Фібоначчі. Спочатку автори визначають (m,t)-розширення p-чисел Фібоначчі та золотих (p,m,t)-пропорцій, де $p \geq 0$ є цілим невід'ємним числом, $m > 0$ і $t > 0$. Вони встановили співвідношення між золотою (p,m,t)-пропорцією, між золотою (p,m)-пропорцією та між золотою p-пропорцією, внаслідок чого було визначено квадратну $G_{p,m,t}$-матрицю Фібоначчі. Також автори показали, що, за умови правильного вибору початкових членів полінома для (m,t)-розширення його p-числами Фібоначчі, можна застосувати процедуру шифрування даних з використанням $G_{p,m,t}$-матриці Фібоначчі. Зроблено висновок, що для $t = 1$ зв'язки між елементами матриці шифрування даних для різних значень p і m збігаються з аналогічними початковими членами чисел Фібоначчі [9].

У роботі [4] розглянуто тип загальнодоступної криптосистеми, що використовує поліноми та послідовностей поліномів Пелла. Автори створили своєрідну криптосистему з відкритим ключем за допомогою поліномів і послідовностей поліномів Пелла шляхом використання властивостей як поліномів, так і послідовностей поліномів Пелла через перетворення поліномів у вісімкову та двійкову систему числення. Захист цифрових даних і їх модифікація вони здійснювали за допомогою сучасних криптографічних методів, які відіграють важливу роль у безпеці мережі.

Отже, за результатами проведеного аналізу останніх досліджень та публікацій стосовно наявних підходів до генерування ключів для шифрування блокових даних у вигляді послідовності поліноміальних матриць Фібоначчі m-го порядку, а також особливостей їх використання для даних матричним методом було встановлено, що навіть за останнє десятиліття виконано багато різноманітних досліджень, в кожному з яких тією чи іншою мірою обґрунтовано різні алгоритми їхньої побудови, а також доведено доцільність їх використання для шифрування даних. Водночас, застосування поліноміальних матриць Фібоначчі як окремої процедури для захисту блокових даних у теорії та практиці криптографії трапляється вкрай рідко. Тому проведення додаткового дослідження щодо розроблення ефективного методу генерування n-ої послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, елементами яких будуть відповідні поліноми Фібоначчі, а також встановлення певних особливостей їхнього використання для шифрування блокових даних тільки як локального ме-

тоду 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 поліномів Фібоначчі. Для генерування послідовності поліномів Фібоначчі використовують рекурентне співвідношення [6]:

$$F^{(n+1)}(x) = xF^{(n)}(x) + F^{(n-1)}(x), \quad (1)$$

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

Застосувавши рекурентне співвідношення (1), послідовність перших декількох і наступних вибіркових поліномів Фібоначчі матимуть такий вигляд:

$$\begin{aligned}
&F^{(0)}(x) = 0;\\
&F^{(1)}(x) = 1;\\
&F^{(2)}(x) = x;\\
&F^{(3)}(x) = x^2 + 1;\\
&F^{(4)}(x) = x^3 + 2x;\\
&F^{(5)}(x) = x^4 + 3x^2 + 1;\\
&F^{(6)}(x) = x^5 + 4x^3 + 3x;\\
&F^{(7)}(x) = x^6 + 5x^4 + 6x^2 + 1;\\
&F^{(8)}(x) = x^7 + 6x^5 + 10x^3 + 4x;\\
&F^{(9)}(x) = x^8 + 7x^6 + 15x^4 + 10x^2 + 1; \quad (2)\\
&F^{(10)}(x) = x^9 + 8x^7 + 21x^5 + 20x^3 + 5x.\\
&F^{(11)}(x) = x^{10} + 9x^8 + 28x^6 + 35x^4 + 15x^2 + 1;\\
&F^{(12)}(x) = x^{11} + 10x^9 + 36x^7 + 56x^5 + 35x^3 + 6x;\\
&F^{(13)}(x) = x^{12} + 11x^{10} + 45x^8 + 84x^6 + 70x^4 + 21x^2 + 1;\\
&F^{(14)}(x) = x^{13} + 12x^{11} + 55x^9 + 120x^7 + 126x^5 + 56x^3 + 7x;\\
&F^{(15)}(x) = x^{14} + 13x^{12} + 66x^{10} + 165x^8 + 210x^6 + 126x^4 + 28x^2 + 1.
\end{aligned}$$

Метод генерування послідовності поліномів Фібоначчі полягає у використанні рекурентного співвідношення (1), згідно з яким наступний поліном утворюють шляхом множення змінної x послідовно на елементи поточного полінома, після чого групують схожі доданки з доданками попереднього полінома. Наприклад, за вхідних поліномів $F^{(6)}(x)$ і $F^{(7)}(x)$ відповідно 5-го і 6-го степенів з послідовності поліномів (2) наступний поліном 7-го степеня матиме такий вигляд:

$$F^{(8)}(x) = xF^{(7)}(x) + F^{(6)}(x) = x(x^6 + 5x^4 + 6x^2 + 1) + (x^5 + 4x^3 + 3x) = x^7 + 5x^5 + 6x^3 + x + x^5 + 4x^3 + 3x = x^7 + 6x^5 + 10x^3 + 4x.$$

Оскільки послідовності поліномів Фібоначчі є природним розширенням відповідних послідовностей чисел Фібоначчі [3, 23], тому багато їхніх властивостей допускають пряме їхнє доведення [46, 56, 71].

2. Механізм утворення послідовності уточнених поліноміальних матриць Фібоначчі. З роботи [67] відомо, що поліноміальна $\bar{\bar{Q}}_2(x)$-матриця Фібоначчі розміром 2×2 має такий вигляд

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

а її визначник отримують за формулою

$$\det\left(\bar{\bar{Q}}_2^{(n+1)}(x)\right) = F^{(n+1)}(x)F^{(n-1)}(x) - (F^{(n)}(x))^2 = (-1)^{n+1}, \quad (4)$$

яку ще називають тотожністю Кассіні [36]. Наприклад, для 4-ої та 5-ої поліноміальних матриць Фібоначчі 2-го порядку їхні визначники матимуть такий вигляд:

$$\begin{aligned}
\det\left(\bar{\bar{Q}}_2^{(4)}(x)\right) &= F^{(4)}(x)F^{(2)}(x) - (F^{(3)}(x))^2 = \\
&= (x^3 + 2x)x - (x^2 + 1)^2 = -1;
\end{aligned}$$

$$\begin{aligned}
\det\left(\bar{\bar{Q}}_2^{(5)}(x)\right) &= F^{(5)}(x)F^{(3)}(x) - (F^{(4)}(x))^2 = \\
&= (x^4 + 3x^2 + 1)(x^2 + 1) - (x^3 + 2x)^2 = 1.
\end{aligned}$$

З роботи [62] також відомо, що поліноміальні $\bar{\bar{Q}}_m^{(2)}(x)$-матриці Фібоначчі 2-го, 3-го, 4-го, 5-го і m-го порядків мають такий вигляд:

$$\begin{aligned}
&\bar{\bar{Q}}_2^{(2)}(x) = \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}_2; \bar{\bar{Q}}_3^{(2)}(x) = \begin{bmatrix} x & 1 & 0 \\ 0 & x & 1 \\ 0 & 1 & 0 \end{bmatrix}_3; \bar{\bar{Q}}_4^{(2)}(x) = \begin{bmatrix} x & 1 & 0 & 0 \\ 0 & x & 1 & 0 \\ 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_4;\\
&\bar{\bar{Q}}_5^{(2)}(x) = \begin{bmatrix} x & 1 & 0 & 0 & 0 \\ 0 & x & 1 & 0 & 0 \\ 0 & 0 & x & 1 & 0 \\ 0 & 0 & 0 & x & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}_5; \bar{\bar{Q}}_m^{(2)}(x) = \begin{bmatrix} x & 1 & 0 & 0 & \cdots & 0 \\ 0 & x & 1 & 0 & \cdots & 0 \\ 0 & 0 & x & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & x & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}_m. \quad (5)
\end{aligned}$$

Для генерування послідовності поліноміальних $\bar{\bar{Q}}_m^{(2)}(x)$-матриць Фібоначчі використовують рекурентне матричне співвідношення, аналогічне співвідношенню (1), яке в нашому випадку матиме такий вигляд:

$$\bar{\bar{Q}}_m^{(n+1)}(x) = x\bar{\bar{Q}}_m^{(n)}(x) + \bar{\bar{Q}}_m^{(n-1)}(x), \quad (6)$$

де $\bar{\bar{Q}}_m^{(n+1)}(x)$, $\bar{\bar{Q}}_m^{(n)}(x)$ і $\bar{\bar{Q}}_m^{(n-1)}(x)$ – відповідно наступний, поточний та попередній вигляд поліноміальних $\bar{\bar{Q}}_m^{(\cdot)}(x)$-матриць Фібоначчі.

Метод генерування послідовності поліноміальних $\bar{\bar{Q}}_m^{(\cdot)}(x)$-матриць Фібоначчі m-го порядку полягає у використанні рекурентного матричного співвідношення (6), згідно з яким наступну поліноміальну $\bar{\bar{Q}}_m^{(n+1)}(x)$-матрицю утворюють шляхом множення змінної x послідовно на елементи поточної $\bar{\bar{Q}}_m^{(n)}(x)$-матриці, якими є відповідні поліноми Фібоначчі, додавання елементів утвореної матриці до елементів попередньої $\bar{\bar{Q}}_m^{(n-1)}(x)$-матриці, після чого у кожному з її утворених елементів групують всі схожі доданки. Наприклад, для $\bar{\bar{Q}}_2^{(1)}(x) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ та $\bar{\bar{Q}}_2^{(2)}(x) = \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}$, $\det(\bar{\bar{Q}}_2^{(2)}(x)) = x \cdot 0 - 1 \cdot 1 = -1$, а наступна поліноміальна матриця Фібоначчі матиме такий вигляд:

$$\begin{aligned}
\bar{\bar{Q}}_2^{(3)}(x) &= x\bar{\bar{Q}}_2^{(2)}(x) + \bar{\bar{Q}}_2^{(1)}(x) = \\
&= x\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x^2 & x \\ x & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x^2 + 1 & x \\ x & 1 \end{bmatrix}; \quad (7)\\
\det(\bar{\bar{Q}}_2^{(3)}(x)) &= (x^2 + 1) \cdot 1 - x \cdot x = 1.
\end{aligned}$$

Оскільки поліноміальні $\bar{\bar{Q}}_m^{(\cdot)}(x)$-матриці Фібоначчі часто використовують для реалізації операцій шифрування даних, то аналогічні оберненні матриці також потрібно мати для зворотного процесу – розшифрування даних. Інтуїтивно зрозуміло, що ці $\bar{\bar{Q}}_m^{-(\cdot)}(x)$-матриці Фібоначчі мають бути оберненими до матриць шифрування даних, які назвемо *оберненими поліноміальними* $\bar{\bar{Q}}_m^{-(\cdot)}(x)$*-матрицями Фібоначчі*. Подібно до поліноміальних матриць – так званих ключів шифрування даних, обернені поліноміальні матриці Фібоначчі мають мати також загальний вигляд.

Для знаходження оберненої матриці 2-го порядку використовують такий вираз [26]:

$$\boldsymbol{A}^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}. \quad (8)$$

Наприклад, для $\overline{\overline{Q}}_2^{(2)}(x)=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}$ маємо

$$\overline{\overline{Q}}_2^{-(2)}(x)=\frac{1}{x\cdot 0-1\cdot 1}\begin{bmatrix} 0 & -1 \\ -1 & x \end{bmatrix}=\begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix},$$

а для матриці (7) отримаємо

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

Покажемо, що матричний вираз $\overline{\overline{Q}}_2^{(n)}(x)\times\overline{\overline{Q}}_2^{-(n)}(x)=\overline{\overline{I}}_2$ можна виконати для будь-якого значення n, наприклад n=2 та n=3, де $\overline{\overline{I}}_2$ – одинична матриця m=2-го порядку.

$$\begin{aligned}
&\overline{\overline{Q}}_2^{(2)}(x)\times\overline{\overline{Q}}_2^{-(2)}(x)=\overline{\overline{I}}_{2\times 2}\Rightarrow\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}\times\begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix}= \\
&=\begin{bmatrix} x\cdot 0+1\cdot 1 & x\cdot 1+1\cdot(-x) \\ 1\cdot 0+0\cdot 1 & 1\cdot 1+0\cdot -x) \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \\
&\overline{\overline{Q}}_2^{(3)}(x)\times\overline{\overline{Q}}_2^{-(3)}(x)=\overline{\overline{I}}_{2\times 2}\Rightarrow\begin{bmatrix} x^2+1 & x \\ x & 1 \end{bmatrix}\times\begin{bmatrix} 1 & -x \\ -x & x^2+1 \end{bmatrix}= \\
&=\begin{bmatrix} (x^2+1)\cdot 1+x\cdot(-x) & (x^2+1)\cdot(-x)+x\cdot(x^2+1) \\ x\cdot 1+1\cdot(-x) & x\cdot(-x)+1\cdot(x^2+1) \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.
\end{aligned} \tag{9}$$

Як видно з матричних виразів (5), а також проведеного аналізу послідовності поліноміальних матриць Фібоначчі від 2-го до 5-го порядків, наведених у роботі [29], традиційний підхід до формування структури елементів таких матриць має деякі недоліки, один з яких стосується кількості (k) різних її елементів, якими є поліноми Фібоначчі не вище (n–1)-го степеня. Наприклад, для матриць Фібоначчі будь-якого порядку (m) таких різних поліномів Фібоначчі буде всього k = 3, степінь яких залежатиме тільки від n-ої послідовності поліноміальної матриці Фібоначчі (див. матричні вирази (16), (19), (20) чи (21) з роботи [29]). Така незначна їхня кількість є не тільки малоінформативною та прозорою для криптоаналітика [5], але й нестійкою щодо криптоаналізу [30].

З огляду на зазначене вище, вважаємо за доцільне дещо уточнити структуру елементів поліноміальних матриць Фібоначчі, кількість яких мала б залежати насамперед від їхнього порядку (m). Окрім цього, для розуміння суті викладеного нижче матералу використаємо не степені поліномів Фібоначчі, а їхні номери з математичних виразів (2), наприклад $F^{(3)}(x)$ чи $F^{(5)}(x)$, де n становитиме відповідно 3 і 5. Тоді, для $\overline{\overline{Q}}_2^{(2)}(x)$-матриці Фібоначчі m = 2-го порядку її структура елементів буде незмінною (16), тобто кількість її різних елементів, якими будуть поліноми Фібоначчі не вище n = 2-го номера, становитиме $k_2 = m$+1 = 2+1 = 3. Водночас, для $\overline{\overline{Q}}_3^{(2)}(x)$-матриці Фібоначчі m = 3-го порядку структуру елементів спробуємо дещо змінити в бік збільшення кількості видів поліномів до 3-го номера, тобто кількість різних елементів матриці, якими будуть поліноми Фібоначчі, тепер становитиме k_3 = 3+1 = 4. Аналогічно змінимо структуру елементів $\overline{\overline{Q}}_4^{(2)}(x)$- та $\overline{\overline{Q}}_5^{(2)}(x)$-матриць Фібоначчі відповідно 4-го і 5-го порядків у бік збільшення кількості видів їхніх поліномів Фібоначчі відповідно до 4-го та 5-го номерів, тобто кількість різних елементів цих матриць становитиме відповідно k_4 = 5 і k_5 = 6. У виразах (16) для $\overline{\overline{Q}}_m^{(2)}(x)$-матриці Фібоначчі в її лівій верхній частині елементів у дужках наведено ідентифікатори значень номерів їхніх відповідних поліномів Фібоначчі, загальна кількість яких у такій матриці становитиме $k_m = m + 1$.

Варто зазначити, що вказані у матричних виразах (10) ідентифікатори номерів поліномів Фібоначчі стосуються тільки n = 2-ої послідовності поліноміальних матриць Фібоначчі m-го порядку. Для більших номерів (n > 3) послідовності матриць Фібоначчі та ще й з урахуванням їхнього порядку (m) номери їхніх поліномів Фібоначчі матимуть дещо інший вигляд. Для встановлення номерів цих поліномів Фібоначчі розглянемо матричні вирази (11), в яких наведено елементи матриць Фібоначчі m-го порядку у вигляді ідентифікаторів відповідних поліномів Фібоначчі для n = 2-ої послідовності поліноміальних матриць. Якщо ж розглянути загалом варіанти n-ої послідовності поліноміальних матриць Фібоначчі m-го порядку, то вони матимуть вигляд, який показано на матричних виразах (12). З цих виразів видно як розміщення елементів матриць Фібоначчі m-го порядку для їхньої n-ої послідовності, так і номери відповідних ідентифікаторів поліномів Фібоначчі, водночас як їхні степені будуть на одиницю менше.

Наведена структура елементів n-ої послідовності поліноміальних матриць Фібоначчі m-го порядку має цікаву властивість, згідно з якою можна уникнути використання рекурентного матричного співвідношення (6), а генерувати відповідні матриці Фібоначчі тільки за номерами (m+n–2–j)-ої послідовності поліномів Фібоначчі (2), які дещо залежать від місця їхнього розташування в матриці та номера її стовпця, а саме $\forall j\in[0\div(m-1)]$. Наприклад, якщо маємо згенерувати (n = 15)-ту послідовність поліноміальних матриць Фібоначчі (m = 10)-го порядку, то її елементами будуть поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го, а саме: 15 – 2 = 13 і 10 + 15 – 2 = 23. Утворена поліноміальна матриця Фібоначчі міститиме таких різних поліномів Фібоначчі аж k_{10} = 10 + 1 = 11 шт., що значно більше, а ніж це було б для традиційної структури матриць Фібоначчі (5).

Нижче наведено так звані ключі для шифрування блокових даних у вигляді послідовності декількох перших уточнених поліноміальних $\overline{\overline{Q}}_m^{(\cdot)}(x)$-матриць Фібоначчі відповідно від 2-го до 5-го порядків, утворені рекурентним матричним співвідношенням (6), елементами яких будуть відповідні поліноми Фібоначчі не вище (m+n–2)-го номера, які повністю відповідатимуть номерам поліномів Фібоначчі з їхньої послідовності (2). Отримані матриці Фібоначчі дають змогу знаходити як їхні визначники, так і обернені матриці, придатні для матричного шифрування блокових даних.

$$\overline{\overline{Q}}_2^{(2)}(x)=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}_2;\ \overline{\overline{Q}}_3^{(2)}(x)=\begin{bmatrix} x^2+1 & x & 0 \\ 0 & x & 1 \\ 0 & 1 & 0 \end{bmatrix}_3;\ \overline{\overline{Q}}_4^{(2)}(x)=\begin{bmatrix} x^3+2x & x^2+1 & 0 & 0 \\ 0 & x^2+1 & x & 0 \\ 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_4;$$

$$\overline{\overline{Q}}_5^{(2)}(x)=\begin{bmatrix} x^4+3x^2+1 & x^3+2x & 0 & 0 & 0 \\ 0 & x^3+2x & x^2+1 & 0 & 0 \\ 0 & 0 & x^2+1 & x & 0 \\ 0 & 0 & 0 & x & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}_5;\ \overline{\overline{Q}}_m^{(2)}(x)=\begin{bmatrix} (m) & (m-1) & 0 & 0 & \cdots & 0 \\ 0 & (m-1) & (m-2) & 0 & \cdots & 0 \\ 0 & 0 & (m-2) & (m-3) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & x & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}_m. \tag{10}$$

$$\bar{\bar{Q}}_2^{(2)}(x)=\begin{bmatrix} F^{(2)}(x) & F^{(1)}(x) \\ F^{(1)}(x) & F^{(0)}(x) \end{bmatrix}_2;\ \bar{\bar{Q}}_3^{(2)}(x)=\begin{bmatrix} F^{(3)}(x) & F^{(2)}(x) & 0 \\ 0 & F^{(2)}(x) & F^{(1)}(x) \\ 0 & F^{(1)}(x) & F^{(0)}(x) \end{bmatrix}_3;\ \bar{\bar{Q}}_4^{(2)}(x)=\begin{bmatrix} F^{(4)}(x) & F^{(3)}(x) & 0 & 0 \\ 0 & F^{(3)}(x) & F^{(2)}(x) & 0 \\ 0 & 0 & F^{(2)}(x) & F^{(1)}(x) \\ 0 & 0 & F^{(1)}(x) & F^{(0)}(x) \end{bmatrix}_4; \tag{11}$$

$$\bar{\bar{Q}}_5^{(2)}(x)=\begin{bmatrix} F^{(5)}(x) & F^{(4)}(x) & 0 & 0 & 0 \\ 0 & F^{(4)}(x) & F^{(3)}(x) & 0 & 0 \\ 0 & 0 & F^{(3)}(x) & F^{(2)}(x) & 0 \\ 0 & 0 & 0 & F^{(2)}(x) & F^{(1)}(x) \\ 0 & 0 & 0 & F^{(1)}(x) & F^{(0)}(x) \end{bmatrix}_5;\ \bar{\bar{Q}}_m^{(2)}(x)=\begin{bmatrix} F^{(m)}(x) & F^{(m-1)}(x) & 0 & \cdots & 0 \\ 0 & F^{(m-1)}(x) & F^{(m-2)}(x) & \cdots & 0 \\ 0 & 0 & F^{(m-2)}(x) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & F^{(2)}(x) & F^{(1)}(x) \\ 0 & 0 & \cdots & F^{(1)}(x) & F^{(0)}(x) \end{bmatrix}_m.$$

$$\bar{\bar{Q}}_2^{(n)}(x)=\begin{bmatrix} F^{(n)}(x) & F^{(n-1)}(x) \\ F^{(n-1)}(x) & F^{(n-2)}(x) \end{bmatrix}_2;\ \bar{\bar{Q}}_3^{(n)}(x)=\begin{bmatrix} F^{(n+1)}(x) & F^{(n)}(x) & 0 \\ 0 & F^{(n)}(x) & F^{(n-1)}(x) \\ 0 & F^{(n-1)}(x) & F^{(n-2)}(x) \end{bmatrix}_3;$$

$$\bar{\bar{Q}}_4^{(n)}(x)=\begin{bmatrix} F^{(n+2)}(x) & F^{(n+1)}(x) & 0 & 0 \\ 0 & F^{(n+1)}(x) & F^{(n)}(x) & 0 \\ 0 & 0 & F^{(n)}(x) & F^{(n-1)}(x) \\ 0 & 0 & F^{(n-1)}(x) & F^{(n-2)}(x) \end{bmatrix}_4;\ \bar{\bar{Q}}_5^{(n)}(x)=\begin{bmatrix} F^{(n+3)}(x) & F^{(n+2)}(x) & 0 & 0 & 0 \\ 0 & F^{(n+2)}(x) & F^{(n+1)}(x) & 0 & 0 \\ 0 & 0 & F^{(n+1)}(x) & F^{(n)}(x) & 0 \\ 0 & 0 & 0 & F^{(n)}(x) & F^{(n-1)}(x) \\ 0 & 0 & 0 & F^{(n-1)}(x) & F^{(n-2)}(x) \end{bmatrix}_5; \tag{12}$$

$$\bar{\bar{Q}}_m^{(n)}(x)=\begin{bmatrix} F^{(m+n-2)}(x) & F^{(m+n-3)}(x) & 0 & 0 & \cdots & 0 \\ 0 & F^{(m+n-3)}(x) & F^{(m+n-4)}(x) & 0 & \cdots & 0 \\ 0 & 0 & F^{(m+n-4)}(x) & F^{(m+n-5)}(x) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & F^{(n)}(x) & F^{(n-1)}(x) \\ 0 & 0 & \cdots & 0 & F^{(n-1)}(x) & F^{(n-2)}(x) \end{bmatrix}_m.$$

2.1. ***Механізм утворення послідовності уточнених поліноміальних матриць Фібоначчі 2-го порядку***. Розглянемо алгоритм побудови послідовності перших 8-ми поліноміальних $\bar{\bar{Q}}_2^{(\cdot)}(x)$-матриць Фібоначчі 2-го порядку, їхніх визначників і відповідно обернених поліноміальних $\bar{\bar{Q}}_2^{-(\cdot)}(x)$-матриць Фібоначчі. З наведених матричних виразів (13) видно, що елементами *n*-ої поліноміальної $\bar{\bar{Q}}_2^{(n)}(x)$-матриці Фібоначчі є відповідні номери поліноми Фібоначчі від (*n*–2)-го до *n*-го ($\forall n\in\{3\div 8\}$) з їхньої послідовності (2).

Для непарної поліноміальної $\bar{\bar{Q}}_2^{(\cdot)}(x)$-матриці Фібоначчі її визначник становить одиниця, а для парної – мінус одиниця, що повністю відповідає формулі (4). Водночас, всі обернені поліноміальні $\bar{\bar{Q}}_3^{-(\cdot)}(x)$-матриці Фібоначчі відповідають матричному виразу (8). Правильність отримання як поліноміальних $\bar{\bar{Q}}_2^{(\cdot)}(x)$-матриць Фібоначчі, так і їхніх обернених еквівалентів перевірена матричним виразом (9), однак тепер вже для 4-ої поліноміальної матриці Фібоначчі, внаслідок виконання якого отримано також одиничну матрицю.

$$\bar{\bar{Q}}_2^{(n+1)}(x)=x\bar{\bar{Q}}_2^{(n)}(x)+\bar{\bar{Q}}_2^{(n-1)}(x);\ \det(\bar{\bar{Q}}_2^{(n)}(x))=(-1)^n;\ \bar{\bar{Q}}_2^{(n)}(x)\times\bar{\bar{Q}}_2^{-(n)}(x)=\bar{\bar{I}}_2$$

$$\bar{\bar{Q}}_2^{(0)}(x)=\bar{\bar{Q}}_2^{(2)}(x)-x\bar{\bar{Q}}_2^{(1)}(x)=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}-x\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(0)}(x))=-1;\ \bar{\bar{Q}}_3^{-(0)}(x)=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(1)}(x)=\bar{\bar{Q}}_2^{(3)}(x)-x\bar{\bar{Q}}_2^{(2)}(x)=\begin{bmatrix} x^2+1 & x \\ x & 1 \end{bmatrix}-x\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(1)}(x))=1;\ \bar{\bar{Q}}_3^{-(1)}(x)=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(2)}(x)=x\bar{\bar{Q}}_2^{(1)}(x)+\bar{\bar{Q}}_2^{(0)}(x)=x\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}+\begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix}=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(2)}(x))=-1;\ \bar{\bar{Q}}_2^{-(2)}(x)=\begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(3)}(x)=x\bar{\bar{Q}}_2^{(2)}(x)+\bar{\bar{Q}}_2^{(1)}(x)=x\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}+\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} x^2+1 & x \\ x & 1 \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(3)}(x))=1;\ \bar{\bar{Q}}_2^{-(3)}(x)=\begin{bmatrix} 1 & -x \\ -x & x^2+1 \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(4)}(x)=x\bar{\bar{Q}}_2^{(3)}(x)+\bar{\bar{Q}}_2^{(2)}(x)=x\begin{bmatrix} x^2+1 & x \\ x & 1 \end{bmatrix}+\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}=\begin{bmatrix} x^3+2x & x^2+1 \\ x^2+1 & x \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(4)}(x))=-1;\ \bar{\bar{Q}}_2^{-(4)}(x)=\begin{bmatrix} -x & x^2+1 \\ x^2+1 & -x^3-2x \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(5)}(x)=x\bar{\bar{Q}}_2^{(4)}(x)+\bar{\bar{Q}}_2^{(3)}(x)=x\begin{bmatrix} x^3+2x & x^2+1 \\ x^2+1 & x \end{bmatrix}+\begin{bmatrix} x^2+1 & x \\ x & 1 \end{bmatrix}=\begin{bmatrix} x^4+3x^2+1 & x^3+2x \\ x^3+2x & x^2+1 \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(5)}(x))=1;\ \bar{\bar{Q}}_2^{-(5)}(x)=\begin{bmatrix} x^2+1 & -x^3-2x \\ -x^3-2x & x^4+3x^2+1 \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(6)}(x)=x\bar{\bar{Q}}_2^{(5)}(x)+\bar{\bar{Q}}_2^{(4)}(x)=x\begin{bmatrix} x^4+3x^2+1 & x^3+2x \\ x^3+2x & x^2+1 \end{bmatrix}+\begin{bmatrix} x^3+2x & x^2+1 \\ x^2+1 & x \end{bmatrix}=\begin{bmatrix} x^5+4x^3+3x & x^4+3x^2+1 \\ x^4+3x^2+1 & x^3+2x \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(6)}(x))=-1;$$

$$\bar{\bar{Q}}_2^{-(6)}(x)=\begin{bmatrix} -(x^3+2x) & x^4+3x^2+1 \\ x^4+3x^2+1 & -x^5-4x^3-3x \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(7)}(x)=x\bar{\bar{Q}}_2^{(6)}(x)+\bar{\bar{Q}}_2^{(5)}(x)=x\begin{bmatrix} x^5+4x^3+3x & x^4+3x^2+1 \\ x^4+3x^2+1 & x^3+2x \end{bmatrix}+\begin{bmatrix} x^4+3x^2+1 & x^3+2x \\ x^3+2x & x^2+1 \end{bmatrix}=\begin{bmatrix} x^6+5x^4+6x^2+1 & x^5+4x^3+3x \\ x^5+4x^3+3x & x^4+3x^2+1 \end{bmatrix};\ \det(\bar{\bar{Q}}_2^{(7)}(x))=1;$$

$$\bar{\bar{Q}}_2^{-(7)}(x)=\begin{bmatrix} x^4+3x^2+1 & -x^5-4x^3-3x \\ -x^5-4x^3-3x & x^6+5x^4+6x^2+1 \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(8)}(x)=x\bar{\bar{Q}}_2^{(7)}(x)+\bar{\bar{Q}}_2^{(6)}(x)=$$

$$=x\begin{bmatrix} x^6+5x^4+6x^2+1 & x^5+4x^3+3x \\ x^5+4x^3+3x & x^4+3x^2+1 \end{bmatrix}+\begin{bmatrix} x^5+4x^3+3x & x^4+3x^2+1 \\ x^4+3x^2+1 & x^3+2x \end{bmatrix}=\begin{bmatrix} x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 \\ x^6+5x^4+6x^2+1 & x^5+4x^3+3x \end{bmatrix}; \tag{13}$$

$$\det(\bar{\bar{Q}}_2^{(8)}(x))=-1;\ \bar{\bar{Q}}_2^{-(8)}(x)=\begin{bmatrix} -x^5-4x^3-3x & x^6+5x^4+6x^2+1 \\ x^6+5x^4+6x^2+1 & -x^7-6x^5-10x^3-4x \end{bmatrix};$$

$$\bar{\bar{Q}}_2^{(4)}(x)\times\bar{\bar{Q}}_2^{-(4)}(x)=\begin{bmatrix} x^3+2x & x^2+1 \\ x^2+1 & x \end{bmatrix}\times\begin{bmatrix} -x & x^2+1 \\ x^2+1 & -x^3-2x \end{bmatrix}=\begin{bmatrix} (x^3+2x)(-x)+(x^2+1)(x^2+1) & (x^3+2x)(x^2+1)+(x^2+1)(-x^3-2x) \\ (x^2+1)(-x)+x(x^2+1) & (x^2+1)(x^2+1)+x(-x^3-2x) \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

2.2. ***Механізм утворення послідовності уточнених поліноміальних матриць Фібоначчі 3-го порядку***. Розглянемо алгоритм побудови послідовності перших 8-ми поліноміальних $\bar{\bar{Q}}_3^{(\bullet)}(x)$-матриць Фібоначчі 3-го порядку, їхніх визначників і відповідно обернених поліноміальних $\bar{\bar{Q}}_3^{-(\bullet)}(x)$-матриць Фібоначчі.

Для знаходження оберненої матриці 3-го порядку використовують такий матричний вираз [26]:

$$\boldsymbol{A}^{-1}=\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & k \end{bmatrix}^{-1}=\frac{1}{\det \boldsymbol{A}}\begin{bmatrix} ek-fh & ch-bk & bf-ce \\ fg-dk & ak-cg & cd-af \\ dh-eg & bg-ah & ae-bd \end{bmatrix}, \quad (14)$$

де $\dfrac{1}{\det \boldsymbol{A}}=\dfrac{1}{aek+bfg+cdh-ceg-bdk-afh}$.

Наприклад, для 2-ої поліноміальної матриці Фібоначчі 3-го порядку $\bar{\bar{Q}}_3^{(2)}(x)$ (див. матричні вирази (10)) її обернений еквівалент матиме такий вигляд:

$$\bar{\bar{Q}}_3^{-(2)}(x)=\begin{bmatrix} x^2+1 & x & 0 \\ 0 & x & 1 \\ 0 & 1 & 0 \end{bmatrix}^{-1};\ \frac{1}{\det \boldsymbol{A}}=\frac{1}{(x^2+1)\cdot x\cdot 0+x\cdot 1\cdot 0+0\cdot 0\cdot 1-0\cdot x\cdot 0-1\cdot 1\cdot (x^2+1)-0\cdot 0\cdot x}=-\frac{1}{x^2+1};$$

$$\bar{\bar{Q}}_3^{(\mathrm{T})}(x)=\begin{bmatrix} 1\cdot(x\cdot 0-1\cdot 1) & -1\cdot(x\cdot 0-0\cdot 1) & 1\cdot(x\cdot 1-0\cdot x) \\ -1\cdot(0\cdot 0-1\cdot 0) & 1\cdot((x^2+1)\cdot 0-0\cdot 0) & -1\cdot((x^2+1)\cdot 1-0\cdot 0) \\ 1\cdot(0\cdot 1-x\cdot 0) & -1\cdot((x^2+1)\cdot 1-x\cdot 0) & 1\cdot((x^2+1)\cdot x-x\cdot 0) \end{bmatrix}=\begin{bmatrix} -1 & 0 & x \\ 0 & 0 & -(x^2+1) \\ 0 & -(x^2+1) & x^3+x \end{bmatrix};$$

$$\bar{\bar{Q}}_3^{-(2)}(x)=\frac{1}{\det \boldsymbol{A}}\cdot\bar{\bar{Q}}_3^{(\mathrm{T})}(x)=-\frac{1}{x^2+1}\begin{bmatrix} -1 & 0 & x \\ 0 & 0 & -(x^2+1) \\ 0 & -(x^2+1) & x^3+x \end{bmatrix}=\begin{bmatrix} \dfrac{1}{x^2+1} & 0 & \dfrac{-x}{x^2+1} \\ 0 & 0 & 1 \\ 0 & 1 & -x \end{bmatrix}.$$

З наведених матричних виразів (16) видно, що елементами n-ої поліноміальної $\bar{\bar{Q}}_3^{(n)}(x)$-матриці Фібоначчі є відповідні поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го ($\forall n\in\{3\div 8\}$) з їхньої послідовності (2). Водночас, для n-ої поліноміальної $\bar{\bar{Q}}_3^{(n)}(x)$-матриці Фібоначчі 3-го порядку її визначник можна отримати за такою формулою

$$\det(\bar{\bar{Q}}_3^{(n)}(x))=(-1)^{n+1}F^{(n)}(x), \quad (15)$$

тобто він є відповідним поліномом Фібоначчі (n–1)-го степеня, який враховує знак n-ої парності номерів відповідних поліномів, що зовсім відрізняється від формули (4). Всі обернені поліноміальні $\bar{\bar{Q}}_3^{-(\bullet)}(x)$-матриці Фібоначчі відповідають набору матричних виразів (14). Правильність отримання як поліноміальних $\bar{\bar{Q}}_3^{(\bullet)}(x)$-матриць Фібоначчі, так і їхніх обернених еквівалентів пропонуємо допитливому читачу перевірити шляхом виконання матричного виразу (16), наприклад, для 3-ої поліноміальної матриці, і спробуйте переконатися, що внаслідок виконання якого отримаємо одиничну матрицю.

$$\bar{\bar{Q}}_3^{(n+1)}(x)=x\bar{\bar{Q}}_3^{(n)}(x)+\bar{\bar{Q}}_3^{(n-1)}(x);\ \det(\bar{\bar{Q}}_3^{(n)}(x))=(-1)^{n+1}F^{(n+1)}(x);\ \bar{\bar{Q}}_3^{(n)}(x)\times\bar{\bar{Q}}_3^{-(n)}(x)=\bar{\bar{I}}_3;$$

$$\bar{\bar{Q}}_3^{(0)}(x)=\bar{\bar{Q}}_3^{(2)}(x)-x\bar{\bar{Q}}_3^{(1)}(x)=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -x \end{bmatrix};\det(\bar{\bar{Q}}_3^{(1)}(x))=-1;\ \bar{\bar{Q}}_3^{-(0)}(x)=\begin{bmatrix} 1 & 0 & 0 \\ 0 & x & 1 \\ 0 & 1 & 0 \end{bmatrix};$$

$$\bar{\bar{Q}}_3^{(1)}(x)=\bar{\bar{Q}}_3^{(3)}(x)-x\bar{\bar{Q}}_3^{(2)}(x)=\begin{bmatrix} x & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};\ \det(\bar{\bar{Q}}_3^{(1)}(x))=x;\ \bar{\bar{Q}}_3^{-(1)}(x)=\begin{bmatrix} 1/x & -1/x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$\bar{\bar{Q}}_3^{(2)}(x)=x\bar{\bar{Q}}_3^{(1)}(x)+\bar{\bar{Q}}_3^{(0)}(x)=\begin{bmatrix} x^2+1 & x & 0 \\ 0 & x & 1 \\ 0 & 1 & 0 \end{bmatrix};\ \det(\bar{\bar{Q}}_3^{(2)}(x))=-(x^2+1);\ \bar{\bar{Q}}_3^{-(2)}(x)=\begin{bmatrix} \dfrac{1}{x^2+1} & 0 & \dfrac{-x}{x^2+1} \\ 0 & 0 & 1 \\ 0 & 1 & -x \end{bmatrix};$$

$$\bar{\bar{Q}}_3^{(3)}(x)=x\bar{\bar{Q}}_3^{(2)}(x)+\bar{\bar{Q}}_3^{(1)}(x)=\begin{bmatrix} x^3+2x & x^2+1 & 0 \\ 0 & x^2+1 & x \\ 0 & x & 1 \end{bmatrix};\ \det(\bar{\bar{Q}}_3^{(3)}(x))=x^3+2x;\ \bar{\bar{Q}}_3^{-(3)}(x)=\begin{bmatrix} \dfrac{1}{x^3+2x} & \dfrac{-(x^2+1)}{x^3+2x} & \dfrac{x^2+1}{x^2+2} \\ 0 & 1 & -x \\ 0 & -x & x^2+1 \end{bmatrix};$$

$$\bar{\bar{Q}}_3^{(4)}(x)=x\bar{\bar{Q}}_3^{(3)}(x)+\bar{\bar{Q}}_3^{(2)}(x)=\begin{bmatrix} x^4+3x^2+1 & x^3+2x & 0 \\ 0 & x^3+2x & x^2+1 \\ 0 & x^2+1 & x \end{bmatrix};\ \bar{\bar{Q}}_3^{-(4)}(x)=\begin{bmatrix} \dfrac{1}{x^4+3x^2+1} & \dfrac{x^4+2x^2}{x^4+3x^2+1} & \dfrac{-(x^5+3x^2+2x)}{x^4+3x^2+1} \\ 0 & -x & x^2+1 \\ 0 & x^2+1 & -(x^3+2x) \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_3^{(4)}(x))=-(x^4+3x^2+1);$$

$$\bar{\bar{Q}}_3^{(5)}(x)=x\bar{\bar{Q}}_3^{(4)}(x)+\bar{\bar{Q}}_3^{(3)}(x)=\begin{bmatrix} x^5+4x^3+3x & x^4+3x^2+1 & 0 \\ 0 & x^4+3x^2+1 & x^3+2x \\ 0 & x^3+2x & x^2+1 \end{bmatrix};\ \bar{\bar{Q}}_3^{-(5)}(x)=\begin{bmatrix} \dfrac{1}{x^5+4x^3+3x} & \dfrac{-(x^4+3x^2+1)}{x^3+3x} & \dfrac{x^6+5x^4+7x^2+2}{x^4+4x^2+3} \\ 0 & x^2+1 & -(x^3+2x) \\ 0 & -(x^3+2x) & x^4+3x^2+1 \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_3^{(5)}(x))=x^5+4x^3+3x;$$

$$\bar{\bar{Q}}_3^{(6)}(x)=x\bar{\bar{Q}}_3^{(5)}(x)+\bar{\bar{Q}}_3^{(4)}(x)=\begin{bmatrix} x^6+5x^4+6x^2+1 & x^5+4x^3+3x & 0 \\ 0 & x^5+4x^3+3x & x^4+3x^2+1 \\ 0 & x^4+3x^2+1 & x^3+2x \end{bmatrix};\ \det(\bar{\bar{Q}}_3^{(6)}(x))=-(x^6+5x^4+6x^2+1); \quad (16)$$

$$\bar{\bar{Q}}_3^{-(6)}(x)=\begin{bmatrix} \dfrac{1}{x^6+5x^4+6x^2+1} & \dfrac{x^8+6x^6+11x^4+6x^2}{x^6+5x^4+6x^2+1} & \dfrac{-(x^9+7x^7+16x^5+13x^3+3x)}{x^6+5x^4+6x^2+1} \\ 0 & -(x^3+2x) & x^4+3x^2+1 \\ 0 & x^4+3x^2+1 & -(x^5+4x^3+3x) \end{bmatrix};$$

$$\bar{\bar{Q}}_3^{(7)}(x)=x\bar{\bar{Q}}_3^{(6)}(x)+\bar{\bar{Q}}_3^{(5)}(x)=\begin{bmatrix} x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 & 0 \\ 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x \\ 0 & x^5+4x^3+3x & x^4+3x^2+1 \end{bmatrix};\ \det(\bar{\bar{Q}}_3^{(7)}(x))=x^7+6x^5+10x^3+4x;$$

$$\bar{\bar{Q}}_3^{-(7)}(x)=\begin{bmatrix} \dfrac{1}{x^7+6x^5+10x^3+4x} & \dfrac{-(x^{10}+8x^8+22x^6+24x^4+9x^2+1)}{x^7+6x^5+10x^3+4x} & \dfrac{x^{10}+9x^8+29x^6+40x^4+22x^2+3}{x^6+6x^4+10x^2+4} \\ 0 & x^4+3x^2+1 & -(x^5+4x^3+3x) \\ 0 & -(x^5+4x^3+3x) & x^6+5x^4+6x^2+1 \end{bmatrix};$$

$$\bar{\bar{Q}}_3^{(8)}(x)=x\bar{\bar{Q}}_3^{(7)}(x)+\bar{\bar{Q}}_3^{(6)}(x)=\begin{bmatrix} x^8+7x^6+15x^4+10x^2+1 & x^7+6x^5+10x^3+4x & 0 \\ 0 & x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 \\ 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x \end{bmatrix}; \qquad (16^*)$$

$$\det(\bar{\bar{Q}}_3^{(8)}(x))=-(x^8+7x^6+15x^4+10x^2+1);$$

$$\bar{\bar{Q}}_3^{-(8)}(x)=\begin{bmatrix} \dfrac{1}{x^8+7x^6+15x^4+10x^2+1} & \dfrac{x^{10}+9x^8+28x^6+34x^4+12x^2}{x^6+6x^4+9x^2+1} & \dfrac{-(x^{13}+11x^{11}+46x^9+91x^7+86x^5+34x^3+4x)}{x^8+7x^6+15x^4+10x^2+1} \\ 0 & -(x^5+4x^3+3x) & x^6+5x^4+6x^2+1 \\ 0 & x^6+5x^4+6x^2+1 & -(x^7+6x^5+10x^3+4x) \end{bmatrix}.$$

2.3. ***Механізм утворення послідовності уточнених поліноміальних матриць Фібоначчі 4-го порядку***. Розглянемо алгоритм побудови послідовності перших 8-ми поліноміальних $\bar{\bar{Q}}_4^{(\bullet)}(x)$ -матриць Фібоначчі 4-го порядку, їхніх визначників і відповідно обернених поліноміальних $\bar{\bar{Q}}_4^{-(\bullet)}(x)$ -матриць Фібоначчі. З наведених матричних виразів (17) і (17*) видно, що елементами n-ої поліноміальної $\bar{\bar{Q}}_4^{(n)}(x)$ -матриці Фібоначчі є відповідні поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го ($\forall n\in\{3\div 8\}$) з їхньої послідовності (2).

Оскільки тут маємо справу з матрицями Фібоначчі 4-го порядку, то для обчислення їхніх визначників доводиться використовувати спеціальні математичні методи [26]. Наприклад, шляхом рекуреного обчислення визначників через пониження їхнього порядку, який називають розширенням Лапласа, за допомогою алгоритму Барейса (англ. *Bareiss algorithm*) чи формули Лейбніца (англ. *Leibniz formula*).

Нагадаємо, алгоритм Е. Барейса призначений для обчислення визначника матриці з цілочисельними елементами шляхом приведення її до ступінчастого вигляду за допомогою винятково цілочисельної арифметики. Тут під цілочисельними елементами розуміють як числові, так і символьні значення елементів матриці, в т.ч. й математичні вирази. Будь-яке ділення, що виконує алгоритм, гарантує точне отримання частки без залишку. Алгоритм можна використати для обчислення визначника матриці навіть з (приблизними) дійсними елементами, що вилучає помилки округлення, за винятком помилок, що вже присутні у вхідних даних.

$$\bar{\bar{Q}}_4^{(n+1)}(x)=x\bar{\bar{Q}}_4^{(n)}(x)+\bar{\bar{Q}}_4^{(n-1)}(x);\ \det(\bar{\bar{Q}}_4^{(n)}(x))=(-1)^{n+1}\bar{F}^{(n+1)}(x);\ \bar{\bar{Q}}_4^{(n)}(x)\times\bar{\bar{Q}}_4^{-(n)}(x)=\bar{\bar{I}}_4;$$

$$\bar{\bar{Q}}_4^{(0)}(x)=\bar{\bar{Q}}_4^{(2)}(x)-x\bar{\bar{Q}}_4^{(1)}(x)=\begin{bmatrix} x & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -x \end{bmatrix};\ \det(\bar{\bar{Q}}_4^{(0)}(x))=-x;\ \bar{\bar{Q}}_4^{-(0)}(x)=\begin{bmatrix} 1/x & -1/x & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix};$$

$$\bar{\bar{Q}}_4^{(1)}(x)=\bar{\bar{Q}}_4^{(3)}(x)-x\bar{\bar{Q}}_4^{(2)}(x)=\begin{bmatrix} x^2+1 & x & 0 & 0 \\ 0 & x & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};\ \det(\bar{\bar{Q}}_4^{(1)}(x))=x^3+x;\ \bar{\bar{Q}}_4^{-(1)}(x)=\begin{bmatrix} \dfrac{1}{x^2+1} & \dfrac{-1}{x^2+1} & \dfrac{1}{x^2+1} & 0 \\ 0 & \dfrac{1}{x} & \dfrac{-1}{x} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};$$

$$\bar{\bar{Q}}_4^{(2)}(x)=x\bar{\bar{Q}}_4^{(1)}(x)+\bar{\bar{Q}}_4^{(0)}(x)=\begin{bmatrix} x^3+2x & x^2+1 & 0 & 0 \\ 0 & x^2+1 & x & 0 \\ 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix};\ \det(\bar{\bar{Q}}_4^{(2)}(x))=-(x^5+3x^3+2x);\ \bar{\bar{Q}}_4^{-(2)}(x)=\begin{bmatrix} \dfrac{1}{x^3+2x} & \dfrac{-1}{x^3+2x} & 0 & \dfrac{1}{x^2+2} \\ 0 & \dfrac{1}{x^2+1} & 0 & \dfrac{-x}{x^2+1} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -x \end{bmatrix};$$

$$\bar{\bar{Q}}_4^{(3)}(x)=x\bar{\bar{Q}}_4^{(2)}(x)+\bar{\bar{Q}}_4^{(1)}(x)=\begin{bmatrix} x^4+3x^2+1 & x^3+2x & 0 & 0 \\ 0 & x^3+2x & x^2+1 & 0 \\ 0 & 0 & x^2+1 & x \\ 0 & 0 & x & 1 \end{bmatrix};\ \bar{\bar{Q}}_4^{-(3)}(x)=\begin{bmatrix} \dfrac{1}{x^4+3x^2+1} & \dfrac{-1}{x^4+3x^2+1} & \dfrac{x^2+1}{x^4+3x^2+1} & \dfrac{-(x^3+x)}{x^4+3x^2+1} \\ 0 & \dfrac{1}{x^3+2x} & \dfrac{-(x^2+1)}{x^3+2x} & \dfrac{x^2+1}{x^2+2} \\ 0 & 0 & 1 & -x \\ 0 & 0 & -x & x^2+1 \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_4^{(3)}(x))=x^7+5x^5+7x^3+2x;$$

$$\bar{\bar{Q}}_4^{(4)}(x)=x\bar{\bar{Q}}_4^{(3)}(x)+\bar{\bar{Q}}_4^{(2)}(x)=\begin{bmatrix} x^5+4x^4+3x & x^4+3x^2+1 & 0 & 0 \\ 0 & x^4+3x^2+1 & x^3+2x & 0 \\ 0 & 0 & x^3+2x & x^2+1 \\ 0 & 0 & x^2+1 & x \end{bmatrix};\ \det(\bar{\bar{Q}}_4^{(4)}(x))=-(x^9+7x^7+16x^5+13x^3+3x);$$

$$\bar{\bar{Q}}_4^{-(4)}(x)=\begin{bmatrix} \dfrac{1}{x^5+4x^4+3x} & \dfrac{-1}{x^5+4x^4+3x} & \dfrac{-(x^3+2x)}{x^4+4x^3+3} & \dfrac{x^2+2}{x^2+3} \\ 0 & \dfrac{1}{x^4+3x^2+1} & \dfrac{x^4+2x^2}{x^4+3x^2+1} & \dfrac{-(x^5+3x^3+2x)}{x^4+3x^2+1} \\ 0 & 0 & -x & x^2+1 \\ 0 & 0 & x^2+1 & -(x^3+2x) \end{bmatrix}; \qquad (17)$$

$$\bar{\bar{Q}}_4^{(5)}(x)=x\bar{\bar{Q}}_4^{(4)}(x)+\bar{\bar{Q}}_4^{(3)}(x)=\begin{bmatrix} x^6+5x^4+6x^2+1 & x^5+4x^3+3x & 0 & 0\\ 0 & x^5+4x^3+3x & x^4+3x^2+1 & 0\\ 0 & 0 & x^4+3x^2+1 & x^3+2x\\ 0 & 0 & x^3+2x & x^2+1 \end{bmatrix};\ \det(\bar{\bar{Q}}_4^{(5)}(x))=x^{11}+9x^9+29x^7+40x^5+22x^3+3x;$$

$$\bar{\bar{Q}}_4^{-(5)}(x)=\begin{bmatrix} \dfrac{1}{x^6+5x^4+6x^2+1} & \dfrac{-1}{x^6+5x^4+6x^2+1} & \dfrac{x^6+4x^4+4x^2+1}{x^6+5x^4+6x^2+1} & \dfrac{-(x^7+5x^5+7x^3+2x)}{x^6+5x^4+6x^2+1}\\ 0 & \dfrac{1}{x^5+4x^3+3x} & \dfrac{-(x^4+3x^2+1)}{x^3+3x} & \dfrac{x^6+5x^4+7x^2+2}{x^4+4x^2+3}\\ 0 & 0 & x^2+1 & -(x^3+2x)\\ 0 & 0 & -(x^3+2x) & x^4+3x^2+1 \end{bmatrix};$$

$$\bar{\bar{Q}}_4^{(6)}(x)=x\bar{\bar{Q}}_4^{(5)}(x)+\bar{\bar{Q}}_4^{(4)}(x)=\begin{bmatrix} x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 & 0 & 0\\ 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x & 0\\ 0 & 0 & x^5+4x^3+3x & x^4+3x^2+1\\ 0 & 0 & x^4+3x^2+1 & x^3+2x \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_4^{(6)}(x))=-(x^{13}+11x^{11}+46x^9+91x^7+86x^5+34x^3+4x);$$

$$\bar{\bar{Q}}_4^{-(6)}(x)=\begin{bmatrix} \dfrac{1}{x^7+6x^5+10x^3+4x} & \dfrac{-1}{x^7+6x^5+10x^3+4x} & \dfrac{-(x^5+4x^3+3x)}{x^4+4x^2+2} & \dfrac{x^8+7x^6+16x^4+13x^2+3}{x^7+6x^4+10x^2+4}\\ 0 & \dfrac{1}{x^6+5x^4+6x^2+1} & \dfrac{x^8+6x^6+11x^4+6x^2}{x^6+5x^4+6x^2+1} & \dfrac{-(x^9+7x^7+16x^5+13x^3+3x)}{x^6+5x^4+6x^2+1}\\ 0 & 0 & -(x^3+2x) & x^4+3x^2+1\\ 0 & 0 & x^4+3x^2+1 & -(x^5+4x^3+3x) \end{bmatrix};$$

$$\bar{\bar{Q}}_4^{(7)}(x)=x\bar{\bar{Q}}_4^{(6)}(x)+\bar{\bar{Q}}_4^{(5)}(x)=$$

$$=\begin{bmatrix} x^8+7x^6+15x^4+10x^2+1 & x^7+6x^5+10x^3+4x & 0 & 0\\ 0 & x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 & 0\\ 0 & 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x\\ 0 & 0 & x^5+4x^3+3x & x^4+3x^2+1 \end{bmatrix}=\begin{bmatrix} F^{(9)}(x) & F^{(8)}(x) & 0 & 0\\ 0 & F^{(8)}(x) & F^{(7)}(x) & 0\\ 0 & 0 & F^{(7)}(x) & F^{(6)}(x)\\ 0 & 0 & F^{(6)}(x) & F^{(5)}(x) \end{bmatrix};\qquad (17^*)$$

$$\det(\bar{\bar{Q}}_4^{(7)}(x))=x^{15}+13x^{13}+67x^{11}+174x^9+239x^7+166x^5+50x^3+4x;$$

$$\bar{\bar{Q}}_4^{-(7)}(x)=\begin{bmatrix} \dfrac{1}{F^{(9)}(x)} & \dfrac{-1}{F^{(9)}(x)} & \dfrac{x^{10}+8x^8+22x^6+24x^4+9x^2+1}{F^{(9)}(x)} & \dfrac{-(x^9+8x^7+21x^5+19x^3+3x)}{x^6+6x^4+9x^2+1}\\ 0 & \dfrac{1}{F^{(8)}(x)} & \dfrac{-(x^{10}+8x^8+22x^6+24x^4+9x^2+1)}{F^{(8)}(x)} & \dfrac{x^{10}+9x^9+29x^6+40x^4+22x^2+3}{x^6+6x^4+10x^2+4}\\ 0 & 0 & F^{(5)}(x) & -F^{(6)}(x)\\ 0 & 0 & -F^{(6)}(x) & F^{(7)}(x) \end{bmatrix};$$

$$\bar{\bar{Q}}_4^{(8)}(x)=x\bar{\bar{Q}}_4^{(7)}(x)+\bar{\bar{Q}}_4^{(6)}(x)=$$

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

$$\det(\bar{\bar{Q}}_4^{(8)}(x))=-(x^{17}+15x^{15}+92x^{13}+297x^{11}+541x^9+553x^7+296x^5+70x^3+5x);$$

$$\bar{\bar{Q}}_4^{-(8)}(x)=\begin{bmatrix} \dfrac{1}{F^{(10)}(x)} & \dfrac{-1}{F^{(10)}(x)} & \dfrac{-(x^{12}+10x^{10}+37x^8+62x^6+46x^4+12x^2)}{F^{(10)}(x)} & \dfrac{x^{13}+11x^{11}+46x^9+91x^7+86x^5+34x^3+4x}{F^{(10)}(x)}\\ 0 & \dfrac{1}{F^{(9)}(x)} & \dfrac{-(x^{10}+8x^8+22x^6+24x^4+9x^2+1)}{F^{(7)}(x)} & \dfrac{x^{10}+9x^9+29x^6+40x^4+22x^2+3}{F^{(9)}(x)}\\ 0 & 0 & -F^{(6)}(x) & F^{(7)}(x)\\ 0 & 0 & F^{(7)}(x) & -F^{(6)}(x) \end{bmatrix}.$$

Для обчислення оберненої поліноміальної матриці Фібоначчі 4-го і більших порядків також доводиться використовувати відповідні математичні методи [26], такі як метод Монтанте, метод елімінації Гауса-Джордана (англ. *Gauss-Jordan elimination*), а також за допомогою ад'югованої матриці (англ. *Adjugate matrix*). Наприклад, метод лінійної алгебри Монтанте призначений для розв'язання системи лінійних рівнянь, знаходження обернених матриць та визначників. Метод названо в честь його першовідкривача Рене Маріо Монтанте Пардо (англ. *Rene Mario Montante Pardo*). Його головна особливість – виконує роботу, використовуючи винятково цілочисельну арифметику для цілочисельних і символьних елементів матриць, а також елементів у вигляді математичних виразів, що дає змогу отримувати точні результати в комп'ютерних реалізаціях.

Всі зазначені вище методи та алгоритми детально описано в мережі Інтернет, тому в цьому дослідженні не будемо зосереджувати увагу на їхній роботі.

2.4. ***Механізм утворення послідовності уточнених поліноміальних матриць Фібоначчі* 5*-го порядку***. Розглянемо алгоритм побудови послідовності перших 8-ми поліноміальних $\bar{\bar{Q}}_5^{(\bullet)}(x)$-матриць Фібоначчі 5-го порядку, їхніх визначників і відповідно обернених поліноміальних $\bar{\bar{Q}}_5^{-(\bullet)}(x)$-матриць Фібоначчі. З наведених матричних виразів (18) і (18*) видно, що елементами n-ої поліноміальної $\bar{\bar{Q}}_5^{(n)}(x)$-матриці Фібоначчі є відповідні поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го ($\forall n\in\{3\div 8\}$) з їхньої послідовності (2). Оскільки тут маємо справу з матрицями Фібоначчі 5-го порядку, то для обчислення їхніх визначників і обернених матриць доводиться використовувати спеціальні математичні методи [26].

Отже, розроблено метод генерування послідовності з n-ої кількості уточнених поліноміальних матриць Фібоначчі m-го порядку, елементами яких є поліноми Фі-

боначчі з номерами від (n–2)-го до (m+n–2)-го ($\forall n \in \{3 \div m\}$). Оскільки поліноміальні матриці Фібоначчі часто використовують для реалізації операцій шифрування даних, то для розшифрування даних також потрібно мати аналогічні поліноміальні оберненні матриці, для отримання яких потрібно застосувати загальний підхід. Розроблено ПЗ, яке дає змогу генерувати не тільки послідовності уточнених 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. Справа в тому, що навіть під час генерування 5-ої поліноміальної матриці Фібоначчі 2-го порядку отримуємо поліноми 4-го степеня, утворені внаслідок множення змінної x на 4-ту поліноміальну матрицю, та додати 3-ту матрицю, де знаходяться поліноми дещо нижчих степенів. 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 [26], наприклад алгоритм Барейса (англ. *Bareiss algorithm*) чи формулу Лейбніца (англ. *Leibniz formula*).

Наступна математична проблема, це обчислення оберненої матриці, для вирішення якої також доводиться використовувати відповідні математичні методи [26], такі як метод Монтанте (англ. *Montante method*), метод елімінації Гауса-Джордана (англ. *Gauss-Jordan elimination*) та за допомогою ад'югованої матриці (англ. *Adjugate matrix*).

І остання проблема – уважність запису n-ої поліноміальної матриці Фібоначчі m-го порядку, елементами якої є поліноми Фібоначчі не вище (m+n–2)-го номера, насамперед тих, які стосуються матриць вищих порядків і поліномів більших степенів. Адже запис не того степеня змінної, неправильного значення коефіцієнта при ній чи його знаку – подальша робота даремна.

$$\bar{\bar{Q}}_5^{(n+1)}(x) = x\bar{\bar{Q}}_5^{(n)}(x) + \bar{\bar{Q}}_5^{(n-1)}(x);\ \det(\bar{\bar{Q}}_5^{(n)}(x)) = (-1)^{n-1}\bar{F}^{(n+1)}(x);\ \bar{\bar{Q}}_5^{(n)}(x) \times \bar{\bar{Q}}_5^{-(n)}(x) = \bar{\bar{I}}_5;$$

$$\bar{\bar{Q}}_5^{(0)}(x) = \bar{\bar{Q}}_5^{(2)}(x) - x\bar{\bar{Q}}_5^{(1)}(x) = \begin{bmatrix} x^2+1 & x & 0 & 0 & 0 \\ 0 & x & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -x \end{bmatrix};\ \det(\bar{\bar{Q}}_5^{(0)}(x)) = -(x^3+x);\ \bar{\bar{Q}}_5^{-(0)}(x) = \begin{bmatrix} \frac{1}{x^2+1} & \frac{-1}{x^2+1} & \frac{1}{x^2+1} & 0 & 0 \\ 0 & \frac{1}{x} & \frac{-1}{x} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & x & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix};$$

$$\bar{\bar{Q}}_5^{(1)}(x) = \bar{\bar{Q}}_5^{(3)}(x) - x\bar{\bar{Q}}_5^{(2)}(x) = \begin{bmatrix} x^3+2x & x^2+1 & 0 & 0 & 0 \\ 0 & x^2+1 & x & 0 & 0 \\ 0 & 0 & x & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix};\ \det(\bar{\bar{Q}}_5^{(1)}(x)) = x^6+3x^4+2x^2;\ \bar{\bar{Q}}_5^{-(1)}(x) = \begin{bmatrix} \frac{1}{x^3+2x} & \frac{-1}{x^3+2x} & \frac{1}{x^3+2x} & \frac{-1}{x^3+2x} & 0 \\ 0 & \frac{1}{x^2+1} & \frac{-1}{x^2+1} & \frac{1}{x^2+1} & 0 \\ 0 & 0 & \frac{1}{x} & \frac{-1}{x} & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix};$$

$$\bar{\bar{Q}}_5^{(2)}(x) = x\bar{\bar{Q}}_5^{(1)}(x) + \bar{\bar{Q}}_5^{(0)}(x) = \begin{bmatrix} x^4+3x^2+1 & x^3+2x & 0 & 0 & 0 \\ 0 & x^3+2x & x^2+1 & 0 & 0 \\ 0 & 0 & x^2+1 & x & 0 \\ 0 & 0 & 0 & x & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix};\ \bar{\bar{Q}}_5^{-(2)}(x) = \begin{bmatrix} \frac{1}{x^4+3x^2+1} & \frac{-1}{x^4+3x^2+1} & \frac{1}{x^4+3x^2+1} & 0 & \frac{-x}{x^4+3x^2+1} \\ 0 & \frac{1}{x^3+2x} & \frac{-1}{x^3+2x} & 0 & \frac{1}{x^2+2} \\ 0 & 0 & \frac{1}{x^2+1} & 0 & \frac{-x}{x^2+1} \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -x \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_5^{(2)}(x)) = -(x^9+6x^7+12x^5+9x^3+2x);\qquad \bar{\bar{Q}}_5^{(3)}(x) = x\bar{\bar{Q}}_5^{(2)}(x) + \bar{\bar{Q}}_5^{(1)}(x) =$$

$$= \begin{bmatrix} x^5+4x^3+3x & x^4+3x^2+1 & 0 & 0 & 0 \\ 0 & x^4+3x^2+1 & x^3+2x & 0 & 0 \\ 0 & 0 & x^3+2x & x^2+1 & 0 \\ 0 & 0 & 0 & x^2+1 & x \\ 0 & 0 & 0 & x & 1 \end{bmatrix};\ \bar{\bar{Q}}_5^{-(3)}(x) = \begin{bmatrix} \frac{1}{x^5+4x^3+3x} & \frac{-1}{x^5+4x^3+3x} & \frac{1}{x^5+4x^3+3x} & \frac{-1}{x^3+3x} & \frac{1}{x^2+3} \\ 0 & \frac{1}{x^4+3x^2+1} & \frac{-1}{x^4+3x^2+1} & \frac{x^2+1}{x^4+3x^2+1} & \frac{-x^3-x}{x^4+3x^2+1} \\ 0 & 0 & \frac{1}{x^3+2x} & \frac{-(x^2+1)}{x^3+2x} & \frac{x^2+1}{x^2+2} \\ 0 & 0 & 0 & 1 & -x \\ 0 & 0 & 0 & -x & x^2+1 \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_5^{(3)}(x)) = x^{12}+9x^{10}+30x^8+45x^6+29x^4+6x^2;$$

$$\bar{\bar{Q}}_5^{(4)}(x) = x\bar{\bar{Q}}_5^{(3)}(x) + \bar{\bar{Q}}_5^{(2)}(x) = \begin{bmatrix} x^6+5x^4+6x^2+1 & x^5+4x^3+3x & 0 & 0 & 0 \\ 0 & x^5+4x^3+3x & x^4+3x^2+1 & 0 & 0 \\ 0 & 0 & x^4+3x^2+1 & x^3+2x & 0 \\ 0 & 0 & 0 & x^3+2x & x^2+1 \\ 0 & 0 & 0 & x^2+1 & x \end{bmatrix}; \tag{18}$$

$$\bar{\bar{Q}}_5^{-(4)}(x) = \begin{bmatrix} \frac{1}{x^6+5x^4+6x^2+1} & \frac{-1}{x^6+5x^4+6x^2+1} & \frac{1}{x^6+5x^4+6x^2+1} & \frac{x^4+2x^2}{x^6+5x^4+6x^2+1} & \frac{-(x^5+3x^3+2x)}{x^6+5x^4+6x^2+1} \\ 0 & \frac{1}{x^5+4x^3+3x} & \frac{-1}{x^5+4x^3+3x} & \frac{-(x^3+2x)}{x^4+4x^2+3} & \frac{x^2+2}{x^2+3} \\ 0 & 0 & \frac{1}{x^4+3x^2+1} & \frac{x^4+2x^2}{x^4+3x^2+1} & \frac{-(x^5+3x^3+2x)}{x^4+3x^2+1} \\ 0 & 0 & 0 & -x & x^2+1 \\ 0 & 0 & 0 & x^2+1 & -(x^3+2x) \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_5^{(4)}(x)) = -(x^{15}+12x^{13}+57x^{11}+136x^9+171x^7+109x^5+31x^3+3x);$$

$$\bar{\bar{Q}}_5^{(5)}(x) = x\bar{\bar{Q}}_5^{(4)}(x) + \bar{\bar{Q}}_5^{(3)}(x) =$$

$$= \begin{bmatrix} x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 & 0 & 0 & 0 \\ 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x & 0 & 0 \\ 0 & 0 & x^5+4x^3+3x & x^4+3x^2+1 & 0 \\ 0 & 0 & 0 & x^4+3x^2+1 & x^3+2x \\ 0 & 0 & 0 & x^3+2x & x^2+1 \end{bmatrix} = \begin{bmatrix} F^{(8)}(x) & F^{(7)}(x) & 0 & 0 & 0 \\ 0 & F^{(7)}(x) & F^{(6)}(x) & 0 & 0 \\ 0 & 0 & F^{(6)}(x) & F^{(5)}(x) & 0 \\ 0 & 0 & 0 & F^{(5)}(x) & F^{(4)}(x) \\ 0 & 0 & 0 & F^{(4)}(x) & F^{(3)}(x) \end{bmatrix};$$

$$\bar{\bar{Q}}_5^{-(5)}(x) = \begin{bmatrix} \frac{1}{F^{(8)}(x)} & \frac{-1}{F^{(8)}(x)} & \frac{1}{F^{(8)}(x)} & \frac{-q'_{14}}{F^{(8)}(x)} & \frac{q'_{15}}{F^{(8)}(x)} \\ 0 & \frac{1}{F^{(7)}(x)} & \frac{-1}{F^{(7)}(x)} & \frac{q'_{24}}{F^{(7)}(x)} & \frac{-q'_{25}}{F^{(7)}(x)} \\ 0 & 0 & \frac{1}{F^{(6)}(x)} & \frac{-q'_{34}}{F^{(6)}(x)} & \frac{q'_{35}}{F^{(6)}(x)} \\ 0 & 0 & 0 & F^{(3)}(x) & -F^{(4)}(x) \\ 0 & 0 & 0 & -F^{(4)}(x) & F^{(5)}(x) \end{bmatrix}; \det(\bar{\bar{Q}}_5^{(5)}(x)) = x^{18}+15x^{16}+93x^{14}+308x^{12}+588x^{10}+651x^8+398x^6+ \\ +118x^4+12x^2; \\ q'_{14}=q'_{24}=q'_{34}=x^6+4x^4+4x^2+1; \\ q'_{15}=q'_{25}=q'_{35}=x^7+5x^5+7x^3+2x;$$

$$\bar{\bar{Q}}_5^{(6)}(x) = x\bar{\bar{Q}}_5^{(5)}(x) + \bar{\bar{Q}}_5^{(4)}(x) =$$

$$= \begin{bmatrix} x^8+7x^6+15x^4+10x^2+1 & x^7+6x^5+10x^3+4x & 0 & 0 & 0 \\ 0 & x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 & 0 & 0 \\ 0 & 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x & 0 \\ 0 & 0 & 0 & x^5+4x^3+3x & x^4+3x^2+1 \\ 0 & 0 & 0 & x^4+3x^2+1 & x^3+2x \end{bmatrix} =$$

$$= \begin{bmatrix} F^{(9)}(x) & F^{(8)}(x) & 0 & 0 & 0 \\ 0 & F^{(8)}(x) & F^{(7)}(x) & 0 & 0 \\ 0 & 0 & F^{(7)}(x) & F^{(6)}(x) & 0 \\ 0 & 0 & 0 & F^{(6)}(x) & F^{(5)}(x) \\ 0 & 0 & 0 & F^{(5)}(x) & F^{(4)}(x) \end{bmatrix}; \bar{\bar{Q}}_5^{-(6)}(x) = \begin{bmatrix} \frac{1}{F^{(9)}(x)} & \frac{-1}{F^{(9)}(x)} & \frac{1}{F^{(9)}(x)} & \frac{q'_{14}}{F^{(9)}(x)} & \frac{-q'_{15}}{F^{(9)}(x)} \\ 0 & \frac{1}{F^{(8)}(x)} & \frac{-1}{F^{(8)}(x)} & \frac{-q'_{24}}{F^{(8)}(x)} & \frac{q'_{25}}{F^{(8)}(x)} \\ 0 & 0 & \frac{1}{F^{(7)}(x)} & \frac{q'_{34}}{F^{(7)}(x)} & \frac{-q'_{35}}{F^{(7)}(x)} \\ 0 & 0 & 0 & -F^{(4)}(x) & F^{(5)}(x) \\ 0 & 0 & 0 & F^{(5)}(x) & -F^{(6)}(x) \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_5^{(6)}(x)) = -(x^{21}+18x^{19}+138x^{17}+588x^{15}+1524x^{13}+2472x^{11}+2488x^9+1489x^7+486x^5+74x^3+4x);$$

$$q'_{14}=q'_{24}=q'_{34}=x^8+6x^6+11x^4+6x^2; q'_{15}=q'_{25}=q'_{35}=x^9+7x^7+16x^5+13x^3+3x;$$

$$\bar{\bar{Q}}_5^{(7)}(x) = x\bar{\bar{Q}}_5^{(6)}(x) + \bar{\bar{Q}}_5^{(5)}(x) =$$

$$= \begin{bmatrix} x^9+8x^7+21x^5+20x^3+5x & x^8+7x^6+15x^4+10x^2+1 & 0 & 0 & 0 \\ 0 & x^8+7x^6+15x^4+10x^2+1 & x^7+6x^5+10x^3+4x & 0 & 0 \\ 0 & 0 & x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 & 0 \\ 0 & 0 & 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x \\ 0 & 0 & 0 & x^5+4x^3+3x & x^4+3x^2+1 \end{bmatrix} =$$

$$= \begin{bmatrix} F^{(10)}(x) & F^{(9)}(x) & 0 & 0 & 0 \\ 0 & F^{(9)}(x) & F^{(8)}(x) & 0 & 0 \\ 0 & 0 & F^{(8)}(x) & F^{(7)}(x) & 0 \\ 0 & 0 & 0 & F^{(7)}(x) & F^{(6)}(x) \\ 0 & 0 & 0 & F^{(6)}(x) & F^{(5)}(x) \end{bmatrix}; \bar{\bar{Q}}_5^{-(7)}(x) = \begin{bmatrix} \frac{1}{F^{(10)}(x)} & \frac{-1}{F^{(10)}(x)} & \frac{1}{F^{(10)}(x)} & \frac{-q'_{14}}{F^{(10)}(x)} & \frac{q'_{15}}{F^{(10)}(x)} \\ 0 & \frac{1}{F^{(9)}(x)} & \frac{-1}{F^{(9)}(x)} & \frac{q'_{24}}{F^{(9)}(x)} & \frac{-q'_{25}}{F^{(9)}(x)} \\ 0 & 0 & \frac{1}{F^{(8)}(x)} & \frac{-q'_{34}}{F^{(8)}(x)} & \frac{q'_{35}}{F^{(8)}(x)} \\ 0 & 0 & 0 & F^{(5)}(x) & -F^{(6)}(x) \\ 0 & 0 & 0 & -F^{(6)}(x) & F^{(7)}(x) \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_5^{(7)}(x)) = x^{24}+21x^{22}+192x^{20}+1003x^{18}+3303x^{16}+7137x^{14}+10212x^{12}+9540x^{10}+5597x^8+1914x^6+330x^4+20x^2; \quad (18^*)$$

$$q'_{14}=q'_{24}=q'_{34}=x^{10}+8x^8+22x^6+24x^4+9x^2+1; \; q'_{15}=q'_{25}=q'_{35}=x^{11}+9x^9+29x^7+40x^5+22x^3+3x;$$

$$\bar{\bar{Q}}_5^{(8)}(x) = x\bar{\bar{Q}}_5^{(7)}(x) + \bar{\bar{Q}}_5^{(6)}(x) =$$

$$= \begin{bmatrix} x^{10}+9x^8+28x^6+35x^4+15x^2+1 & x^9+8x^7+21x^5+20x^3+5x & 0 & 0 & 0 \\ 0 & x^9+8x^7+21x^5+20x^3+5x & x^8+7x^6+15x^4+10x^2+1 & 0 & 0 \\ 0 & 0 & x^8+7x^6+15x^4+10x^2+1 & x^7+6x^5+10x^3+4x & 0 \\ 0 & 0 & 0 & x^7+6x^5+10x^3+4x & x^6+5x^4+6x^2+1 \\ 0 & 0 & 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x \end{bmatrix} =$$

$$= \begin{bmatrix} F^{(11)}(x) & F^{(10)}(x) & 0 & 0 & 0 \\ 0 & F^{(10)}(x) & F^{(9)}(x) & 0 & 0 \\ 0 & 0 & F^{(9)}(x) & F^{(8)}(x) & 0 \\ 0 & 0 & 0 & F^{(8)}(x) & F^{(7)}(x) \\ 0 & 0 & 0 & F^{(7)}(x) & F^{(6)}(x) \end{bmatrix}; \bar{\bar{Q}}_5^{-(8)}(x) = \begin{bmatrix} \frac{1}{F^{(11)}(x)} & \frac{-1}{F^{(11)}(x)} & \frac{1}{F^{(11)}(x)} & \frac{q'_{14}}{F^{(11)}(x)} & \frac{-q'_{15}}{F^{(11)}(x)} \\ 0 & \frac{1}{F^{(10)}(x)} & \frac{-1}{F^{(10)}(x)} & \frac{-q'_{24}}{F^{(10)}(x)} & \frac{q'_{25}}{F^{(10)}(x)} \\ 0 & 0 & \frac{1}{F^{(9)}(x)} & \frac{q'_{34}}{F^{(9)}(x)} & \frac{-q'_{35}}{F^{(9)}(x)} \\ 0 & 0 & 0 & -F^{(6)}(x) & F^{(7)}(x) \\ 0 & 0 & 0 & F^{(7)}(x) & -F^{(8)}(x) \end{bmatrix};$$

$$\det(\bar{\bar{Q}}_5^{(8)}(x)) = -(x^{27}+24x^{25}+255x^{23}+1580x^{21}+6330x^{19}+17184x^{17}+32211x^{15}+41700x^{13}+36690x^{11}+21201x^9+7583x^7+1521x^5+ \\ +145x^3+5x); \; q'_{14}=q'_{24}=q'_{34}=x^{12}+10x^{10}+37x^8+62x^6+46x^4+12x^2; q'_{15}=q'_{25}=q'_{35}=x^{13}+11x^{11}+46x^9+91x^7+86x^5+34x^3+4x;$$

3. Метод шифрування блокових даних уточненими поліноміальними матрицями Фібоначчі. Розглянемо особливості реалізації матричного методу шифрування блокових даних [22, 32, 46], ключем шифрування якого будуть уточнені поліноміальні матриці Фібоначчі m-го порядку. Щоб реалізувати 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 у матриці – рядками чи стовпцями [8], а чи зробити початкову перестановку елементів [28, 30], тому відправнику та одержувачу повідомлення залишається визначати розташування елементів у вхідній матриці. Наприклад, вхідне повідомлення "*Рідний_край_–_земний_рай.*" можна подати матрицею 5-го порядку, заповнюючи її поелементно рядками, паралельно вказуючи їхні числові значення згідно з таблицею кодів символів ASCII:

$$\overline{\overline{M}} = \begin{bmatrix} P & i & д & н & и \\ й & _ & к & р & а \\ й & _ & – & _ & з \\ е & м & н & и & й \\ _ & р & а & й & ! \end{bmatrix} \Rightarrow \begin{bmatrix} 208 & 179 & 228 & 237 & 232 \\ 233 & 95 & 234 & 240 & 224 \\ 233 & 95 & 150 & 95 & 231 \\ 229 & 236 & 237 & 232 & 233 \\ 95 & 240 & 224 & 233 & 33 \end{bmatrix}.$$

Після узгодження між відправником і одержувачем елементів ключа, а саме – цілого числа $x \neq 0$ та n-ої уточненої поліноміальної матриці Фібоначчі m-го порядку, відповідну матрицю шифрування даних вибирають з виразів (13), (16), (17) чи (18), наведених вище. Потім цю матрицю потрібно помножити справа на матрицю вхідного повідомлення $\overline{\overline{M}}$, щоб отримати матрицю зашифрованого повідомлення $\overline{\overline{E}}$. Наприклад, для $m = 5$, $n = 5$ та $x = 5$ отримаємо такі значення як поліномів Фібоначчі, визначника матриці та деякі елементи оберненої матриці:

$$F^{(3)}(x) = x^2 + 1; \qquad F^{(3)}(5) = 26;$$
$$F^{(4)}(x) = x^3 + 2x; \qquad F^{(4)}(5) = 135;$$
$$F^{(5)}(x) = x^4 + 3x^2 + 1; \qquad F^{(5)}(5) = 701;$$
$$F^{(6)}(x) = x^5 + 4x^3 + 3x; \qquad F^{(6)}(5) = 3640;$$
$$F^{(7)}(x) = x^6 + 5x^4 + 6x^2 + 1; \qquad F^{(7)}(5) = 18901;$$
$$F^{(8)}(x) = x^7 + 6x^5 + 10x^3 + 4x; \qquad F^{(8)}(5) = 98145;$$
$$\det(\overline{\overline{Q}}_5^{(5)}(x)) = x^{18} + 15x^{16} + 93x^{14} + 308x^{12} + 588x^{10} + 651x^8 + 398x^6 + 118x^4 + 12x^2;$$
$$\det(\overline{\overline{Q}}_5^{(5)}(5)) = 6752340667787;$$
$$q'_{14} = q'_{24} = q'_{34} = x^6 + 4x^4 + 4x^2 + 1 = 18226;$$
$$q'_{15} = q'_{25} = q'_{35} = x^7 + 5x^5 + 7x^3 + 2x = 94635.$$

Маючи вівдповідні значення поліномів Фібоначчі, підставляємо їх у 5-ту поліноміальну матрицю Фібоначчі 5-го порядку, внаслідок чого отримаємо такі значення її елементів:

$$\overline{\overline{Q}}_5^{(5)}(x) = \begin{bmatrix} F^{(8)}(x) & F^{(7)}(x) & 0 & 0 & 0 \\ 0 & F^{(7)}(x) & F^{(6)}(x) & 0 & 0 \\ 0 & 0 & F^{(6)}(x) & F^{(5)}(x) & 0 \\ 0 & 0 & 0 & F^{(5)}(x) & F^{(4)}(x) \\ 0 & 0 & 0 & F^{(4)}(x) & F^{(3)}(x) \end{bmatrix};$$

$$\overline{\overline{Q}}_5^{(5)}(5) = \begin{bmatrix} 98145 & 18901 & 0 & 0 & 0 \\ 0 & 18901 & 3640 & 0 & 0 \\ 0 & 0 & 3640 & 701 & 0 \\ 0 & 0 & 0 & 701 & 135 \\ 0 & 0 & 0 & 135 & 26 \end{bmatrix}.$$

Тепер, обчислюючи відповідний матричний вираз, отримаємо зашифроване повідомлення, а саме:

$$\overline{\overline{E}} = \overline{\overline{Q}}_5^{(5)}(5) \times \overline{\overline{M}} =$$
$$= \begin{bmatrix} 98145 & 18901 & 0 & 0 & 0 \\ 0 & 18901 & 3640 & 0 & 0 \\ 0 & 0 & 3640 & 701 & 0 \\ 0 & 0 & 0 & 701 & 135 \\ 0 & 0 & 0 & 135 & 26 \end{bmatrix} \times \begin{bmatrix} 208 & 179 & 228 & 237 & 232 \\ 233 & 95 & 234 & 240 & 224 \\ 233 & 95 & 150 & 95 & 231 \\ 229 & 236 & 237 & 232 & 233 \\ 95 & 240 & 224 & 233 & 33 \end{bmatrix} =$$
$$= \begin{bmatrix} 24818093 & 19363550 & 26799894 & 27796605 & 27003464 \\ 5252053 & 2141395 & 4968834 & 4882040 & 5074664 \\ 1008649 & 511236 & 712137 & 508432 & 1004173 \\ 173354 & 197836 & 196377 & 194087 & 167788 \\ 33385 & 38100 & 37819 & 37378 & 32313 \end{bmatrix}.$$

Елементи матриці зашифрованого повідомлення $\overline{\overline{E}}$ відправник надсилає одержувачу каналом зв'язку рядками в порядку e_1, e_2, ..., e_{25}, за якими слідує окремо значення її визначника $\det(\overline{\overline{Q}}_5^{(5)}(5)) = 6752340667787$.

Припускаючи, що передана послідовність чисел отримана без помилок, тоді одержувач, шляхом множення оберненої $\overline{\overline{Q}}_5^{-(5)}(5)$ -матриці Фібоначчі на матрицю зашифрованого повідомлення $\overline{\overline{E}}$, отримує початкову матрицю повідомлення, а саме:

$$\overline{\overline{Q}}_5^{-(5)}(x) = \begin{bmatrix} \frac{1}{F^{(8)}(x)} & \frac{-1}{F^{(8)}(x)} & \frac{1}{F^{(8)}(x)} & \frac{-q'_{14}}{F^{(8)}(x)} & \frac{q'_{15}}{F^{(8)}(x)} \\ 0 & \frac{1}{F^{(7)}(x)} & \frac{-1}{F^{(7)}(x)} & \frac{q'_{24}}{F^{(7)}(x)} & \frac{-q'_{25}}{F^{(7)}(x)} \\ 0 & 0 & \frac{1}{F^{(6)}(x)} & \frac{-q'_{34}}{F^{(6)}(x)} & \frac{q'_{35}}{F^{(6)}(x)} \\ 0 & 0 & 0 & F^{(3)}(x) & -F^{(4)}(x) \\ 0 & 0 & 0 & -F^{(4)}(x) & F^{(5)}(x) \end{bmatrix};$$

$$\overline{\overline{Q}}_5^{-(5)}(5) = \begin{bmatrix} 0{,}000010 & -0{,}000010 & 0{,}000010 & -0{,}185705 & 0{,}964237 \\ 0 & 0{,}0000053 & -0{,}000053 & 0{,}964288 & -0{,}5006878 \\ 0 & 0 & 0{,}000275 & -5{,}007143 & 25{,}998626 \\ 0 & 0 & 0 & 26 & -135 \\ 0 & 0 & 0 & -135 & 701 \end{bmatrix}.$$

$$\overline{\overline{M}} = \overline{\overline{Q}}_5^{-(5)}(5) \times \overline{\overline{E}} =$$
$$= \begin{bmatrix} 0{,}000010 & -0{,}000010 & 0{,}000010 & -0{,}185705 & 0{,}964237 \\ 0 & 0{,}0000053 & -0{,}000053 & 0{,}964288 & -0{,}5006878 \\ 0 & 0 & 0{,}000275 & -5{,}007143 & 25{,}998626 \\ 0 & 0 & 0 & 26 & -135 \\ 0 & 0 & 0 & -135 & 701 \end{bmatrix} \times$$
$$\times \begin{bmatrix} 24818093 & 19363550 & 26799894 & 27796605 & 27003464 \\ 5252053 & 2141395 & 4968834 & 4882040 & 5074664 \\ 1008649 & 511236 & 712137 & 508432 & 1004173 \\ 173354 & 197836 & 196377 & 194087 & 167788 \\ 33385 & 38100 & 37819 & 37378 & 32313 \end{bmatrix} =$$
$$= \begin{bmatrix} 208 & 179 & 228 & 237 & 232 \\ 233 & 95 & 234 & 240 & 224 \\ 233 & 95 & 150 & 95 & 231 \\ 229 & 236 & 237 & 232 & 233 \\ 95 & 240 & 224 & 233 & 33 \end{bmatrix} \Rightarrow \begin{bmatrix} P & i & д & н & и \\ й & _ & к & р & а \\ й & _ & – & _ & з \\ е & м & н & и & й \\ _ & р & а & й & ! \end{bmatrix}.$$

З огляду на викладене вище, констатуємо факт результативної реалізації матричного методу шифрування блокових даних на підставі ключа у вигляді уточненої поліноміальної матриці Фібоначчі, в якому для матриці вхідного повідомлення над алфавітом {0, 1,..., 255} і для цілого числа $x = 5$ використано $\overline{\overline{Q}}_5^{(5)}(5)$ -матрицю Фібоначчі 5-го порядку, елементами якої є поліноми Фібоначчі від 2-го до 7-го степеня. Для отримання визначника матриці використано алгоритм Барейса (англ. *Bareiss algorithm*), а для знаходження оберненої матриці застосовано метод Монтанте (англ. *Montante method*).

Отже, показана можливість вирішення проблеми генерування ключів для шифрування блокових даних у вигляді n-ої послідовності уточнених поліноміальних

матриць Фібоначчі m-го порядку, елементами яких є поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го. Традиційний метод генерування таких матриць використовує матричне рекурентне співвідношення, аналогічне рекурентному співвідношенню для генерування чисел Фібоначчі, а за отриманими матрицями можна знаходити як їхні визначники, так і обернені матриці відповідного порядку.

Виявлено, що запропонована структура елементів n-ої послідовності поліноміальних матриць Фібоначчі m-го порядку має цікаву властивість, згідно з якою можна уникнути використання рекурентного матричного співвідношення, а генерувати відповідні уточнені поліноміальні матриці Фібоначчі тільки за номерами (m+n–2–j)-ої послідовності поліномів Фібоначчі, конкретні значення яких залежать від місця їхнього розташування в матриці та номера її стовпця, а саме $\forall j \in [0 \div (m-1)]$. На конкретному прикладі показана особливість застосування матричного методу шифрування блокових даних з використанням 5-ої поліноміальної матриці Фібоначчі 5-го порядку.

Обговорення результатів дослідження. У математиці поліноміальні матриці Фібоначчі – це поліноміальна послідовність матриць різного порядку, елементами яких є відповідні поліноми Фібоначчі з певної їхньої послідовності [62]. Водночас, різні результати дослідження послідовностей таких поліноміальних матриць під загальною назвою поліноміальні матриці Фібоначчі трапляються в науковій літературі хоча і давно, позаяк тісно пов'язані між собою, проте вони не так широко досліджені, як відповідні послідовності поліномів Фібоначчі. Застосування ж таких поліноміальних матриць з'являються в різних областях знань, в тому числі й для шифрування блокових даних, насамперед матричним методом.

У роботі [1] наведено нові результати для двох узагальнених класів поліномів Фібоначчі та Лукаса, а також особливості їх використання у скороченні деяких радикалів. Автори вважають, що вони розробили нові формули для обчислення зв'язків між двома узагальненими класами поліномів Фібоначчі та Лукаса. Вказано, що гіпергеометричні функції виду ${}_2F_1(z)$ входять до всіх коефіцієнтів зв'язку для конкретного значення z. Дедекілька нових формул зв'язку між деякими відомими поліномами, такими як поліноми Фібоначчі, Лукаса, Пелла, Ферма, Пелля–Лукаса та Ферма–Лукаса, вони вивели як окремі випадки похідних формул зв'язку. Деякі з наведених авторами формул також узагальнюють деякі з відомих у наявній літературі. Як можливість застосування двох похідних формул зв'язку наведено деякі нові формули, що зв'язують деякі відомі числа, а також виведено нові формули для певних зважених інтегралів. На підставі використання двох узагальнених класів поліномів Фібоначчі та Лукаса розроблено нові формули зведення деяких парних і непарних радикалів.

У роботі [19] 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 [27] наведено тотожності Фібоначчі та Лукаса, отримані з матриць Тепліца–Гессенберга. Автори розглянули визначники для деяких сімейств матриць Тепліца–Гессенберга, що мають різні подання чисел Фібоначчі та Лукаса для ненульових елементів. Формули цих визначників можна також подати як тотожності, що містять суми добутків чисел Фібоначчі та Лукаса, а також їхніх мультиноміальних коефіцієнтів. У дослідженні наведено результат комбінаторного доведення декількох визначників, які використовують знакозмінні інволюції та визначення визначника як суми зі знаком над симетричною групою. Це призвело до загального узагальнення формул Фібоначчі та Лукаса в термінах так званих чисел Гібоначчі.

У роботі [44] наведено новий метод шифрування даних з використанням Q-матриць Фібоначчі, заснований на матрицях заблокованих повідомлень. Головною перевагою такого методу є шифрування кожної матриці вхідного повідомлення ключами різної величини [36]. Як стверджують автори, такий підхід не тільки підвищує безпеку зашифрованих повідомлень від криптографічних атак, але й має високу коригувальну здатність, однак не вказують, як саме це забезпечується.

У роботі [9] запропоновано нову теорію шифрування даних з використанням m-розширення p-чисел Фібоначчі. Автори навели квадратну $G_{p,m}$-матрицю Фібоначчі, де $p \geq 0$ є цілим невід'ємним числом і $m>0$. Також описали різні властивості $G_{p,m}$-матриці, яка є основою теорії шифрування даних, встановили зв'язки між елементами цієї матриці для різних значень p і m. Вони показали, що співвідношення між елементами $G_{p,m}$-матриці для різних значень p і $m = 1$ збігаються з відношенням між елементами матриці шифрування для різних значень числа p [7]. Загалом, достовірність запропонованого методу зростає зі збільшенням цього значення, але вона не залежить від значення m.

У роботі [62] розроблено матрицю Фібоначчі, наведено узагальнення формули Кассіні та нову теорію шифрування даних. Автори розглядали новий клас квадратних матриць розміром $(p+1)\times(p+1)$, елементами яких були p-числа Фібоначчі (p = 0, 1, 2, 3, …), а їхній визначник становить ±1. Ця унікальна властивість матриць Фібоначчі приводить до узагальнення формули Кассіні. Запропонований оригінальний метод шифрування даних числами Фібоначчі випливає з аналогічних матриць n-порядку. На відміну від класичних надлишкових кодів основною особливістю запропонованого методу є те, що він дає змогу коригувати зашифровані елементи матриці, які теоретично можуть бути необмеженими цілими числами. Для найпростішого випадку коригувальна здатність цього методу становить 93,33 %, що значно перевищує відомі коригувальні можливості інших методів.

У роботі [53] розглянуто узагальнені співвідношення між елементами матриці шифрування даних, запропоновано нову комплексну $H_{p,n}$-матрицю Фібоначчі, елементами якої є відповідні числа. Розроблено метод шифрування даних, що випливає з цієї комплексної $H_{p,n}$-матриці Фібоначчі, а також встановлено зв'язки між її елементами. Запропоновано підхід до виявлення та виправлення помилок у зашифрованих повідомленнях, що ґрунтується на потребі розв'язування діофантових рівнянь.

У роботі [22] розроблено метод шифрування даних на підставі поліномів Фібоначчі з можливістю виявлення та виправлення помилок у зашифрованих повідом-

леннях. Для цілих чисел $m \geq 2$, $x \geq 1$ і $n \geq 1$ розроблено Q_m^n-матрицю n-го степеня розміром $m \geq m$, яку названо $Q_m^n(x)$-матрицю шифрування даних, елементами якої є поліноми Фібоначчі. Для дешифрування даних автори наводять обернену $Q_m^{-n}(x)$-матрицю, особливість якої у тому, що їхній визначник становить ±1. Наведено простий критерій виявлення помилок і відповідний метод їх виправлення для цього класу матриць. Також показано, що ймовірність появи помилок у зашифрованих повідомленнях майже нульова за досить великих значень m. Наведено наочні приклади шифрування даних, а також різні випадки виявлення та виправлення помилок у зашифрованих повідомленнях.

У роботі [20] розроблено новий метод шифрування даних на підставі поліномів Фібоначчі з високою швидкістю їх генерування. Для цілих чисел m, n і $x \geq 1$ можна згенерувати квадратну $Q_{2m}^n(x)$-матрицю n-го степеня $2m$-го порядку, елементами якої є поліноми Фібоначчі, і відповідну обернену $Q_{2m}^{-n}(x)$-матрицю для їх дешифрування [35, 36]. Також показано, що швидкість шифрування даних за допомогою цих матриць значно вища, ніж з оригінальними матрицями на підставі звичайних чисел Фібоначчі.

У роботі [50] запропоновано нову теорію шифрування даних на ($h(x)$, $g(y)$)-розширенні поліномів p-числами Фібоначчі. Визначено також золоті (p, $h(x)$, $g(y)$)-пропорції, де $p \geq 0$ – цілі числа, $h(x) > 0$, $g(y) > 0$ – поліноми з дійсними коефіцієнтами. Встановлено, що співвідношення між елементами квадратної $G_{p,h,g}$-матриці Фібоначчі повністю збігаються зі співвідношеннями між елементами матриці шифрування для різних значень p і поліномів $h(x) = m$ і $g(y) = t$ [10]. Також співвідношення між елементами матриці шифрування для поліномів $h(x) = 1$ і $g(y) = 1$ збігаються з узагальненими співвідношеннями між елементами матриці шифрування числами Фібоначчі [7]. Завдяки відповідному вибору початкових членів у ($h(x)$, $g(y)$)-розширенні поліномів p-числами Фібоначчі квадратну $G_{p,h,g}$-матрицю можна застосувати для шифрування даних різної величини. Під час обговорення результатів дослідження автори стверджують, що достовірність їхнього методу зростає зі збільшенням значення p, але вона не залежить від значень поліномів $h(x)$ і $g(y)$, які значно підвищують криптографічну стійкість зашифрованих повідомлень [28]. Встановлено, що складність цього методу зростає зі збільшенням степеня поліномів $h(x)$ і $g(y)$. Також знайдено зв'язок між золотою (p, $h(x)$, $g(y)$)-пропорцією, між золотою (p, $h(x)$)-пропорцією та між золотою p-пропорцією.

У роботі [54] 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 обніну ключами та забезпечує великий простір їхнього генерування.

У роботі [18] розглянуто особливості супершифрування даних з матрицями та графіками Пелла-Лукаса через перетворення Лапласа. Автори пропонують новий метод шифрування даних під назвою багатофазне шифрування (англ. *Multiphase Encryption*). Цей метод шифрує вхідні дані дедекілька разів за допомогою різних потужних алгоритмів шифрування на кожному етапі. Метод багатофазного шифрування використовує властивості дерев теорії графів, матриць Пелла-Лукаса та шифру Віженера, що значно підвищує криптографічну стійкість алгоритму шифрування. Нову методику супершифрування даних з використанням перетворень Лапласа через числа Фібоначчі, використовуючи властивості дерев теорії графів за допомогою шифру Бофорта (англ. *Beaufort Cipher*), часто застосовують для шифрування простого тексту, який є більш безпечним, ніж симетрична криптосистема, оскільки звичайний текст можна зашифрувати у багато шарів.

У роботі [70] 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.

Внаслідок обговорення результатів дослідження стосовно наявних підходів до генерування послідовності поліноміальних матриць Фібоначчі різних модифікацій, а також можливостей 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 не наведено приклади їхнього конкретного вигляду, однак доведено доцільність їх використання для шифрування блокових даних. Водночас було з'ясовано, що як окрему процедуру захисту блокових даних поліноміальними матрицями Фібоначчі в теорії та практиці криптографії практично не використовують. Тому проведене нами дослідження щодо розроблення ефективного методу генерування послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, наведення робочих прикладів їхнього конкретного вигляду, а також встановлення певних особливостей їхнього використання для шифрування блокових даних тільки як локального методу є частковим вирішенням цієї актуаль-

ної 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 ключів для шифрування блокових даних у вигляді n-ої послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, структура елементів яких містить m+1 поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го, який, на відміну від відомих методів, використовує матричне рекурентне співвідношення, аналогічне рекурентному співвідношенню для генерування чисел Фібоначчі, а за отриманими матрицями Фібоначчі можна знаходити як їхні визначники, так і обернені матриці відповідного порядку.

Практична значущість результатів дослідження – розроблений метод генерування послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, елементами яких є поліноми Фібоначчі відповідних номерів, а також запропоновані методи знаходження їхніх 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 ключів для шифрування блокових даних у вигляді n-ої послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, структура елементів яких міститиме значну кількість поліномів Фібоначчі з номерами від (n–2)-го до (m+n–2)-го, а отримані матриці дадуть можливість знаходити як їхні визначники, так і обернені матриці, що сукупно уможливить їхнє застосування у матричному методі 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 уточнених поліноміальних матриць Фібоначчі m-го порядку як 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 блокових даних. Водночас, застосування поліноміальних матриць Фібоначчі як окремої процедури для захисту блокових даних у теорії та практиці криптографії трапляється вкрай рідко.

2. Проведений аналіз послідовності поліноміальних матриць Фібоначчі від 2-го до 5-го порядків показав, що традиційний підхід до формування структури елементів таких матриць має деякі недоліки, один з яких стосується кількості (k) різних її елементів, якими є поліноми Фібоначчі не вище (n–1)-го степеня. Наприклад, для матриць Фібоначчі будь-якого порядку (m) таких різних поліномів Фібоначчі буде всього $k = 3$, структура яких залежатиме тільки від номера (n) послідовності поліноміальної матриці Фібоначчі. Така незначна їх кількість є не тільки малоінформативною та прозорою для криптоаналітика, але й не стійкою щодо криптоаналізу. Було прийнято рішення щодо уточнення структури елементів поліноміальних матриць Фібоначчі, кількість яких мала б залежати насамперед від їхнього порядку, а саме $k = m + 1$.

3. Розроблено метод генерування n-ої послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, елементами яких є поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го, 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 уточнених 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, якими є відповідні поліноми Фібоначчі, додавання елементів утвореної матриці до елементів попередньої матриці, після чого у кожному з її утворених елементів групують усі схожі доданки.

4. Наведено механізми утворення послідовності з 8-ми поліноміальних матриць Фібоначчі від 2-го до і 5-го порядків, елементами яких стали поліноми Фібоначчі з номерами від (n–2)-го до (m+n–2)-го ($\forall n \in \{3 \div 8\}$), що дало змогу проаналізувати не тільки особливості їхньої побудови загалом, але й усвідомити процедури знаходження їхніх визначників і обернених матриць зокрема. Розроблено ПЗ, яке дає змогу генерувати як послідовності уточнених поліноміальних матриць Фібоначчі m-го порядку, так і знаходити їхні визначники та обернені поліноміальні матриці аналогічного порядку.

5. Виявлено, що запропонована структура елементів n-ої послідовності поліноміальних матриць Фібоначчі m-го порядку має цікаву властивість, згідно з якою можна уникнути використання рекурентного матричного співвідношення, а генерувати відповідні поліноміальні матриці Фібоначчі тільки за номерами (m+n–2–j)-ої послідовності поліномів Фібоначчі, конкретні значення яких залежать від місця їхнього розташування в матриці та номера її стовпця, а саме $\forall j \in [0 \div (m-1)]$.

6. Наведено приклад застосування матричного методу шифрування блокових даних уточненою поліноміальною матрицею Фібоначчі, що дає змогу зацікавленому читачу зрозуміти основний принцип шифрування як початкового повідомлення, так і розшифрування зашифрованих даних. У наведеному прикладі для матриці вхідного повідомлення над алфавітом {0, 1,..., 255} і для цілого числа $x = 5$ використано 5-ту поліноміальну матрицю Фібоначчі 5-го порядку, елементами якої є поліноми Фібоначчі від 2-го до 7-го степеня. Для отримання визначника матриці використано формулу Лейбніца, а для знаходження оберненої матриці застосовано метод Монтанте (англ. *Montante method*).

7. За результатами виконаного дослідження зроблено обґрунтовані висновки та надано відповідні рекомендації щодо їх практичного використання як ключів для шифрування блокових даних, що дає змогу ефективно передавати каналами зв'язку відповідні повідомлення різної величини.

References

1. Abd-Elhameed, Waleed Mohamed, Philippou, Andreas N., & Zeyada, Nasr Anwer. (2022). Novel Results for Two Generalized

Classes of Fibonacci and Lucas Polynomials and Their Uses in the Reduction of Some Radicals. *Mathematics*, 10(7), article ID 2342. https://doi.org/10.3390/math10132342
2. 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
3. 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
4. Ashok, G., Ashok Kumar, S., Chaya Kumari, D., & Ramakrishna, M. (2022). A type of public cryptosystem using polynomials and pell sequences. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(7), 1951–1963. https://doi.org/10.1080/09720529.2022.2133237
5. Ashok, Gudela, Sadasivuni, Ashok Kumar, & Kumari, Dushma. (2023, August). An Approach of Cryptosystem using Polynomials and Lucas Numbers. *Journal of Harbin Engineering University*, 44(8), 25–31. URL: https://www.researchgate.net/publication/372991199_An_Approach_of_Cryptosystem_using_Polynomials_and_Lucas_Numbers
6. Basin, S. L. (1963). The Appearance of Fibonacci Numbers and the Q Matrix in Electrical Network Theory. *Mathematics Magazine*, 36(2), 84–97. https://doi.org/10.2307/2688890
7. 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
8. 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
9. Basu, Manjusri, & Prasad, Bandhu. (2009, November). Coding theory on the *m*-extension of the Fibonacci *p*-numbers. *Chaos, Solitons, & Fractals*, Vol. 42, issue 4, 30, 2522–2530. https://doi.org/10.1016/j.chaos.2009.03.197
10. 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
11. Bednar, Urszula, & Wołowiec-Musiał, Małgorzata. (2020). Distance Fibonacci Polynomials. *Symmetry*, 12(3), 1540 p. https://doi.org/10.3390/sym12091540
12. Berg, Christian. (2011). Fibonacci numbers and orthogonal polynomials. *Arab Journal of Mathematical Sciences*, Vol. 17, 75–88. https://doi.org/10.1016/j.ajmsc.2011.01.001
13. 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
14. 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
15. Catalani, M. (2004). Some formulae for Bivariate Fibonacci and Lucas polynomials. arXiv:math/0406323. Combinatorics. https://doi.org/10.48550/arXiv.math/0406323
16. 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
17. Cheon, G. S., Kim, H., & Shapiro, L. W. (2009). A generalization of Lucas polynomial sequence. *Discrete Applied Mathematics*, Vol. 157, no. 5, 920–927. https://doi.org/10.1016/j.dam.2008.03.034
18. Domada, Triveni, Sadasivuni, Ashok Kumar, Ashok, Gudela, & Kumari, Dushma. (2023, August). Super-Encryption with Pell-Lucas Matrices and Graphs via Laplace Transformations. *Journal of Harbin Engineering University*, 44(8), 975–980. URL: https://harbinengineeringjournal.com/index.php/journal/article/view/992
19. 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
20. Esmaeili, M., Esmaeili, M., & Gulliver, T. A. (2011). High-rate Fibonacci polynomial codes. In: *Proceedings of IEEE International Symposium on Information Theory Proceedings, St. Petersburg, Russia*, pp. 1921–1924. https://doi.org/10.1109/ISIT.2011.6033886
21. Esmaili, M., Moosavi, M., & Gulliver, T. A. (2017, January). A new class of Fibonacci sequence based error correcting codes. *Cryptography and Communications*, Vol. 9, 379–396. https://doi.org/10.1007/s12095-015-0178-x
22. Esmaili, Mostafa, & Esmaeili, Morteza. (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
23. Falcon, S., & Plaza, A. (2009, February). 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
24. 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
25. Flaut, Cristina, & Savin, Diana. (2017, April). Some remarks regarding generalized Fibonacci-Lucas numbers and generalized Fibonacci-Lucas quaternions. arXiv:1705.00361v2 [math.RA]. https://doi.org/10.48550/arXiv.1705.00361
26. 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
27. Goy, Taras, & Shattuck, Mark. (2019, December). Fibonacci and Lucas Identities from Toeplitz–Hessenberg Matrices. *Applications and Applied Mathematics: An International Journal*, 14(2), 699–715. URL: https://www.researchgate.net/publication/337906242_Fibonacci_and_Lucas_Identities_from_Toeplitz-Hessenberg_Matrices
28. Gryciuk, Yurij, Grytsyuk, Pavlo. (2015). Perfecting of the matrix Affine cryptosystem information security. Computer Science and Information Technologies: Proceedings of Xth International Scientific and Technical Conference (CSIT2015), 14–17 September, 2015, (pp. 67–69). https://doi.org/10.1109/stc-csit.2015.7325433
29. 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
30. Grytsiuk, P. Yu., & Hrytsiuk, Yu. I. (2015). Peculiarities of the implementation of the matrix Affine cryptosystem of information protection. *Scientific Bulletin of UNFU*, 25(5), 346–356. URL: https://nv.nltu.edu.ua/index.php/journal/article/view/1092
31. Hoggat, V. E. Jr. (1969). Fibonacci and Lucas numbers. *Palo Alto* (CA): Houghton-Mifflin. URL: https://www.peliti.org/Notes/fibonacciLucas.pdf
32. 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
33. Hoggatt, V. E. Jr., & Lind, D. A. (1968). Symbolic Substitutions in to Fibonacci Polynomials. *The Fibonacci Quarterly*, Vol. 6, no. 5, 55–74. https://doi.org/10.1080/00150517.1968.12431206
34. Hoggatt, V. E. Jr., Leonard, H. T. Jr., & Philips, J. W. (1971). Twenty-four Master Identities. *The Fibonacci Quarterly*, 9(1), 1–17. URL: https://www.fq.math.ca/Scanned/9-1/hoggatt.pdf; https://doi.org/10.1080/00150517.1971.12431028
35. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2015). Methods and means of generating Fibonacci Q_p-matrices – keys for implementing cryptographic transformations. *Scientific Bulletin of UNFU*, 25(6), 334–351. URL: https://nv.nltu.edu.ua/index.php/journal/article/view/974
36. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci Q_p-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
37. Jin, Z. (2018). On the Lucas polynomials and some of their new identities. *Adv Differ Equ*, 126 (2018). https://doi.org/10.1186/s13662-018-1527-9
38. Karaaslan, N. (2019). A Note on Modified Pell Polynomials. *Aksaray University Journal of Science and Engineering*, 3(1), 1–7. https://doi.org/10.29002/asujse.511850
39. Kaygisiz, K., & Sahin, A. (2012). New Generalizations of Lucas Numbers. *Gen Mathematics Notes*, Vol. 10, no. 1, 63–77. URL: https://users.dimi.uniud.it/~giacomo.dellariccia/Glossary/Lucas/KaygisizSahin2012b.pdf
40. Koshy, Thomas. (2001). Fibonacci and Lucas Numbers with Applications. A Wiley-Interscience Publication. Toronto, New York, NY, USA, 654 p. https://doi.org/10.1002/9781118033067
41. 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
42. Lupas, Alexandru. (1999). A Guide of Fibonacci and Lucas Polynomial. *Octagon Mathematics Magazine*, Vol. 7(1), 2–12.
43. 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
44. Nihal Tas, Sumeyra Ucar, Nihal Yilmaz Ozgur, & Oztunc Kaymak. (2018). A new coding/decoding algorithm using Fibonacci numbers. *Discrete Mathematics, Algorithms and Applications*, Vol. 10, No. 02, article ID 1850028. https://doi.org/10.1142/S1793830918500283
45. Özkan, E., Taştan, M., & Aydoğdu, A. (2018). 2-Fibonacci polynomials in the family of Fibonacci numbers. *Notes on Number Theory and Discrete Mathematics*, 24(3), 47–55. https://doi.org/10.7546/nntdm.2018.24.3.47-55
46. 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
47. Panwar, Yashwant K., Singh, B., & Gupta, V. K. (2013). Generalized Fibonacci Polynomials. *Turkish Journal of Analysis and Number Theory*, 1(1), 43–47. https://doi.org/10.12691/tjant-1-1-9
48. 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
49. Postavaru, Octavian. (October 2023). An efficient numerical method based on Fibonacci polynomials to solve fractional differential equations. *Mathematics and Computers in Simulation*, Vol. 212, 406–422. https://doi.org/10.1016/j.matcom.2023.04.028
50. Prasad, Bandhu. (2014). Coding theory on (*h*(*x*), *g*(*y*))-extension of Fibonacci *p*-numbers polynomials. *Universal Journal of Computational Mathematics*, Vol. 2(1), 6–10. https://doi.org/10.13189/ujcmj.2014.020102
51. Prasad, Bandhu. (2014). High rates of Fibonacci polynomials coding theory. *Discrete Mathematics, Algorithms and Applications*, Vol. 06, No. 04, article ID 1450053. https://doi.org/10.1142/S1793830914500530
52. Prasad, Bandhu. (2016). Coding theory on Lucas *p*-numbers. *Discrete Mathematics, Algorithms and Applications*, Vol. 08, No. 04, article ID 1650074. https://doi.org/10.1142/S1793830916500749
53. Prasad, Bandhu. (2019). The generalized relations among the code elements for a new complex Fibonacci matrix. *Discrete Mathematics, Algorithms and Applications*, Vol. 11, No. 02, article ID 1950026. https://doi.org/10.1142/S1793830919500265
54. 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
55. 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
56. Robbins, N. (1991). Vieta's triangular array and a related family of polynomials. *International Journal of Mathematics and Mathematical Sciences*, Vol. 14, no. 2, 239–244. https://doi.org/10.1155/S0161171291000261
57. 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
58. Sentürk, G. Y., Gürses, N., & Yüce, S. (2022). Construction of dual-generalized complex Fibonacci and Lucas quaternions. *Carpathian Mathematical Publications*, 14(2), 406–418. https://doi.org/10.15330/cmp.14.2.406-418
59. 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
60. Sikhwal1, Omprakash, & Vyas, Yashwant. (2014). Fibonacci Polynomials and Determinant Identities. *Turkish Journal of Analysis and Number Theory*, 2(5), 189–192. https://doi.org/10.12691/tjant-2-5-6
61. 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
62. Stakhov, A. P. (2006, October). Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory. *Chaos, Solitons, & Fractals*, Vol. 30, issue 1, 56–66. https://doi.org/10.1016/j.chaos.2005.12.054
63. Swamy, M. N. S. (1965). Problem B-74. *The Fibonacci Quarterly*, Vol. 3, no. 3, 236 p. URL: https://www.sciepub.com/reference/152291
64. Taştan, M., & Özkan, E. (2021). Catalan transform of the *k*-Pell, *k*-Pell–Lucas and modified *k*-Pell sequence. *Notes on Number Theory and Discrete Mathematics*, 27(1), 198–207. https://doi.org/10.7546/nntdm.2021.27.1.198-207
65. 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
66. Uçar, Sümeyra, Tas, Nihal, & Özgür, Nihal. (2019, May). A New Application to Coding Theory via Fibonacci and Lucas Numbers. *Mathematical Sciences and Applications E-Notes*, 7(1), 62–70. https://doi.org/10.36753/mathenot.559251
67. Vajda, S. (2007, December). Fibonacci and Lucas Numbers, and the Golden Section. *Theory and Applications* (Dover Books on Mathematics). Dover Publications, 192 p. URL: https://www.amazon.com/Fibonacci-Lucas-Numbers-Golden-Section/dp/0486462765
68. Wang, W., & Wang, H. (2015). Some results on convolved (*p*,*q*)-Fibonacci polynomials. *Integral Transforms and Special Functions*, 26(5), 340–356. https://doi.org/10.1080/10652469.2015.1007502
69. Wang, Weiping, & Wang, Hui. (2017, August). Generalized Humbert polynomials via generalized Fibonacci polynomials. *Applied Mathematics and Computation*, Vol. 307, 204–216. https://doi.org/10.1016/j.amc.2017.02.050
70. 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
71. 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
72. Yilmaz, N. (2024). Some new results for the generalized bivariate Fibonacci and Lucas polynomials. Corpus ID: 271426809. *Mathematica Moravica*. https://doi.org/10.5937/matmor2401097y

73. 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 WITH REFINED FIBONACCI POLYNOMIAL MATRICES

The possibility of solving the problem of generating keys for block data encryption in the form of an nth sequence of refined Fibonacci polynomial matrices of the mth order, the elements of which are Fibonacci polynomials with numbers from $(n–2)$th to $(m+n–2)$th, is shown. The obtained Fibonacci matrices make it possible to find both their determinants and inverse matrices suitable for the matrix method of block data encryption. It has been found that even over the past decade, a significant number of publications have been published, each of which substantiates different approaches to generating sequences of Fibonacci polynomial matrices and proves the feasibility of their use for data encryption. At the same time, the use of Fibonacci polynomial matrices as a separate procedure for protecting block data in the theory and practice of cryptography is extremely rare. It has been established that a well-known method for generating a sequence of Fibonacci polynomials consists in using a recurrence relation, according to which the next polynomial is formed by multiplying the variable x sequentially by the elements of the current polynomial, after which similar terms are grouped with the terms of the previous polynomial. The method of generating a sequence of Fibonacci polynomial matrices consists in using a recurrent matrix relation, according to which the next polynomial matrix is formed by multiplying the variable x successively by the elements of the current matrix, adding the elements of the formed matrix to the elements of the previous matrix, after which all similar terms are grouped in the formed elements. Algorithms for forming a sequence of 8th Fibonacci polynomial matrices from the 2nd to the 5th order are given, the elements of which are Fibonacci polynomials of no more $(n–1)$th power, are presented, which made it possible to analyze not only the features of their construction, but also to understand the procedures for finding their determinants and inverse matrices. Software has been developed that allows generating both sequences of Fibonacci polynomial matrices of the mth order, and finding their determinants and inverse polynomial matrices of a similar order. An example of using the matrix method of encrypting block data with a Fibonacci polynomial matrix is provided, which allows the interested reader to understand the basic principle of encrypting both the original message and decrypting the encrypted message.

Keywords: sequence of Fibonacci polynomials; recurrent matrix relation; sequence formation mechanism; inverse Fibonacci polynomial matrix; encrypted message; matrix data encryption method.