https://doi.org/10.31891/2307-5732-2026-365-33
УДК 004.04

ДАВЛЕТОВА АЛІНА
Західноукраїнський національний університет
https://orcid.org/0000-0002-1192-2532
e-mail: a7davletova@gmail.com

АНАМОРФНА КРИПТОСИСТЕМА НА ОСНОВІ MCELIECE-ПОДІБНОЇ СХЕМИ НАД НЕБІНАРНИМИ ПОЛЯМИ

Розглянуто підхід до побудови асиметричної криптографічної системи, що поєднує методи кодової криптографії з анаморфним механізмом шифрування. Запропоновано підхід, що базується на використанні вектора помилок кодового шифрування як додаткового носія прихованої інформації, що не порушує коректності дешифрування основного каналу. Реалізовано асиметричну анаморфну криптосистему на основі модифікованої McEliece-подібної конструкції з використанням GRS-кодів над скінченними полями Галуа GF(p). Для узгодження параметрів повідомлень із кодовою конструкцією системи застосовано перехід до системи числення залишкових класів. Проведено теоретичний аналіз та експериментальні дослідження ефективності запропонованого рішення. Отримані результати показали, що криптографічна стійкість запропонованої системи базується на складності задачі декодування випадкових небінарних лінійних кодів з помилками.

Ключові слова: *асиметрична криптосистема, кодова криптографія, коди для корекції помилок, скінченні поля Галуа, анаморфне шифрування, система залишкових класів.*

DAVLETOVA ALINA
West Ukrainian National University

ANAMORPHIC CRYPTOSYSTEM BASED ON McELIECE-TYPE CONSTRUCTION OVER NON-BINARY FIELDS

Considers an approach to the construction of an asymmetric cryptographic system that combines methods of code-based cryptography with an anamorphic encryption mechanism, in which the same ciphertext may admit different informational interpretations depending on the secret parameters available to the receiver. The proposed approach is based on using the error vector of code-based encryption not only as a masking mechanism for the transmitted message but also as an additional carrier of hidden information, without violating the correctness of decryption of the main channel. An asymmetric anamorphic cryptosystem based on a modified McEliece-like construction using GRS codes over finite Galois fields GF(p) is implemented. To align the parameters of the messages with the code construction of the system, a transition to the residue number system is applied, which reduces the bit-width of arithmetic operations and computational costs while preserving the cryptographic properties of the scheme, and also enables adaptation of the capacities of the main and hidden channels without modifying the cryptographic core. A theoretical analysis and experimental evaluation of the efficiency of the proposed solution are carried out. The scalability of code parameters, timing characteristics of the main cryptographic operations, the impact of the hidden channel on ciphertext and key sizes, and robustness against additional errors are analyzed. It is shown that the implementation of the hidden anamorphic channel does not alter the structure of the public key, does not affect the statistical properties of the ciphertext, and does not reduce the error-correcting capability of the code. The obtained results indicate that the cryptographic security of the proposed system is based on the hardness of decoding random non-binary linear codes with errors. The proposed approach is promising for applications in secure and covert information transmission systems.

Keywords: *asymmetric cryptosystem, code-based cryptography, error-correcting codes, finite Galois fields, anamorphic encryption, residue number system.*

Стаття надійшла до редакції / Received 14.02.2026
Прийнята до друку / Accepted 15.03.2026
Опубліковано / Published 28.05.2026

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Швидкий розвиток обчислювальних технологій, зокрема поява та еволюція квантових обчислювальних моделей, зумовлює необхідність перегляду підходів до побудови криптографічних систем, орієнтованих на довгостроковий захист інформації. Кодові криптосистеми, є одним із перспективних напрямів постквантової криптографії, проте їх функціональні можливості, як правило, обмежуються класичною моделлю одноцільового шифрування, спрямованої виключно на забезпечення конфіденційності основного повідомлення.

Сучасний етап розвитку криптографії характеризується зростанням вимог до надійності та захищеності процесу передавання інформації, а також до стійкості та функціональної гнучкості алгоритмів, що реалізують ці процеси. Актуальності набувають криптосистеми, здатні забезпечувати не лише конфіденційність основного каналу, а й можливість прихованого обміну додатковими даними в умовах контролю мережевого трафіку та наявності пасивного або активного спостерігача.

Більшість існуючих рішень у сфері стеганографії реалізуються на прикладному рівні та не інтегруються безпосередньо в математичну структуру алгоритмів, що ускладнює формальний аналіз їх стійкості та знижує рівень захисту в умовах цілеспрямованих атак. Тому актуальною задачею є розробка криптографічних систем, у яких прихований канал передавання інформації не є зовнішнім доповненням, а випливає з алгебраїчної природи шифрування. Такий підхід дозволяє забезпечити невідрізнюваність шифротекстів для зовнішнього спостерігача при збереженні коректності, надійності та криптографічної стійкості основного каналу передавання даних.

Перспективним напрямом є використання методів кодової криптографії, які використовують надлишковість коригуючих кодів не лише для виправлення помилок, а й як ресурс для кодування додаткових даних. Поєднання кодових криптосистем з анаморфними механізмами створює передумови для побудови багаторівневих криптографічних моделей доступу, у яких один і той самий криптографічний об'єкт може мати різну семантичну інтерпретацію залежно від набору доступних секретних параметрів.

Таким чином, дослідження анаморфних кодових криптосистем є актуальним як з теоретичної точки зору – у контексті розвитку постквантових алгоритмів, так і з практичної – з огляду на вимоги до захисту та функціональних можливостей сучасних засобів захисту інформації.

Аналіз досліджень та публікацій

Дослідження криптографічних систем зосереджені на пошуку компромісу між високою стійкістю до квантових атак та функціональною гнучкістю протоколів.

Кодові системи типу McEliece [1-3] характеризуються високою криптографічною стійкістю та потенційною придатністю до використання в постквантовому середовищі. Поєднання криптографічних перетворень із механізмами корекції помилок [4, 5] є перспективним та ефективним напрямом підвищення надійності передавання зашифрованих даних й розвитку криптографічних систем. Водночас класичні реалізації таких схем орієнтовані виключно на захист одного інформаційного каналу та не передбачають прихованого передавання додаткових даних без зміни зовнішніх статистичних властивостей шифротексту. Традиційні стеганографічні методи [6-8], що використовують мультимедійні контейнери для приховування даних, зазвичай розглядаються окремо від криптографічних протоколів та не інтегровані на рівні алгебраїчної структури шифрування. Ці особливості можна віднести до недоліків, оскільки виявлення факту використання стеганографії або прихованих каналів може призвести до компрометації або стати підставою для примусового розкриття ключів. Вирішенням цієї проблеми є концепція анаморфного шифрування [9], яка на відміну від класичного підходу, використовує криптографічні об'єкти та випадкові параметри протоколів як засіб передачі додаткової прихованої інформації. Основною особливістю анаморфних систем є здатність одного шифротексту містити два незалежні повідомлення, що відновлені різними ключами, при забезпеченні повної невідрізнюваності між звичайним та анаморфним режимами роботи. Це дозволяє користувачеві зберігати безпеку в умовах «примусу до розкриття ключа», надаючи контролюючій стороні лише основний ключ, тоді як існування прихованого каналу залишається математично невиявленим.

Аналіз останніх досліджень [10-15] дозволяє виділити кілька ключових напрямів розвитку даної галузі, зокрема формування фундаментальних моделей безпеки й доведення невідрізнюваності анаморфних каналів від стандартних криптографічних перетворень та пошук нових алгебраїчних структур, які здатні забезпечити високу ємність прихованого каналу без порушення функціональності основної схеми.

У роботі [10] запропоновано розширену модель анаморфного шифрування, яка дозволяє додавати приховані канали після генерації основної пари ключів. Такий підхід дозволяє гнучко створювати приховані повідомлення без зміни публічного ключа. Досліджено властивість робастності, яка гарантує, що при спробі анаморфного дешифрування звичайного тексту система виявить помилку, а не випадкові дані. Перевагами даного методу є можливість масштабування кількості прихованих повідомлень в одному каналі.

У роботі [11] запропоновано реалізацію анаморфної схеми на основі еліптичних кривих (ECC), де приховане повідомлення впроваджується у випадкове значення, що дозволяє значно підвищити продуктивність у порівнянні з методами на базі дискретного логарифмування. Авторами досліджено використання алгоритму Baby-Step Giant-Step для швидкого відновлення прихованих даних. Проведений аналіз обчислювальної складності демонструє високу швидкість роботи.

У [12] запропоновано концепцію широкомовного анаморфного шифрування, що дозволяє передавати різні приховані повідомлення різним групам користувачів у межах одного публічного каналу. Досліджено застосування схеми Dual Regev для маскування кількості каналів. Проаналізовано стійкість до виявлення при великій кількості тіньових груп. Перевагами такого підходу є висока ефективність використання пропускної здатності каналу.

У [13] запропоновано схему анаморфних цифрових підписів, що забезпечує властивості непідробності як з боку цензора («диктатора»), так і з боку отримувача. Розглянуто механізми вбудовування значних обсягів прихованих даних у структуру цифрового підпису без порушення його коректної верифікації стандартними методами. Проаналізовано математичні припущення, необхідні для забезпечення стійкості до атак підміни повідомлень в анаморфному каналі. Перевагами підходу є можливість передавання великих обсягів даних через підпис фіксованої довжини та підвищений рівень безпеки прихованого каналу за умови компрометації лише публічної частини основного ключа.

У [14] запропоновано розширення анаморфного шифрування в квантовий контекст. Підхід базується на квантових матрицях щільності та дозволяє вбудовувати один квантовий стан (повідомлення B) у інший (повідомлення A). Доведено, що квантові стани є статистично невідрізнюваними для зовнішнього спостерігача. Проведено аналіз стійкості схеми до атак з використанням квантових комп'ютерів, підтверджує її стійкість до класичного криптоаналізу.

У роботі [15] запропоновано спрощену та ефективну конструкцію анаморфного шифрування та підпису з підтримкою кількох одночасно прихованих повідомлень. Підхід дозволяє інтегрувати анаморфні властивості у стандартні криптосистеми без суттєвих змін, використовуючи внутрішню структуру шифру для вбудовування

додаткових повідомлень. Перевагами методу є простота впровадження та масштабованість, що дозволяє гнучко налаштовувати кількість прихованих каналів залежно від вимог до безпеки та ємності каналу.

Проведений аналіз свідчить про перехід концепції анаморфного шифрування від теоретичних конструкцій до практично орієнтованих рішень, що базуються на алгебраїчних структурах еліптичних кривих та кодових систем з корекцією помилок. Попри високий рівень теоретичної невідрізнюваності, досягнутий у сучасних моделях анаморфного шифрування, та значний розвиток у їх формалізації, більшість реалізацій обмежені низькою пропускною здатністю прихованого каналу та значними обчислювальними витратами при обробці великих обсягів даних. Методи, що базуються на дискретному логарифмуванні або ітеративних пошуках у складних графах, залишаються ефективними лише для передачі коротких повідомлень, що суттєво обмежує їх функціональність у практичних сценаріях захищеного зв'язку.

З метою усунення виявлених обмежень запропоновано поєднання теоретико-числових підходів до формування інформаційних потоків з алгебраїчними кодовими конструкціями для їх інтеграції у структуру шифротексту. Такий підхід дозволяє масштабувати обсяг прихованої інформації без порушення статистичних властивостей основного каналу та забезпечити необхідний рівень стійкість до квантового криптоаналізу. Це створює передумови для розробки ефективних систем прихованого зв'язку, де ємність та безпека стеганографічного каналу є математично обґрунтованими та адаптованими до сучасних вимог інформаційної безпеки.

Формулювання цілей статті

Метою роботи є розробка криптографічної системи, що поєднує McEliece-подібну кодову основу з анаморфним двоканальним механізмом передавання даних, а також дослідження ефективності її функціонування, структурної узгодженості й збереження криптографічних властивостей.

Аналіз методів і алгоритмів побудови анаморфної криптосистеми

Вибір методів та алгоритмів для реалізації запропонованого рішення зумовлений необхідністю поєднання криптографічної стійкості, гарантованої корекції помилок і відновлення повідомлення, а також можливості прихованої передачі інформації в межах одного шифротексту.

За основу обрано кодову криптосистему McEliece, яка забезпечує стійкість до відомих класичних та квантових атак [16, 17]. На відміну від криптографічних алгоритмів, що базуються на задачах факторизації або дискретного логарифмування, кодова криптографія розглядається як один із найбільш перспективних напрямів постквантового захисту інформації для систем довготривалого зберігання та передавання даних [18-20]. Як базовий код для корекції помилок використано узагальнені коди Ріда-Соломона (GRS) над небінарними полями [21, 22], які забезпечують чітко визначену коригувальну здатність і можливість ефективного алгебраїчного декодування [23-25], що є принципово важливим для реалізації анаморфного механізму та гарантованого відновлення основного повідомлення. Генераторна матриця GRS-коду G маскується шляхом множення на випадкову оборотну матрицю S та матрицю перестановки P [26], що ускладнює відновлення структури коду з публічного ключа та відповідає класичній моделі кодової криптографії, де складність атаки зводиться до задачі декодування випадкового лінійного коду.

Застосування скінченного поля $\mathrm{GF}(p)$ підвищує інформаційну щільність кодових символів, оскільки кожна ненульова помилка може містити до $\log_2 p$ біт інформації. Це дозволяє ефективно використовувати надлишковість коду не лише для корекції помилок, але й для реалізації прихованого інформаційного каналу без суттєвого збільшення обчислювальних витрат.

На відміну від відомих підходів, у яких система залишкових класів (RNS) використовується як безпосередній обчислювальний простір криптографічних перетворень [27–29], у запропонованій криптосистемі RNS застосовується як структурний механізм декомпозиції повідомлення. Перехід від позиційного представлення до RNS забезпечує подання повідомлення у вигляді набору незалежних залишків за системою попарно взаємно простих модулів, що дозволяє розглядати вхідні дані не як єдиний числовий об’єкт, а як сукупність незалежних компонентів, загальна інформаційна ємність яких визначається добутком модулів RNS. Отримане подання у RNS є проміжною формою між вхідними даними та їх позиційним представленням над скінченним полем $\mathrm{GF}(p)$, що використовується для побудови GRS-кодів. При цьому перехід до RNS не спрямований на безпосереднє підвищення криптографічної стійкості, а забезпечує структурну адаптацію двоканального шифрування та узгодження ємності основного і прихованого каналів з параметрами коду без модифікації криптографічного ядра системи.

Реалізація анаморфного каналу передбачає визначення позицій помилок, що несуть приховану інформацію за допомогою псевдовипадкової функції (PRF), параметризованої секретним ключем. Для формування цього ключа застосовується асиметричний механізм капсуляції на основі протоколу Діффі–Хеллмана (DH) [30], що дозволяє встановити спільний секрет без розкриття параметрів прихованого каналу у відкритих компонентах криптосистеми. Отриманий у результаті обміну ключ використовується виключно для параметризації PRF не впливає на коректність відновлення основного. Поєднання PRF і DH забезпечує додатковий рівень логічного розподілу між основним та прихованим каналами. Навіть у разі компрометації основного секретного ключа криптосистеми структура прихованого каналу залишається недоступною без доступу до додаткового секрету, сформованого в результаті DH протоколу.

Таким чином, криптографічна частина запропонованої системи ґрунтується на поєднанні відомих та досліджених алгоритмічних підходів, однак формує узгоджену багаторівневу криптографічну архітектуру з чітким функціональним розподілом компонентів. Кодова криптографія на основі McEliece-подібної схеми

забезпечує базову криптографічну стійкість і коректність відновлення повідомлення, RNS реалізує структурну декомпозицію та адаптивність інформаційного простору, анаморфний механізм забезпечує приховане передавання додаткових даних у межах одного шифротексту. Контроль позицій помилок за допомогою PRF та незалежного асиметричного секрету забезпечує керованість, масштабованість і криптографічну коректність прихованого каналу без порушення базових принципів кодової криптографії та невідрізнюваності шифротекстів.

Математична модель анаморфної криптосистеми

Особливістю запропонованої криптосистеми є анаморфний механізм шифрування, який забезпечує одночасну передачу двох логічно незалежних інформаційних потоків у межах одного шифротексту. Основна ідея полягає у використанні вектора помилок e не лише як механізму підвищення надійності передачі, а й як додаткового інформаційного носія. У межах запропонованого підходу виділяються два логічні канали передачі інформації:

- основний канал, призначений для передавання відкритого повідомлення, яке коректно відновлюється стандартним алгоритмом декодування коду;
- прихований канал, інформація якого вбудовується у структуру вектора помилок e і є недоступним без спеціального секретного ключа.

Для формалізації описаного механізму та подальшого аналізу його властивостей розглянемо математичну модель запропонованої криптосистеми. Нехай p – просте число. Всі операції виконуються в скінченному полі $GF(p)$. Параметри коду задаються параметрами $(\mathrm{n}, \mathrm{k}, t)$, де n - довжина кодового слова, k - розмірність простору повідомлень над полем $GF(p)$. Приховане повідомлення кодується шляхом формування вектора помилок, у якому частина ненульових компонент використовується для передавання прихованої інформації. Кількість таких компонент визначається параметром t_{hide}. Додатково формується t_{noise} випадкових ненульових компонент, що забезпечує статистичну невідрізнюваність прихованого каналу від випадкового шуму. Загальна кількість помилок не перевищує коригувальну здатність коду $t_{correct}$ і задовольняє умову:

$$t_{hide} + t_{noise} \leq t_{correct}. \quad (1)$$

Властивістю запропонованої криптосистеми є те, що при $t_{hide} = 0$ процес формування шифротексту виконується з випадковим вибором вектора помилок, який обмежений коригувальною здатністю коду. Відповідно, статистичні властивості отриманого шифротексту не відрізняються від розподілу шифротекстів McEliece-подібної схеми без анаморфного каналу. Коригувальна здатність $t_{correct}$, при цьому для обраного класу MDS-кодів виконується співвідношення

$$n = k + 2t_{correct}. \quad (2)$$

Публічний ключ містить генераторну матрицю коду

$$G_{pub} \in GF(p)^{k \times n} \quad (3)$$

яка визначається перетворенням

$$G_{pub} = S \cdot G \cdot P\,. \quad (4)$$

Приватний ключ основного каналу включають обернену матрицю лінійного маскування

$$S^{-1} \in GF(p)^{k \times k}, \quad (5)$$

обернену матрицю перестановки

$$P^{-1} \in \{0,1\}^{n \times n}, \quad (6)$$

та алгоритм декодування базового GRS-коду, що використовується для відновлення інформаційної частини повідомлення з k координат скоригованого кодового слова. Застосування матриць S та P забезпечує маскування алгебраїчної структури базового коду та відповідає класичній побудові криптосистем типу McEliece.

Для узгодження параметрів повідомлення використовується система попарно взаємно простих модулів RNS $\{m_i\}$, добуток яких

$$M = \prod_i m_i \quad (7)$$

перевищує числове представлення повідомлення, що відповідно до китайської теореми про залишки забезпечує однозначність його кодування у RNS.

Базовий GRS-код визначається множиною точок оцінювання

$$\alpha_j = g^j \ (mod\ p), j = 0 \ldots n-1, \quad (8)$$

де g - первісний корінь мультиплікативної групи поля $\mathrm{GF(p)}^*$. Колонкові ваги $v_i \in \mathrm{GF(p)}^*$ задають відповідний GRS-код є секретними параметрами системи.

Вектор основного повідомлення, отриманий у результаті детермінованого відображення відкритих даних, поданих через RNS, у простір повідомлень коду, має вигляд

$$u \in GF(p)^k. \quad (9)$$

Відповідне кодове слово без урахування помилок визначається лінійним відображенням

$$c_0 = uG_{pub} \in GF(p)^n. \quad (10)$$

Вектор помилок

$$e \in GF(p)^n. \quad (11)$$

формується таким чином, що його вага $wt(e)$ задовольняє умову (1).

Шифротекст у запропонованій системі визначається як

$$c = c_0 + e. \quad (12)$$

Процес дешифрування розглядається як обернене відображення, яке складається з усунення

маскувальних перетворень та застосування алгоритму декодування базового коду. За умови виконання обмеження на сумарну кількість помилок коректність відновлення основного повідомлення гарантується властивостями використаного коду.

Доступ до прихованого каналу формально не впливає на відновлення основного повідомлення та визначається наявністю додаткового секретного параметра, незалежного від приватного ключа основного каналу. За відсутності такого параметра шифротекст інтерпретується виключно в межах класичної McEliece-подібної моделі, а прихований канал залишається недоступним.

Принцип роботи запропонованого алгоритму

На основі математичної моделі на рисунку 1 наведено алгоритми генерації ключів (а), шифрування (б) та дешифрування (в), що реалізують запропоновану криптосистему з анаморфним каналом передавання інформації.

1. Алгоритм генерації ключів. Вхід: параметри поля GF(p), вимоги до максимальної довжини основного повідомлення та ємності прихованого каналу, параметр маскування. Вихід: публічний ключ PK та секретні ключі $\mathrm{SK}_{\mathrm{main}}$, $\mathrm{SK}_{\mathrm{hidden}}$.

На основі заданих вимог обираються параметри коду (n, k) та коригувальна здатність $t_{correct}$, які задовольняють умови (1) та (2), а також обмеження $n < p$.

Відповідно до співвідношення (7) формується система попарно взаємно простих модулів RNS$\{m_i\}$, добуток яких забезпечує однозначність RNS -кодування основного повідомлення або заданої ємності каналу. Будується базовий GRS-код над GF(p) з точками оцінювання α_j визначеними співвідношенням (8). Генераторна матриця базового коду маскується відповідно до (4). Секретний ключ основного каналу формується як

$$SK_{main} = (S^{-1}, P^{-1}, G_k^{-1}). \quad (13)$$

Для анаморфного каналу генерується додатковий секретний ключ SK_{hidden}, призначений для деккапсуляції прихованої інформації.

2. Алгоритм шифрування. Вхід: публічний ключ PK, основне повідомлення m, приховане повідомлення h (може бути порожнім). Вихід: шифротекст c.

Повідомлення m перетворюється у числове представлення

$$X = Int(m), \quad (14)$$

де $Int(\cdot)$ визначає детерміноване відображення байтового подання повідомлення у невід'ємне ціле число.

Числове представлення X кодується в RNS шляхом обчислення вектора остач

$$r = (r_1, \dots, r_s), r_i = X \bmod m_i, \quad (15)$$

Вибір модулів m_i здійснюється таким чином, що виконується умова (7). Вектор остач r детерміновано відображається у вектор над полем

$$u = \varphi(r) \in GF(p)^k, \quad (16)$$

який використовується як інформаційна частина кодового слова. Відображення $\varphi(\cdot)$ є фіксованим, однозначним і узгодженим з розмірністю коду.

На основі вектора u та публічного ключа G_{pub} обчислюється кодове слово c_0 відповідно до (10). Формується вектор помилок (11) так, що його вага не перевищує $t_{correct}$. Якщо приховане повідомлення відсутнє, вектор e містить лише випадкові помилки, призначені для маскування. Якщо приховане повідомлення присутнє, частина ненульових компонент вектора e використовується для кодування прихованих даних, а решта - для випадкового шуму.

Фінальний шифротекст формується відповідно до (12), де додавання виконується покомпонентно в полі $GF(p)$. У результаті отриманий шифротекст є елементом $GF(p)^n$ і за своїми зовнішніми статистичними властивостями не відрізняється від шифротексту класичної McEliece-подібної схеми, тоді як приховане повідомлення інкапсульоване у структурі вектора помилок.

3. Алгоритм дешифрування. Вхід: шифротекст c, секретний ключ SK_{main}. Вихід: відновлене основне повідомлення $\widehat{m}$. З шифротексту знімається перестановка координат:

$$c' = c \cdot P^{-1}. \quad (17)$$

До вектора c' застосовується алгоритм декодування GRS-коду, внаслідок чого, при виконанні умови (2) відновлюється скориговане кодове слово $\hat{c}$. З k координат вектора $\hat{c}$ відновлюється інформаційна частина повідомлення:

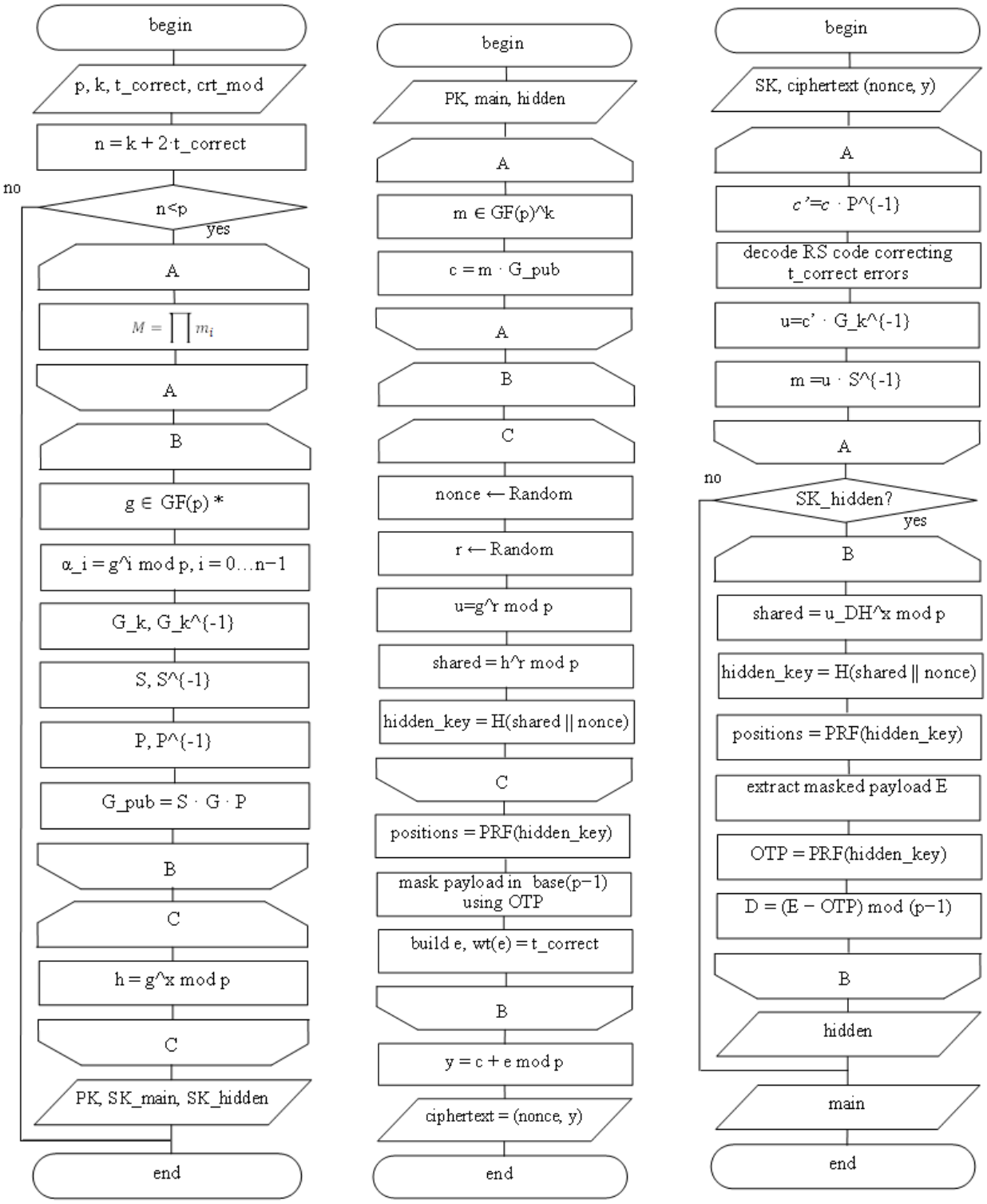
$$\hat{u} = \hat{c}_{[1\dots k]} \cdot G_k^{-1}. \quad (18)$$

Основне повідомлення відновлюється як

$$\widehat{m} = \hat{u} \cdot S^{-1}, \quad (19)$$

після чого виконується зворотне до етапу шифрування детерміноване перетворення, яке включає відновлення числового представлення повідомлення з вектора остач та подальше відображення у початкове байтове подання.

Якщо доступний додатковий секретний ключ SK_{hidden}, з вектора помилок можуть бути вилучені компоненти, що відповідають прихованому повідомленню. У протилежному випадку прихований канал залишається недоступним, тоді як коректність відновлення основного повідомлення зберігається.



а) б) в)

Рис. 1 Блок-схема роботи запропонованого алгоритму

Дослідження ефективності запропонованого алгоритму

Проведені дослідження ефективності запропонованої анаморфної криптосистеми, спрямовані на аналіз масштабування параметрів коду, часових характеристик основних криптографічних операцій, а також впливу прихованого каналу на розміри шифротексту та ключового матеріалу.

У запропонованій системі прихований канал реалізується за рахунок вектора помилок, а кількість помилок t_{hide} , необхідних для передавання прихованого повідомлення заданого обсягу, визначається параметрами скінченного поля GF(p). Параметр t_{hide} відповідає мінімальному числу символів $p-1$, необхідних для кодування прихованого повідомлення заданої бітової довжини (B)

$$t_{hide} = \left\lceil \frac{B}{log_2(p-1)} \right\rceil. \quad (20)$$

Таким чином, t_{hide} зростає обернено пропорційно логарифму розміру поля. На рисунку 2 наведено графік залежності значення t_{hide} від розміру прихованого повідомлення для різних значень параметра поля p.

З наведених даних видно, що зі збільшенням розміру поля кількість помилок, необхідних для передавання прихованого повідомлення фіксованого обсягу, зменшується, що знижує навантаження на механізм корекції помилок і дозволяє використовувати менші параметри коду. Водночас збільшення бітності поля призводить до зростання складності арифметичних операцій над елементами поля, що формує компроміс між обчислювальною складністю та корекційною ефективністю.

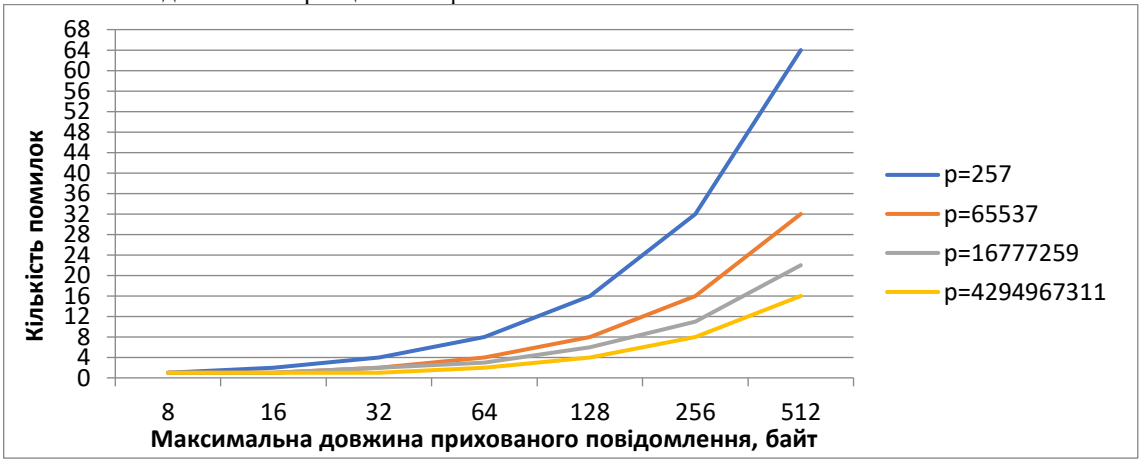


Рис. 2 Графік залежності кількості t_{hide} від розміру прихованого повідомлення для різних значень параметра поля p

Для дослідження запропонованої криптосистеми проведено серії експериментальних досліджень за фіксованих параметрів $GF(2^{16})$, де $p = 65537$ та розрядності модулів RNS 16 біт. Дослідження проведено для різних значень максимальної довжини основного повідомлення (main) у діапазоні 16–256 байт. Для кожного значення main забезпечувався прихований канал (hidden) ємністю до 50 % від обсягу основного каналу, що безпосередньо визначало параметри кодової конструкції (n, k, t) та впливало на час виконання матричних операцій над полем GF(p).

У таблиці 1 наведено отримані оцінки часових затрат етапів роботи криптосистеми.

Таблиця 1

Часові характеристики виконання основних етапів

Максимальна довжина основного повідомлення, байт	Час генерації ключів, мс	Час шифрування, мс	Час повного дешифрування, мс	Час дешифрування лише основного повідомлення, мс
16	20,305	0,301	4,869	4,793
32	120,911	0,552	15,822	15,997
64	748,590	1,457	66,065	67,051
128	5764,549	5,058	307,548	305,968
256	6236,447	19,014	653,029	647,521

Складність етапу генерації ключів визначається операціями формування та інвертування матриць над полем GF(p). Шифрування зводиться до множення вектора на публічну матрицю та додавання вектора помилок, що має обчислювальну складність $O(nk)$. Тому навіть при $main = 256\ B$ час шифрування залишається в межах десятків мс і є на порядок меншим за час дешифрування.

Отримані дані демонструють, що часова складність усіх етапів зростає пропорційно масштабуванню параметрів коду (n, k, t), які визначаються ємністю основного повідомлення та корекційною здатністю коду, що узгоджується з теоретичною складністю використаних алгоритмів.

На рисунку 3 наведено залежність часу шифрування для різних варіантів RNS-представлення при фіксованому значенні $main = 128\ B$ та полі $GF(2^{16})$. Перехід до модулів RNS більшої розрядності (24 та 32 біти) дозволяє зменшити часові витрати за рахунок скорочення фактичної розмірності кодових параметрів. Для шифрування коротких повідомлень та блоків фіксованого розміру розрядність 16 біт є достатньою та оптимальною. Збільшення розрядності модулів RNS розглядається як інженерна оптимізація для обробки великих блоків даних і не впливає на криптографічні властивості системи.

Основну обчислювальну складність дешифрування формує алгебраїчне декодування GRS-коду, що визначається параметрами (n, k, t). Обробка прихованого каналу реалізується у вигляді додаткових лінійних операцій і не має істотного впливу на загальний час етапу дешифрування.

На рисунку 4 наведено залежність часу дешифрування від обсягу прихованого каналу для значення $main = 128\ B$ за фіксованих параметрів поля та 16-бітного RNS -представлення.

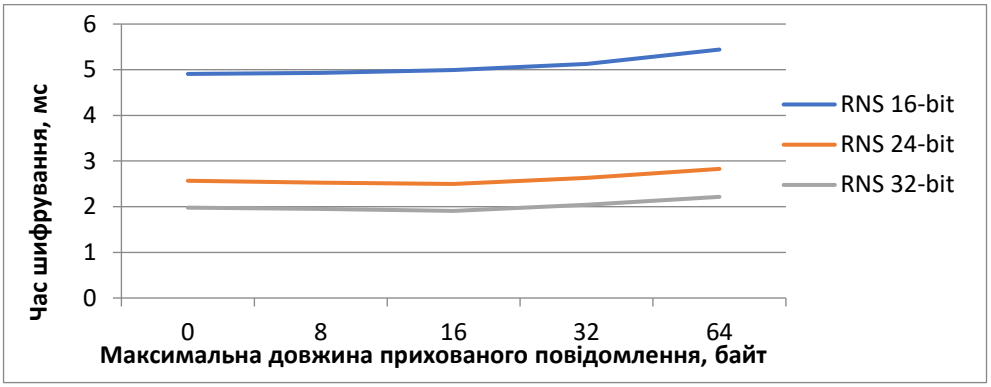


Рис. 3 Залежність часу шифрування від розрядності представлення даних

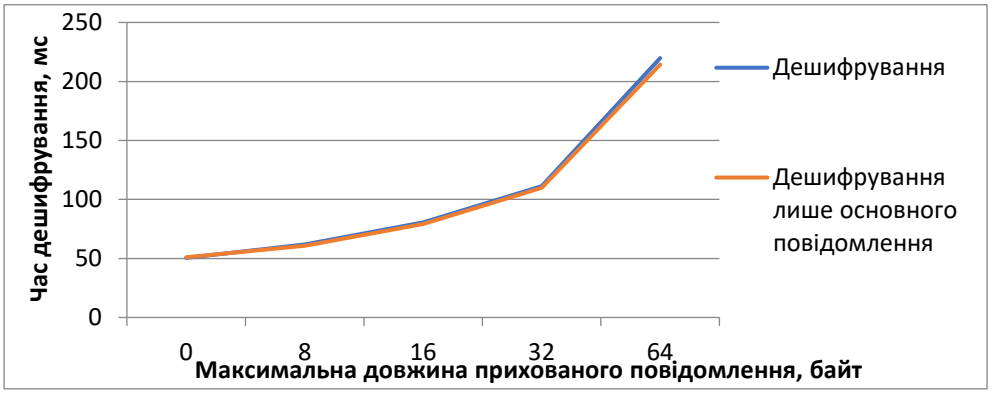


Рис. 4 Залежність часу дешифрування від обсягу прихованого каналу

Практично однакові значення часу повного дешифрування та дешифрування лише основного каналу підтверджують, що реалізація анаморфного каналу не вносить додаткових обчислювальних витрат і не впливає на асимптотичну складність основних криптографічних операцій.

У таблиці 2 наведено вплив обсягу прихованого повідомлення на параметри шифротексту.

Таблиця 2

Вплив прихованого каналу на параметри шифротексту

Максимальна довжина основного повідомлення, байт	Кількість помилок прихованого каналу t_{hide}	Довжина вектора шифро-тексту	Розмір серіалізо-ваного шифротексту, байт	Вага вектора помилок	Коректність відновлення основного повідомлення	Коректність відновлення прихованого повідомлення
0	0	35	277,7	1	TRUE	FALSE
8	4	43	324,56	5	TRUE	TRUE
16	8	51	370,5	9	TRUE	TRUE
32	16	67	464,5	17	TRUE	TRUE

З таблиці 2 видно, що збільшення обсягу прихованого повідомлення реалізується шляхом лінійного зростання кількості помилок, що несуть приховану інформацію. При цьому коригувальна здатність коду зберігається, а неконтрольовані збої дешифрування відсутні.

У таблиці 3 наведено залежність фактичного розміру серіалізованого шифротексту від параметрів прихованого каналу та кількості маскувальних помилок t_{noise} за фіксованих параметрів кодової конструкції для $main = 64\ B$. Для порівняння також наведено теоретичний мінімальний розмір шифротексту у вигляді вектора над полем $GF(2^{16})$.

Таблиця 3

Вплив параметрів прихованого каналу на характеристики шифротексту

Максимальна довжина прихованого повідомлення, байт	Розмір серіалізованого шифротексту, байт						Теоретичний розмір вектора шифротексту, байт
	$t_{noise} = 0$	$t_{noise} = 2$	$t_{noise} = 4$	$t_{noise} = 6$	$t_{noise} = 8$	$t_{noise} = 10$	
0	280	273	282	277	281	282	105
8	312	314	318	313	312	316	123
16	359	357	359	361	367	360	147
32	541	459	456	449	453	456	195

З отриманих даних видно, що зміна параметра t_{noise} не призводить до систематичної зміни розміру шифротексту. Збільшення обсягу прихованого повідомлення викликає зростання довжини кодового слова та відповідного теоретичного й фактичного розміру шифротексту.

У таблиці 4 наведено експериментальні результати зміни розмірів публічного PK та основного SK_{main} та додаткового SK_{hidden} секретних ключів запропонованої криптосистеми.

Таблиця 4

Залежність розмірів ключів від параметрів основного та прихованого повідомлень

Максимальна довжина основного повідомлення, байт	Максимальна довжина прихованого повідомлення, байт	Розмір публічного ключа PK, байт	Розмір основного секретного ключа SK_{main}, байт	Розмір додаткового секретного ключа SK_{hidden}, байт
16	8	1654	303	44
32	16	4566	353	44
64	32	14877	449	44
128	64	53396	649	44

З наведених даних видно, що PK має значно більший розмір і зростає зі збільшенням параметрів коду, тоді як розміри SK_{main} і SK_{hidden} залишаються стабільно компактними. Така властивість є важливою для сценаріїв прихованого зберігання ключового матеріалу на пристроях з обмеженими ресурсами.

На рисунку 5 наведено графічне порівняння розмірів ключів наведених в таблиці 4.

Рис. 5 Залежність розміру ключів від параметрів коду

Отримані дані демонструють, типовий для McEliece-подібних криптосистем асиметричний дисбаланс розміру ключів. Розмір SK_{hidden} практично не залежить від обсягу переданих даних, оскільки він виконує роль компактного криптографічного seed для детермінованого відтворення позицій прихованого каналу. Такий підхід забезпечує високу ефективність системи за мінімальних витрат пам'яті та підтверджує відсутність додаткових ключових накладних витрат, пов'язаних із реалізацією прихованого каналу.

У таблиці 5 наведено результати дослідження стійкості запропонованої криптосистеми до додаткових помилок, навмисно внесених у шифротекст після етапу шифрування.

Таблиця 5

Стійкість до додаткових помилок

Кількість додаткових помилок у шифротексті	Частка успішного відновлення основного повідомлення, %	Частка успішного відновлення прихованого повідомлення, %
0	100	100
1	14	0
2	6	0
3	0	0
4	0	0

Результати підтверджують, що запропонована криптосистема демонструє чітко визначену межу корекції помилок та відсутність неконтрольованого або часткового витоку інформації за межами цієї межі. Коректне відновлення основного повідомлення можливе лише в окремих випадках за умови, що ефективна вага вектора помилок не перевищує коригувальної здатності коду.

Для оцінки статистичної невідрізнюваності шифротексту використано χ^2-статистику Пірсона, обчислену для розподілів позицій і значень помилок. Результати наведено в таблиці 6. Значення в таблиці відповідають середнім значенням χ^2-статистик, що обчислені за серією незалежних експериментів для фіксованих параметрів коду $main = 64\ B$, для оцінки відхилення розподілів позицій і значень помилок від рівномірного.

Таблиця 6

Порівняння статистик розподілу помилок у стандартному та анаморфному режимах

Режим роботи	χ^2-статистика розподілу позицій помилок	χ^2-статистика розподілу значень помилок
Стандартний (без hidden)	13.56	30.97
Анаморфний (hidden = 16 В)	11.06	31.27
Анаморфний (hidden = 32 В)	11.76	31.26

З наведених даних видно, що значення χ^2-статистик для стандартного та анаморфного режимів знаходяться в одному діапазоні та не демонструють систематичних відмінностей. Збільшення обсягу прихованого каналу не призводить до зростання χ^2-статистик, що свідчить про відсутність статистично помітних змін у розподілі позицій і значень помилок. Отже, реалізація прихованого каналу не порушує емпіричну невідрізнюваність шифротексту та не створює спостережуваних статистичних ознак, доступних для зовнішнього спостерігача.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

У роботі запропоновано анаморфну асиметричну криптосистему, що базується на McEliece-подібній конструкції з використанням GRS-кодів над небінарними полями. Запропонований підхід поєднує методи кодової криптографії з механізмом анаморфного шифрування, у межах якого один і той самий шифротекст може мати різну інформаційну інтерпретацію залежно від наявних у отримувача секретних параметрів.

За результатами проведених досліджень та теоретичного аналізу підтверджено, що інтеграція прихованого каналу не впливає на коректність дешифрування основного каналу та не змінює коригувальної здатності коду. Використання RNS дозволяє гнучко адаптувати параметри кодової конструкції (n, k, t) під вимоги до ємності каналів.

Отримані оцінки часових характеристик показали, що для основного повідомлення обсягом 128 байт час шифрування не перевищує 5 мс, тоді як час дешифрування становить близько 300 мс і визначається виключно складністю алгебраїчного декодування GRS-коду, що є прийнятним для систем захищеного зв'язку. Час обробки прихованого каналу становить менше 2 % від загального часу дешифрування, що підтверджує ефективність обраного методу вбудовування даних.

Аналіз розмірів ключів показав характерну для McEliece-подібних криптосистем виражену асиметрію розмірів ключів. Зокрема, при збільшенні максимального обсягу основного повідомлення від 16 до 128 байт розмір публічного ключа збільшується з приблизно 1,6 КБ до 53 КБ, тоді як розмір основного секретного ключа зростає помірно (від 303 до 649 байт), а розмір додаткового стеганографічного ключа залишається сталим і становить 44 байти незалежно від параметрів коду.

Дослідження стійкості до додаткових помилок підтвердило наявність чітко визначеної межі корекції. Коректне відновлення основного та прихованого повідомлень можливе лише за умови, що ефективна вага вектора помилок не перевищує коригувальної здатності коду. Перевищення цієї межі не призводить до часткового або неконтрольованого витоку інформації, а супроводжується неможливістю детермінованого дешифрування.

Статистичний аналіз шифротекстів із використанням χ^2-статистики Пірсона показав, що значення χ^2 для розподілів позицій і значень помилок у стандартному та анаморфному режимах перебувають в одному діапазоні ($\chi^2 \approx 11–13$ для позицій та $\chi^2 \approx 31$ для значень) і не демонструють систематичних відмінностей при збільшенні обсягу прихованого каналу. Це підтверджує емпіричну невідрізнюваність анаморфного режиму від стандартного режиму роботи криптосистеми.

Криптографічна стійкість запропонованої системи зводиться до складності задачі декодування випадкових небінарних лінійних кодів з помилками, що дозволяє розглядати її як криптографічно еквівалентну класичним McEliece-подібним конструкціям із розширеною функціональністю. Реалізований анаморфний механізм не створює додаткових спостережуваних ознак для зовнішнього атакуючого та забезпечує невідрізнюваність режимів роботи криптосистеми.

Отримані результати підтверджують перспективність запропонованого підходу для застосування в системах захищеного зв'язку, прихованого передавання інформації та сценаріях, де необхідне поєднання криптографічної стійкості з можливістю анаморфної інтерпретації даних. Подальші дослідження можуть бути спрямовані на аналіз формальних моделей безпеки, оптимізацію параметрів коду та розширення реалізації на інші класи кодових криптосистем.

Література

1. Meyer A. (2025). Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems. https://doi.org/10.48550/arXiv.2505.08791.

2. Ojha V.P., Chauhan S., Yarahmadian S., Carvalho D. (2025). Unfolding Post-Quantum Cryptosystems: CRYSTALS-Dilithium, McEliece, BIKE, and HQC. Mathematics, 13(17), 2841. https://doi.org/10.3390/math13172841

3. Freudenberger, J., Thiers, J.-P. (2021). A New Class of Q-Ary Codes for the McEliece

Cryptosystem. Cryptography, 5(1), 11. https://doi.org/10.3390/cryptography5010011

4. Давлетова А. (2024). Алгоритм шифрування даних з корекцією помилок. Вісник Хмельницького національного університету. Технічні науки, 341(5), 168-176. https://doi.org/10.31891/2307-5732-2024-341-5-26

5. Davletova A., Yatskiv V., Ivasiev S., Tsavolyk T., Albanskiy I. (2025). Combined Asymmetric Encryption Algorithm with Error Correction. // Proceedings of the 5th International Conference on Advanced Computer Information Technologies (ACIT). – Šibenik, Croatia, 2025. – P. 461–465. – DOI: 10.1109/ACIT65614.2025.11185734.

6. Abed A., Hermassi H., Barhoumi W. (2024). A New Encryption-Based Algorithm for Embedded Image Steganography. International Journal of Sociotechnology and Knowledge Development. 16. 1-28. 10.4018/IJSKD.349224.

7. Al Saffar N.F.H., Mohammed H.A. (2021). MSB Based Image Steganography Using Mceliece Cryptosystem. MINAR International Journal of Applied Sciences and Technology. 3. 31-40. 10.47832/2717-8234.3-3.5.

8. Kallapu B., Janardhan A. N., Hejamadi R.M., Shrinivas K.R.N., Saritha, Ramesh R.K., Gabralla, L.A. (2025). Multi-Layered Security Framework Combining Steganography and DNA Coding. Systems, 13(5), 341. https://doi.org/10.3390/systems13050341

9. Persiano G., Phan D., Yung M. (2022). Anamorphic Encryption: Private Communication Against a Dictator. 10.1007/978-3-031-07085-3_2.

10. Banfi F., Gegier K., Hirt M., Maurer U., Rito G. (2024). Anamorphic Encryption, Revisited. 10.1007/978-3-031-58723-8_1.

11. Buchanan W., Gilchrist J. (2025). Anamorphic Cryptography using Baby-Step Giant-Step Recovery. 59-71. 10.5121/csit.2025.151704.

12. Do X., Persiano G., Phan D., Yung M. (2025). Anamorphism Beyond One-to-One Messaging: Public-Key with Anamorphic Broadcast Mode. 10.1007/978-3-031-91131-6_15.

13. Deo, A., Libert, B. (2026). Anamorphic Signatures With Dictator and Recipient Unforgeability for Long Messages. In: Hanaoka, G., Yang, BY. (eds) Advances in Cryptology – ASIACRYPT 2025. ASIACRYPT 2025. Lecture Notes in Computer Science, vol 16250. Springer, Singapore. https://doi.org/10.1007/978-981-95-5119-4_12

14. Ganguly S., Chaudhury S.(2025) Computational Quantum Anamorphic Encryption and Anamorphic Secret Sharing. https://eprint.iacr.org/2025/399

15. Banerjee S., Pal T., Rupp A., Slamanig D. (2025) Simple Public Key Anamorphic Encryption and Signature using Multi-Message Extensions IACR Cryptol. ePrint Arch. 2025. https://ia.cr/2025/370

16. Classic McEliece Team. Guide for security reviewers (23 Oct 2022) https://classic.mceliece.org/mceliece-security-20221023.pdf

17. Classic McEliece Team. Notes on a recent claim that a mceliece348864 distinguisher uses only 2^{529} operations (17 Apr 2025). https://classic.mceliece.org/mceliece-529-20250417.pdf

18. Ojha V.P., Chauhan S., Yarahmadian S., Carvalho D. (2025) Unfolding Post-Quantum Cryptosystems: CRYSTALS-Dilithium, McEliece, BIKE, and HQC. Mathematics, 13(17), 2841. https://doi.org/10.3390/math13172841

19. Richter M., Bertram M., Seidensticker J., Tschache, A. (2022) A Mathematical Perspective on Post-Quantum Cryptography. Mathematics, 10(15), 2579. https://doi.org/10.3390/math10152579

20. Li Y., Wang L.-P. (2023) Security analysis of the Classic McEliece, HQC and BIKE schemes in low memory, Journal of Information Security and Applications, Volume 79. https://doi.org/10.1016/j.jisa.2023.103651.

21. Шевчук О. Рандомізована симетрична криптосистема Мак-Еліса на основі узагальнених кодів Ріда-Соломона. Радіотехніка, 1(200), 2020, 25–36. https://doi.org/10.30837/rt.2020.1.200.03

22. Almeida P., Beltrá M., Napp D., Sebastião C. (2023) Smaller Keys for the McEliece Cryptosystem: A Convolutional Variant with GRS Codes. arXiv:2104.06809. https://doi.org/10.48550/arXiv.2104.06809

23. Tang N., Han Y.S., Pei D., Chen C. (2025) A Fast Decoding Algorithm for Generalized Reed-Solomon Codes and Alternant Codes. ArXiv, abs/2502.02356.

24. Welch L.R., Berlekamp E.R. (1986) Error Correction for Algebraic Block Codes. US Patent 4633470. https://www.google.com/patents/US4633470

25. Riasat S., Mahdavifar H. (2025) Efficient Covering Using Reed--Solomon Codes. 10.48550/arXiv.2502.01984.

26. McEliece R.J. (1978) A Public-Key Cryptosystem Based on Algebraic Coding Theory. Coding Thv., DSN Progress Report 4244, 114-116.

27. Николайчук Я.М., Якименко І.З., Возна Н.Я., Касянчук М.М. (2022) Асиметричні алгоритми шифрування у системі залишкових класів. Кібернетика та системний аналіз. Т. 58, № 4. С. 129–138. doi: https://doi.org/10.1007/s10559-022-00494-7 URL: http://jnas.nbuv.gov.ua/article/UJRN-0001335526

28. Kasianchuk M., Yakymenko I., Nykolaychuk, Ya. (2021). Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis. 57. 10.1007/s10559-021-00358-6.

29. Yatskiv V., Kulyna S., Ivasiev S. (2025). Data Encryption Method Based on the McEliece Cryptosystem and the Redundant Residue Number System. Advances in Cyber-Physical Systems. 10. 214-222. 10.23939/acps2025.02.214.

30. Diffie W., Hellman M. (1976) New directions in cryptography, in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654. doi: 10.1109/TIT.1976.1055638.

References

1. Meyer A. (2025). Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems. https://doi.org/10.48550/arXiv.2505.08791.

2. Ojha V.P., Chauhan S., Yarahmadian S., Carvalho D. (2025). Unfolding Post-Quantum Cryptosystems: CRYSTALS-Dilithium, McEliece, BIKE, and HQC. Mathematics, 13(17), 2841. https://doi.org/10.3390/math13172841

3. Freudenberger, J., Thiers, J.-P. (2021). A New Class of Q-Ary Codes for the McEliece Cryptosystem. Cryptography, 5(1), 11. https://doi.org/10.3390/cryptography5010011

4. Davletova A. Data Encryption Algorithm With Error Correction. Herald of Khmelnytskyi National University. Technical sciences 341.5 (2024): 168-176.

5. Davletova A., Yatskiv V., Ivasiev S., Tsavolyk T., Albanskiy I. (2025). Combined Asymmetric Encryption Algorithm with Error Correction. // Proceedings of the 5th International Conference on Advanced Computer Information Technologies (ACIT). – Šibenik, Croatia, 2025. – P. 461–465. – DOI: 10.1109/ACIT65614.2025.11185734.

6. Abed A., Hermassi H., Barhoumi W. (2024). A New Encryption-Based Algorithm for Embedded Image Steganography. International Journal of Sociotechnology and Knowledge Development. 16. 1-28. 10.4018/IJSKD.349224.

7. Al Saffar N.F.H., Mohammed H.A. (2021). MSB Based Image Steganography Using Mceliece Cryptosystem. MINAR International Journal of Applied Sciences and Technology. 3. 31-40. 10.47832/2717-8234.3-3.5.

8. Kallapu B., Janardhan A. N., Hejamadi R.M., Shrinivas K.R.N., Saritha, Ramesh R.K., Gabralla, L.A. (2025). Multi-Layered Security Framework Combining Steganography and DNA Coding. Systems, 13(5), 341. https://doi.org/10.3390/systems13050341

9. Persiano G., Phan D., Yung M. (2022). Anamorphic Encryption: Private Communication Against a Dictator. 10.1007/978-3-031-07085-3_2.

10. Banfi F., Gegier K., Hirt M., Maurer U., Rito G. (2024). Anamorphic Encryption, Revisited. 10.1007/978-3-031-58723-8_1.

11. Buchanan W., Gilchrist J. (2025). Anamorphic Cryptography using Baby-Step Giant-Step Recovery. 59-71. 10.5121/csit.2025.151704.

12. Do X., Persiano G., Phan D., Yung M. (2025). Anamorphism Beyond One-to-One Messaging: Public-Key with Anamorphic Broadcast Mode. 10.1007/978-3-031-91131-6_15.

13. Deo, A., Libert, B. (2026). Anamorphic Signatures With Dictator and Recipient Unforgeability for Long Messages. In: Hanaoka, G., Yang, BY. (eds) Advances in Cryptology – ASIACRYPT 2025. ASIACRYPT 2025. Lecture Notes in Computer Science, vol 16250. Springer, Singapore. https://doi.org/10.1007/978-981-95-5119-4_12

14. Ganguly S., Chaudhury S.(2025) Computational Quantum Anamorphic Encryption and Anamorphic Secret Sharing. https://eprint.iacr.org/2025/399

15. Banerjee S., Pal T., Rupp A., Slamanig D. (2025) Simple Public Key Anamorphic Encryption and Signature using Multi-Message Extensions IACR Cryptol. ePrint Arch. 2025. https://ia.cr/2025/370

16. Classic McEliece Team. Guide for security reviewers (23 Oct 2022) https://classic.mceliece.org/mceliece-security-20221023.pdf

17. Classic McEliece Team. Notes on a recent claim that a mceliece348864 distinguisher uses only 2^{529} operations (17 Apr 2025). https://classic.mceliece.org/mceliece-529-20250417.pdf

18. Ojha V.P., Chauhan S., Yarahmadian S., Carvalho D. (2025) Unfolding Post-Quantum Cryptosystems: CRYSTALS-Dilithium, McEliece, BIKE, and HQC. Mathematics, 13(17), 2841. https://doi.org/10.3390/math13172841

19. Richter M., Bertram M., Seidensticker J., Tschache, A. (2022) A Mathematical Perspective on Post-Quantum Cryptography. Mathematics, 10(15), 2579. https://doi.org/10.3390/math10152579

20. Li Y., Wang L.-P. (2023) Security analysis of the Classic McEliece, HQC and BIKE schemes in low memory, Journal of Information Security and Applications, Volume 79. https://doi.org/10.1016/j.jisa.2023.103651.

21. Shevchuk O. (2020). Randomized symmetric McEliece cryptosystem based on generalized Reed-Solomon codes. Radiotekhnika, 1(200), 25–36. https://doi.org/10.30837/rt.2020.1.200.03

22. Almeida P., Beltrá M., Napp D., Sebastião C. (2023) Smaller Keys for the McEliece Cryptosystem: A Convolutional Variant with GRS Codes. arXiv:2104.06809. https://doi.org/10.48550/arXiv.2104.06809

23. Tang N., Han Y.S., Pei D., Chen C. (2025) A Fast Decoding Algorithm for Generalized Reed-Solomon Codes and Alternant Codes. ArXiv, abs/2502.02356.

24. Welch L.R., Berlekamp E.R. (1986) Error Correction for Algebraic Block Codes. US Patent 4633470. https://www.google.com/patents/US4633470

25. Riasat S., Mahdavifar H. (2025) Efficient Covering Using Reed--Solomon Codes. 10.48550/arXiv.2502.01984.

26. McEliece R.J. (1978) A Public-Key Cryptosystem Based on Algebraic Coding Theory. Coding Thv., DSN Progress Report 4244, 114-116.

27. Nykolaychuk, Ya.M., Yakymenko I.Z., Vozna N.Ya, Kasianchuk M.M. (2022) Asymmetric Encryption Algorithms in the Residue Number System. Cybernetics and Systems Analysis. 2022. Vol. 58, № 4. pp. 129–138. doi: https://doi.org/10.1007/s10559-022-00494-7 URL: http://jnas.nbuv.gov.ua/article/UJRN-0001335526

28. Kasianchuk M., Yakymenko I., Nykolaychuk, Ya. (2021). Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis. 57. 10.1007/s10559-021-00358-6.

29. Yatskiv V., Kulyna S., Ivasiev S. (2025). Data Encryption Method Based on the McEliece Cryptosystem and the Redundant Residue Number System. Advances in Cyber-Physical Systems. 10. 214-222. 10.23939/acps2025.02.214.

30. Diffie W., Hellman M. (1976) New directions in cryptography, in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654. doi: 10.1109/TIT.1976.1055638.