УДК 658.52; 681.3

МЕТОД НАКЛАДЕННЯ ЕЛІПТИЧНИХ КРИВИХ У ЗАДАЧАХ КРИПТОГРАФІЧНОГО ЗАХИСТУ ГРАФІЧНОЇ ІНФОРМАЦІЇ

Юдін О. К., д-р техн. наук, проф., ***Вадясов К. А.***

Національний авіаційний університет

kszi@ukr.net

У статті запропоновано новітні методи криптографічного захисту інформаційних ресурсів, засновані на особливостях алгоритмів еліптичних кривих та методах асиметричного шифрування. Розроблено метод накладення еліптичних кривих та алгоритм генерації випадкових чисел, заснований на шифруванні інформації різноманітних класів зображень.

Ключові слова: криптографія, захист інформації, стиснення зображень, шифрування, шифр, криптографічна система, ключ, еліптичні криві.

In the articles offered the newest methods of cryptographic defence of informative resources are based on the features of algorithms of elliptic curves and methods of the asymmetric enciphering, the algorithm of generation of random numbers is worked out based on шифруємій information and various types of images.

Keywords: cryptography, information security, image compression, encryption, cipher, cryptographic system, key, elliptic curves.

Вступ

Розвиток інформаційних технологій, призводить до широкого використання супутникових каналів зв'язку з метою якісної та достовірної обробки цифрових зображень. Зазначена тенденція встановлює необхідність захисту інформаційних потоків даних з умови відповідності технічним вимогам та можливостям каналів зв'язку. Постійне збільшення кількості переданих супутникових зображень та їх конфіденційність і цінність з погляду прийняття якісних управлінських рішень призвело до потреби використання та розробки сучасних систем криптографічного захисту графічної супутнико-вої інформації, що становить близько 90 % від загального обсягу інформаційних потоків даних. Зазначені системи поряд з методами компактного представлення даних повинні використовувати сучасні методи криптозахисту інформаційних ресурсів. Особливу необхідність в організації таких систем відчувають авіаційні, рятувальні та військові служби. Таким чином, актуальним є розв'язання задач:

- адаптації сучасних методів криптографічного захисту інформації до методів стиску та компактного представлення інформаційних потоків зображень;
- шифрування зазначених потоків на базі нових методів криптозахисту інформаційних ресурсів каналів зв'язку.

Зростання необхідності вирішення питань захисту інформації призводить до постійного розвитку такої науки, як криптографія. Розвиток інформаційних технологій призвів до виникнення окремого розділу криптографії — блочного шифрування. Сьогодні все більшу популярність набирають методи криптографії, засновані на еліптичних кривих, але не адаптованість цих методів до захисту графічної інформації не дає можливості використовувати їх у сучасному супутниковому зв'язку.

Постановка задачі

Розробка та подальше використання адаптованих алгоритмів, заснованих на методі еліптичних кривих, дає свої переваги при шифруванні інформаційних потоків графічної інформації в супутникових каналах зв'язку. Сучасною задачею можна вважати формування нових теоретико-практичних підходів криптозахисту з умов, що:

- ✓ ключ шифру для кожної транзакції генерується на базі конкретного зображення;
- ✓ відсутня необхідність використання спеціальних генераторів псевдовипадкових чисел.

Зрозуміло, що новим та актуальним підходом для вирішення зазначених завдань є використання інформації, яка міститься в графічному зображенні при шифруванні інформаційного потоку даних. Такий вид створення ключів, із використанням частини відкритого повідомлення, надає додаткової криптостійкості алгоритму та спрощує процедуру шифрування.

Мета роботи — розробка та дослідження сучасних методів криптозахисту графічної інформації при формуванні криптосистем на базі алгоритму еліптичних кривих.

Аналіз сучасних підходів до формування криптосистем на базі еліптичних кривих

Криптографія на еліптичних кривих — напрям асиметричного шифрування даних, що швидко розвивається з використанням сучасних

інформаційних технологій. У криптографії на еліптичних кривих усі обчислення (наприклад, вибір значення ключа) проводяться над точками еліптичної кривої, тобто, замість звичайного складання двох чисел виконується за певними правилами складання двох точок кривої, при цьому як результат виходить третя точка.

Цифровий підпис файлів або електронних поштових повідомлень виконується з використанням криптографічних алгоритмів, що використовують несиметричні ключі. Власне для підпису використовується секретний ключ, а для перевірки чужого підпису відкритий. Ключі є числами досить великої довжини (від 512 до 4096 біт) математично або функціонально пов'язаними між собою.

Криптографічним алгоритмом, що стандартно використовується для методів шифрування симетричними ключами (для цілей поширення) є *RSA* (*Rivest, Shamir* і *Adleman*). Хоча *RSA* має високу міру захисту і широко застосовується. Його застосування пов'язане з деякими проблемами та питанням криптостійкості при сучасному розвитку технологій. Альтернативна технологія криптографії на еліптичних кривих, заснована на математичному методі використання функції еліптичних кривих та дає істотні переваги перед *RSA*.

В алгоритмах цифрового підпису активно використовуються обчислення в кінцевих полях Галуа. Ціле позитивне число a порівняно з b за модулем $p\,(a \equiv b \bmod p)$, якщо залишок від ділення b на p дорівнює a.

Можна ввести операції складання і множення за модулем p. Результатом складання двох чисел за модулем p, вважатиметься залишок від ділення їх суми на число p. Неважко помітити, що результати операцій складання або множення пари довільних ненегативних цілих чисел за модулем p не перевершуватимуть число p. У результаті, можна обмежиться розглядом безлічі чисел $0,1...p-1$ із заданими на них операціями складання і множення за модулем p. Множина $0,1...p-1$ із заданими операціями складання і множення, що підкоряються звичайним законам складання, множення і розкриття дужок, утворюють кільце класів розрахунків за модулем p. Елемент b називається зворотним до елементу a, якщо $ab = 1$. Зворотній елемент позначається a^{-1}. Оперуючи тільки цілими ненегативними числами, неважко ввести операцію ділення як множення на зворотний елемент, операцію віднімання і навіть негативні числа. Виявляється, якщо p — просте число, то зворотний елемент існує для усіх елементів кільця (окрім природно числа О). Кільце класів розрахунків, для кожного елементу якого (окрім О) існує зворотний елемент, називають простим полем (чи кінцевим полем, або полем Галуа) і позначається $GF(p)$.

Еліптичною кривою називають безліч пар точок (X, Y), що задовольняють рівнянню: $y^2 = x^3 + ax + b$. Можна накласти обмеження на безліч значень змінних x, y і коефіцієнтів a, b, c. Обмежуючи область визначення рівняння значущою для застосувань числовою множиною ми отримаємо еліптичну криву, задану над даним полем. У додатку до ДСТУ 4145-2002 еліптична крива над кінцевим простим полем $GF(p)$ визначається як безліч пар (x, y), таких що $x, y \equiv GF(p)$, що задовольняють рівнянню:

$$y^2 = x^3 + ax + b \bmod p; \quad a, b \equiv GF(p). \qquad (1)$$

Пари (x, y) називатимемо точками. Точки еліптичної кривої можна складати. Сума двох точок, у свою чергу, теж лежить на еліптичній кривій.

Математична властивість, яка робить еліптичні криві корисними для криптографії, полягає в тому, що якщо взяти дві різні точки на кривій, то хорда, що сполучає їх, перетне криву в третій точці (оскільки ми маємо кубічну криву). Дзеркально відбивши цю точку по осі X, ми отримуємо ще одну точку на кривій (оскільки крива симетрична відносно осі X). Якщо позначити дві первинні точки як P і Q, то отримаємо останню — відбиту точку $P + Q$ (рис. 1). Це складання задовольняє всім відомим правилам алгебри для цілих чисел.

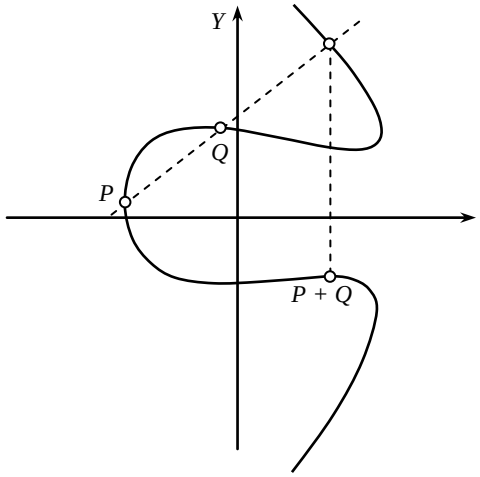

Рис.1. Додавання точок на еліптичній кривій

Окрім точок, що лежать на еліптичній кривій, розглядається також нульова точка. Вважається, що сума двох точок — A з координатами (XA, YA) і B з координатами (XB, YB) — рівна О, якщо $XA = XB$, $YA = -YB \pmod p$. Нульова точка не лежить на еліптичній кривій, але, проте, бере участь в обчисленнях. Її можна розглядати як нескінченно видалену точку.

Таким чином, можна визначити кінцеву абелеву групу точок кривої, де нулем буде нескінченно видалена точка. Зокрема, якщо точки P і Q збігаються, то можна вичислити $P + P$, тобто $2P$. Розвиваючи цю ідею, можна визначити kP для будь-якого цілого числа k, і отже, визначити значення P і значення найменшого цілого числа k, такого, що $kP = F$, де F — нескінченно видалена точка. Тепер можна сформулювати проблему дискретного логарифма еліптичної кривої, на якій заснована дана система: «базова точка P і розташована на кривій точка kP; знайти значення k».

Для еліптичних кривих і базових точок рішення таких рівнянь представляє дуже і дуже велику трудність. З точки ж зору криптографії, ми маємо можливість визначити нову криптографічну систему на основі еліптичних кривих. Врахуйте, що будь-яка стандартна система, заснована на проблемі дискретного логарифма, аналогічна системі заснованій на проблемі дискретного логарифма еліптичної кривої. Наприклад, Еліптична крива *DSA* вже стандартизована (ANSI X9.62) і на її основі може бути реалізований протокол відкритого обміну ключами Дефі–Хелмана.

Для кожної еліптичної кривої кількість точок в групі звичайно, але досить велике. Оцінка порядку (кількості елементів) групи точок еліптичної кривої m така:

$$p+1-2\sqrt{p} \le m \le p+1+2\sqrt{p}, \qquad (2)$$

де p — порядок поля, над яким визначена крива.

Якщо в схемі Эль–Гамаля рекомендується використовувати число p близько 2512, то у разі еліптичної кривої достатньо взяти $p > 2255$.

Кратні точки еліптичної кривої є аналогом мір чисел в простому полі. Завдання обчислення кратності точки еквівалентне завданню обчислення дискретного логарифма. Власне, на складності обчислення кратності точки еліптичної кривої і заснована надійність цифрового підпису та взагалі алгориму. Хоча еквівалентність завдання дискретного логарифмування і завдання обчислення кратності і доведена, друга має велику складність. Саме тому при побудові алгоритмів підпису в групі точок еліптичної кривої виявилося можливим обійтися коротшими ключами порівняно з простим полем при забезпеченні більшої стійкості.

Секретним ключем, як і раніше, покладемо деяке випадкове число x. Відкритим ключем вважатимемо координати точки на еліптичній кривій P, визначувану як $P = xQ$, де Q — вибрана точка еліптичної кривої (базова точка).

Координати точки Q разом з коефіцієнтами рівняння, задаючого криву, є параметрами схеми підпису і мають бути відомі усім учасникам обміну повідомленнями. Вибір точки Q залежить від використовуваних алгоритмів і дуже непростий. При побудові конкретного алгоритму, що реалізовує обчислення цифрового підпису, американський стандарт припускає використання алгоритму *DSA*. Деякі фахівці відмічають, що опис алгоритму цифрового підпису Эль–Гамаля на еліптичній кривій простіший і природніший.

За очевидної трудності використання криптоаналізу (зламу) до алгоритму, криптографію на еліптичних кривих можна застосовувати для високо захищених систем, забезпечуючи порівнянний рівень безпеки. Алгоритм має значно менші розміри ключа, чим, наприклад, алгоритми *RSA* або *DSA*.

Використання еліптичних кривих дозволяє будувати високо захищені системи з ключами явно менших розмірів порівняно з аналогічними традиційними системами типу *RSA* або *DSA*. Такі системи менш вимогливі до обчислювальної потужності і об'єму пам'яті устаткування і тому добре підходять, наприклад, для літаків або супутників.

Зрозуміло, існують і проблеми, які обмежують повсюдне поширення криптографічних систем на основі еліптичних кривих.

Реальну безпеку таких систем недостатньо усвідомлено. Головна проблема полягає в тому, що істинна складність проблеми дискретного логарифма еліптичної кривої не усвідомлена повністю. Недавнє дослідження показало, що деякі шифрування, що використалися для відробітку алгоритмів, еліптичні криві, фактично не підходять для таких операцій. Наприклад, якщо координати базової точки P дорівнюють положенню p, то проблема дискретного логарифма еліптичної кривої має просте рішення. Такі криві є аномальними кривими.

Складність генерації відповідних кривих. При визначенні системи еліптичною кривою вимагаються сама крива і базова точка P. Ці елементи не є таємницею і можуть бути однаковими для усіх користувачів системи. Для цієї кривої і точки нескладно згенерувати відкриті і приватні ключі для користувачів (приватний ключ — випадкове ціле число k, а відкритий ключ — точка Pk на кривій). Отже, надзвичайно важко створити відповідну криву і точку. Треба підрахувати кількість точок на кривій. Для цього необхідно вибрати відповідну базову точку P, координати якої повинні мати досить велике значення, щоб гарантувати складність зламу дискретного логарифма еліптичної кривої. Але, координати P по-

винні ділитися на кількість точок на кривій. Можна стверджувати, що створення кривих — непросте завдання. Користувачі можуть використовувати стандартні криві, використовуючи спеціальне програмне забезпечення, або створювати власні криві, що займає багато часу.

Відносно повільна перевірка цифрового підпису. Як вже було згадано, системи на основі еліптичної кривої використовують ключі малих розмірів. Це знижує вимоги до обчислювальних потужностей порівняно з вимогами систем на основі *RSA*. При незначному збільшенні розмірів ключа створення підписів за допомогою криптографії на еліптичних кривих, проводиться значно швидше чим в аналогічних RSA системах. Це відмінність в ще більшою мірою проявляється для однопроцесорних систем. З іншого боку перевірка підпису за допомогою криптографії на еліптичних кривих проводиться набагато повільніше чим ця сама процедура в системах *RSA* і знову ж таки ця відмінність посилюється для систем з одним процесором. Обробка криптогра-фії на еліптичних кривих дещо прискорюється в парному випадку. Потужність процесора витрачена на перевірку підпису при використанні, криптографії на еліптичних кривих, може уповільнити виконання інших застосувань в системі. Безліч систем мають велику кількість видалених пристроїв, сполучених з центральним сервером і час, витрачений видаленим пристроєм для створення підпису — декілька секунд, не впливає на продуктивність системи в цілому, але сервер повинен також і підтверджувати підписи причому дуже швидко і в деяких випадках системи *RSA* (навіть використовуючі великі ключі) можливо, будуть прийнятніше для використання, чим криптосистеми на основі еліптичної кривої.

Криптосистеми на основі еліптичної кривої набувають усього більшого поширення швидше, як альтернатива, а не заміна системам на основі *RSA*, оскільки системи на основі криптографії на еліптичних кривих мають деякі переваги, особливо при використанні в пристроях з малопотужними процесорами і/або маленькою пам'яттю.

Типові сфери застосування:

- *m* — commerce (наприклад, WAP стільникові телефони, кишенькові комп'ютери);
- смарт-карти (наприклад, EMV);
- e — commerce (електронна торгівля) і банківські операції (наприклад, SET);
- інтернет-застосування (наприклад, SSL).

Метод накладення еліптичних кривих на матрицю зображення

Адаптація алгоритмів еліптичних кривих до стиснення вузького спектру інформації (рис. 2) тісно пов'язана із типом цієї інформації.

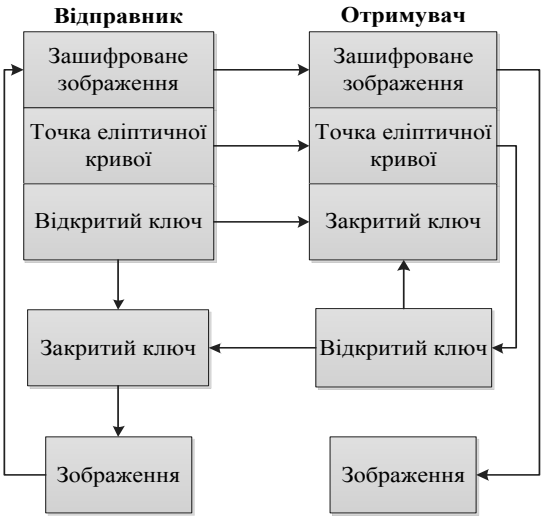

Рис. 2. Схема роботи криптографії на еліптичних кривих з графічною інформацією

Тому необхідно визначити основні параметри та структуру інформації до якої буде адаптований алгоритм еліптичних кривих. У сучасній роботі з графічною інформацією, частіше за все розглядають зображення в декількох кольорових моделях, розглянемо найбільш популярні з них *RGB* та *YUV* (рис. 3).

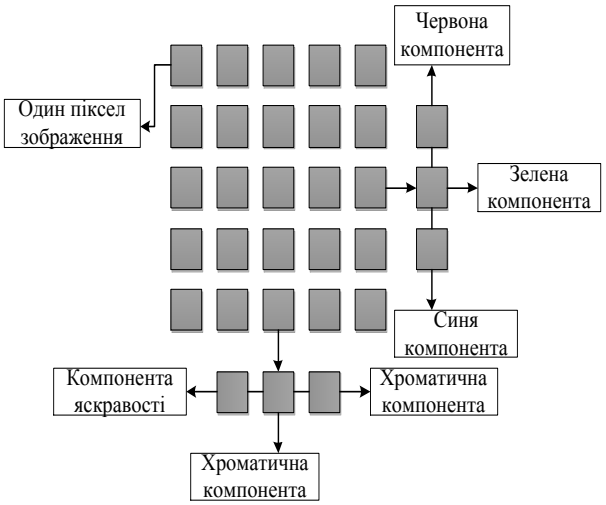

Рис. 3. Кольорові моделі RGB та YUV

У моделі *RGB* колір описуються за допомогою складання трьох колірних пучків — червоного (*Red*), зеленого (*Green*), і синього (*Blue*). Їх також називають колірними каналами моделі *RGB*.

При їх попарному складанні виходять жовтий (*Yellow*), блакитний (*Cyan*), і ясно-пурпурний (*Magenta*) кольори. При складанні усіх трьох виходить білий (*White*) колір. Кожен з базових кольорів може приймати інтенсивність в діапазоні від 0 до 255.

Повна кількість кольорів, що являються цією моделлю рівна 256 × 256 × 256 = 16 777 216.

Чорний колір виходить, якщо інтенсивність усіх базових кольорів дорівнює нулю. Білий колір виходить при їх максимальній інтенсивності (255), тобто, *RGB* — аддитивна модель до сприйняття.

YUV — це специфічний вид кодування кольорової інформації в аналогових телевізійних системах (стандарти *NTSC, PAL* та *SECAM*). Модель *YUV* має компоненту яскравості (*Y*) та дві хроматичні компоненти (*U, V*).

Нерідко у наші дні намагаючись відокремити специфіку кодування *YUV* — кольору у аналоговому телебаченні та при роботі з цифровими даними, використовують терміни *YPbPr* (*YDbDr*) для *YUV* — аналогового та *YCbCr* для YUV — цифрового.

YDbDr — варіант *YUV* — аналогового, що був дуже поширений у Франції та інших країнах (східного блоку) використовувався у стадарті PAL-N.

Сьогодні під терміном *YUV* прийнято розуміти і використовувати саме його для опису формату передачі та збереження інформації про колір у файлових форматах, закодованих у вигляді *YCbCr* (*YCC* чи *YBR*) як *MPEG* чи *JPEG*.

Оскільки дана стаття орієнтована скоріше на роботу з цифровими графічними даними, оминаючи історичні аспекти і усі неоднозначності та нюанси, далі під *YUV* слід розуміти саме *YCbCr*.

Слід зазначити що існують функціональні залежності для переходу з однієї кольорової моделі до іншої, для переходу із моделі *YUV* до моделі *RGB* використовують такі рівності:

$$R = Y + 1{,}13983 \times V; \quad (3)$$

$$G = Y + 0{,}39465 \times U - 5 - 0{,}58060 \times V; \quad (4)$$

$$B = Y + 2{,}03211 \times U. \quad (5)$$

Для переходу від моделі *RGB* до моделі *YUV* використовуються такі рівності:

$$Y = 0{,}299 \times R + 0{,}587 \times G + 0{,}114 \times B; \quad (6)$$

$$U = -0{,}14713 \times R - 0{,}28886 \times G + 0{,}436 \times B; \quad (7)$$

$$V = 0{,}615 \times R - 0{,}51499 \times G - 0{,}10001 \times B. \quad (8)$$

Розглянемо принципи формування ключів у алгоритмах з еліптичними кривими з умов використання функцій переходів базового зображення. Для формування ключа на базі еліптичної кривої візьмемо деяку точку $G(x, y)$ яка належить еліптичній групі $B(a, b)$. Так здійснюватиметься обмін зображенням між двома пристроями — відправником та отримувачем, необхідно погодити всю відкриту інформацію якою будуть обмінюватись відправник та отримувач. Для отримання відкритого ключа *P* обома сторонами необхідно щоб точка $G(x, y)$ була передана від відправника до отримувача. Далі використовуючи відому обом учасникам передачі точку $G(x, y)$ вони генерують відкриті ключі:

$$P_a = n_a G; \quad (9)$$

$$P_b = n_b G, \quad (10)$$

де n_a і n_b випадкові множники.

Зазвичай множники вибираються сторонами обміну у випадковому порядку з використанням генераторів псевдовипадкових чисел, що не залежать від переданої інформації. Зазвичай використовуються так звані генератори випадкових чисел (ГВЧ).

Нарівні з існуючою необхідністю генерувати легко відтворні послідовності випадкових чисел, також існує необхідність генерувати абсолютно непередбачувані або просто абсолютно\або псевдо випадкові числа. Такі генератори називаються генераторами випадкових чисел (ГВЧ — англ. *random number generator*, RNG). Оскільки такі генератори найчастіше застосовуються для генерації унікальних симетричних і асиметричних ключів для шифрування, вони найчастіше будуються з комбінації криптостійкого ГПВЧ і зовнішнього джерела ентропії (і саме таку комбінацію тепер і прийнято розуміти під ГВЧ).

Майже всі великі виробники мікрочипів поставляють апаратні ГВЧ з різними джерелами ентропії, використовуючи різні методи для генерації та їх очищення від неминучої передбачуваності. Отже, на цій момент швидкість збору випадкових чисел усіма існуючими мікрочіпами (декілька тисяч біт за секунду) не відповідає швидкодії сучасних процесорів.

Такий метод генерації випадкових чисел не гарантує повного забезпечення надійності і крім того використовує додаткові ресурси апаратури. Для уникнення цієї проблеми можна використовувати елементи переданої інформації, тобто частину інформації зображення, використовуючи наступні ітерації впровадження нового методу.

1. Побудова еліптичної кривої за формулою (1).

2. Розбиття зображення на кольорові компоненти за моделлю RGB.

3. Накладання еліптичної кривої на матрицю зображення (рис. 4).

4. Вибір точки $G(x, y)$ на еліптичній кривій.

5. Знаходження перетину точки $G(x, y)$ та пікселя зображення.

6. Визначення значення пікселя для кожної (червона, зелена, синя) компоненти.

7. Здійснення переходу зображення з моделі *RGB* до моделі *YUV* за формулами (6), (7), (8).

8. Повторне накладання еліптичної кривої на матрицю зображення.

9. Знаходження перетину точки $G(x, y)$ та пікселя зображення.

10. Визначення значення пікселя для кожної (яскравість, хроматична, хроматична) компоненти.

11. Використання отриманих даних для розрахунку випадкового значення.

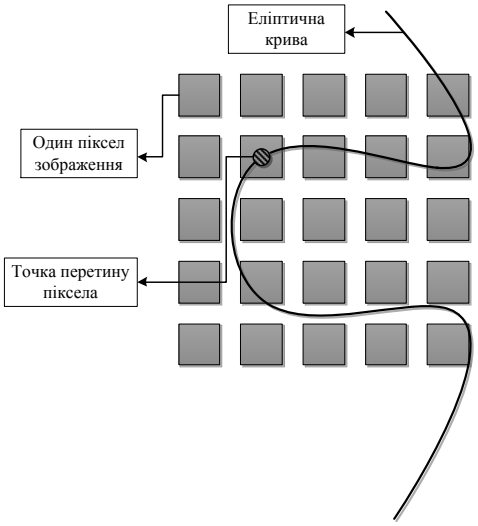

Рис.4. Накладання еліптичної кривої на матрицю зображення

Такий метод використання еліптичних кривих та генерації випадкових чисел є більш надійним та майже не використовує апаратних ресурсів. Надійність та криптостійкість такого методу генерації випадкових чисел, забезпечена природною унікальністю кожного зображення. Але слід враховувати що такий метод генерації випадкових чисел буде мати доволі малу криптостійкість при використанні штучних зображень, графіки, малюнків, тощо. Цей алгоритм адаптовано для використання із супутниковими зображення, зображеннями с камер спостереження тощо.

Треба зазначити, що подібний алгоритм працюватиме лише зі сторони відправника, але також можливе застосування і з боку отримувача за наявності у останнього зображення які не є відкритими та доступними для громадськості.

Ґрунтуючись на проведених дослідженнях запропонованих систем криптографічного захисту інформації, можна виділити такі переваги та недоліки розробленого методу.

Переваги:

– велику швидкість роботи алгоритму;

– малу кількість необхідних апаратних ресурсів;

– більш надійну систему генерації випадкових чисел;

– більшу криптостійкість.

Недоліки:

– неможливість використання алгоритму обома сторонами обміну;

– малу криптостійкість при використані штучних зображень;

– можливу повторюваність згенерованих чисел.

Висновки

Розроблено нові методи формування системи криптографічного захисту інформаційних потоків даних супутникових каналів зв’язку на базі накладення еліптичних кривих на матрицю зображень.Системи криптографічного захисту з адаптованим до графічного зображення алгоритмом еліптичних кривих можуть формувати криптостійкий шифротекст, який буде залежати від типу використаного зображення; якості зображення; типу вибраної кривої; доступність зображення; послідовність виконання алгоритмів криптографічної системи, тощо.

За різних показників цих параметрів можна ефективно регулювати як криптостійкість системи так і коефіцієнт неповторюваності ключа, досягти оптимальних значень показників криптостійкості для кожного окремого класу зображень.

ЛІТЕРАТУРА

1. *Рябко Б. Я.* Основы современной криптографии для специалистов в информационных технологиях / Б. Я. Рябко, А. Н. Фионов. — М. : Научный мир, 2004. — С. 305.

2. *Юдін О. К.* Кодування в інформаційно-комунікаційних мережах: монографія. — К. : НАУ, 2007. — 308 с.

3. *Венбо Мао*. Современная криптография: теория и практика = Modern Cryptography: Theory and Practice / Мао Венбо. — М. : «Вильямс», 2005. — С. 768.

4. *Луцький М. Г*. Інноваційні методи криптографічного захисту інформації на основі систем стиснення зображень/ М. Г. Луцький, О. К. Юдін, К. А. Вадясов // Вісник Інженерної академії України. — К. : Видавництво Інженерної академії України, 2010. — Вип. 1. — С. 144—148.

5. *Joseph H*. Silverman The Arithmetic of Elliptic Curves / H. Joseph. — New York : Springer, 1986. — С. 402.

Стаття надійшла до редакції 21.12.2010.