РЕФЕРАТ

ПЗ: 105 с., 34 рис., 13 табл., 29 джерел

Об’єктом дослідження є криптографія, яка використовує еліптичні криві та спарювання точок на еліптичних кривих.

Предметом дослідження є методи спарювання точок на еліптичних кривих.

Мета роботи та задачі дослідження. Мета роботи полягає у проведенні порівняльного аналізу методів спарювання точок на еліптичних кривих та визначені найпривабливішого алгоритму по критерію швидкодії для заданого рівня криптографічної безпеки.

Наукова новизна результатів:

1. Досліджена математична модель спарювань точок на еліптичних кривих.
2. Порівняння спарювань точок на еліптичних кривих за двома критеріями часу та відповідному рівню безпеки.
3. Показана ефективність застосування спарювань точок на еліптичних кривих зокрема для криптографічного короткого підпису BLS.

КРИПТОГРАФІЯ, ЕЛІПТИЧНА КРИВА, СКІНЧЕНЕ ПОЛЕ, РОЗШИРЕНЕ ПОЛЕ, ДИВІЗОР, ДИСКРЕТНИЙ ЛОГАРИФМ, СПАРЮВАННЯ ТОЧОК, АЛГОРИТМ МІЛЛЕРА

ЗМІСТ

Вступ 8
1. Актуальність криптографії на спарюванні точок еліптичних кривих 10
1.1 Сучасний стан криптографії 10
1.2 Застосування спарювання на еліптичній кривій 11
1.2.1 Криптосистеми на основі ідентифікаційних даних 12
1.2.2 Застосування у SNARKS 13
1.2.3 Застосування при MOV-атаці 14
1.2.4 Короткий підпис BLS 14
1.3 Задача дискретного логарифмування в групі точок еліптичної кривої 15
1.4 Висновки до розділу 17
2 Математичний апарат спарювань точок еліптичних кривих 19
2.1 Еліптичні криві 19
2.2 Дивізори 22
2.3 Класифікація еліптичних кривих призначених для спарювання 26
2.4 Спарювання точок на еліптичних кривих 32
2.4.1 Типи спарювань та підгрупи r-кручення 34
2.4.2 Спарювання Вейля 38
2.4.3 Спарювання Тейта 40
2.4.4 Алгоритм Міллера 41
2.4.5 Оптимальне спарювання Ейта 44
2.4.6 Спарювання etaT 46
2.5 Висновки до розділу 2 49
3 Програмна реалізація та дослідження швидкісних характеристик методів спарювання точок еліптичних кривих 50
3.1 Застосування криптографічної бібліотеки MIRACL 50
3.2 Реалізації методів спарювання 51
3.3 Реалізація короткого підпису BLS 60
3.4 Порівняльний аналіз методів спарювання точок еліптичних кривих 61
3.5 Висновки до розділу 3 67

4 Охорона праці та безпека у надзвичайних ситуаціях 69
4.1 Аналіз потенційних небезпек 69
4.2 Заходи щодо забезпечення безпеки 70
4.3 Заходи щодо виробничої санітарії та гігієни праці 73
4.4 Заходи з пожежної безпеки 78
4.5 Заходи безпеки у надзвичайних ситуаціях 80
5 Економічна частина 84
5.1 Актуальність проекту 84
5.2 Розрахунок витрат на практичну реалізацію проекту 85
5.3 Розрахунок заробітної плати 85
5.4 Розрахунок відрахувань на єдиний соціальний внесок 86
5.5 Розрахунок витрат на обладнання 86
5.6 Розрахунок витрат на послуги сторонніх організацій 87
5.7 Розрахунок загальногосподарських витрат 88
5.8 Розрахунок на амортизацію об'єктів основних засобів 89
5.9 Бальна оцінка економічної ефективності проекту 90
Висновок 94
Список використаних джерел 96
Додаток А 99
Додаток Б 100
Додаток В 101
Додаток Г 103
Додаток Д 105

СПИСОК СКОРОЧЕНЬ

КСОІД - Криптосистеми на основі ідентифікаційних даних

PKI – інфраструктура відкритих ключів

MNT– криві Мияджі, Накабаяші та Такано

CP - криві Cocks-Pinch

BN – криві Баррето і Наехріг

KSS – криві Качіза, Шефер та Скотт

BLS – криві Боне, Лін, Шахам

HCC – несуперсингулярні криві

CC – суперсингулярні криві

PKG – генератор відкритих ключів

MOV – Менезес, Окамото и Ванстон

ZCash - криптовалюта

ВСТУП

Комп'ютерні технології вже повністю увійшли в повсякденне життя. Зараз важко собі уявити підприємство чи компанію, яка з легкістю може обходитися без персональних комп'ютерів. Вже неможливо тримати всю інформацію в голові або на папері, тому комп'ютерні технології мають таку велику цінність. Обчислювальна техніка направлена на допомогу людству, але разом з необмеженими можливостями інноваційні технології приносять і нові проблеми. Головною з них стала проблема захисту інформації від тих, хто не має будь-якого права користуватися нею. Тому паралельно з удосконаленням технологій стали швидко розвиватися методи захисту інформації, що є більш важливим процесом, ніж розробка нових інформаційних технологій. Адже одночасно з поліпшеннями систем захисту удосконалюються і алгоритми злому. А це в свою чергу вимагає негайного вдосконалення і підвищення надійності захисту персональних даних.

Для цього був створений розділ науки під назвою криптологія, яка вивчає математичні методи захисту інформації шляхом її шифрування та дешифрування. Основний напрямок криптології - криптографія. [1]

Криптографія займається вивченням методів перетворення інформації для забезпечення її конфіденційності, цілісності та автентичності.

Ці методи можуть застосовуватися в будь-яких сферах діяльності людини. Вони використовуються як для захисту, так і для приховування справжньої інформації яка передається по каналах зв'язку. [2]

Широке використання еліптичних кривих в криптографії засновано на тому властивості, що завдання дискретного логарифмування на еліптичних кривих є більш трудомісткою, ніж завдання дискретного логарифмування в скінчених полях.

Також треба відмітити, що перевагами еліптичної криптографії є:

1. Набагато менша довжина ключа в порівнянні з «класичною» асиметричною криптографією.

2. Швидкість роботи еліптичних алгоритмів набагато вище, ніж у класичних. Це пояснюється як розмірами поля, так і застосуванням ближчої для комп'ютерів структури бінарного скінченного поля.

3. Через маленьку довжину ключа і високу швидкість роботи, алгоритми асиметричної криптографії на еліптичних кривих можуть використовуватися в смарт-картах та інших пристроях з обмеженими обчислювальними ресурсами.

Еліптичні криві над скінченими полями широко застосовуються в різних криптосхемах. Нещодавно А. Джоукс запропонував використовувати білінійні відображення точок еліптичних кривих над скінченими полями, зокрема, спарювання Вейля і Тейта. Його робота спричинила за собою цілий потік робіт в даній області. За допомогою зазначених відображень (спарювань) можна отримувати криптосхеми з новими цікавими властивостями. Для їх ефективної реалізації необхідно вміти досить швидко обчислювати значення цих відображень.

1 АКТУАЛЬНІСТЬ КРИПТОГРАФІЇ НА СПАРЮВАННІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

У 70-ті роки минулого століття в сучасній криптографії стався великий прорив - вперше були створені алгоритми шифрування, які не вимагали передачі закритих (секретних) ключів між користувачами по каналу зв'язку. Такі алгоритми були названі асиметричними алгоритмами шифрування.

Перша згадка про асиметричних шифри було представлено в роботі «Нові напрямки в сучасній криптографії» Уитфилда Діффі і Мартіна Хеллмана, опублікованій в 1976 році. Вивчаючи роботи Ральфа Меркле про передачу відкритого ключа, вони розробили метод отримання секретних ключів, по відкритому каналу зв'язку. Цей спосіб експоненціального обміну ключами, який згодом став називатися обмін ключами Діффі-Хеллмана.

Сама ідея криптографії, яка використовує відкритий ключ для шифрування даних, безпосередньо пов'язана з односторонніх функцій [3], тобто існує така функція f (x), що за відомим x можна без зусиль знайти значення f (x), тоді як визначення x з f (x) досить непросто. Але використання односторонньої функції в криптографії марно, так як за допомогою неї можна лише зашифрувати повідомлення, але розшифрувати не можна. У цьому випадку вчені придумали алгоритм для досягнення мети розшифровки даних. Вони стали використовувати односторонні функції з «секретом». Цей якийсь секрет сприяє розшифровки тексту. Тобто існує якийсь y, що, знаючи f (x), можна обчислити x.

1.1 Сучасний стан криптографії

На теперішній час криптографічні методи знайшли широке застосування в практичній інформатиці для вирішення чисельних проблем інформаційної безпеки. Сучасна криптографія нараховує ряд проблем:

1. Обмежена кількість робочих моделей. Алгоритми класичної криптографії, можуть бути створені у великій кількості шляхом комбінування різних методів елементарних перетворень. Кожна нова модель ґрунтується на

"нерозв’язній" задачі. В результаті кількість функціонуючих моделей криптографії з відкритим ключем досить невелика.

2. Постійне збільшення обсягу переданих блоків даних і ключів, обумовлене інноваціями в обчислювальної техніки та розвитком математичного апарату. [4]

3. Потенційна ненадійність загально прийнятої криптографії. Зараз теорією обчислювальної складності розглядається питання щодо вирішення задач даного типу за поліноміальний час. В рамках даної теорії вже було доведено зв'язок більшості використовуваних обчислювально-складних задач з іншими аналогічними завданнями. Тобто, якщо буде зламана хоча б одна сучасна криптосистема, то інші будуть піддані такій же небезпеці.

4. Відсутність перспективи. Зараз вже відомо, що сучасна криптографія знаходиться під загрозою через квантові обчислювальні системи, за допомогою яких можна вирішити задачі у багато разів швидше, ніж на звичайних комп'ютерах.[5] Вчені припускають, що серйозні квантові комп'ютери з'являться в нашому світі приблизно через 20-25 років, і як наслідок - майбутнє криптографії стає туманним. В результаті для сучасної криптографії стала актуальна задача підвищення криптостійкості і зменшення обсягу переданих блоків даних шляхом зміни вже існуючих криптосистем.

Необхідно було розвивати нові напрямки в методах захисту інформації. Виходом з цієї ситуації став відносно молодий розділ науки - еліптична криптографія. Даний розділ науки вивчає асиметричні криптосистеми, які базуються на еліптичних кривих над скінченими полями.

1.2 Застосування спарювань на еліптичній кривій

При роботі з еліптичними кривими корисним інструментом являється спарювання точок кривої. Область їх використання за останні роки збільшилась.

Ефективне обчислення білінійної відображення побудовану на основі спарювання Вейля дозволяє ефективно вирішувати як розпізнавальну, так і обчислювальну задачу Діффі-Хеллмана. [6]

Білінійні спарювання дозволили спростити деякі криптосистеми, а також вирішити специфічні завдання криптографії. [7] Наприклад, з використанням білінійних спарювань легко реалізується схема шифрування на основі ідентифікаційних даних, в якій відкритий ключ користувача виходить явно з його ідентифікатора, а закритий генерується і видається центром генерації закритих ключів.

Також білінійні спарювання використовуються для проведення MOV-атаки, обміну організації короткого підпису BLS та у криптовалюті ZCash.

1.2.1 Криптосистеми на основі ідентифікаційних даних

КСОІД (Identity Based Encryption, IBE) - асиметрична криптосистема, в якій відкритий ключ користувача обчислюється відомим способом на основі ідентифікаційних даних цього користувача. Як ідентифікаційної інформації може виступати ім'я користувача, адресу електронної пошти (e-mail), номер мобільного телефону і т.п. Головною перевагою перед класичними асиметричними криптосистемами (відкритий ключ, сертифікат відкритого ключа, закритий ключ) є спрощення інфраструктури відкритих ключів (Public Key Infrastructure, PKI).

На етапі ініціалізації схеми потрібні послуги центру генерації ключів для обчислення закритого ключа користувача. За запитом користувача і проходженню певної процедури аутентифікації центр передає йому закритий ключ. Очевидно, що центр повинен користуватися безумовною довірою. Ідея криптосистем на основі ідентифікаційних даних належить Шаміру. Боні і Франклін зі своєю схемою шифрування на основі ідентифікаційних даних, яка є першою повнофункціональної, ефективної і доказово стійкою КСОІД і заснована на властивостях білінійних спарювань на еліптичних кривих. Криптосистеми на основі білінійних спарювань дозволяють вирішувати основні завдання криптографії: шифрування, вироблення загального ключа, електронний підпис.

Протоколи шифрування на основі ідентифікаційних даних використовуються для досягнення секретності (конфіденційності) обміну

інформацією між двома абонентами. Проблема розподілу відкритих ключів усунена, відкритий ключ користувача B виходить відомим способом з його ідентифікатора. Для розшифрування повідомлення користувач B проходить процедуру аутентифікації у PKG і отримує свій закритий ключ [8].

1.2.2 Застосування у SNARKs

Регулярні конструкції еліптичних кривих використовуються в механізмі роботи системи доказів з нульовим розголошенням SNARKs застосованих у криптовалюті zCash та призначені для таких речей, як цифрові підписи. Точки на кривій утворюють циклічну групу: їх можна скласти і помножити скалярами. Вважається, що неможливо знайти множинну заданої точки, що називається "задачею дискретного логарифму еліптичної кривої".

Ця асиметрія (легкість множення, але складність зворотного) використовується для створення ряду корисних інструментів і протоколів. Наприклад: обмін ключами Діффі-Хеллмана.

Криптографія на спарюваннях є розширенням цих понять. Вважається, що є дві циклічні групи: G_1 і G_2, написані додатково, і відображення до третьої циклічної групи форми e: $G_1 \times G_2 \rightarrow G_T$, де G_T записується мультиплікативно. Якщо це відображення є білінійним, то:

$$e: (ag_1, bg_2) = e(g_1, g_2)^{ab} \quad (1.1)$$

де a та b - скаляри, а g_1 і g_2 - генератори для їх відповідних груп.

Zcash використовує оптимальне спаровування Ate, яке засноване на спрощеному спарюванні Тейта і може бути обчислено більш ефективно, ніж спарювання точок Тейта.

По суті, скалярне множення однієї з перших двох елементів групи еквівалентно експоненції скінченого елементу групи. [9]

1.2.3 Застосування при MOV-атаці

MOV-атака, зводиться до відображення пари точок кривої E над деяким розширенням F_q^k поля F_q в елемент поля розширення, що при невеликих значеннях k катастрофічно знижує складність дискретного логарифмування.

Нехай задані еліптична крива EC: $y^2 = x^3 + ax + b \pmod{p^r}$, і точки P, Q ∈ EC порядку r, де r - просте число, причому існує m таке, що Q = mP. Потрібно знайти множник m. Відображення Вейля будемо позначати через e (X, Y). Алгоритм обчислення m полягає в наступному:

1. Знаходимо випадкову точку T ∈ EC (F_q^k).

2. Знаходимо порядок M точки T.

3. Знаходимо d = Н.О.Д. (N, M). Якщо d = 1, то повертаємося до п.1. Інакше, перейдемо до наступного пункту. Визначимо, що в цьому випадку точка T має порядок r.

4. Обчислимо a = e (P, T) і c = e (Q, T).

5. Обчислюючи дискретний логарифм в поле F_q^k, знайдемо шуканий множник m.

Відзначимо, що можна виконувати цей алгоритм з складовим r, тоді число d може виявитися власним дільником r і знайдений множник виявиться рівним m mod d. В цьому випадку можна повторювати обчислення з різними точками T_i, обчислюючи $m_i = m \bmod d_i$ доти, поки добуток різних d_i не стане більше або дорівнювати r.

Зауваження. Якщо мова йде про довільну точку Q, то перш, ніж визначать дискретний логарифм, корисно знати, чи знайдеться таке m, що Q = mP [10].

1.2.4 Короткий піднпис BLS

У криптографії схема підписів Boneh-Lynn-Shacham (BLS) дозволяє користувачеві перевіряти, чи є підписувач справжнім. У схемі використовується білінійне спарювання для перевірки, а підписання - елементи групи еліптичних кривих. [11]

Робота в групі еліптичних кривих забезпечує деякий захист від атак обчислення індексу.

Якщо існує циклічна група з білінійним відображенням (спарюванням), то група, де є обчислювальна проблема Діффі-Хеллмана вважається важкою, однак цей варіант легко вирішити. Такі групи іноді називають Gap Diffie-Hellman (GDH) групами, і вони передбачають схему підписів, часто називають схемою підписів BLS.

Алгоритм короткого підпису BLS:

Етап 1: обрати GDH групу G2 з простим порядком r. Генератор групи G2 є точка Q.

Етап 2: генерація ключів. Обрати випадковий s у {1,…,r-1}. Обчислити публічний ключ Q^s, де s – секретний ключ.

Етап 3: підпис. Отримане повідомлення хешується точкою R∈G1, обчислюється R^s.

Етап 4: верифікація. Обчислюється спарювання e(Q, Q^s) та e(R, R^s). Короткий підпис справжній при рівності цих спарювань. [12]

Корисними властивостями короткого підпису BLS є:

- кілька підписів, створених за допомогою кількох відкритих ключів для декількох повідомлень, можуть бути об'єднані в єдиний підпис;
- для даного ключа і повідомлення, є тільки один дійсний підпис. [13]

1.3 Задача дискретного логарифмування в групі точок еліптичної кривої

Стійкість основного криптографічного перетворення, що використовується для обчислення цифрового підпису на еліптичній кривій, визначається складністю вирішення задачі дискретного логарифмування в циклічній підгрупі ⟨P⟩ великого простого порядку n групи точок еліптичної кривої, тобто складністю рішення рівняння $Q = kP, Q \in \langle P \rangle$відносно k, k – ціле число, $1 < k < n$.

Складність рішення задачі, що задається вхідною послідовністю довжиною t бітів, визначається як число бітових операцій L(t), які необхідно виконати для отримання рішення. Якщо функція L(t) являє собою многочлен, то таке завдання має поліноміальну складність і вважається простим. Як приклади таких задач можна привести задачу піднесення цілого числа до степеня по модулю цілого числа, задачу обчислення найбільшого загального дільника двох цілих чисел або задачу доказу простоти цілого числа. Якщо функція L(t) має вигляд $L(t) = e^{\lambda t}$, де λ - постійна, то кажуть, що задача має експоненційну складність.[14] Такі задачі вважаються дуже складними і становлять найбільший інтерес для криптографії, що використовуються у несиметричних алгоритмах. В теорії складності розглядаються функції L(t), що мають проміжну швидкість росту. Ці функції залежать від трьох параметрів і мають вигляд $L(t, v, \lambda) = \exp(\lambda t^{v}(\log t)^{1-v})$, де $0 \leq v \leq 1$, $\lambda > 0$. При v = 0 $L(t,0,\lambda)=t^{\lambda}$ отримуємо поліноміальну складність, при v=1 - $L(t,1,\lambda)=e^{\lambda t}$ маємо експоненційну складність. Якщо ж 0 < v <1, то ця проміжна складність називається субекспоненційною.

У нашому випадку довжина вхідної послідовності для задач дискретного логарифмування - це довжина двійкового представлення числа n. Тому стосовно до задачі дискретного логарифмування експоненційна складність має порядок зростання n^{λ}, а субекспоненційна складність для завдання дискретного логарифмування має порядок $exp(\lambda(\log n)^{v} (\log\log n)^{1-v})$. Очевидно, що чим менше v, тим простіше в обчислювальному значенні завданню, отже, практично воно може бути вирішене для великих значень n.

У довільній скінченній циклічній групі завдання дискретного логарифмування можна вирішити за допомогою методу Шенкса або ρ-методом та λ-методом Полларда. [15]

На даний момент найшвидшим і ефективним алгоритмом, який вирішує проблему дискретного логарифмування на еліптичних кривих, є алгоритм, придуманий Деніелом Шенксом під назвою «алгоритм великих і малих кроків». Складність даного алгоритму обчислюється за формулою $0\sqrt{n}$. З цієї формули випливає, що розмір обраного поля еліптичної кривої повинен як мінімум в 2 рази перевищувати розмір ключа. Так, наприклад, для стійкого алгоритму

шифрування з ключем довжиною 256 біт необхідно вибрати еліптичну криву з характеристикою поля $p \approx 2^{512}$.

Хоча в самій групі точок еліптичної кривої немає субекспоненціальних алгоритмів дискретного логарифмування і малоймовірно їх поява в майбутньому, завжди є можливість зведення вихідної задачі дискретного логарифмування до аналогічної задачі в інших групах, де субекспоненціальні алгоритми існують. При певних умовах це дає можливість отримати субекспоненціальний алгоритм для вихідної задачі.

Перше таке зведення за допомогою спарювання Вейля зведення вихідної задачі над полем $GF(2^m)$ до задачі дискретного логарифмування в мультиплікативної групі деякого розширення $GF(2^{km})$ вихідного поля.

Якщо ступінь розширення k малий, то для вихідної задачі дискретного логарифмування існує субекспоненціальний алгоритм.

Наприклад, в разі вкрай привабливих з обчислювальної точки зору суперсінгулярних кривих k <=6, тому довелося відмовитися від застосування таких кривих в криптографії. Відомо легко перевіряється умова (умова Менезеса- Окамото-Венстона), за допомогою якої можна вибрати криву з будь-яким заданим значенням k.

Найбільш інтересні для захищеності діапазони повинні бути при k> 30. Цю умову можна назвати локальним в тому сенсі, що над будь-яким полем існує багато кривих, на яких завдання дискретного логарифмування не зводиться до субекспоненціальної нагоди і перевірка незвідність проводиться індивідуально для кожної конкретної кривої.

Аналогічне зведення виконується і за допомогою спарювання Тейта[4].

1.4 Висновки до розділу 1

Оскільки в групі точок еліптичної кривої немає субекспоненціальних алгоритмів дискретного логарифмування, спарювання точок з різних груп має хороші показники захищеності.

Виграшом застосування спарювання є зменшення числа інформаційних обмінів по мережі.

При роботі з еліптичними кривими корисним інструментом являється спарювання точок кривої. Область їх використання за останні роки збільшилась.

Ефективне обчислення білінійного відображення збудована на основі спарювання Вейля дозволяє ефективно вирішувати як розпізнавальну, так і обчислювальну задачу Діффі-Хеллмана.

Так, наприклад, ще в минулому столітті спарювання використовувалось у криптосистемах на основі ідентифікаційних даних та для проведення MOV-атаки, то в наші часи спарювання (оптимальне спарювання Ейта) використовується у криптовалюті zCash.

Також, спарювання можуть використовуватися для електронно цифрових підписів, зокрема короткий підпис BLS.

2 МАТЕМАТИЧНИЙ АПАРАТ СПАРЮВАННЯ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

2.1 Еліптичні криві

Найбільш очевидний шлях вирішення проблеми підвищення стійкості - уявлення шифрованих блоків інформації в криптографічних алгоритмах не тільки за допомогою чисел, але і за допомогою інших алгебраїчних елементів більшої складності. Найбільш відповідними типами таких елементів є точки еліптичних кривих.

Еліптична крива над полем F_q — це множина точок проективної площини $(x, y) \in Fq \oplus Fq$, що задовольняють рівнянню Вейерштрасса:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (2.1)$$

разом з точкою на нескінченності. [17]

Загалом у криптографії на еліптичних кривих розглядається два види кривих над скінченими полями:

- простими полями непарною характеристики F_q, де $q > 3$ є простим числом;
- полями характеристики 2 ($GF(2^n)$ – бінарне скінчене поле).

У еліптичних кривих над полем $GF(2^n)$ є одна важлива перевага, елементи поля $GF(2^n)$ можуть бути легко представлені у вигляді n – бітових кодових слів, це дозволяє збільшити швидкість апаратної реалізації еліптичних алгоритмів.

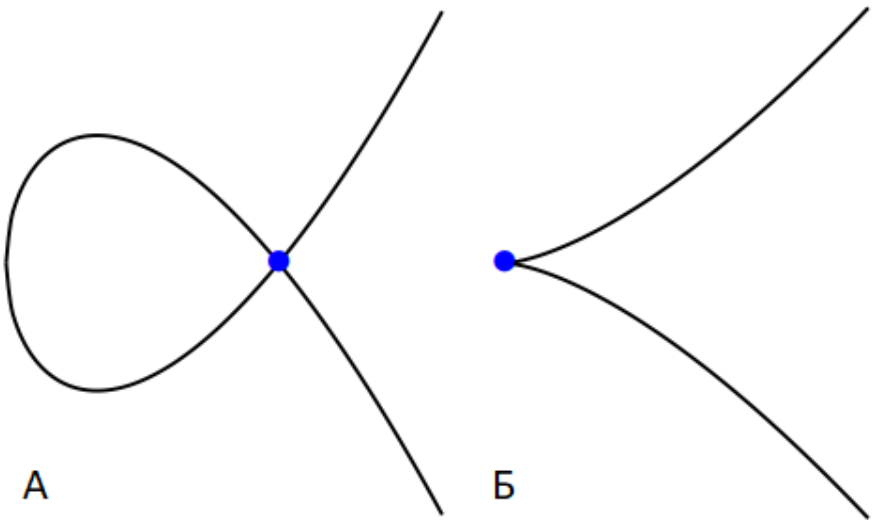
Всі математичні операції на еліптичних кривих над скінченим полем виконуються за законами скінченого поля над яким побудована еліптична крива. Тобто для обчислення, наприклад, суми двох точок кривої E над кільцем відрахувань всі операції проводяться по модулю числа p.

Якщо характеристика поля F_q (Char K) не рівна 2 або 3, то рівняння за допомогою заміни координат приводиться до канонічної форми:

$$y^2=x^3+ax+b \quad (2.2)$$

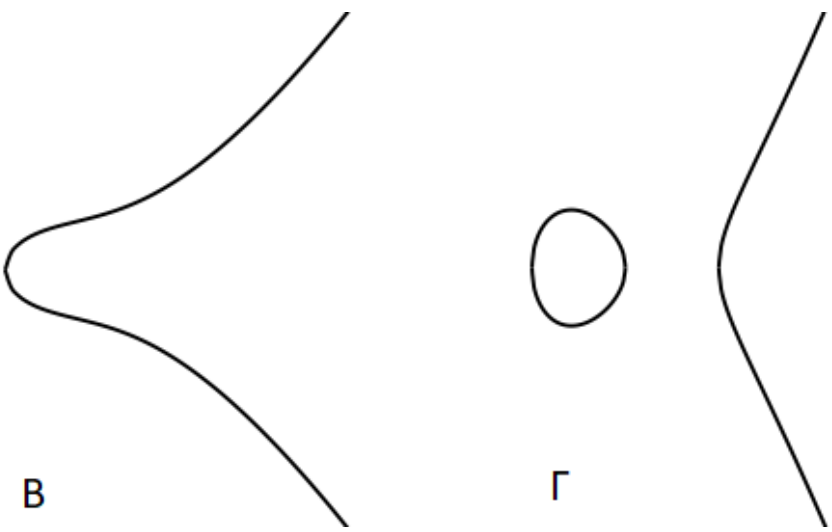
де a,b ∈ F_q, яке називається скороченим рівнянням Вейерштрассе.

У криптографії використовуються еліптичні криві, визначені над скінченими полями. Ілюстрацію різниці між сингулярними та несингулярними (гладкими) еліптичними кривими можна побачити на рис. 2.1-2.2.



А) $y^2 = x^3 - 3x + 2$; Б) $y^2 = x^3$

Рисунок 2.1 - Сингулярні криві



В) $y^2 = x^3 + x + 1$; Г) $y^2 = x^3 - x$.

Рисунок 2.2 - Несингулярні криві:

Для несингулярних (гладких) еліптичних кривих виконується наступна нерівність (2.3):

$$4a^3+27b^2\neq0 \tag{2.3}$$

Тоді як для сингулярних кривих ця умова, не виконується. В математиці сингулярністю позначається така точка, в якій функція має незвичайну поведінку, наприклад, прямує до нескінченності. Вчені вважають, що використання сингулярних кривих в алгоритмах криптографії призводять до зменшення криптостійкості алгоритму. Тому використання таких кривих заборонено.

Над бінарним скінченим полем використовуються два види еліптичних кривих (2.4) та (2.5):

- суперсингулярна крива

$$y^2+\mathrm{a}y=x^3+\mathrm{b}x+\mathrm{c}; \tag{2.4}$$

- несуперсингулярна крива

$$y^2+\mathrm{a}xy=x^3+\mathrm{b}x^2+\mathrm{c}. \tag{2.5}$$

Ще одним важливим поняттям еліптичної криптографії є порядок еліптичної кривої, який показує кількість точок кривої над скінченим полем.

Оскільки скінчене поле GF_q складається з q елементів, можна сказати, що порядок кривої $E(\mathrm{F_q})(a,b)$ за теоремою Хассе (2.6) дорівнює:

$$\#E(F_q) = q + 1 - t, \tag{2.6}$$

де $|t| \leq 2\sqrt{q}$ слід Фробеніуса.

З цього випливає, що груповий порядок еліптичної кривої лежить у інтервалі $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$, отже число еліптичних кривих, які визначаються над полем F_q дорівнює сумі групових порядків на інтервалі за формулою (2.6).

З числом t пов'язано таке визначення: еліптична крива над скінченим полем називається суперсінгулярною, якщо t ділиться на характеристику поля без залишку, у іншому випадку криву називають звичайною.

2.2 Дивізори

Поняття дивізорів засноване на тому спостереженні, що коефіцієнти будь– якого полінома можна обчислити з точністю до ненульового множника, знаючи коріння цього многочлена і їх кратність. Якщо многочлен $P(x)$ має своїм корінням кратності r_i елементи x_i, то:

$$\mathrm{P(x)} = \mathrm{a} * \prod(\mathrm{x} - \mathrm{x_i})^{r_i}. \tag{2.7}$$

Нехай тепер E: $y^2=x^3+ax+b$ еліптична крива над полем K, а $f(x,y)$: $E \to K$ дрібно-раціональна функція. Якщо f не константа, то існує числа точок $P \in E$, в яких $f(P)=0$, або $f(P)=\infty$. Точки першого виду називаються *нулями функції* f, а другого *плюсами* f. [17]

З точністю до ненульового множника функцію f можна задати, перераховуючи всі її нулі і полюси і задаючи їх кратність. Якщо f має нуль (полюс) кратності k в точці P, то f можна представити у вигляді добутку $gf = u_P^k * g$, де u_P має в точці P нуль (полюс) першого порядку, а $g(P) \neq 0, \neq \infty$. Функція u_P називається уніформізатором функції f в точці P.

Розглянемо криву $y^2 = x^3 - x$ та функцію $f(x,y) = x/y$. Перепишемо функцію f у наступному вигляді:

$$f(x,y) = \frac{x}{y} = \frac{xy}{y^2} = \frac{xy}{x^3-x} = \frac{y}{x^2-1} = y * \frac{1}{x^2-1}. \tag{2.8}$$

З цього представлення випливає, що точка P(0,0) є нулем першого порядку функції $f(x,y)=x/y$, а функція $u(x,y)=y$ її уніформізатором в точці P(0,0).

Нехай M1 множина нулів, а M2 множина полюсів функції $f(x,y)$. Тоді порівнявши функції маємо формальне вираження:

$$f(x,y)\sim\sum_{P\in \mathrm{M}_1} r_P[P]-\sum_{P\in \mathrm{M}_2} r_P[P], \tag{2.9}$$

де r_p – кратність нуля (полюса) P.

Визначення 2.1. Нехай $y^2=x^3+ax+b$ еліптична крива над полем k. Дивізором D над кривою E називається формальна сума виду:

$$D=\sum_{P\in E} r_P[P] \tag{2.10}$$

в якій коефіцієнти $r_p\in Z$ цілі числа (позитивні або негативні).

Множина точок P, для яких $r_p\neq 0$, називається носієм (support) дивізора D та позначається $supp(D)$. Ціле число $k=\Sigma r_p$, $P\in supp(D)$ називається степенем D та позначається $deg(D)$. Точка еліптичної кривої дорівнює $D=\Sigma r_p\cdot P, P\in E$ називається сумою дивізора D та позначається $sum(D)$.

Нехай $P,Q,R,S\in \mathrm{E}(F_q)$, та $D1=2(P)-3(Q)$, $D2=3(Q)+(R)-(S)$. Тоді $Deg(D1)=2-3=-1$ та $Deg(D2)=3+1-1=3$. Сума дивізорів $sum(D1+D2)=2(P)+(R)-(S)$.

Ступінь дивізорів $Deg(D1+D2)=Deg(D1)+Deg(D2)=2$. З цього випливає, що множина точок $supp(D1)=\{P,Q\}$, $supp(D2)=\{Q,R,S\}$ та $supp(D1+D2)=\{P,R,S\}$.

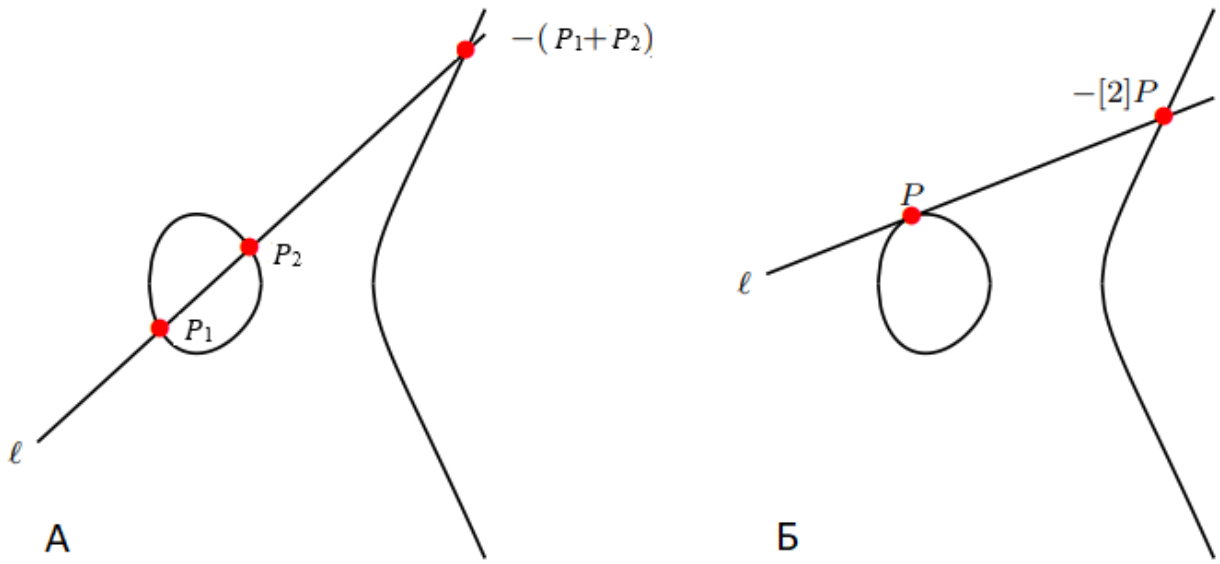
Сума дивізорів визначається природним чином. Множина дивізорів еліптичної кривої утворює адитивну групу щодо операції додавання, а нулем є дивізор, у якого всі коефіцієнти рівні 0, та визначається як $Div^0(E)$. У групі дивізорів найбільш важливу роль відіграють дивізори функцій, які називаються головними дивізорами (principal divisors).

Для будь-якої раціональної функції f кривої E та будь-якої точки з цієї кривої можна визначити ціле число $ord_p(f)$, що називається порядком цієї функції в точці P. Тоді дивізором функції f називається:

$$div(f) = \sum_{P \in E} ord_p(f)(P). \tag{2.11}$$

Такі дивізори називаються головними (2.11).

Якщо дивізор прямої l: $ax + by + c$, що проходить через дві точки P_1 та P_2 та l перетинає E в третій точці, тоді $(l) = [P] + [Q] + [-(P + Q)] - 3[\infty]$ (рис. 2.3 А). Якщо l є дотичною в точці P, тоді $(l) = 2[P] - 2[P] - 3[\infty]$ (рис. 2.3 Б).



А – проходить через точки P_1 та P_2; Б – являється дотичною точки P

Рисунок 2.3 - Дивізор прямої l

Баланс, який відбувся між нулями та полюсами, що призвело до $Deg\,((\ell)) = 0$, не є випадковим. Фактично, для будь-якої функції f на еліптичній кривій E завжди маємо $Deg\,((f)) = 0$. Ця властивість випливає з того, що ступінь афінного рівняння, що вирішує для нулів функції f на еліптичній кривій E, відповідає ступінь проективного рівняння, що визначає кратність

полюса функції f на ∞, тобто проективна версія функції f є g / h, де g та h мають обидва ті самі ступені, що і f.

Обчислимо дивізор прямої l: $ax+by+c$, що проходить через дві задані точки $P_1\,(x_1,y_1)$ та $P_2\,(x_2,y_2)$ еліптичної кривої E. Якщо l не є дотичною в точках P_1 та P_2, то вона перетинає E і в третій точці $P_3(x_3,y_3)$, а також в нескінченно віддаленій точці ∞. В точках P_1, P_2 та P_3 пряма l має нулі 1 порядку, а в т. ∞ – полюс 3 порядку. Щоб це побачити, перепишемо рівняння ЕК $y^2=x^3+Ax+B$ в наступному вигляді:

$$(x/y)^2 = x^{-1}(1+A/x^2+B/x^3). \qquad (2.12)$$

Звідки :

$$x^{-1} = (x/y)^2(1+A/x^2+B/x^3)^{-1}. \qquad (2.13)$$

З рівняння (2.5) слідує, що x/y перетворюється на 0 в точці ∞, а рівняння (2.6) показує, що функція x/y є уніформізатором x^{-1} в точці ∞ и точці ∞ є нулем другого порядку для x^{-1}. Отже точка ∞ є полюсом 2 порядку для x. Так як $y=x*(y/x)$, точка ∞ є полюсом 3 порядку для y і для функції $l=Ax+By+C$. Звідси дивізор прямої l має вигляд :

$$div(l_{P1,P2})=1[P_1]+1[P_2]+1[P_3]-3[\infty]. \qquad (2.14)$$

Проведемо через точку P_3 вертикальну пряму $v=x-x_3$. Вона проходить через точку $P_3(x_3,y_3)$, $-P_3(x_3,-y_3)$ та точку ∞, а її дивізор має вигляд :

$$div(v_{P3})=1[P_3]+1[-P_3]-2[\infty]. \qquad (2.15)$$

З формул (2.14) та (2.15) отримаємо :

$$div[(A_x+B_y+C)/(x-x_3)]=div(A_x+B_y+C)-div(x-x_3)=[P_1]+[P_2]-[-P_3]-[\infty] \quad .(2.16)$$

Так як $P_1+P_2=-P_3$ на кривій E, то останню формулу можна переписати у вигляді

$$[P_1]+[P_2]=[P_1+P_2]+[\infty]+div[(A_x+B_y+C)/(x-x_3)]. \quad (2.17)$$

З формул (2.14) та (2.15) можна побачити, що згідно з визначенням (2.7) ступені прямих $l_{P1,P2}$ та v_{P3} дорівнюють 0, а їх сума дорівнює ∞, що є прикладом загального факту, що виражається наступною теоремою:

Теорема 2.1. Дивізор D еліптичної кривої E, що має ступінь 0, є дивізором деякої функції тоді і тільки тоді, коли $sum(D)=\infty$.

Відображення, що задається формулою (2.9), є груповим гомоморфізмом з адитивної групи дивізорів в мультиплікативну групу поля F_q, тому що

$$f(D1+D2)=f(D1)\cdot f(D2),\ f(D1-D2)=f(D1)/f(D2). \quad (2.18)$$

Поширюючи формули (2.17) на довільні дивізори, отримаємо формулу:

$$f(\Sigma kP)=\Pi f(P)^k. \quad (2.19)$$

Наступна теорема носить назву закону взаємності Вейля (Weil reciprocity).

Теорема 2.2**.** Якщо f і g – функції на еліптичній кривій такі, що $div\ (f)$ і $div\ (g)$ не мають спільних точок, тоді виконується наступна формула:

$$f(div\ (g))=g(div\ (f)). \quad (2.20)$$

2.3 Класифікація еліптичних кривих призначених для спарювання

Найбільш поширеними спарюваннями, що використовуються в програмах, є спарювання Тейта та Вейля на еліптичних кривих над скінченими полями. Загалом спарювання беруть в якості вхідних точок на еліптичній кривій

E, яка визначена над скінченим полем F_q, і виділяють як вихідний елемент розширення поля F_q^k. Для того, щоб система була безпечною використовується задача дискретного логарифму в групі E (F_q).

Найбільш відомий алгоритм дискретного логарифмування на еліптичних кривих - це розпаралельований алгоритм Полларда «ро», який має час роботи O ($\sqrt{r}$), де r - розмір найбільшої підгрупи основного порядку E (F_q).

З іншого боку, найкращим алгоритмом обчислення дискретного логарифму в скінчених полях є атака обчислення індексу, що має субекспоненціальний алгоритм. Таким чином, щоб досягти такого ж рівня безпеки в обох групах, розмір q^k розширеного поля повинен бути значно більшим, ніж r. Співвідношення цих розмірів вимірюється за двома параметрами: ступенем вкладу, який є ступенем k розширеного поля, та розміру поля q.

Параметр ρ=log(q)/log(r) вимірює розмір поля відносно розміру підгрупи основного порядку на кривій. Загалом криві з малими ρ - значеннями бажані, щоб прискорити арифметику на еліптичній кривій. За параметрами ρ та r, можна дізнатися рівень захищеності, розмір підгрупи, розмір розширеного поля та ступінь вкладу (табл. 2.1).

Таблиця 2.1. Бітові розміри параметрів кривих і відповідних ступенів вкладу для отримання бажаних рівнів безпеки

Рівень безпеки (біт)	Розмір r підгрупи (біт)	Розмір розширеного поля q^k (біт)	Ступінь вкладу k	
			ρ≈1	ρ≈2
80	160	640-1280	6-8	2,3-4
112	224	2200-3600	10-16	5-8
128	256	3000-5000	12-20	6-10
192	384	8000-10000	20-26	10-13
256	512	14000-18000	28-36	14-18

Еліптична крива з невеликим ступенем вкладу та великою підгрупою головного порядку називається еліптичною кривою, яка підходить для спарювання (pairing-friendly elliptic curve). [18]

Діаграма, що описує цю класифікацію, наведена на рис. 2.4.

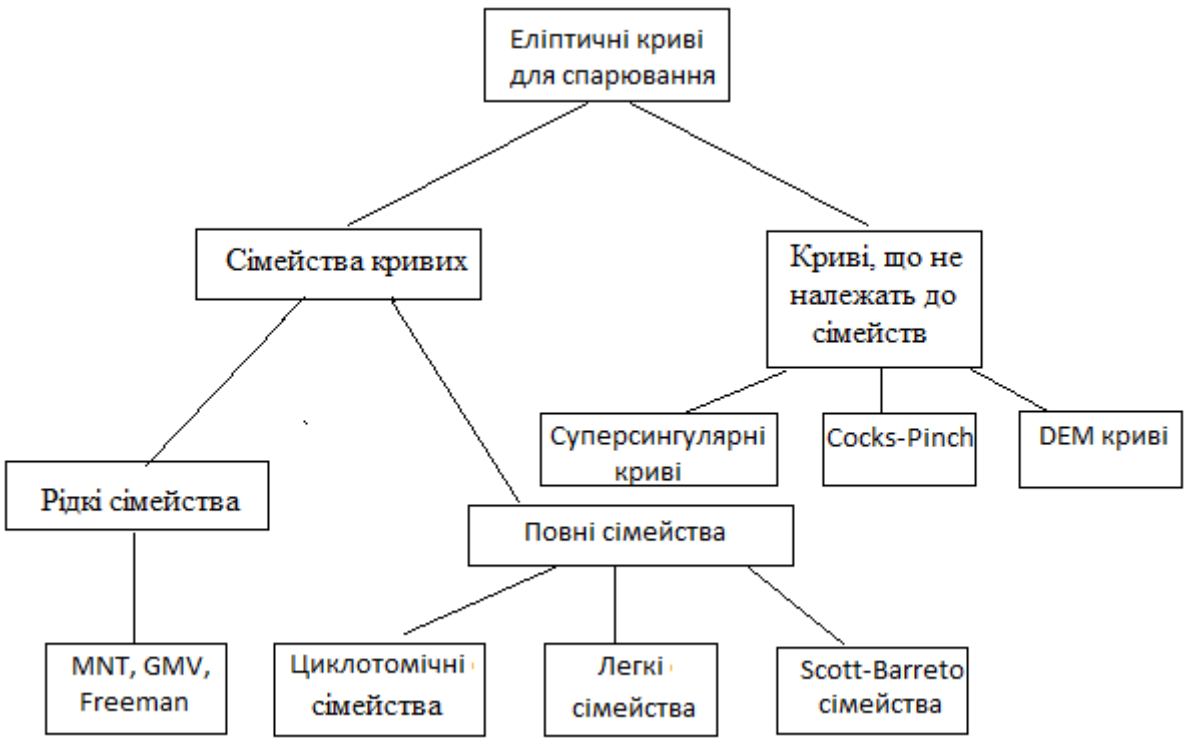


Рисунок 2.4 - Класифікація еліптичних кривих для спарювання

Побудова кривих залежить від вміння знаходити цілі числа x, y, що задовольняють рівнянню форми (2.21):

$$Dy^2 = 4q(x) - t(x)^2 \tag{2.21}$$

для деякого постійного цілого числа D та многочленів *q(x)* і *t(x)*. Параметр D - це "дискримінант CM". В деяких випадках це рівняння матиме лише рішення для деякого набору (*x*, *y*), що зростає експоненціально, такі сім'ї являються легкими «рідкісними». В інших це рівняння може бути виконане для будь-якого

x, тобто y записується як поліном з x і рівняння дає рівність многочленів, такі сім'ї називаються повними.

МНТ криві

Мияджі, Накабаяші та Такано - перші автори, які запропонували звичайні криві, що придатні до спарювання точок, при ступенях вкладу k = 3, 4 та 6. Фактично, звичайні криві первинного порядку із вкладеними ступенями 3, 4 і 6 були повністю характеризованими наступним чином:

Нехай q буде просте та E/F_q буде звичайною еліптичною кривою, такою що порядок кривої r = #E(F_q) простий. Нехай слід Фробеніуса t=q+1-r, тоді:

- поле E має ступінь вкладання k = 3 тоді і тільки тоді, коли існує x ∈ Z такий, що $t = -1 \pm 6x$ та $q = 12 * x^2 - 1$;

- поле E має ступінь вкладання k = 4 тоді і тільки тоді, коли існує x ∈ Z такий, що $t = -1$ або $t = x + 1$ та $q = x^2 + x + 1$;

- поле E має ступінь вкладання k = 6 тоді і тільки тоді, коли існує x ∈ Z такий, що $t = 1 \pm 2x$ і $q = 4x^2 - 1$.[19]

BN криві

Криві BN - це сімейство еліптичних кривих, що застосовується для спарювання над великими простими полями, введений в 2005 році Баррето і Наехріг. Вони є однією з переважних сімей для здійснення асиметричних спарювань, оскільки вони досягають принципово оптимальних параметрів для отримання білінійних груп на 128-бітному рівні безпеки. Дійсно, криві BN мають прямий порядок (зокрема, вони задовольняють ρ = 1) і ступінь вкладання k = 12; таким чином, спарювання на кривій BN над 256-бітним простим полем F_q приймає значення в полі F_q^{12} розміру 256 × 12 = 3072. Тоді, вирішуючи задачу дискретного логарифму як у групі точок кривої, так і в розширеному полі $F^{\times}{}_q^k$ займає близько 2128 часу, як того вимагає. Деталі побудови кривих БН, засновані на методі СМ (комплексного множення).[20] Достатньо сказати, що алгоритм Баррето та Наехріг видає еліптичну криву форми: E : $y^2 = x^3 + b$ над полем F_q з $q \equiv 1 \ (mod\ 3)$ (для зручності вони пропонують вибрати q, що задовольняє, $q \equiv 31 \ (mod\ 36)$), так що порядок #E (F_q). є простим, разом з генератором

$G = (1, \sqrt{b} + 1 \bmod q) \in E(F_q)$. Число b є дуже маленьким цілим числом таким, що b + 1 є квадратичним залишком по модулю q.

Криві BN зазвичай використовують для ступеня вкладу k = 12 дискримінант D = 3. Хитрість полягає в тому, щоб вибрати u(x) ступеня 2 та сподіватися, що $F_{12}(u(x))$ має нетривіальну факторизацію. Тоді можна використовувати незвідний множник для r(x).

$$\begin{cases} q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1 \\ t(x) = 6x^2 + 1 \end{cases} \quad (2.22)$$

Це призводить до сімейства з оптимальним ρ = 1. В даний час k = 12 є найвищим ступенем вкладу, для відомих сімейств з ρ = 1.

Cocks-Pinch криві

Метод Cocks-Pinch - це один з найбільш гнучких алгоритмів для побудови дружніх кривих з довільним ступенем вкладу та підгрупами з простим порядком майже довільного розміру. [21]

Цей алгоритм визначає ступінь вкладу k та дискримінант D, потім виконує наступні кроки:

- виберіть простий r такий, що $k|r-1$ і $\left(\frac{-D}{r}\right) = 1$;
- виберіть ціле число $g \in Z$;
- запишіть $t' = g + 1$ і виберіть ціле число $u' \equiv (t'-2)/\sqrt{-D}\ (mod\ r)$;
- нехай $t \in Z$ буде відповідним до t' за модулем r, та $u \in Z$ буде відповідним u' за модулем r; підставивши отримуємо:

$$q = (t^2 + Du^2) / 4. \quad (2.23)$$

- Якщо q ціле та просте, то існує еліптична крива E над полем F_q з підгрупою порядку-r і ступенем вкладу k.

Якщо дискримінант D не великий, то E можна ефективно побудувати за допомогою методу CM.

Основною проблемою методу Cocks-Pinch є значення ρ. Оскільки t та u мають розмір навколо r, а q виводиться з них, тоді $q \approx r^2$, а отже з цього випливає, що ρ(Cocks-Pinch) = 2.

KSS криві

Качіза, Шефер та Скотт запропонували сімейство не суперсингулярних еліптичних кривих вкладеного ступеню k = {16, 18, 32, 36, 40} з використанням елементів у циклотомічному полі. [22]

Розглянемо криву зі ступенем вкладання k = 16 та дискримінантом D=1, визначеною над полем розширення F_q^{16} наступним чином:

$$E/F_{q^{16}}: Y^2 = X^3 + aX, (a \in F_q) \text{ та } a \neq 0 \tag{2.24}$$

де X, Y ∈ F_q^{16}. Подібно до інших дружніх кривих, характеристики q, сліду Фробеніусу t та порядку r цієї кривої визначають наступними многочленами:

$$\begin{cases} q(x) = \left(\frac{x^{10}+2x^9+5x^8+48x^6+152x^5+240x^4+625x2+2398x+3125}{980}\right) \\ r(x) = x^8 + 48x^4 + 625 \\ t(x) = \frac{2x^5+41x+35}{35} \end{cases} \tag{2.25}$$

де x≡25 або 45 (mod 70), а значення ρ= ($\log_2 q / \log_2 r$) ≈ 1.25.

Існує також сімейство зі ступенем вкладання k = 18 та D = 3, де ρ=4/3.

BLS криві

Баррето, Лінн та Скотт пропонують поліноміальні параметризації для деяких сімейств кривих, що можуть використовуватись для спарювання з певними ступенями вкладу. [23]

Всі криві, що відносяться до однієї з так званих циклотомічних сімейств має CM дискримінант D=3 (тобто j-інваріантний j = 0) і може бути заданий коротким рівнянням Вейєршрасса E: $y^2=x^3+b$.

Для ступеня вкладу k = 24 сімейство Баррето-Лінн-Скотт (BLS) дається наступною параметризацією (2.26):

$$\begin{cases} q(x) = \frac{(x-1)^2(x^8-x^4+1)}{3} + x \\ r(x) = x^8 - x^4 + 1 \\ t(x) = x + 1 \\ n(x) = \frac{(x-1)^2(x^8-x^4+1)}{3} \\ f(x) = \frac{(x-1)(2x^4-1)}{3} \end{cases} \quad (2.26)$$

Знаходження конкретної кривої BLS досягається за допомогою цілих значень $x_0 \equiv 1(mod\ 3)$, доки $q\ (x_0)$ і $r\ (x_0)$ не є обома простими (при x0 ≡ 1(mod 3) всі включені параметри є цілими числами) . Для кожного набору параметрів існує еліптична крива E над F_q така, що $\#E(F_q) = n\ (x_0)$. Правильну криву E можна знайти, намагаючись змінити різні значення для b і перевіряти правильний груповий порядок.

Криві BLS досягають найменшого p-значення при k = 24 (ρ = 1.25). Вони мають повороти ступеня 6 і дозволяють реалізувати оптимізацію при обчисленні спарювання, подібних до кривих Barreto Naehrig (BN).

Відповідно до рекомендацій ключового розміру (таблиця 2.1.) криві BLS є хорошим вибором для спарювання на 256-бітовому рівні безпеки.

2.4 Спарювання точок на еліптичній кривій

Спарюванням називається невироджене білінійне відображення:

$$e\colon G_1 \times G_2 \rightarrow G_T. \quad (2.27)$$

Саме властивість білінійності робить спарювання таким потужним примітивом у криптографії.

В даний час єдиними відомими спарюваннями, придатними для криптографії, є спарювання Вейля, Тейта та Ейта на групах дивізорів класів алгебраїчних кривих, а в найпростіших та найбільш ефективних випадках - на еліптичних кривих. Нехай F_{q^k} деяке скінчене розширення поля F_q з ступенем вкладу k ≥ 1. Групи G1 і G2 визначаються на еліптичній кривій $E\ (F_{q^k})$, а цільова група G_T визначена в мультиплікативній групі $F_{q^k}^*$, тому G1 і G2 записуються адитивно, в той час як GT мультиплікативно. [24]

Спарювання точок P та Q які належать до груп G1 та G2 відповідно схематично представлені на рис. 2.5.

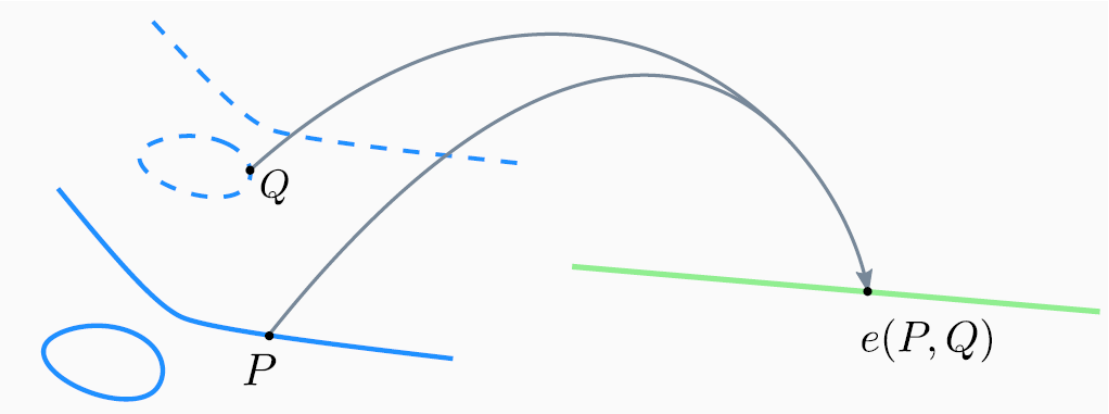


Рисунок 2.5. Загальна схема спарювання точок P та Q

Таким чином, для $P, P' \in G1$ та $Q, Q' \in G2$, білінійність e означає, що:

$$e(P + P', Q) = e(P, Q) * e(P', Q), \quad (2.28)$$

$$e(P, Q + Q') = e(P, Q) * e(P, Q'), \quad (2.29)$$

звідки випливає, що для скалярів $a, b \in Z$ (рис 2.6.):

$$e([a]P, [b]Q) = e(P, [b]Q)^a = e([a]P, Q)^b = e(P, Q)^{ab} = e([b]P, [a]Q). \quad (2.30)$$

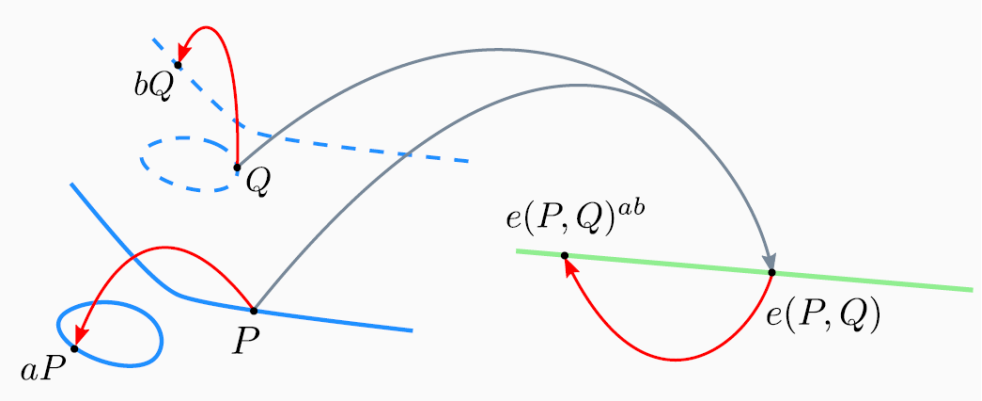


Рисунок 2.6 - Властивість спарювання білінійність

Якщо для обчислення спарювання відомий поліноміальний алгоритм, то його можна застосовувати для створення криптосистем. Серед нескінченної кількості спарювань виділяють 4 класи спарювань, часто використовуваних в еліптичній криптографії, – спарювання Weil, Tate, Ate, та ηT(etaT).

2.4.1Типи спарювань та підгрупи r-кручення

При обчисленні спарювання e(P, Q) на прикладі спарювання Вейля або Тейта потрібно, щоб P і Q походили з непересічних циклічних підгруп одного і того ж простого порядку r. Якщо P і Q знаходяться в одній циклічній підгрупі, то розрахунок спарювання може не вдатися, тому що носій дивізора може небажано збігатися. [24]

Для знаходження більше ніж однієї циклічної підгрупи порядку r на еліптичній кривій E (F_q) яка містить лише одну підгрупу треба розширити поле F_q до F_q^2. Якщо E (F_q^2) \ E (F_q) має хоча б одну іншу підгрупу порядку r, тоді можна визначити точку Q, а потім обчислити спарювання e (P, Q).

Для отримання двох окремих підгруп порядку-r необхідно знайти найменше розширення F_q^k поля F_q, таке що еліптична крива E (F_q^k) фіксує більше точок порядку r. Ціле число $k \geq 1$, за допомогою якого це досягається називається ступенем вкладу, і воно відіграє вирішальну роль при обчислені спарювання.

Ціла група точок порядку r на еліптичній кривій E (F_q) називається r-кручення та позначається E [r] і визначається як:

$$E\,[r] \;=\; \{P \;\in\; E \mid [r]\,P \;=\; \infty\}. \qquad (2.31)$$

Ця підгрупа ізоморфна адитивній групі $Z_r \times Z_r$.

Це означає що порядок підгрупи #E[r]=r^2. Оскільки точка на нескінченності ∞ перекриває всі подгрупи порядку r, з рівняння (2.29) випливає, що (для простого r) r-кручення складається з r + 1 циклічних підгруп порядку порядку r.

Умови для ступеня вкладу k:

- k мале натуральне число, таке що r | ($q^k - 1$);
- k мале натуральне число, таке, що F_q^k містить всі r корені одиниці в F_q (тобто μr ⊂ F_q^k);
- k - мале натуральне число, таке, що E [r] ⊂ E (F_q^k).

Якщо r | #E (F_q), а r2∤ #E (F_q), то підгрупа r-кручення в E (F_q) є унікальною. У цьому випадку при k> 1 та (2.29) випливає, що F_q^k - найменше розширення поля F_q, яке надає додаткові точки r-кручення, що відносяться до E (F_q^k)/E (F_q).

Таким чином, існує унікальна підгрупа порядку r в E [r], яка визначена над полем F_q та називається підгрупою базового поля g1. Оскільки ендоморфізм Фробеніуса π діє на g1, та ніде більше в E [r], то його можна визначити як g1 = E [r] ∩ Ker (π - [1]). Тобто, g1 - це [1] - поле π обмежене в E [r]. Існує ще одна підгрупа E [r], яка може бути виражена за допомогою власного простору π. Визначається як підгрупа g2 з E [r], g2 = E [r] ∩ Ker (π - [q]).

Типи спарювання виникають внаслідок розміщення G1 і G2 в різних підгрупах E [r].

Основними факторами, що впливають на класифікацію, є здатність до хешування та випадковий вибір елементів G2, існування ізоморфізму ψ: G2 → G1, яке часто вимагається для забезпечення безпеки роботи, і проблеми зберігання та ефективності.

Тип спарювання 1 (рис. 2.7). Нехай еліптична крива E суперсингулярна, де G1 = G2 = g1 (при P1 = P2 = p1).

При обчислені спарювання e між точками P та Q, можна використовувати перекручене відображення φ для позначення Q як φ (Q) і визначити спарювання

$$e(P, Q) = e(P, \varphi(Q)), \quad (2.32)$$

де e – це спарювання Вейля або Тейта(2.22). Немає проблем хешування та існує ізоморфізм ψ від G2 до G1. Недоліками спарювання типу 1 є пропускна здатність та ефективность.

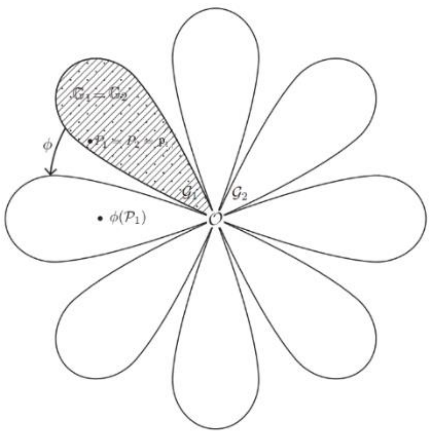


Рисунок 2.7 - Спарювання типу 1

Інші 3 типи спарювань визначаються над звичайними еліптичними кривими.

Тип спарювання 2 (рис. 2.8.). У цьому випадку група G2 є будь-якою з підгруп r-1 в E [r]. Відображення ψ: G2 → G1 як слід Tr. Для переміщення елементів з G2 в g2 для ефективності можна використовувати відображення анти-сліду.

Недоліком є те, що не існує відомого способу хешування в групі G2 та генерації випадкових елементів у групі G2. Генератор P2 ∈ G2 і генерує елементи за допомогою скалярного множення P2, але це небажано в протоколах, оскільки не можна генерувати випадкові елементи без знання дискретного логарифму відносно P2.

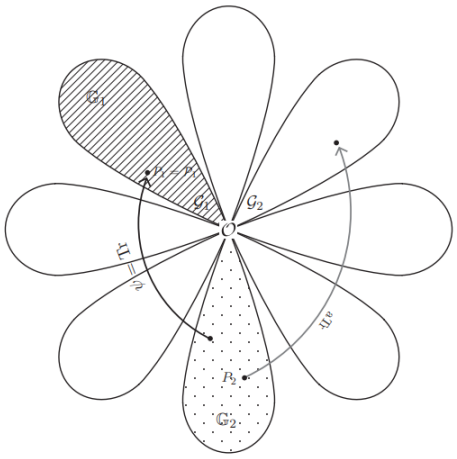


Рисунок 2.8 - Спарювання типу 2

Спарювання типу 3 (рис. 2.9). У цьому випадку група G2 = g2, нульова підгрупа сліду. Тепер можна хешувати у підгрупі G2. Ізоморфізм ψ: G2 → G1 тривіально існує, але немає ефективного способу його обчислення.

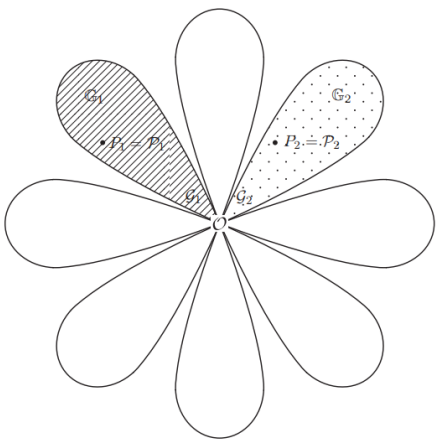


Рисунок 2.9 - Спарювання типу 3

Спарювання типу 4 (рис. 2.10). У цьому випадку група G2 вважається повним r-крученням E [r], тобто групою порядку r^2. Хешування в G2 можливе, але не дуже ефективне, однак група G2 не є циклічною.

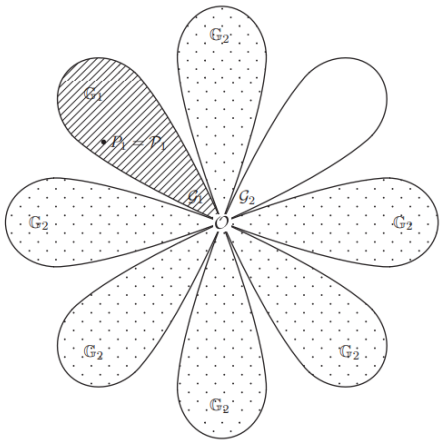


Рисунок 2.10 - Спарювання типу 4

Існуючі рівні безпеки спарювання типу 1 на порядок дорожче, ніж спарювання типу 3. Сьогодні всі сучасні реалізації спарювань відбуваються за допомогою несуперсингулярних кривих, які передбачають сценарій спарювань типу 3, де єдиною потенційною жертвою є відображення ψ: G2 → G1. [24]

Спарювання типу 2 які мають відображення ψ - це просто неефективна реалізація спарювань типу 3.

2.4.2 Спарювання Вейля

У 1983 році Менезес, Окамото і Ванстоун показали, що для суперсингулярних кривих існує ефективний спосіб відобразити пари точок кривої у невироджений елемент скінченого поля.

Ізоморфізм використаний для цього називається спарювання Вейля. Він дозволяє відобразити безліч точок еліптичної кривої в безліч відрахувань по модулю великого числа.

Спарювання Вейля має вид:

$$e_r = E(F_q^k)[r] \times E(F_q^k)[r] \rightarrow \mu_r, \qquad (2.33)$$

де μ_r – підгрупа по множенню коренів r–го ступеня поля F_q^k.

Нехай точка P∈E[r], та дивізор функції f_r, P = r[P]−r[∞]. P, Q∈$E(F_q^k)$[r] та дивізорі D_P і D_Q Його ступінь дорівнює 0, а сума ∞. По теоремі 2.1 найдеться функція f, дивізор якої дорівнює D:

$$div(f_T)= r[T]-n[\infty]. \quad (2.34)$$

Будемо називати функцію f_T, задовольняючу (2.34), функцією Вейля. Нехай т. $P\in E$[r] не належить орбіті т. T, тобто не співпадає ні з яким кратним $kT, k\leq r$, точки T. Розглянемо дивізори:

$$D_S=[S]-[\infty],\ D_T=[T+R]-[R], \quad (2.35)$$

де R довільно вибрана точка E[r].

Нехай E: $y^2=x^3+ax+b$ еліптична крива над алгебраїчно замкнутим полем K, r натуральне число та E[r] підгрупа точок кривої E порядка r, тоді спарювання Вейля має вид:

$$e_r=E[r]\times E[r]\rightarrow \mu_r. \quad (2.36)$$

Оскільки μ_r – підгрупа по множенню коренів r –го ступеня поля F_q^k, тоді спарювання задається наступною формулою:

$$e_r(T,S)=f_T(D_S)/f_S(D_T)=f_T([S]-[\infty])/f_S([T+R]-[R]). \quad (2.37)$$

За допомогою дивізорів, в силу їх визначення, можливо представити тільки спарювання, визначені на групах точок еліптичних кривих.

Використовуючи формулу (2.36), можна переписати формулу (2.37) у вигляд:

$$e_r(T,S)=f_T(R)\cdot f_T(S)/f_T(\infty)\cdot f_T(T+R). \quad (2.38)$$

Основні властивості спарювання Вейля:

1. Білінійність, описана співвідношеннями (2.28, 2.29).

2. Невиродженість: для будь-якої точки $P \in E[\mathrm{r}]$ існує точка $Q \in E[\mathrm{r}]$ така, що $e_{\mathrm{r}}(P,Q) \neq 1$.

3. Альтернативність: якщо $P \in E[\mathrm{r}]$, тоді $e_{\mathrm{r}}(P,P)=1$. При білінійності якщо $P,\mathrm{Q} \in E[\mathrm{r}]$, тоді $e_{\mathrm{r}}(\mathrm{Q},P)= e_{\mathrm{r}}(\mathrm{Q},P)^{-1}$ зазвичай називають кососиметричною або антисиметрією.

Можна довести, що перетворення Вейля не залежить від вибору т. R, тому у формулі (2.18) в якості R можна узяти будь-яку точку ЭК.

2.4.3 Спарювання Тейта

Першим аргументом перетворення Тейта як і раніше являється довільна т. $T \in E[\mathrm{r}]$. Позначимо через $\mathrm{r}E$ множину точок $\{\mathrm{r}Q \mid Q \in E\}$, а через $E/\mathrm{r}E$ множина класів еквівалентності кривої E по множині $\mathrm{r}E$.

Спаровування Тейта - це білінійне відображення:

$$\tau_{\mathrm{r}}: E(\mathrm{F_q^k})[\mathrm{r}] \times E(\mathrm{F_q^k})/\mathrm{r}E(\mathrm{F_q^k}) \rightarrow \mu_{\mathrm{r}}, \qquad (2.39)$$

де μ_{r} – підгрупа по множенню коренів r – го ступеня поля $F_q{}^k$, що задається наступною формулою :

$$\tau_{\mathrm{r}}(T,S)=f_T(S+R)/f_T(R), \qquad (2.40)$$

де $R \notin \{T,-S,T-S,\infty\}$.

Однією з важливих відмінностей спарювання Тейта являється те, що воно не вироджене (не рівне 1) при $P=Q$. Це дозволяє обчислити множник m такий, що $Q=mP$ за одне обчислення.

Дійсно, $\tau(P,Q)=\tau(P,mP)=\tau(P,P)^m=b(mod\ q)$. Щоб знайти тепер m достатньо обчислити дискретний логарифм $\log_a b(mod\ q)$, де $a=\tau(P,P)$, в полі F_q.

Відмітимо, що значення спарювання Тейта $\tau(P,Q)$ визначається точками P і Q не однозначно, а з точністю до множника з групи μ_r. Щоб отримати унікальне значення, елемент $\tau(P,Q)$ підносять до степені $(q^k-1)/r$.

Позначимо цю функцію через τ_{ur}:

$$\tau_{ur}(P,Q) = \tau(P,Q)^{(qk-1)/r}. \quad (2.41)$$

2.4.4 Алгоритм Міллера

Головною проблемою в обчисленні перетворень Вейля і Тейта є знаходження функції f, дивізор якої співпадає із заданим дивізором D. Нехай т. $T \in E[r]$. В цьому розділі функцію Вейля з дивізором $r[T]-r[\infty]$ через $f_{r,T}$, підкреслюючи її залежність від порядку r точки T. Визначимо допоміжні дивізори $D_j = j[S+R]-j[R]-[jS]+[\infty]$, які задовольняють умовам теореми 2.1. Позначимо через $f_{j,T}$ функцію, дивізор якої дорівнює D_j. Ці функції називаються функціями Міллера.

Функцію Вейля $f_{r,P}(Q)$ можна обчислити за допомогою рекурсивного алгоритму Міллера, заснованого на обчисленні проміжних функцій Міллера $f_{j,P}(Q)$ для $j<r$, $f_{1,T}(Q)=1$ для будь – якої т. $Q \in E(K)$ по наступній формулі:

$$f_{i+j,T}(Q) = f_{i,T}(Q) \cdot f_{j,T}(Q) \cdot l_{i,j} / v_{i+j}, \quad (2.42)$$

де $l_{i,j}=Ax+By+C$ – рівняння прямої, що проходить через т. iT та jT,

$v_{i+j}=x-x_0$ – рівняння вертикальної прямої, що проходить через точку $R=(i+j)T$.

Приведемо формули для обчислення коефіцієнтів A, B і C прямої $l_{P,Q}$, що проходить через т. $P(x_1,y_1)$ та $Q(x_2,y_2)$:

1. $P=Q$. Кутовий коефіцієнт λ нахилу дотичної дорівнює

$$\lambda = (3x_1^2+a)/(2y_1) (mod\ p). \quad (2.43)$$

2. $P \neq Q$. Кутовий коефіцієнт λ в цьому випадку дорівнює

$$\lambda=(y_2-y_1)/(x_2-x_1)(mod\ p). \quad (2.44)$$

В обох випадках рівняння прямої, що проходить через точку $P(x_1,y_1)$ і коефіцієнт нахилу λ, має вигляд $y-y_1=\lambda\cdot(x-x_1)$, звідки отримаємо рівняння l:

$$l=y-\lambda x+(\lambda x_1-y_1). \quad (2.45)$$

Останніми випишемо формули для обчислення координат суми точок $P+Q=(x_3,y_3)$ (формули для подвоєної точки можна отримати, прирівнюючи $x_2=x_1$):

$$x_3=\lambda^2-x_1-x_2, \quad y_3=-y_1+\lambda(x_1-x_3). \quad (2.46)$$

Функцію f можна знайти за алгоритмом Міллера.

Вхідні дані: точка P генератор підгрупи порядку r

Вихідні дані: функція $f_{r,Z}$

1. Знайдемо бінарне представлення числа $r = (r_t \ldots r_0)_2$.

2. Визначимо початкові значення змінної точки Z і функції f рівними P і 1 відповідно.

3. Виконуємо цикл по i від $i=t-1$ до $i=0$:

3.1 $f = f^2 \cdot \frac{l_{Z,Z}}{v_{2,Z}}$

3.2 $Z = 2Z$

4. Якщо $r_i=1$, тоді виконаємо операцію складання $P + Z$:

4.1 $f = f^2 \frac{l_{P,Z}}{v_{P+Z}}$

4.2 $Z = P + Z$

Завершуємо цикл.

5. Визначимо вихідне значення функції Вейля $f_{r,Z}$.

Приклад. Дана крива $y^2=x^3+11$ над полем F_{31}. Вона містить 25 точок та ізоморфна група $Z_5\times Z_5$. Ця група породжується точками $P=(2;9)$ і $Q=(3;10)$, що має порядок $r=5$. Ступінь вкладу $k=1$, так як $p^1-1=30$ ділиться на $r=5$. Визначимо функцію Вейля $f_{5,P}$, використовуючи алгоритм Міллера:

1. Знайдемо двійкове представлення $r=5=(101)_2$, $t=2$.

2. Положимо $Z=(2;9)$. Виконаємо обчислення кроку 3 алгоритма Міллера при $i=t-1=1$.

$$\lambda=\frac{3\cdot 2^2}{2\cdot 9}mod\ 31=\frac{2}{3}mod\ 31=2\cdot 21\ mod\ 31=11.$$

$$l=y-\lambda x+(\lambda x_1-y_1)=y-11x+11\cdot 2-9=y-11x+13.$$

$$Z=2Z=\left(\lambda^2-2x_1;-y_1-\lambda(x_2-x_1)\right)=(24,28).$$

$$v=x-24\equiv x+7.$$

$$f_{2,P}=\frac{-11x+y+13}{x+7}$$

Перевіримо умову $r_i=1$. Так як $r_i=0$, то операція додавання на i – му кроці не виконується. Переходимо к наступній ітерації при $i=0$.

3. $Z=(24;28)$. Виконаємо операцію подвоєння т. Z: $\lambda=22$, $l_{2,2}=9x+y+4$, $2Z=(2;22)$, $v_4=x-2$.

Звідси :

$$f_{5,P}=f_{4,P}\cdot(x-2)=\frac{(-11x+y+13)^2(9x+y+4)}{(x+7)^2}$$

Вичислимо значення перетворення Тейта $\tau(P,Q)$, узявши $Q=(3;10)$. Для цього знадобиться допоміжна точка R. Візьмемо, наприклад, $R=Q$.

Обчислимо суму $S=2Q=(-1;14)$. Обчислимо функцію Вейля в точках S та R: $f(S)=f((-1;14)=20$, $f(Q)=f(3;10)=10$. $\tau(P,Q)=\frac{20}{10}mod\ 31=2$.

Знову обчислимо значення перетворення Тейта $\tau(P,Q)$, взявши $R=2Q$. Візьмемо, наприклад $R=2Q=(-1;14)$. Обчислимо суму $S=2Q+Q=(-1;17)$. Тоді: $f(S)=f(-1;17)=23, f(2Q)=20, \tau(\mathrm{P},\mathrm{Q})=\frac{23}{20} mod\ 31=2.$

Значення перетворення Тейта залежить від вибору точки R.

Для отримання унікального значення необхідно отримане значення піднести до ступеня $\frac{q^k-1}{r}$. У прикладі воно дорівнює $\frac{31-1}{5}=6$.

Маємо:

$$2^6(mod\ 31)=2, \qquad 12^6(mod\ 31)=2.$$

2.4.5 Оптимальне спарювання Ейта

Широкий спектр криптографічних протоколів у криптографії на основі спарювання базується на трьох основних циклічних групах G_1, G_2, G_T порядку r та білінійної операції спарювання.

Білінійне відображення e: $G_1 \times G_2 \rightarrow G_T$ приймає елемент з двох підгруп G_1 і G_2, відповідно, відображає їх до мультиплікативної групи G_T і має кілька властивостей:

1. Білінійність.
2. Невиродженність: $P \in G_1$, $Q \in G_2$, при $e(P, Q) \neq 1$.
3. Обчислювальність: e(P, Q) повинно обчислюватись ефективно.

Групи G_1, G_2, як правило, є групами над еліптичними кривими, а GT - це підгрупа великого поля розширення. Проте лише певні еліптичні криві дозволяють визначити G_1, G_2, G_T з допустимим білінійним спарюванням, наприклад, еліптичні криві Баррето і Наехріг виду E: $y^2 = x^3 + b$, при $b\neq 0$ (криві BN). Спарювання Ейта можна описати так:

$$a: E(F_q^k)[r] \times E(F_q^k) \rightarrow F^*_q{}^k/(F^*_q{}^k)^r. \qquad (2.47)$$

Треба звернути увагу, що G_1, G_2 і G_T мають однаковий простий порядок r, G_2 і G_T повинні бути підгрупами E (F_q^{12}) і $F^*_q{}^{12}$, відповідно. Криві BN використовують ступінь вкладу k=12, щоб досягти бажаного рівня безпеки. Це дає змогу обчислити простий q і порядок r пріоритетних груп залежно від x.

В якості ще однієї переваги, криві BN мають ефективну обчислюваність груповим гомоморфізмом, який використовує поворот шостого ступеня кривої E. Використання цього гомоморфізму дозволяє хешувати елементи в G_2, що призводить до більш ефективного обчислення за допомогою спарювання Ейта (рис. 2.11), а саме:

$$A: G_2 \times G_1 \rightarrow G_T : E'(F_q^2) \times E(F_q) \rightarrow F^*_q{}^{12} . \quad (2.48)$$

Спарювання саме складається з оцінки раціональної функції $f_{\lambda, Q}$, де λ=t-1 і кінцевої експоненціації (для отримання унікального значення необхідно піднести до ступеня $\frac{q^k-1}{r}$):

$$e(Q,P) = f_{\lambda,Q}(P)^{\frac{q^{12}-1}{r}}. \quad (2.49)$$

Завдяки гомоморфізму Фробениуса, остаточне експонування на $(q^{12} - 1)/r$ можна розділити на легку частину $(q^6 - 1)(q^2 + 1)$ і тяжку частину $(q^4 - q^2 + 1) / r$.

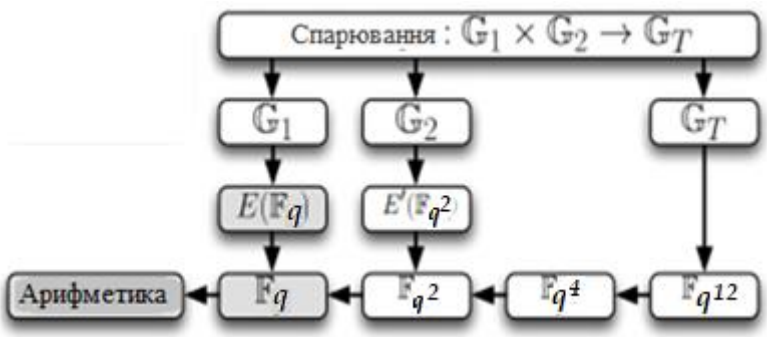


Рисунок 2.11 - Арифметика, яка потрібна для спарювань над кривими Барретo-Наехріг

Вхід $P \in \mathbb{G}_1, Q \in \mathbb{G}_2, r = |6u+2| = \sum_{i=0}^{\log_2(r)} r_i 2^i$
Вихід $a_{opt}(Q,P)$
1. $T \leftarrow Q,\ f \leftarrow 1$
2. **для** $i = \lfloor \log_2(r) \rfloor - 1$ **до** 0 **виконати**
3. $\quad f \leftarrow f^2 \cdot l_{T,T}(P), T \leftarrow 2T$
4. **якщо** $r_i = 1$ **тоді**
5. $\quad\quad f \leftarrow f \cdot l_{T,Q}(P), T \leftarrow T + Q$
6. **завершити для**
7. $Q_1 \leftarrow \pi_p(Q), Q_2 \leftarrow \pi_p^2(Q)$
8. **якщо** $u < 0$ **тоді**
9. $\quad T \leftarrow -T, f \leftarrow f^{-1}$
10. **завершити якщо**
11. $f \leftarrow f \cdot l_{T,Q_1}(P), T \leftarrow T + Q_1$
12. $f \leftarrow f \cdot l_{T,-Q_2}(P), T \leftarrow T - Q_2$
13. $f \leftarrow f^{(q^{12}-1)/n}$
14. **вертає** f

Рисунок 2.12 - Алгоритм оптимального спарювання Ate для BN кривих

Функція $f_{\lambda, Q}$ взагалі не може бути оцінена безпосередньо. Проте Міллер описав важливу властивість раціональних функцій, а саме:

$$f_{i+j,P} = f_{i,P} \cdot f_{j,P} = l_{[i]P,[j]P} / \nu_{[i+j]P} . \quad (2.50)$$

Властивість дозволяє обчислити $f_{\lambda,Q}$ за поліномиальний час, просто оцінюючи вертикальні (ν) і прямі (l) лінії в точках еліптичної кривої, використовуючи подвоєння та додавання. Значення λ з низькою вагою Хеммінга призводять до особливо швидкого обчислення $f_{\lambda,Q}$, таким чином спарювання стає оптимальним [6].

2.4.6Спарювання ЕтаТ

Спарювання η визначається лише на суперсингулярних кривих і може розглядатися як оптимізована версія спарювання Tate-a.

Нехай E є еліптичною або гіпереліптичною суперсингулярною кривою з ступенем вкладу ступеня k > 1, тобто найменшим натуральним числом, таким, що r визначається над полем F^q (де $q = p^m$) з єдиною раціональною точкою на

нескінченності. Нехай існує також відображення перекручувань, позначена як ψ, яка дозволяє виключати знаменник (тобто, якщо P ∈ E(F_q), то ψ (P) ∈ E (F_q^k) має x-координату, визначену над F_q^k / 2). [27]

Нехай D, D' - це зменшені дивізори ступеня нуля на еліптичній кривій E над полем F_q, які представляють класи дивізорів порядку розподілу N. Нехай r ∈ N. Використовуємо позначення D_r для приведеного двійника, еквівалентного rD, і $f_{r, D}$ для функції, чий дивізор є rD – D_r. У цьому випадку D = [P] - [∞], і тому D_r = r[P] - [∞] і $f_{r, D}$ - функція Міллера з дивізором r[P] - [rP] - (r-1) [∞]. Якщо r ∈ Z та r < 0, тоді rD = (-r) (- D).

Для T ∈ Z спарювання EtaT буде:

$$\eta_T\,(D, D') = \; f_{T,D}\;\big(\psi(D')\big). \tag{2.51}$$

Для точок P, Q визначимо:

$$\eta T\,(P, Q) \;=\; f_{T,P}(Q)^{\frac{(q^k-1)}{r}}. \tag{2.52}$$

Загалом, це визначення не дасть невиродженого, білінійного спарування, але в деяких випадках можливо отримати невироджене спарювання. Мета полягає у виборі значень T, які є меншими, ніж N. Метод Дюршма-Лі виникає з вибору T = q, тоді як вдосконалена версія, зазначена як ηT, використовує вибір T = q - N.

Нехай E: $y^2 + y = x^3 + x + b$ - суперсингулярна еліптична крива, задана над полем F_2^m, де b ∈ {0, 1} та m непарний. У цьому випадку степінь вкладу k=4.

Таблиця 2.2 - Порядок еліптичної кривої $E: y^2 + y = x^3 + x + b$ над полем F_{2^m}, b ∈ {0,1}.

$\#E(F_{2^m})$	Умова
$2^m + 1 + (-1)^b 2^{(m+1)/2}$	m = 1,7(mod 8)
$2^m + 1 - (-1)^b 2^{(m+1)/2}$	m = 3,5(mod 8)

Поле F_2^{4m} має елементи s, t такі, що $s^2 = s + 1$ і $t^2 = t + s$. Використовуючи відображення перекручувань ψ (x, y) = (x + s^2, y + sx + t) можна визначити спарювання ЕтаТ за алгоритмом:

Обчислення спарювання $\eta T(P, Q)$ на $E(F_{2^m})$: $y^2 + y = x^3 + x + b$ при m = 3 mod 8:

Вхідні данні: P,Q.

Вихідні дані: $\eta T(P, Q)$.

1. u ← $x_P + 1$;
2. $f \leftarrow u(x_P + x_Q + 1) + y_P + y_Q + b + 1 + (u + x_Q)s + t$;
3. цикл $for\ i \leftarrow 1,2, \ldots \frac{m+1}{2}\ do$:

3.1 $u \leftarrow x_P, x_P \leftarrow \sqrt{x_P}, y_P \leftarrow \sqrt{y_P}$;

3.2 $g \leftarrow u(x_P + x_Q) + y_P + y_Q + x_P + (u + x_Q)s + t$;

3.3 $f \leftarrow f \cdot g$;

3.4 $x_Q \leftarrow x_Q^2, y_Q \leftarrow y_Q^2$;

4. вертає $f^{(2^m-1)(2^m-2^{\frac{m+1}{2}}+1)}$.

Коефіцієнт захисту k (ступінь вкладу) - це найменше натуральне число, таке що $q^k \equiv 1 \bmod (r)$. В супесингулярному випадку k ділиться на 6. E [r] ⊆ E (F_q^k) - це вільний E(F_q) / r(F_q) - модуль рангу 2, який розпадається на прямі суми власних просторів 2-го рангу під дією q- Фробениуса (позначений далі як F), зі значеннями 1 і q (якщо (r, k) = 1 і k> 1).

Спарювання Eta визначається на підгрупі E [r] x E [r], заданої G1 x G2, де P ∈ G1, якщо F (P) = P і Q ∈ G2, якщо F (Q) = [q] Q.

G1 - це просто E (F_q) [r]. Якщо R - довільна точка r-кручення в E (F_q^k), то k його G1-компонент - це лише F-слід з R. Це можна використовувати для пошуку нетривіальних точок у G2.

2.5 Висновки до 2 розділу

При аналізі математичного апарату методів спарювання на еліптичних кривих було визначено, що для симетричних алгоритмів криптографії застосовується спарювання типу 1 (спарювання Вейля). Для асиметричного систем криптографії використовуються спарювання типу 2 і 3.

Спарювання типу 2 - це неефективна реалізація спарювання типу 3 і не рекомендована для використання в криптографічних алгоритмах. У той час як спаровування типу 3 часто використовується в криптографії заснованої на спарюванні.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДІВ СПАРЮВАННЯ ЕЛІПТИЧНИХ КРИВИХ

3.1 Застосування криптографічної бібліотеки MIRACL

MIRACL - це безкоштовна криптографічна бібліотека для багатозадачної арифметики з цілими та раціональними числами. Більша частина бібліотеки написана на C, але вона також має інтерфейс C ++. Згідно з інструкцією, всі процедури були ретельно оптимізовані для швидкості та ефективності. [28]

Для реалізації алгоритмів спарювання, вона містить велику кількість арифметичних функцій і два типи даних, які називаються big та flash. Де big тип даних для великих цілих чисел та flash тип даних для великих раціональних чисел. Обидва типи даних можуть мати довільний розмір в бітах. Арифметичні функції працюють з цими двома типами і можуть обчислювати додавання, віднімання, множення та ділення, потужність, n-й корінь, найбільший загальний дільник тощо. Більшість з цих функцій також реалізуються для використання над простим скінченим і бінарним полями. MIRACL містить повну реалізацію ECC для афінних і проективних формул кривих Вейєрштрасса.

3.2 Реалізації спарювань

За допомогою бібліотеки MIRACL можливо організувати методи спарювання точок на еліптичній кривій використовуючи різні структури та класи. В якості точок використовуються класи ECn, ECn2, які містять функції для маніпулювання точками. Якщо дано скінчене поле GF_q з простим q тоді використовується клас ECn.

Дослідження ефективності методів спарювання еліптичних кривих у цій роботі буде показано за допомогою двох критеріїв: криптостійкості та часу на обчислення. В якості порівняння буде розглянуто спарювання Тейта та Єйта.

Перед тим, як зробити порівняльний аналіз методів спарювання точок еліптичних кривих, необхідно провести кілька експериментів з різними

методами спарювання та ступенями вкладу. Кожний експеримент буде складатися з декількох етапів, які будуть характеризувати різні параметри та методи спарювання точок еліптичних кривих.

Експеримент 1. Спарювання Тейта при ступеню вкладу k=2 (Додаток Б).

Функція void ecurve(Big a, Big b, Big q, int type)

На вхід даної функції подається 3 параметри типу Big та 1 параметр типу integer. Ініціалізує параметри активної еліптичної кривої над полем GF(q). Крива має вигляд y2 = x3 + Ax + B mod q, модель Вейерштрасса (2.2). Параметр type повинен бути у стані MR_PROJECTIVE або MR_AFFINE. Нічого не вертає.

Функція ECn hash_and_map(Char *ID, Big cof)

На вхід даної функції подається параметр типу та параметр типу char Big. Функція вертає хешовану точку символом ID та кофактором cof.

Функція BOOL tate(ECn P, ECn Q, Big q, ZZn r)

На вхід даної функції подається 2 точки типу ECn, порядок еліптичної кривої q типу Big та комплексне число r типу ZZn. Функція обчислює спарювання Тейта та вертає булеве значення при успішному спарюванні.

Етап 1. Використовуючи не суперсингулярну еліптичну криву побудовану за допомогою алгоритму Cocks-Pinch з параметрами :

q=74011411878741084276309789405729920969050239777634374575447294099205168087001771400374707329824613419366803976196626970522150956037180606742103970613859 39 (512 біт);

r = 730750818665451459101842416358141509827966402561 (159 біт)

Швидкість алгоритму рис. (3.1).

Рисунок 3.1 - Швидкість алгоритму спарювання Тейта (1 типу) на кривій Cocks-Pinch при ступеню вкладу k=2

Етап 2. Використовуючи несуперсингулярну еліптичну криву побудовану за алгоритмом Cocks-Pinch та спарювання Тейта (типу 2) з тими же параметрами було отримано такі результати (рис. 3.2.).

Рисунок 3.2 - Швидкість алгоритму спарювання Тейта (2 типу) на кривій Cocks-Pinch при ступеню вкладу k=2

Етап 3. Використовуючи спарювання Тейта на несуперсингулярній еліптичній кривій з параметрами:

q=114574756839954938063531741862058253145354612367675974411155337285050705278231545326576569912344739866417031939403435598236286688787343269095020893934936 43 (512 біт);

r= 14615016373309029183621423666706313094764901826 57 (159 біт).

Швидкість алгоритму складає 0.026 секунди (рис. 3.3).

Рисунок 3.3 - Швидкість алгоритму спарювання Тейта (1 типу) на несуперсингулярній еліптичній кривій при ступеню вкладу k=2

Етап 4. Використовуючи спарювання Тейта на суперсунгулярній еліптичній кривій з параметрами:

q=731329576256467855322039941411215536384068289627312830254310277821058411810144462486413246228592183502383911176278505421042514024101864935444574549103938 7 (512 біт);

r= 730750818665451459101842416358141509827966402561 (159 біт).

Швидкість спарювання точок P та Q (рис. 3.4).

Рисунок 3.4 - Швидкість алгоритму спарювання Тейта на суперсингулярній еліптичній кривій при ступеню вкладу k=2

Експеримент 2. Спарювання Тейта при ступені вкладу k=4 (Додаток В):

Функція void set_frobenius_constant(ZZn2 &X)

На вхід даної функції подається параметр типу ZZn2, який містить 2 поля (a і b типу big). Ці числа a та b можна розглядати як реальну і уявну частини відповідно.

Значення zzn2 це a + ib, де i - уявний квадратний корінь$\sqrt{-1}$. Змінна zzn2 є представленням елемента квадратного поля розширення по відношенню до простого модуля q. Ця функція обирає константу Фробеніусу від значення залишку по модулю q.

Етап 1. Використовуючи не суперсингулярну еліптичну криву побудовану за допомогою алгоритму Cocks-Pinch з параметрами:

q=13074886681532770279763317787894821286452824947065171650344868772922925759171725921854512166353033707836778380948202823784042271142383576859061220145812539 (512 біт);

r=313855086769334038191789471160383320805117772223201725645 3 (192 біт).

Швидкість алгоритму спарювання Тейта на еліптичній кривій побудованої за допомогою алгоритму Cocks-Pinch відображено на рис. 3.5.

Рисунок 3.5 - Швидкість алгоритму спарювання Тейта на еліптичній кривій Cocks-Pinch при ступеню вкладу k=4

Етап 2. Використовуючи не суперсингулярну еліптичну криву побудовану за допомогою алгоритму MNT з параметрами:

q= 13013690311946177981854107644609133346751180608 93 (160 біт)

r= 382755597410181705348649889319201858321724906 93 (155 біт)

Швидкість алгоритму спарювання Тейта на еліптичній кривій побудованої за допомогою алгоритму MNT відображено на рис. 3.6.

Рисунок 3.6 - Швидкість алгоритму спарювання Тейта на еліптичній кривій MNT при ступеню вкладу k=4

Етап 3. Використовуючи не суперсингулярну еліптичну криву (звичайну) з параметрами:

q=330834540866291994040950336878685123996049234435076633578656 84465927197075453 (255 біт);

r= 258030633999040616611279763111083046893634287172 69 (160 біт).

Швидкість алгоритму спарювання Тейта на несуперсингулярній еліптичній кривій відображено на рис. 3.7.

Рисунок 3.7 - Швидкість алгоритму спарювання Тейта на несуперсингулярній еліптичній кривій при ступеню вкладу k=4

Експеримент 3. Спарювання Ейта при ступені вкладу k=4 (Додаток Г):

Функція power_pairing(P,Q,t1,cf,Fr,a,r,res)

Вхідними параметрами цієї функції є:

- 2 точки P та Q, де точка P типу ECn2 та точка Q типу ECn ;
- t1 (тип big) – це різниця між кількістю елементів у полі F_q та порядком еліптичної кривої E(Fq);
- масив cf [] типу big має 2 значення: перше - $\frac{(q^2+1)}{r}/q$, друге $\frac{(q^2+1)}{r}\%q$.
- константа Фробеніуса fr типу ZZn2;
- число *a* типу big яке обирається випадково за кількістю точок на еліптичній кривій r;
- порядок підгрупи еліптичної кривої r.

Етап 1. Використовуючи несуперсингулярну еліптичну криву (звичайну) з параметрами:

q=731904531763712330319228747172604882425072613137475862542944632970307249304 53 (256 біт);

r= 703996816956383171620336150804745406802561314010 1 (160 біт)

Швидкість алгоритму спарювання Ейта на несуперсингулярній еліптичній кривій відображено на рис. 3.8.

```
P: ([7B2DAE4F94135A0BEF8A0D82C48535116E7942D1911A36A10811CB4B50ACE956,0],
[0,75838CA0D57A46A187AB01D2941F609C50242D0C80331CFC5B5F06C04F3969BA])
Q: (61A9124B2DDDDC0E05844FF0FDA12822B2D2807E37C2A9C5DE023DC9DBEF6711,2894
C032F2BEB223F58A2EE7D4A38E486F09EA2925A88A9448091E871FA71B4D)
Time speed: 0.073000
```

Рисунок 3.8 - Швидкість алгоритму спарювання Ейта на несуперсингулярній еліптичній кривій при ступеню вкладу k=4

Етап 2. Використовуючи несуперсингулярну еліптичну криву побудовану за допомогою алгоритму MNT з параметрами:

q = 13013690311946177981854107644609133346751180608 93 (160 біт);

r = 382755597410181705348649889319201858321724906 93 (155 біт)

Швидкість алгоритму спарювання Ейта на еліптичній кривій побудованої за допомогою алгоритму MNT відображено на рис. 3.9.

Рисунок 3.9 - Швидкість алгоритму спарювання Ейта на еліптичній кривій MNT при ступеню вкладу k=4

Експеримент 4. Спарювання Тейта при ступені вкладу k=6.

Використовуючи несуперсингулярну еліптичну криву побудовану за допомогою алгоритму MNT з параметрами:

q = 71854447761800440449509600741961620427186073677 1 (160 біт);

r = 35927223880900220224754748462004793848980907051 9 (159 біт)

Швидкість алгоритму спарювання Тейта на еліптичній кривій побудованої за допомогою алгоритму MNT відображено на рис. 3.10.

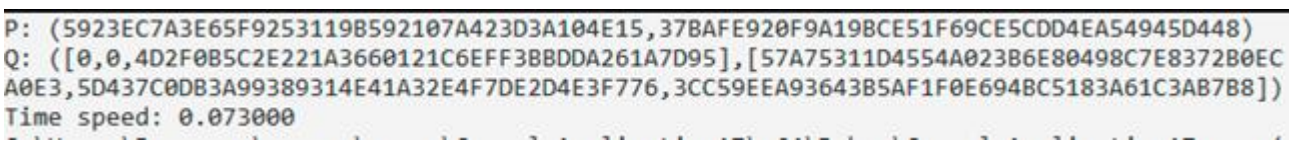


Рисунок 3.10 - Швидкість алгоритму спарювання Тейта на еліптичній кривій MNT при ступеню вкладу k=6

Експеримент 5. Спарювання Тейта при ступені вкладу k=8.

Використовуючи несуперсингулярну еліптичну криву побудовану за допомогою алгоритму Cocks-Pinch з параметрами:

q=89363090833897616253606598100733812331148096717116648876201914077601903214038398517444446034170341402852921512103761424074202905076767346259294703125278 59 (512 біт);

r=13479973333575319897333507543509815336818572211270286240551805132801 (224 біт).

Швидкість алгоритму спарювання Тейта на еліптичній кривій побудованої за допомогою алгоритму Cocks-Pinch відображено на рис. 3.11.

```
P: (3855F6664399ADD467CF8F261D0ADD55271ABFEAB90DD9F0BBE08B47E8F2CD454D82A6127153D56DEF8A4FB81B70F
4A3361DAFF997CD784C03B6EF7AAE38DA7F,7C44903D162643406449FB305E60E40D475796F2DFD73012CADB0EB7CF766
3791F2E8137750CB88721DB67398BBAD225C8871285FB9A4419A8479F08FB789DC9)
Q: ([[206BEC97F25F1F7622A53B84482A6CBDC1C747803C7DB52307FAB61DA90EFE87DE7F2E0240CE5B151AC3377CCD2
C6A088DF3A6C0C698A3BC93C115A5F1F1CAD8,0],[0,0]],[[4BC2AC745D0C1AACCBDACEAA8C69BA80FFAB7F75783866E
B1B73A9D4DCE8ED3055A4E5DC4D8006DE7E3406F7837C31DE7FB60D551F6F806E529BE996EE90E290,8E9079DD13A7DDA
ACEAF201C577204A58EAB257B44389330FD122065DF5A465ABD931AAB2CCD36D18944E16843CAE19E6FAC90C0464B9493
54CE624A11787293],[F34196F9A38A164532FC0A9344147A120B23BD2E3C13E9D1BC755E3C298DDD7AD5F7A74402A3A1
4553D0FA550B0CDDF2A1BB30C6001B4B022B44124E929AC76,7647F6B56AA19A584A61291023C8CC61E9765AF97BAC474
B0A266B41F486294331C7218E353B93876F3826B4A9C2194E20BF1BBEF4C9F4AF301414B225699A40]])
Time speed: 0.544000
```

Рисунок 3.11 - Швидкість алгоритму спарювання Тейта на еліптичній кривій CP при ступеню вкладу k=8

Експеримент 6. Спарювання Ейта за допомогою нового класу PFC (Pairing-friendly curve) при ступенях вкладу k=2,6,12,18,24 (додаток Ґ):

Конструктор Pfc (int security)

Вхідним параметром являється ціле число яке характеризує рівень захищеності. Ініціалізує еліптичну криву призначену для спарювання (Pairing-friendly curve) відповідну до рівня захищеності.

Клас G1, G2, GT характеризують точки у підгрупах G1,G2 та мультиплікативній групі *GT*.

Функції pfc.random(P) та pfc.random(Q) генерують випадкові точки у підгрупах G1 та G2 відповідно.

Функції pfc.precomp_for_mult(P) та pfc.precomp_for_mult(Q) попередньо обчислюють точки P та Q для оптимізації спарювання.

Функція pfc.pairing(Q,P) обчислює спарювання Ейта типу 3 на еліптичній кривій, де GT = e(Q∈G2, P∈G1).

Етап 1. Спарювання Ейта за допомогою класу спеціального PFC при ступеню вкладу k=2.

r = 730750818665451459101842416358141509827966402561(160 біт)

Швидкість алгоритму спарювання Ейта 3 типу на еліптичній кривій побудованої за допомогою спеціального класу PFC за алгоритмом CP відображено на рис. 3.12.

```
P: (172D647A1D251B5580BEE34C1D8A2855E4C8EEBD1A3FC9F48A1F7C9E85AF6D2A41CC3C8D46B01684FC938CFA8676042BFC3
6A2235EC04F8E04191E1B9D38F25C,CFAC37635DD699FC65829EDD24CD4DD911EF9ED3FC126CBA96FB21F7E3B1C095EAF6CC06A
88A1CD94DA3FF9C6CB89A0EA7D082E681CE1F59ED01E5C25607C62)
Q: (5DC5D84F4855D1D74A0C2B45CE604EEDDA6962229ACCC157BEFB10C6A230BF3C439C8C9BFFE516457D62375D6BBCA3E471C
F74B6DC7EA0A7085FB018CEB7232F,24ADCAE699C161098DB494E3D81D7442BD7677E1F95BC4FB206C728627A336155CBAA26C8
669053E99DDD33E335554112FC8FBB4A75D77D8C319A3BFCB62A30C)
Time speed: 0.039000
```

Рисунок 3.12 - Швидкість алгоритму спарювання Ейта на еліптичній кривій CP при ступеню вкладу k=2

Етап 2. Спарювання Ейта за допомогою спеціального класу PFC при ступеню вкладу k=6.

r= 98836621565501761988183324930976035222839950370 3 (160 біт)

Швидкість алгоритму спарювання Ейта 3 типу на еліптичній кривій побудованої за допомогою спеціального класу PFC за алгоритмом MNT відображено на рис. 3.13.

```
P: (82A390B6A80CC24E189831531B36BFE2D6E5E906,7937D2B05DADF27F8A5B7E77FA80347D63D1FE4)
Q: ([894D717DCD20D88205E4B1C809C160DC5764B578,4384D7AD048BCC02ED6D98F36074F764E7F9AC6D,8BAE3073C0D8DF61
23CF071C053CCD0F17F02C95],[89BD2BB3A8ADB438B878392A610186C5FF6A7326,23C0E450803065O3D09C9BAE92AB5492C4E
57B3F,1E3ADD3701D7F08AFC398C3D789E5953E652C46E])
Time speed: 0.108000
```

Рисунок 3.13 - Швидкість алгоритму спарювання Ейта на еліптичній кривій MNT при ступеню вкладу k=6

Етап 3. Спарювання Ейта за допомогою спеціального класу PFC при ступеню вкладу k=12.

r=167981087310158322849408041422317339097595796034047527490283
78864165570215949 (256 біт).

Швидкість алгоритму спарювання Ейта 3 типу на еліптичній кривій побудованої за допомогою кривої BN відображено на рис. 3.14.

```
P: (2412313B8464F6BA5421CE2A15AC3BE10D678C0D1FC3865A2F950A22F0458AAF,DD66087DFD63DFF584A8BD
43500AC44CA761AD3B85B62048F323B0E266F1AC2)
Q: ([771052FF012FA73F79CF3345E7FE5FD6F1B5346AB3617F793F23F62BCF3DD17,19E20AB3F7001A3AC97062
68D1EEFE40D1959221D2DB03BAE0ED5A7BEC5EC962],[20D2B41E3E717E31989C5565A523949A895EF5A01E19D5
4CC6999F3FEA92B63B,17E955491EB7F1A78090C2B1F4DE8921366F67C2521E398193034C9C98BD8704])
Time speed: 0.138000
```

Рисунок 3.14 - Швидкість алгоритму спарювання Ейта на еліптичній кривій BN при ступеню вкладу k=12

Етап 4. Спарювання Ейта за допомогою спеціального класу PFC при ступеню вкладу k=18.

r=587246027211942247148236007590430373140616613289746746573733085827716656262959990593105404802355239507374177792001 (384 біт)

Швидкість алгоритму спарювання Ейта 3 типу на еліптичній кривій побудованої за допомогою спеціального класу PFC за алгоритмом KSS відображено на рис. 3.15.

```
P: (2DDF3BC6FCBC86AF904313529BA5183053936C3520A8A82E18E8074150F8D15556F54454073C5FD549F93249D2B48A9
735D2807D16671550CC1211EE6D3D314,E198A7F19CCA986D379E55867CBF252FA044B3128ED840CDB713FC6115F6D481E0
4EB14DEEF166583DC1631A2C9873BD0C1ECD64E58BCA40D63D4DBC94E761F)
Q: ([3433D9D3FA3BD952F5797DB7CDE5ACCB42465BA6FC9A55ACFB08B9B2589F42A564A828D3F959CA7C78D409F745750B
1A33B0ACE30909E0A0FB047EA9EBEB1241,4856BF9C3B83B245C95C036EABD25E16466CF5021FAAA5CCC8A11891C2CABB0A
C28F06F92E997C087A13AEEC7B45F89460F21C94B583C09F8E5B909E7A3ED625,220CF65DB694ECCF642BC6D75AFFF49A16
1AB920F2E9FE1328874B17809B3FDF692BA0E601F755F05036254EF7A263EB99A6B807C3E4F8E7F563E74FFEE44C8A],[18
77F37CC7FF273E7F5EE41B83DAE642A10227183837D1C1D7F33A53BE9BC8B75861272D84F955A8C676097B02C6110C2DFD6
336A085E36953D32643CAD4BEB9,47760072629398BDD93DE61B55AE05F3E66D07222EFE4A57FCA0AE467476C0036D6D852
D2CCF9ADAE10FADAA67CDAD85F4779BC88F688248D50EAA937AB0E89,532005261E62585B3CEF0097C9DF4996360F67A4C5
7D1268DD51EE422CE9FC39AE9BDB7658FB4DC34BEFCBBAC9B32EE754B302B2BA796E2BC620983CCE18A7BA])
Time speed: 0.677000
```

Рисунок 3.15 - Швидкість алгоритму спарювання Ейта на еліптичній кривій KSS при ступеню вкладу k=18

Етап 5. Спарювання Ейта за допомогою спеціального класу PFC при ступеню вкладу k=24.

r=525791885745905693689350992344963050472888193614979405904302547310273664254214479540497681727646802528670501449087472996563430464471593867542954141286 41 (512 біт)

Швидкість алгоритму спарювання Ейта 3 типу на еліптичній кривій побудованої за допомогою спеціального класу PFC за алгоритмом BLS відображено на рис. 3.16.

```
P: (AB4ACD7899FCB850053B3DF01675DE6DCDAB9BF79E5A119731977BFE0669ED09D9B14CC926F30A72A0E1D19D9978B46A
94B862259283C6C4BAB85D84696306D7B4AB2F874697225CCE05C53823BA3,1A1E3FF9EAF7DBEF9C5985BEE90DD5362D4D59
E233EB4AB3CB5B1A542FEDA21ECA1E2F734B10192BBCC95578B77E2B2CCBBCC9DE7F082231CA927978FCEE3489EF807E943A
0C400B7F53561BC36EE)
Q: ([[D57BFCABF01A33017149A2F632AEE39A50906BD6FE8C4C9CBDB68F16A70912C55950F36EFA9CD2843ED4772E065E79
59576B76FFC652EF845A67AD1AE3CEA8B5A8EB301D26755C47EAC55701A22D3,C9591ED11F822ED7EE13CF46DE3B527153D9
DD415795FA2D3DDF13519637AAB6120FF74CA67E68EA8EE560EC3D56CA851F6807060DDEB49CD08EB466A0E9A072E83FBD47
EDF57AC9D130C5384687A],[135B2780BDBC75704B4AE6376CB0ECA3EEE6A5C15FF960B1E5B460A0DF4F6C8DAC77B31F015C
88FC34F0B67CA4966723E5D5495C9224ACDFEB4D6E80FD7B686908B3AC3E6D8916FA5584C3ABFBA9B4,80F81A31A8DA0CB74
53C692018CC798DD1AD4122B4FE32E7B3BAB8247E2D12A4D8466D4547F552C23E66DAA553AC78021E9E822DA80BA06CB0354
D94287C23368FAD79AD3423AA8C91460DC9AEE0E]],[[129AB2F86F321029A70981EF2EA20DB66220457FF93425402D52399
9ADC2A7C48CBD6C89CA1D9114B9DF9CBA7A275CC15F6023717A436EFD6F11A1BDAFACC786F73BBAF6257D41BC8D8EA126473
E30,5C0BC6BE2E97414D49754DEAC70790C7EDDC77750F98046C86715F110DD052EE160AD0037FACCE48E785E3AD55FEF3B7
04A3531EF3E93B3189DD8318C906B06A75C7F6433C7EE19B76A6C74BF1AE1],[3E72302C0A2F7BB7D00CD1252C935558FB0C
3F3BAE3D682CDB78AB01AFD029CE993333CE39C79032F0029416A441800D7FD9815184ADD277370056AE57F21DDD81DF02F1
7E502BE617E622C9600D0,32C0084EAEBB6789668D76DBC43D82A2A780B1A422A13367B4BF0BC06E77AB36D621C10B18F17D
02034E20533742FE50E52D38A76E408CDED80EE9F611C222988E340C99ACBA3DF5E2DD87A47D933]])
Time speed: 1.106000
```

Рисунок 3.16 - Швидкість алгоритму спарювання Ейта на еліптичній кривій BLS при ступеню вкладу k=24

3.3 Реалізація короткого підпису BLS

Для програмної реалізації алгоритму короткого підпису BLS (Додаток А) за допомогою бібліотеки MIRACL було використано такі функції.

Функція pfc.random(G2& w).

Вхідним параметром функції є об’єкт класу G2. Вона обчислює випадкову точку, яка належить до підгрупи G2 та нічого не вертає.

Функція pfc.mult(const G2& w,const Big& k)

Вхідними параметрами функції є об’єкт класу G2 та число k типу Big. Вона виконує скалярне множення точки підгрупи G2 та числа k, вертаючи точку підгрупи G2.

Функція pfc.hash_and_map(G1& w,char[] *ID)

Вхідними параметрами функції є об’єкт класу G1 та масив символів ID типу char. Вона обчислює хешування повідомлення на точці підгрупи G1 та вертає точку з хешованим повідомленням типу G1.

Функція S.g.get(Big& x)

Вхідним параметром функції є число типу Big. Вона знаходиться у класі ECn та за значенням числа x вертає молодший біт точки S.

Функція S.g.set(const Big& x,int cb)

Вхідними параметрами функції є число x типу Big та ціле число cb. Вона знаходиться у класі ECn та відновлює точку S за допомогою побітового зсуву cb.

Функція pfc.multi_pairing(int n,G2 **y,G1 **x)

Вхідними параметрами функції є ціле число n, масивb точок підгруп G1 та G2. Вона викликає n кількість спарювань Ейта одночасно використовуючи алгоритм Міллера.

3.4 Порівняльний аналіз методів спарювання точок еліптичних кривих

Безпека криптографії, основаної на спарюванні, безпосередньо залежить від нерозв'язного рівня задачі дискретного логарифмування на еліптичних кривих (ECDLP) у групі E (F_q) або задачі дискретного логарифму (DLP) у групі F_q^k. Це означає, що протоколи, які побудовані на криптографії зі спарюваннями повинні працювати в робочому середовищі з параметрами 1024 біт, щоб забезпечити рівень безпеки AES - 80 біт. Через цей недолік криптографія, основана на спарюваннях, поступається іншим ассиметричним криптоалгоритмам. Але недолік ефективності криптосистем, що базується на спарюваннях, через постійне поліпшення методів, стає менш значним щодо криптосистем, таких як RSA або DSA.

Для організації криптографічних систем на спарюванні, необхідно спочатку порівняти та проаналізувати різні види спарювання точок на еліптичній кривій.

Програмна реалізація спарювання точок еліптичних кривих велась на комп’ютері з такими характеристиками:

- процесор Intel Pentium 2117u;
- відеокарта Nvidia Geforce 740m;

- твердий накопичувач SSD.

Для систематизації отриманих результатів використовуються таблиці та графіки зі спільним ступенем вкладу k. У порівнянні було реалізовано 2 види спарювання точок еліптичних кривих Тейта та Ейта.

Швидкісні характеристики методів спарювання точок Тейта та Ейта при ступеню вкладу k=2 наведені у таблиці 3.1.

Таблиця 3.1 - Спарювання Тейта та Ейта при ступеню вкладу k=2

Тип спарювання	Вид кривої	Розмір r підгрупи, біт	Рівень безпеки (AES), біт	Розмір розширеного поля q^k, біт	ρ	Час, сек
Tate	CP	159	80	512	1.6	0.034
Tate (2 type)	CP	159	80	512	1.6	0.041
Tate	HCC	159	80	512	1.6	0.026
Tate	CC	159	80	512	1.6	0.037
Ate	CP	159	80	512	1.6	0.039

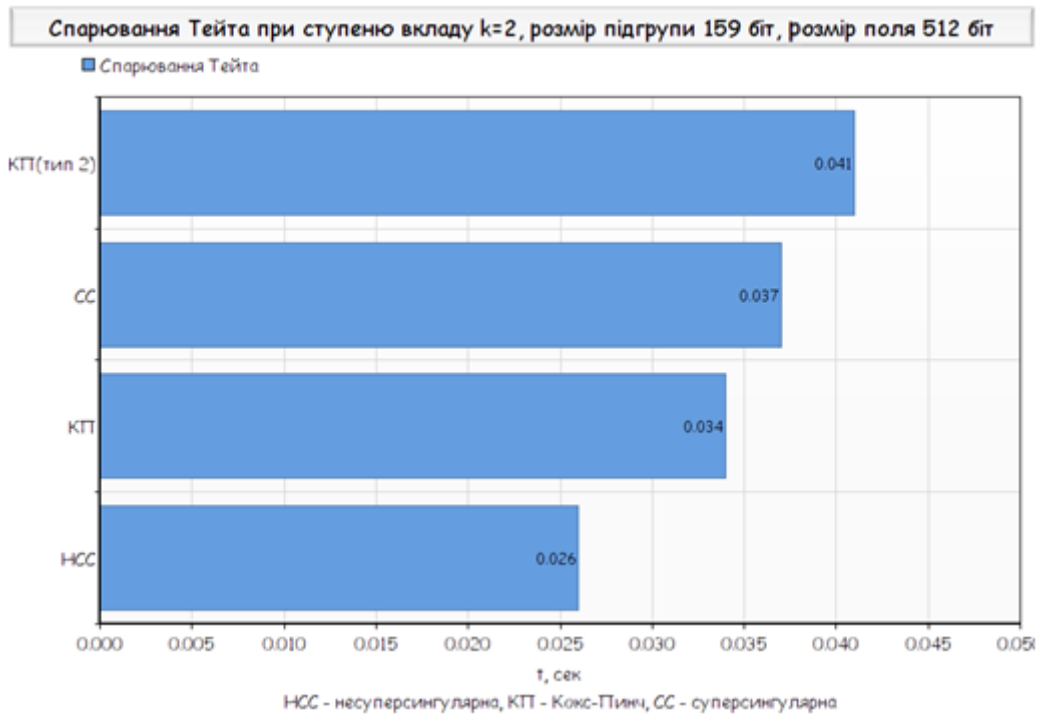


Рисунок 3.17 - Спарювання точок методом Тейта при ступеню вкладу k=2

При порівнянні швидкісних характеристик метода спарювання точок Тейта (рис. 3.17) на різних еліптичних кривих при однакових вхідних параметрах для організації рівня безпеки AES 80 спарювання Тейта на несуперсингулярній кривій з підгрупою розміром 159 біт та розширеним полем 512 біт швидше, ніж спарювання Тейта (типу 2) на кривій побудованій методом Cocks-pinch на 57%. Як було зазначено у розділі 2, спарювання типу 2 не є вигідним рішенням, стосовно швидкості та ефективності.

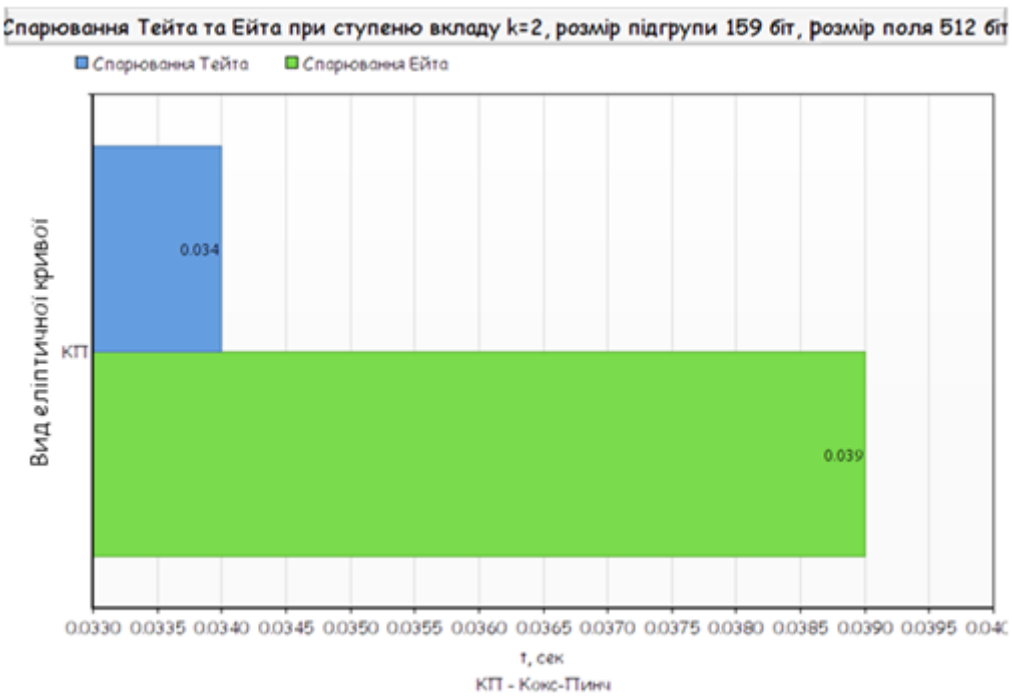


Рисунок 3.18 - Спарювання точок методами Тейта та Ейта на КП кривих при ступені вкладу k=2

У порівнянні методів спарювання точок Тейта та Ейта (рис. 3.18) з ідентичними параметрами видно, що спарювання Тейта швидше за свого конкурента на 15%. Хоча в теорії, спарювання точок Ейта на еліптичній кривій має кращі швидкісні показники, але при малому ступеню вкладу k=2 поступається методу спарюванню Тейта.

Серед методів спарювання точок еліптичних кривих при ступеню вкладу k=2 ефективним рішенням виявилося спарювання Тейта на несуперсингулярній кривій.

Швидкісні характеристики методів спарювання точок Тейта та Ейта при ступеню вкладу k=4 наведені у таблиці 3.2.

Таблиця 3.2 - Спарювання Тейта та Ейта при ступеню вкладу k=4

Тип спарювання	Вид кривої	Розмір r підгрупи, біт	Рівень безпеки (AES), біт	Розмір розширеного поля q^k, біт	ρ	Час, сек
Tate	CP	192	80	1536	2	0.111
Tate	MNT	155	80	640	1	0.045
Tate	HCC	160	80	1280	2	0.078
Ate	HCC	160	80	1280	2	0.073
Ate	MNT	155	80	640	1	0.029

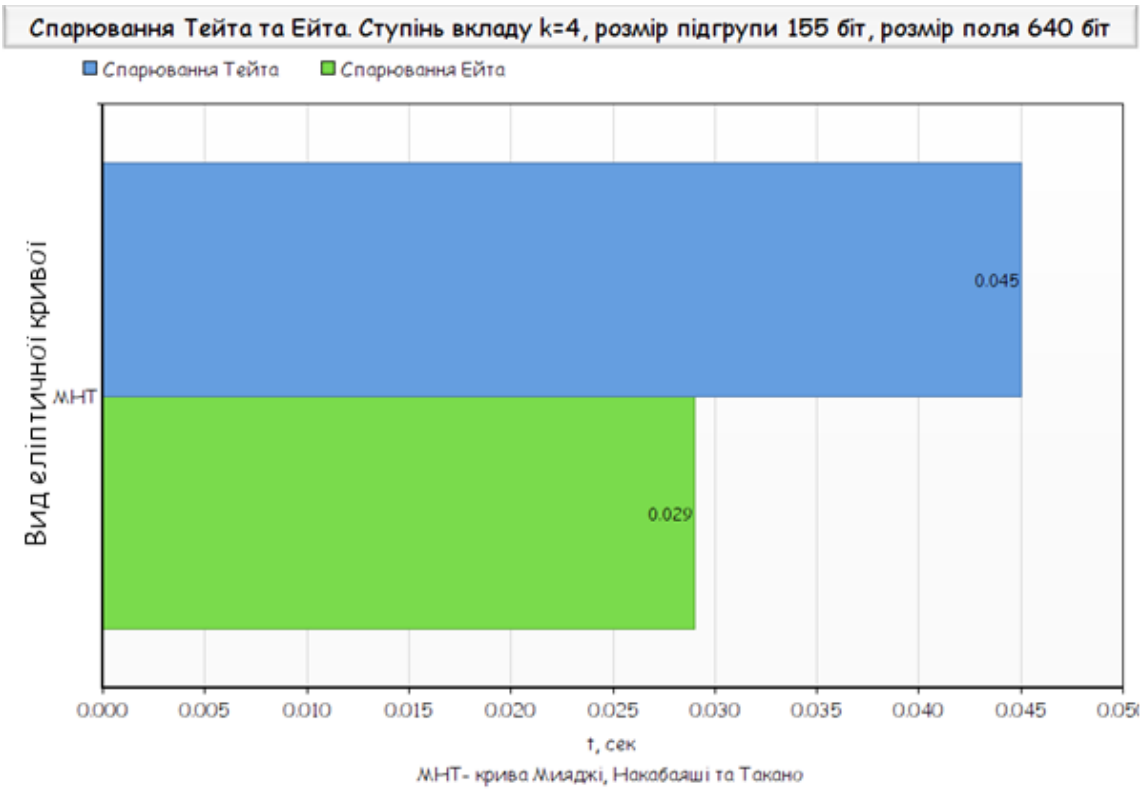


Рисунок 3.19 - Спарювання точок методами Тейта та Ейта на MHT кривих при ступеню вкладу k=4

При порівнянні швидкісних характеристик спарювання точок методом Тейта та Ейта при ступеню вкладу k=4 та на еліптичній кривій побудованій за

алгоритмом МНТ (рис. 3.19) для забезпечення рівня безпеки AES-80, метод спарювання Ейта на еліптичній кривій з розміром підгрупи 155 біт та розміром розширеного поля 640 біт випередило спарювання Тейта. Виграшом застосування спарювання Ейта на МНТ кривих склало 55%.

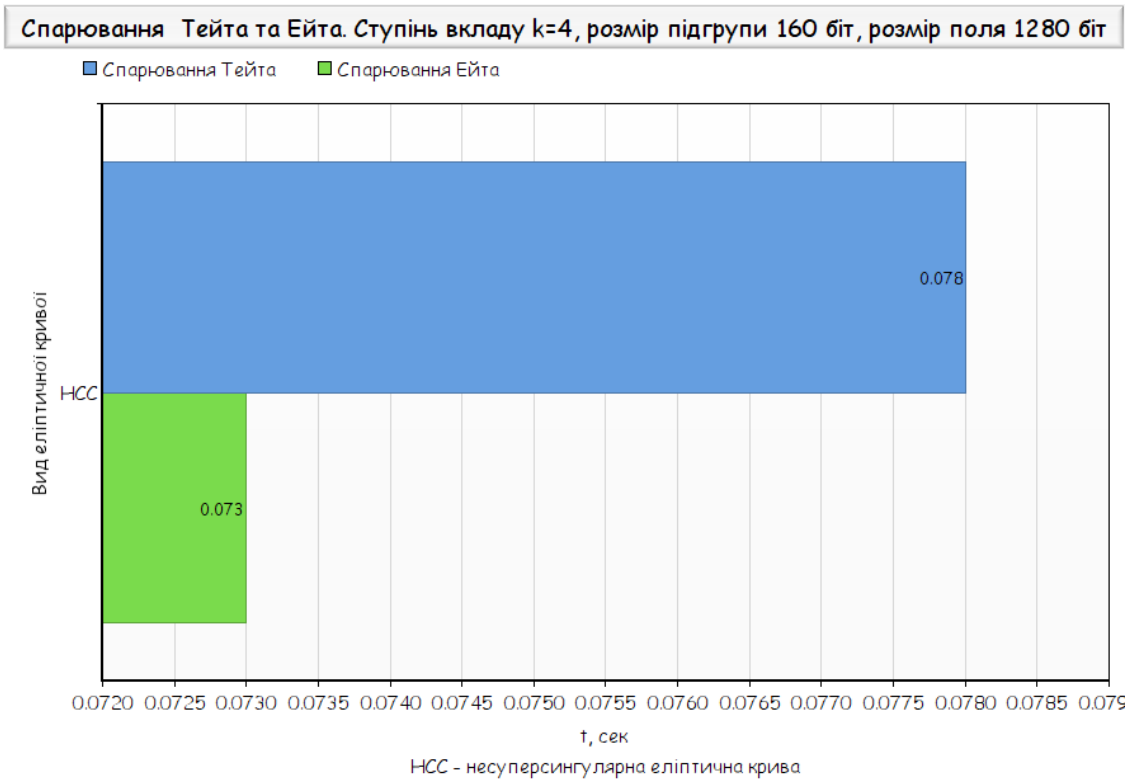


Рисунок 3.20 - Спарювання точок методами Тейта та Ейта на HCC кривих при ступеню вкладу k=4

При порівнянні спарювання точок еліптичних кривих методом Тейта та Ейта при ступеню вкладу k=4 на несуперсингулярній еліптичній кривій для забезпечення рівня безпеки AES-80, метод спарювання Ейта з розміром підгрупи 160 біт та розміром розширеного поля 1280 біт виявився скорішим рішенням, ніж спарювання Тейта з тими ж параметрами підгрупи та поля. Ефективність у використанні спарювання Ейта склала 7%.

Швидкісні характеристики методів спарювання точок Тейта та Ейта при ступеню вкладу k≥6 наведені у таблиці 3.3.

Таблиця 3.3 - Спарювання Тейта та Ейта при ступеню вкладу k≥6.

Тип спарювання	Вид кривої	Розмір r підгрупи, біт	Рівень безпеки (AES), біт	Розмір розширеного поля q^k, біт	Ступінь вкладу k	ρ	Час, сек.
Tate	MNT	160	80	960	6	1	0.073
Tate	CP	224	112	4096	8	2	0.544
Ate	MNT	160	80	960	6	1	0.108
Ate	BN	256	128	3072	12	1	0.138
Ate	KSS	384	192	9192	18	1.33	0.677
Ate	BLS	512	256	15360	24	1.25	1.106

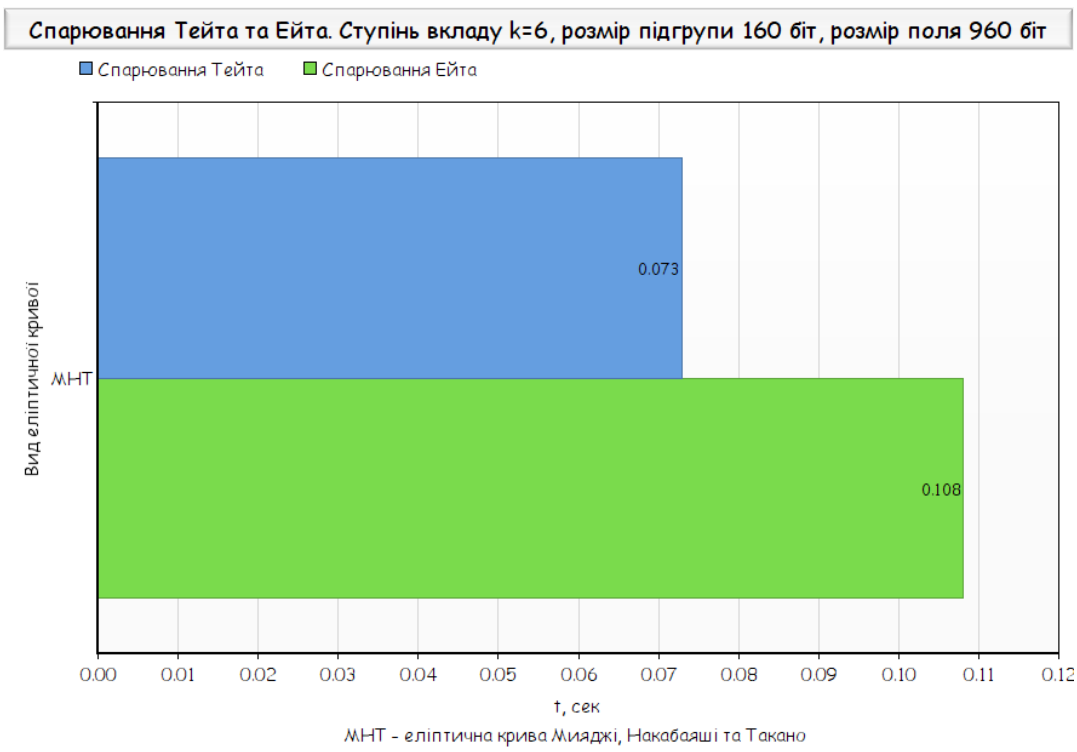


Рисунок 3.21 - Спарювання точок методами Тейта та Ейта на MHT кривих при ступеню вкладу k=6

При порівнянні швидкісних характеристик спарювання точок методом Тейта та Ейта при ступеню вкладу k=6 на еліптичній кривій побудованій за алгоритмом MHT (рис. 3.21) для забезпечення рівня безпеки AES-80, метод

спарювання Тейта на еліптичній кривій з розміром підгрупи 160 біт та розміром розширеного поля 960 біт випередило спарювання Ейта. Виграшом застосування спарювання Тейта на МНТ кривих склало 48%.

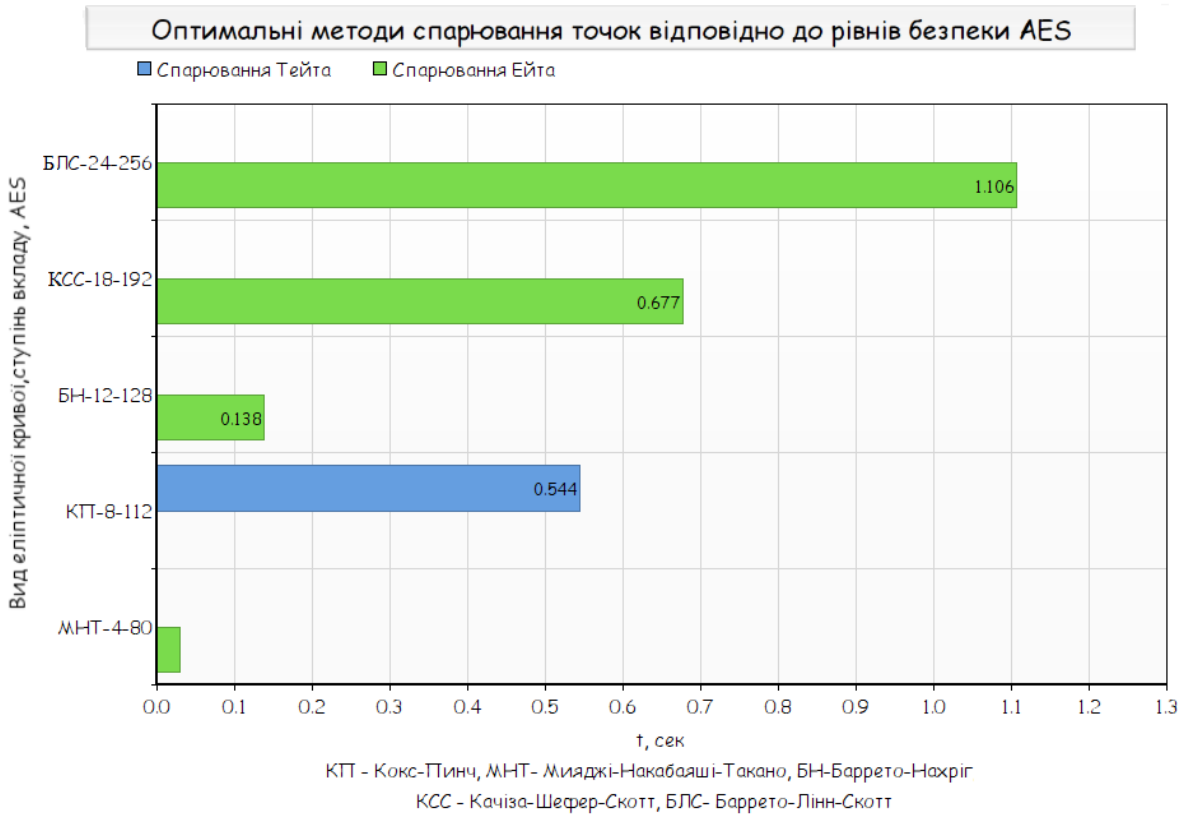


Рисунок 3.22 - Оптимальні методи спарювання точок відповідно до рівнів безпеки AES

При порівняльному аналізі методів спарювання точок еліптичних кривих було обрано найкращі, за критерієм швидкості та ефективності, методи спарювання, які задовольняють сучасним рівням безпеки AES (рис. 3.22).

3.5 Висновки до 3 розділу

Розробка велась за допомогою спеціальних класів та функцій бібліотеки MIRACL.

У цьому розділі було реалізовано 16 методів спарювання точок еліптичних кривих в різних підгрупах та з різними ступенями вкладу. Основною

метою реалізації було визначення швидкісних характеристик методів спарювання при різних вхідних параметрах, зокрема ступеню вкладу, розміру підгруп, розміру розширеного поля та відповідному рівню безпеки.

У порівнянні було реалізовано 2 види спарювання точок еліптичних кривих Тейта та Ейта.

Для систематизації отриманих результатів використовувалися таблиці та графіки зі спільним ступенем вкладу k, різними еліптичними кривими, розмірами підгруп та полів.

При дослідженні методів спарювання еліптичних кривих було виявлено, що для забезпечення рівня безпеки AES-80 оптимальним рішенням для використання методів спарювання у криптосистемах є спарювання Ейта на МНТ еліптичних кривих зі ступенем вкладу k=4 та часом на виконання 0.029 секунд.

Для забезпечення рівня безпеки AES-112 необхідно використовувати метод спарювання Тейта на КП еліптичних кривих при швидкості алгоритма 0.544 секунди.

Для забезпечення рівня безпеки AES-128 було обрано метод спарювання Ейта на еліптичній кривій БН зі швидкістю 0.138 секунд. Також на основі цього методу спарювання точок еліптичних кривих було реалізовано короткий підпис BLS.

Для забезпечення рівня безпеки AES-192 та AES-256 було обрано оптимальний метод спарювання точок Ейта на КСС та БЛС еліптичних кривих відповідно.

.

4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Аналіз потенційних небезпек

Процес роботи програміста відбувається в офісному приміщенні і безпосередньо пов'язаний з використанням певних інструментів навколишнього середовища таких, як обчислювальні пристрої, оргтехніка та комп'ютер. В результаті такої взаємодії співробітник може піддаватися впливу різних чинників, негативно впливаючих на організм.

Умови праці поділяють на чотири класи: оптимальні (I), допустимі (II), шкідливі (III) та небезпечні або екстремальні (IV).

Перші два класи не перевищують гранично допустимі величини ПДВ - умови праці є безпечними. Для III класу чинники перевищують ПДВ, можливо професійне захворювання. У разі IV класу ризик професійного захворювання дуже високий. Оцінка класу умов праці проводиться на основі інструментальних вимірювань факторів виробничого середовища і порівняння їх з ПДВ.

ПДВ фактора - це мінімальна або максимальна величина, при якій людина може працювати нормальну робочу зміну весь трудовий період до виходу на пенсію і при цьому у нього не виникає відхилень здоров'я, викликаних цим фактором. Перевищення допустимих значень є порушенням правил охорони праці і вимагає вжиття заходів щодо їх зниження, або доплат за ризик.

При експлуатації персонального комп'ютера на програміста можуть впливати наступні небезпечні і шкідливі виробничі фактори:

- небезпека ураження електричним струмом, внаслідок недотримання правил електробезпеки або виходу з ладу електроприладів;
- напруга в електричному ланцюзі, замикання якого може відбутися через тіло людини;
- порушення роботи кістково-м’язового апарату внаслідок тривалих статичних навантажень при роботі з ПК.
- електромагнітне випромінювання від ПК, екранів моніторів та іншої оргтехніки;

- незадовільні ергономічні характеристики робочого місця внаслідок нераціонального планування робочого місця, що може призвести до механічних травм, уражень електричним струмом та порушень кістково м’язового апарату;
- негативний вплив недостатнього освітлення робочої зони на зір та продуктивність роботи працюючого, внаслідок несправності освітлювальних приладів або неправильного проектування освітлювальної системи;
- негативний вплив незадовільних параметрів повітряного середовища робочої зони на здоров’я працюючого, внаслідок неправильного проектування системи вентиляції або несправності її несправності;
- небезпека загоряння у зв'язку із несправністю електричного обладнання, недотримання, або порушення правил протипожежної безпеки обслуговуючим персоналом, що може призвести до пожежі;
- неправильні дії працюючого у надзвичайних ситуаціях.

При експлуатації електрообладнання небезпечним виробничим фактором є електричний струм.

Види ураження електричним струмом:

- електричний удар (параліч серця і дихання);
- термічний опік;
- технічні пошкодження;
- електро-офтальмія - запалення очей внаслідок дії електроструму.

Гранично допустима величина змінного струму 0,3 мА. При збільшенні струму до 0,6-1,6 мА людина починає відчувати його вплив.

4.2 Заходи щодо забезпечення безпеки

Приміщення офісу, в якому працює програміст, відносять до приміщень без підвищеної небезпеки ураження електричним струмом. Обладнання, що використовується в приміщенні є споживачем електроенергії, що живиться від змінного струму 220 В від мережі з заземленою нейтраллю, та відноситься до електроустановок до 1000В закритого виконання.

У приміщенні розміщена електропроводка з напругою в мережі 220В. При цьому існує небезпека ураження струмом при електричному пробої на корпус, який може статися як у системному блоці комп'ютера, так і в периферійних пристроях.

За способом захисту людини від ураження електричним струмом відповідає згідно з ГОСТ 12.2.007.0-75* (2001) «ССБТ. Изделия электротехнические. Общие требования безопасности».

I група (стаціонарні комп’ютери,) та II (освітлювальні прилади, кондиціонери, опалювальні пристрої, ноутбуки, сканери).

Згідно «Правилам улаштування електроустановок» (далі «ПУЕ») виконані такі групи заходів з електробезпеки:

Конструктивні заходи забезпечують захист від випадкового дотику до струмопровідних частин за допомогою їх ізоляції та захисних оболонок. Згідно з ГОСТ 12.1.009-76 (1999) «ССБТ. Электробезопасность. Термины и определения» у приладах II класу захисту використовується подвійна ізоляція - електрична ізоляція, що складається з робочої і додаткової ізоляції. Так як згідно з НПАОП 40.1-1.32-01 «Правила устройства электроустановок. Электрооборудование специальных установок» офісні приміщення у більшості своїй відносяться до класу пожежонебезпечної зони

П-IIа (приміщення, в яких містяться тверді горючі речовини), тому передбачений ступінь захисту ізоляції обладнання IP44.

Схемо-конструктивні заходи призначені для забезпечення захисту від ураження електричним струмом при дотику до металевих оболонок, які можуть опинитися під напругою в результаті аварій. Згідно з ГОСТ 12.1.030-81 (2001) «ССБТ. Электробезопасность. Защитное заземление, зануление» у приміщенні влаштовується занулення.

Організаційні заходи.

Експлуатація електроустановок і електроустаткування проводиться відповідно до НПАОП 40.1-1.01-97 «Правила безпечної експлуатації електроустановок» та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів».

Для запобігання статистичного навантаження при користуванні ПК рекомендовано використовувати перерви в роботі 10 хв. через кожні дві години.

Синдром зап’ястного каналу, або тунельний синдром зап’ястя, який може бути наслідком хронічної травми, трапляється у людей внаслідок тривалої роботи з мишею: постійні напруга і здавлювання приводить до мікротравм, здавлювання нерва прилеглими оточуючими тканинами, через що виникає набряк. Щоб тунельний синдром програміста не турбував, потрібно дотримуватися кількох правил організації робочого місця:

- оптимальна висота клавіатури від підлоги – 65-75 см;
- наявність ергономічних і зручних особисто для вас миші і клавіатури;
- можливість регулювання висоти і нахилу клавіатури (відстань від поверхні стола до середини клавіатури – не більше 30 мм, кут підйому клавіатури – від 2° до 15°);
- наявність у клавіатури підставки для рук;
- наявність килимка для миші з захистом від тунельного синдрому (спеціальний виступ забезпечує правильне положення кисті);
- наявність стільця або крісла з підлокітниками;

Площа на одне робоче місце, обладнане комп'ютером для користувачів повинна складати не менше 6м^2, а обсяг не менше - 20м^3.

Робоче місце, обладнане персональним комп'ютером по відношенню до світлових прорізів повинно розташовуватися так, щоб природне світло падало збоку, бажано зліва.

При роботі з мишкою і клавіатурою також слід дотримуватися певних правила. Коли ви набираєте текст, рука повинна бути зігнута в лікті під прямим кутом, а при роботі з мишкою стежте, щоб кисть була прямою і лежала на столі якнайдалі від краю. Час роботи з комп'ютером слід обмежити до дійсно необхідного.

Щоб попередити тунельний синдром потрібно робити спеціальні вправи для кистей – чим частіше, тим краще. Ці вправи допоможуть поліпшити

кровообігу в м'язах і розтягнути їх. Комплекс вправ потрібно повторювати приблизно кожні 45 хвилин, тривалість однієї вправи – 1-2 хв.

Нервове напруження впливає на серцево-судинну систему, збільшуючи артеріальний тиск і частоту пульсу, а також на терморегуляцію організму та емоційні стани співробітника. Особливу роль в запобіганні втоми працівників відіграють професійний відбір, організація робочого місця, правильне робоче положення, ритм роботи, використання емоційних і матеріальних стимулів, впровадження раціональних режимів праці та відпочинку.

Боротьба з втомою, в першу чергу, зводиться до поліпшення санітарно-гігієнічних умов виробничого середовища - ліквідація забруднення повітря, шуму, вібрації, нормалізація мікроклімату, раціональне освітлення робочого місця і приміщення в цілому.

4.3 Заходи щодо виробничої санітарії та гігієни праці

Головним об'єктом охорони праці є людина в процесі праці і при розробці вимог виробничої санітарії використовуються результати досліджень ряду медичних і біологічних дисциплін.

Успіх у вирішенні проблем охорони праці у великій мірі залежить від якості підготовки фахівців, від їхнього вміння приймати правильні рішення в складних умовах сучасного виробництва.

Організація і поліпшення умов праці на робочому місці є одним з найважливіших резервів продуктивності праці і економічної ефективності виробництва, а також подальшого розвитку самого співробітника. Для підтримки тривалої працездатності людини велике значення має режим праці і відпочинку.

Фізіологічно раціональним режимом праці і відпочинку є таке чергування періодів роботи з періодом відпочинку, при якому досягається висока ефективність суспільно-корисної діяльності людини, хороший стан здоров'я, високий рівень працездатності і продуктивності.

Після встановлення нормального виробничого процесу, змінний режим праці та відпочинку робітників стає ефективним засобом попередження стомлення працюючих.

Раціональна організація праці на робочому місці пов'язана з проблемою правильної організації роботи протягом усього тижня, що забезпечується систематичної наукової організацією виробництва. Для підтримки тривалої працездатності людини має велике значення не тільки добовий і тижневий режим праці і відпочинку, але і місячний, щорічний.

Для створення оптимальних умов праці на робочому місці необхідно встановлювати оптимальні показники умов для кожного виду виробництва характеризують виробничу середу. Для отримання доступу до роботи співробітники повинні пройти медичний огляд.

Важливим чинником в роботі програміста є виробниче освітлення, яке буває природним та штучним.

Природним - обумовлено прямими сонячними променями і розсіяним світлом небосхилу. Змінюється в залежності від географічної широти, часу доби, ступеня хмарності.

Штучним - створюється штучними джерелами світла (лампи, світильники). Застосовується при відсутності або нестачі природного. За призначенням буває - робочим, аварійним, евакуаційним, охоронним, черговим. Влаштовувати одне місцеве освітлення не можна. При недостатності природного освітлення використовується поєднане (комбіноване) освітлення - при якому в світлий час доби використовується одночасно природний і штучне світло.

Значення освітленості на поверхні робочого столу в зоні розміщення документів становить 300 лк. Як джерела штучного освітлення в приміщенні застосовуються люмінесцентні лампи типу ЛБ.

Для того, щоб визначити загальну штучну освітленість приміщення програміста проведемо розрахунок.

Вихідні дані:

- довжина приміщення (А) – 6 м;
- ширина (В) – 4 м;

- висота (Н) – 3 м;
- тип світильника – ЛПО;
- L/h – 1,4;
- Колір стелі, стін, підлоги ($\rho_{ст}$, $\rho_{с}$, $\rho_{п}$) – 70%, 50%, 30%.

Нормовані показники штучного освітлення для адміністративних будівель, а саме кабінетів та робочих кімнат, згідно ДБН В.2.5-28-2006 «Природне і штучне освітлення»: висота робочої поверхні над підлогою ($h_р$) – 0,8 м, розряд та підрозряд зорової роботи – Б-1, освітленість робочих поверхонь при загальному освітленні ($E_н$) – 300 лк.

Значення коефіцієнту запасу ($k_з$) при проектуванні штучного освітлення для кабінетів і робочих приміщень дорівнює 1,4.

Спочатку проведемо розрахунок кількості рядів світильників у приміщенні $N_р$ (4.1):

$$N_p = \frac{B}{(H-h_p)(L/h)} \quad (4.1)$$

$$N_p = \frac{4}{(3-0.8)*1.4} = 1.3 \approx 2 \text{ шт.}$$

Наступною визначимо максимально припустиму відстань між рядами світильників L_{max} (4.2.):

$$L_{max} = \frac{B}{N_p} \quad (4.2)$$

$$L_{max} = \frac{4}{2} = 2 \text{ м.}$$

Далі визначаємо значення індексу приміщення i, що характеризує співвідношення розмірів освітлювального приміщення і висоти розміщення світильників (4.3.):

$$i = \frac{A*B}{(H-h_p)(A+B)} \quad (4.3)$$

$$i = \frac{6 * 4}{(3 - 0.8)(6 + 4)} = 1{,}09$$

З огляду на те, що тип світильника ЛПО,L/h – 1,4, колір стелі, стін, підлоги (ρст, ρс, ρп) відповідно 70%, 50%, 30%, а індекс приміщення (i) – 1,09, слідує, що значення коефіцієнта використання світлового потоку (η), створюваного світильниками вибраного типу, приймає значення 48%.

Визначимо сумарний світловий потік освітлювальної установки у даному приміщені $Ф_с$ (4.4):

$$Ф_с = \frac{E_Н * A * B * k_з * z}{\eta} \quad (4.4)$$

$$Ф_с = \frac{300 * 6 * 4 * 1.4 * 1{,}1}{0{,}48} = 23100 \text{ лм.}$$

Розрахуємо умовну загальну кількість світильників у приміщені $N_{св}^*$ (4.5):

$$N_{св^*} = \frac{A * B}{L^2 max} \quad (4.5)$$

$$N_{св^*} = \frac{6 * 4}{2^2} = 6 \text{ шт}$$

Визначимо загальну кількість ламп у світильнику $N_л^*$, за формулою (4.6):

$$N_{л^*} = n * N_{св^*} \quad (4.6)$$

$$N_{л^*} = 2 * 6 = 12 \text{ шт.}$$

Розрахуємо світловий потік умовного джерела світла $Ф_л^*$(4.7):

$$Ф_{л^*} = \frac{Ф_с}{N_{л^*}} \quad (4.7)$$

$$Ф_{л^*} = \frac{23100}{12} = 1925 \text{ лм.}$$

Вибираємо тип стандартної лампи ЛД 30 з найближчим значенням фактичного світлового потоку лампи $Ф_л$ – 1640 лм(1800), і знаходимо коефіцієнт m (4.8) (співвідношення між розрахунковим світловим потоком лампи $Ф_л^*$ та фактичним світловим потоком вибраної стандартної лампи $Ф_л$):

$$m = \frac{Ф_{л^*}}{Ф_л} \tag{4.8}$$

$$m = \frac{1925}{1800} = 1{,}07.$$

Далі визначаємо оптимальну (фактичну) кількість світильників у приміщенні $N_{св}$ (4.9):

$$N_{св} = m * N_{св^*} \tag{4.9}$$

$$N_{св} = 1{,}07 * 6 = 6{,}42 = 6 \text{ шт.}$$

Наступним визначаємо фактичну кількість ламп у приміщенні $N_л$:

$$N_л = N_{св} * n \tag{4.10}$$

$$N_л = 6 * 2 = 12 \text{ шт.}$$

Як підсумок, можна сказати, що для створення штучної освітленості 300 лк у кабінеті площею 24 м^2 , вибираємо 6 світильників, розташованих по 3 у кожному ряді.

Показники мікроклімату в офісних приміщеннях відповідають встановленим санітарно-гігієнічним вимогам ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень», ГОСТ 12.1.005-88 (1991) «ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны» і ГН 2152-80 «Санітарно-гігієнічні норми допустимих рівнів іонізації повітря виробничих та громадських приміщень».

Робота програміста в приміщенні належить до категорії Іб - легка робота, тому встановлені наступні оптимальні значення параметрів мікроклімату:

а) у холодний період року:

- температура 21-23С; --- 3

- відносна вологість: 40-60%;
- швидкість переміщення повітря: 0,1 м/с;

б) у теплий період року:

- температура 22-24С;
- відносна вологість: 40-60%;
- швидкість переміщення повітря: 0,2 м/с.

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях у приміщення нормуються згідно ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» та ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

Зниження рівня шуму в приміщенні здійснено за допомогою:

- використання більш сучасного обладнання;

- розташування принтерів та різноманітного устаткування колективного користування на значній відстані від більшості робочих місць працівників;

- переведення жорсткого диска в режим сну, якщо комп'ютер не працює протягом визначеного часу;

- використання блоків живлення ПК з вентиляторами на гумових підвісках.

4.4 Заходи з пожежної безпеки

Закон України «Про пожежну безпеку» визначає загальні правові, економічні та соціальні основи забезпечення пожежної безпеки на території України, регулює відносини державних органів, юридичних і фізичних осіб у цій галузі незалежно від виду їх діяльності та форм власності.

Пожежна безпека – стан об’єкта, при якому з регламентованою ймовірністю виключається можливість виникнення та розвиток пожежі і впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей.

Метою пожежної безпеки об’єкта є попередження виникнення пожежі на визначеному чинними нормативами рівні, а у випадку виникнення пожежі – обмеження її розповсюдження, своєчасне виявлення, гасіння пожежі, захист людей і матеріальних цінностей.

Для забезпечення пожежної безпеки в установах проводять пожежну профілактику, яка включає в себе комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження її поширення, а також на створення умов для успішного гасіння пожежі.

Для ліквідації пожежі у початковій стадії її розвитку силами персоналу об’єктів застосовуються первинні засоби пожежогасіння. До них відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, ящики з піском, пожежні відра, совкові лопати, ломи, сокири тощо), системи автоматичного пожежогасіння.

Своєчасне виявлення ознак займання й виклик пожежних підрозділів дає змогу швидко локалізувати осередки пожежі та вжити заходи щодо її ліквідації, а отже, створює можливість суттєво зменшити обсяги заподіяної шкоди. Найшвидшим та найнадійнішим засобом сповіщення про виникнення пожежі вважаються установки електричної пожежної сигналізації.

В кільцевій установці ЕПС в приміщенні програміста встановлено адресований пожежний сповіщувач. Адресований сповіщувач постійно або періодично активно формує сигнал про стан пожежонебезпечності у захищеному приміщенні та про власну працездатність із зазначенням свого номера (адреси).

В дію введено також тепловий автоматичний пожежний сповіщувач типу ІТМ.

Первинні засоби пожежогасіння, в залежності від категорії приміщень, можуть розташовуватись як окремо, так і в складі пожежних щитів.

Електромережі, електроприлади та апаратура повинні експлуатуватися тільки у справному стані з урахуванням вказівок і рекомендацій заводів-виробників. У разі пошкоджень електромереж, вимикачів, розеток та інших електроприладів слід негайне вимкнути їх і вжити необхідних заходів щодо приведення до пожежобезпечного стану.

Струмові перевантаження виникають при ввімкненні до мережі додаткових споживачів струму або при зниженні напруги в мережі. Тривале перевантаження призводить до нагрівання провідників, що може викликати займання ізоляції.

Залежно від агрегатного стану й особливостей горіння різних горючих речовин і матеріалів пожежі за ДБН В.1.1.7-2002 «Пожежна безпека об’єктів будівництва» поділяються на відповідні класи.

В офісному приміщенні знаходиться дерев`яна мебель, електронна апаратура, бумажні носії інформації.

Клас пожежі у офісному приміщенні (згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об’єктів будівництва») – пожежі твердих речовин, переважно органічного походження, горіння яких супроводжується тлінням (деревина, пластмаси, папір) визначається як клас А. Категорія приміщення (згідно із НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою») – визначається як категорії П-IIа.

Згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об’єктів будівництва» – для кабінету програміста площею 24 м^2 застосовано вогнегасники типу ВВ-5 та ВП-3.

Крім цього кабінет програміста повинен бути обладнаний автоматичними пожежними сповіщувачами, що реагують на підвищення температури, дим, полум’я. Наприклад, сповіщувачі моделей ДТЛ, ІТМ.

4.5 Заходи безпеки у надзвичайних ситуаціях

Захисні споруди цивільної оборони призначаються для захисту в мирний час персоналу, який переховується від наслідків аварій, катастроф та стихійного лиха, які загрожують масовому ураженню людей, а також у воєнний час - від сучасної зброї масового ураження. В мирний час захисні споруди використовуються для господарчих потреб.

До захисних споруд цивільного захисту належать:

- сховище;
- протирадіаційне укриття;
- швидко споруджувана захисна споруда цивільного захисту.

Сховища є найбільш надійним захистом від усіх уражальних чинників: високих температур і шкідливих газів у зонах пожеж, вибухонебезпечних, радіоактивних і сильнодіючих отруйних речовин, обвалів і уламків зруйнованих будинків і споруд тощо, а також засобів масового ураження і звичайних засобів ураження. Воно обладнане комплексом інженерних споруд, що забезпечують необхідні умови життєдіяльності протягом певного часу. За місцем знаходження сховища бувають збудованими (у підвалах будинків) і відокремленими (поза будинками). Їх споруджують заздалегідь, у мирний час, але можуть будувати і в період загрози нападу або під час воєнних дій (швидко зведені). За місткістю розрізняють малі сховища (150-300 чол.), середні (300-600 чол.) і великі (понад 600 чол.). Сховища мають фільтровентиляційні установки (ФВУ) промислового виготовлення, ФВУ очищає зовнішнє повітря, розподіляє його по відсіках і створює у захисному приміщенні надлишковий тиск, що перешкоджає проникненню зараженого повітря через тріщини і щілини.

Протирадіаційними укриттями (ПРУ) називаються негерметичні захисні споруди, що забезпечують захист людей в умовах надзвичайних ситуацій. Захисні властивості укриття визначаються коефіцієнтом послаблення радіації, що залежить від товщини огороджувальних конструкцій, властивостей матеріалу, з якого виготовлені конструкції, а також від енергії гамма-випромінювання. Для підсилення захисних властивостей у приміщенні забивають вікна і зайві двері, насипають шар ґрунту на перекриття і роблять, якщо треба ґрунтову підсипку ззовні біля стін, що виступають вище поверхні землі. Для герметизації приміщень ретельно замуровують тріщини, щілини, отвори у стінах і стелі, біля вікон і дверей, припасовують двері, оббивають їх повстю, ущільнюють дверні рами валиком з повсті або з іншої м'якої тканини. Укриття, що вміщує до 30 чоловік, провітрюється природною вентиляцією через припливний і витяжний короби.

Швидко споруджувана захисна споруда цивільного захисту – захисна споруда, що зводиться із спеціальних конструкцій за короткий час для захисту людей від дії засобів ураження в особливий період.

Для захисту людей від деяких факторів небезпеки, що виникають внаслідок надзвичайних ситуацій у мирний час, та дії засобів ураження в особливий період також використовуються споруди подвійного призначення та найпростіші укриття.

Споруда подвійного призначення – це наземна або підземна споруда, що може бути використана за основним функціональним призначенням і для захисту населення. (підземний простір метрополітену, підземні паркінги, підземні переходи тощо);

Найпростіше укриття - це фортифікаційна споруда, цокольне або підвальне приміщення, що знижує комбіноване ураження людей від небезпечних наслідків надзвичайних ситуацій, а також від дії засобів ураження в особливий період.

Алгоритм підготовки приміщення під захисну споруду:

- провітрити і при необхідності здійснити дезінфекцію приміщень;
- винести з приміщень громіздке устаткування, що перешкоджає розміщенню людей;
- встановити нари і лавки для розміщення людей, при цьому необхідно зберегти максимальну місткість захисної споруди;
- забезпечити необхідний запас медикаментів, води.

Правила поведінки у захисній споруді.

1. Забороняється приносити у захисну споруду легкозаймисті речовини або речовини, що мають сильний запах, а також громіздкі речі, приводити тварин;

2. У захисній споруді забороняється палити, шуміти, запалювати без дозволу гасові лампи, свічки, не слід ходити по приміщеннях без особливої необхідності, необхідно дотримуватись дисципліни, якнайменше рухатися. Слід організувати позмінний відпочинок людей на місцях, обладнаних для лежання.

3. Для повноцінного відпочинку можна тримати у захисній споруді або брати з собою легкі підстилки і невеликі подушки з поролону, губчатої гуми або іншого синтетичного матеріалу.

5. ЕКОНОМІЧНА ЧАСТИНА

5.1 Актуальність проекту

Широке використання обчислювальних мереж, призводить до того, що з’являється велика можливість для несанкціонованого доступу до переданої інформації.

Останнім часом зріс інтерес до питань захисту інформації. Це пов'язують з тим, що стали більш широко використовуватися обчислювальні мережі, що призводить до того, що з'являються великі можливості для несанкціонованого доступу до переданої інформації.

Важливість і актуальність питань захисту інформації вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються в процесі проектування, створення та використання сучасних інформаційних систем. Причини такої підвищеної уваги до цієї проблеми цілком очевидні - від якості заходів захисту інформації безпосередньо залежить економічна безпека організацій та підприємств.

Захист інформації та проблема забезпечення цілісності і конфіденційності набуває актуальності для дуже багатьох людей, в тому числі, чия діяльність знаходиться поза області, де ці питання вирішують державні органи.

У наші дні для підтвердження цілісності даних в електронній формі та для ідентифікації підписувача використовуються різноманітні електронні цифрові підписи.

Загалом цифровий підпис – це електронний документ, отриманий за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Електронний цифровий підпис як засіб контролю походження і цілісності інформації є ефективним інструментом забезпечення інформаційної безпеки на

всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави.

5.2 Розрахунок витрат на практичну реалізацію проекту

У складі витрат на реалізацію проекту враховується вартість всіх ресурсів, необхідних для реалізації короткого підпису.

З метою визначення витрат на реалізацію проекту складаємо розрахунок витрат, наведених у таблиці 5.1.

Таблиця 5.1 – Розрахунок витрат на реалізацію проекту

Витрати	Сума	
	грн.	%
Заробітна плата персоналу	78000	46.6
Відрахування на єдиний соціальний внесок	17160	10.2
Спеціальне обладнання	65000	38.8
Витрати на послуги сторонніх організацій	420	0.3
Загальногосподарські витрати	2840	1.7
Амортизаційні відрахування	4047	2.4
Загальна сума витрат	167467	100

Розрахунок витрат показав, що найбільшу частку складають виплати заробітної плати та відрахування на єдиний соціальний внесок. Так само важливу частину займають витрати на придбання техніки, необхідної для реалізації проекту.

5.3 Розрахунок заробітної плати

Витрати заробітної плати складаються виходячи з планового фонду заробітної плати всіх категорій працюючих, задіяних при реалізації проекту.

Розрахунок витрат проводиться на основі даних про трудомісткість роботи (таблиця 5.2).

Кількість місяців роботи над проектом складається виходячи з термінів реалізації проекту. В даному випадку очікуваний час реалізації проекту становить не більше 3 місяців. Результати розрахунків наводяться в таблиці 5.2.

Таблиця 5.2 - Розрахунок витрат на виплату заробітної плати учасникам проекту.

Посада	Кількість днів	Заробітна плата, грн / місяць	Заробітна плата, грн
Керівник проекту	90	15000	45000
Програміст	90	11000	33000
Всього			78000

5.4 Розрахунок відрахувань на єдиний соціальний внесок

Витрати на соціальні відрахування розраховуються в розмірі 22% від основної та додаткової заробітної плати. Розрахунок наведено в таблиці 4.3.

Таблиця 5.3 – Розрахунок витрат відрахувань на єдиний соціальний внесок.

Посада	Заробітна плата за весь період, грн	Соціальні відрахуання
Керівник проекту	45000	9900
Програміст	33000	7260
Всього	78000	17160

5.5 Розрахунок витрат на обладнання

Для виконання завдань з моделювання та програмування короткого підпису знадобиться наступне технічне обладнання, представлене в таблиці 5.4.

Таблиця 5.4 - Розрахунок витрат на спеціальне обладнання

Обладнання	Кількість, шт	Вартість, грн
Комп’ютер	2	64000
Wi-Fi маршрутизатор	1	1000
Всього	3	65000

На комп’ютері у ролі спеціального оснащення в даному випадку буде встановлена ОС Windows 10.

Програмне забезпечення, зокрема драйвери для системи та бібліотека MIRACL є повністю безкоштовними, або вільно надаються розробниками на обмежений термін.

Вартість спеціального обладнання та спеціального оснащення закладається у вартість комп'ютерного обладнання і становить 64000 грн.

5.6 Розрахунок витрат на послуги сторонніх організацій

В розділ витрат включається оплата робіт і виробничих послуг, проведених іншими організаціями при виконанні даної дослідницької роботи відповідно до укладених договорів.

В даному випадку до витрат на послуги сторонніх організацій належать витрати на доступ в мережу Інтернет, а саме, Інтернет-провайдера «Київстар». Провайдер не бере початковий внесок за підключення, а щомісячна вартість за послуги провайдера - 140 гривень.

Wi-Fi маршрутизатор буде купуватися окремо для забезпечення надійної роботи з інтернетом. Маршрутизатор D-Link DIR-825/AC був включений у розрахунок витрат на спеціальне обладнання (табл.4.4.) та становить 1000грн.

Сума витрат за інтернет на термін 3 місяці буде складати: 140·3 = 420 грн.

5.7 Розрахунок загальногосподарських витрат

Загальногосподарські витрати розраховуються в разі якщо вони безпосередньо пов'язані з виконанням даних робіт.

До даних витрат відносяться витрати на електроенергію, водопостачання та водовідведення.

При щомісячному споживанні електроенергії близько 200 кВт·год при тарифі Запоріжжяобленерго 2.143 грн/кВт·год витрати складуть (табл 5.5):

Таблиця 5.5 - Розрахунок витрат на електроенергію

Кількість	Вартість за 1 місяць, грн	Витрати за 3 місяці, грн
200 кВт	428.67	1286

При щомісячному використанні води близько 35 $м^3$ витрати за ставкою КП «Водоконал» м. Запоріжжя при тарифах на водопостачання 9.18 грн. за 1 $м^3$ та водовідведення 5.616 грн. за 1 $м^3$ витрати будуть складати табл. 5.6.

Таблиця 5.6 - Розрахунок витрат на водопостачання та водовідведення

Послуга	Кількість	Вартість за 1 місяць, грн	Витрати за 3 місяці, грн
Водопостачання	35	321.3	963.90
Водовідведення	35	196.56	589.68
Всього			1553.58

Таким чином загальногосподарські витрати за термінами реалізації проекту складуть 1286+1553.58 = 2840 грн.

5.8 Розрахунок на амортизацію об'єктів основних засобів

Амортизація - це процес перенесення вартості основних засобів і нематеріальних активів у міру їх фізичного або морального зносу по частинах на собівартість виробленої продукції. В процесі виробництва ряд ресурсів (оборотні кошти - сировина і матеріали) повністю перетворюються або списуються при кожному циклі виробництва. Вартість повністю входить до складу собівартості кінцевої продукції.

Інша частина ресурсів (основні засоби - обладнання, будівлі, споруди), беруть участь в кількох виробничих циклах, часто довго зберігаючи при цьому свою натуральну форму. Але через деякий час основні засоби потребуватимуть ремонту, модернізації або заміни, в тому числі з-за морального зносу.

Амортизація - в широкому сенсі - бухгалтерська і податкова концепції, які використовуються для оцінки втрати величини вартості активів з часом.

Амортизація об'єктів основних засобів.

Комп'ютер. Первісна вартість 32000 грн. Повний термін його корисного використання 4 роки (48 місяців). Для розрахунку коефіцієнта амортизації скористаємося формулою 5.1.

$$К = 1 / N \cdot 100\% \qquad (5.1)$$

Відповідно до формули 4.1, коефіцієнт амортизації: 1/48 · 100% = 2,08%. Амортизаційні відрахування на один комп'ютер за один місяць становитимуть: 32000 · 2,08% = 666 грн.

Так як будуть використовуватися 2 комп'ютери упродовж 3 робочих місяців, амортизаційні відрахування по одному комп'ютеру складатимуть: 666 · ·3 = 1998 грн.

Амортизаційні відрахування на два комп'ютери складуть 1998·2= 3996грн.

Wi-Fi маршрутизатор. Первісна вартість 1000 грн. Повний термін його корисного використання 5 роки (60 місяців). Для розрахунку коефіцієнта амортизації скористаємося формулою (4.1) : 1/60 · 100% = 1.67%.

Амортизаційні відрахування на Wi-Fi маршрутизатор за один місяць становитимуть: 1000 · 1.67% = 17 грн. Так як буде використовуватися Wi-Fi маршрутизатор протягом трьох робочих місяців, амортизаційні відрахування розраховуються на весь період реалізації проекту: 17 · 3 = 51 грн.

Повні амортизаційні відрахування в період виконання робіт за 3 місяці складуть: Σ = 3996 + 51 = 4047 грн.

5.9 Бальна оцінка економічної ефективності проекту

Бальна оцінка проводиться за такими важливими показниками:

- важливість розробки K_1;
- можливість використання результатів розробки K_2;
- теоретична значущість і рівень новизни дослідження K_3;
- складність розробки K_4.

Таблиця 5.7 - Шкала для оцінки важливості розробки K_1

№ п/п	Показник	Бали
1	Ініціативна робота, що не є частиною комплексної програми, або завданням відомчих органів	1
2	Робота, виконувана за договором про науково-технічну допомогу	3
3	Робота представляє частину відомчої програми	5
4	Робота представляє частину відомчої комплексної програми	7
5	Робота представляє частину міжнародної комплексної програми	8

Для даної роботи коефіцієнт важливості розробки K_1 дорівнює 5.

Шкала для оцінки можливості використання результатів розробки, оцінки рівня новизни, оцінки складності розробки наведені в таблицях, 5.8, 5.9, 5.10.

Таблиця 5.8 - Шкала оцінки можливості використання результатів розробки $К_2$

№ п/п	Показник	Бали
1	У даному підрозділі	1
2	У даній організації	3
3	У багатьох організаціях	5
4	У масштабах країни	8

Для даної роботи коефіцієнт можливості використання результатів розробки $К_2$ дорівнює 5.

Таблиця 5.9 - Шкала оцінки теоретичної значимості та рівня новизни дослідження $К_3$

№ п/п	Показник	Бали
1	Аналіз, узагальнення й класифікація відомої інформації. Подібні результати були відомі в досліджуваній області	2
2	Одержання нової інформації, що доповнює знання про сутність досліджуваних процесів, не відомі в досліджуваній області	3
3	Одержання нової інформації, що змінює уявлення про сутність досліджуваних процесів, не відомої раніше	5
4	Створення нових теорій, методик	6
5	Одержання інформації, що сприяє формуванню напрямків, не відомих раніше	8

Для даної роботи коефіцієнт теоретичної значущості і рівня новизни дослідження $К_3$ дорівнює 2.

Таблиця 5.8 - Шкала оцінки показників складності дослідження $К_4$

№ п/п	Показник	Бали
1	Робота виконується одним підрозділом, витрати менш 10000 грн.	1
2	Робота виконується одним підрозділом, витрати 10000-50000 грн.	3
3	Робота виконується одним підрозділом, витрати 50000-100000 грн.	5
4	Робота виконується за участю багатьох підрозділів, витрати 100000-500000 грн.	7
5	Робота виконується декількома організаціями, витрати понад 500000 грн.	8

Для даної роботи коефіцієнт складності розробки ($К_4$) дорівнює 5.

Загальна оцінка встановлюється за добутком коефіцієнтів:

$$Пс = К_1 \cdot К_2 \cdot К_3 \cdot К_4 \quad (5.2)$$

де K_1 - коефіцієнт важливості розробки; K_2-коефіцієнт можливості використання результатів розробки; K_3 - коефіцієнт теоретичної значущості і рівня новизни дослідження; K_4 коефіцієнт складності розробки.

Відповідно до формули 5.2 розраховується загальна оцінка:

$$Пс = К_1 \cdot К_2 \cdot К_3 \cdot К_4 = 5 \cdot 5 \cdot 2 \cdot 5 = 250$$

Питомий ефект на кожний бал - 2 000 грн. Загальний ефект від розробки складає: $А = Пс \cdot 2000 = 250 \cdot 2000 = 500000$ грн.

Економічна ефективність від реалізації дипломного проекту визначається за допомогою коефіцієнта ефективності, що характеризує частку загального ефекту від розробки, що приходиться на одну грн. витрат (собівартості НДР) згідно з формулою 5.3.

$$К_е = \frac{А}{\Sigma} \quad (5.3)$$

де $К_е$ - коефіцієнт ефективності; A - загальний ефект від розробки, грн; Σ- загальна сума витрат на реалізацію проекту, грн.

Розрахуємо коефіцієнт ефективності за формулою 5.3:

$$К_е = \frac{500000}{167467} = 2.99$$

В результаті проведених розрахунків, можна сказати, що реалізація проекту може принести дохід 500000 грн, при витратах 162318 грн та 3 місяців на виконання завдання. Це є економічно вигідним вкладенням для забезпечення оптимального рівня захищеності та конфіденційності.

ВИСНОВОК

Безпека криптографії, основаної на спарюванні, безпосередньо залежить від нерозв'язного рівня задачі дискретного логарифмування на еліптичних кривих (ECDLP) у групі E (F_q) або задачі дискретного логарифму (DLP) у групі F_q^k. Це означає, що протоколи, які побудовані на криптографії зі спарюваннями повинні працювати в робочому середовищі з параметрами 1024 біт, щоб забезпечити рівень безпеки AES - 80 біт. Через цей недолік криптографія, основана на спарюваннях, поступається іншим ассиметричним криптоалгоритмам. Але недолік ефективності криптосистем, що базується на спарюваннях, через постійне поліпшення методів, стає менш значним щодо криптосистем, таких як RSA або DSA.

Оскільки в групі точок еліптичної кривої немає субекспоненціальних алгоритмів дискретного логарифмування, спарювання точок в різних групах має хороші показники захищеності.

Виграшом застосування спарювання є зменшене число інформаційних обмінів по мережі.

При аналізі математичного апарату методів спарювання на еліптичних кривих було визначено, що для симетричних алгоритмів криптографії застосовується спарювання типу 1 (спарювання Вейля та Тейта). Для асиметричного систем криптографії використовуються спарювання типу 2 і 3.

Спарювання типу 2 - це неефективна реалізація спарювання типу 3 і не рекомендована для використання в криптографічних алгоритмах. У той час як спаровування типу 3 часто використовується в криптографії заснованої на спарюванні.

При дослідженні методів спарювання еліптичних кривих було виявлено, що для забезпечення рівня безпеки AES-80 оптимальним рішенням для використання методів спарювання у криптосистемах є спарювання Ейта на МНТ еліптичних кривих зі ступенем вкладу k=4 та часом на виконання 0.029 секунд.

Для забезпечення рівня безпеки AES-112 необхідно використовувати метод спарювання Тейта на КП еліптичних кривих при швидкості алгоритма 0.544 секунди.

Для забезпечення рівня безпеки AES-128 було обрано метод спарювання Ейта на еліптичній кривій БН зі швидкістю 0.138 секунд. Також на основі цього методу спарювання точок еліптичних кривих було реалізовано короткий підпис BLS.

Для забезпечення рівня безпеки AES-192 та AES-256 було обрано оптимальний метод спарювання точок Ейта на КСС та БЛС еліптичних кривих відповідно.

Апробація результатів роботи відбулася на всеукраїнській науково - практичній конференції здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації» (м. Кропивницький, 27–29 листопада 2018 р.)

Методи спарювання точок використовувались у криптосистемах на основі ідентифікаційних даних (IEEE p1363.3) та для проведення MOV-атаки. В наші часи спарювання (оптимальне спарювання Ейта) використовується у криптовалюті ZCash та можуть використовуватися для короткого підпису BLS.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Болотов А.А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. / Болотов А.А., Гашков С.Б., Фролов А.Б.- М.: КомКнига, 2006. – 280 с.

2. Баричев С.Г. Основы современной криптографии: Учебное пособие. / Баричев С.Г., Серов Р.Е. - М.: Горячая линия - Телеком, 2002. - 152 с.

3. Рябко Б.Я. Криптографические методы защиты информации. / Рябко Б.Я., Фионов А.Н.- М.: Горячая линия - Телеком, 2005. – 229 с.

4. Смарт Н.Г. Криптография. -М.: Техносфера, 2005. – 528 с.

5. Кнепп Э. Эллиптические кривые. -М.: Факториал Пресс, 2004.– 488с.

6. Анохин М. И. Спаривание Вейля и его применение к задачам Диффи—Хеллмана [Електронний ресурс] – Режим доступу: http://cryptography.ru /wp-content/uploads/2015/01/weil_pairing_anokhin.pdf

7. Pairing-Based Cryptographic Protocols: A Survey [Електронний ресурс] – Режим доступу: https://eprint.iacr.org/2004/064.pdf

8. Схемы шифрования, основанные на идентификаторах [Електронний ресурс] – Режим доступу: http://clc.am/m9xDag

9. Pairing cryptography in Rust [Електронний ресурс] – Режим доступу: https://blog.z.cash/pairing-cryptography-in-rust/

10. Бессалов А.В. О некорректности стандартного условия для MOV-атаки на эллиптические кривые [Електронний ресурс] – Режим доступу: http://elibrary.kubg.edu.ua/948/1.

11. Lynn B. On the implementation of pairing-based cryptosystems [Електронний ресурс] – Режим доступу: https://crypto.stanford.edu/pbc/thesis.pdf.

12. Drake J. Pragmatic signature aggregation with BLS [Електронний ресурс] – Режим доступу: https://ethresear.ch/t/pragmatic-signature-aggregation-with-bls/2105.

13. Boneh-Lynn-Shacham [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Boneh%E2%80%93Lynn%E2%80%93Shacham

14. Долгов В.И. Эллиптические кривые в криптографии. – Х: ХНУРе, 2008. – 36 с.

15. Р-алгоритм Поларда [Електронний ресурс] – Режим доступу: http://clc.am/bfd1pg

16. Еліптична крива [Електронний ресурс] – Режим доступу: http://clc.am/Z3Ik4A

17. Ишмухаметов Ш.Т. Математические основы защиты информации / Ишмухаметов Ш.Т., Рубцова Р.Г. – К: Учебное пособие, 2012. – 139 с.

18. A taxomy of Pairing-Friendly Elliptic Curves [Електронний ресурс] – Режим доступу: http://clc.am/x7jH3A.

19. Naehrig M. How to construct pairing-friendly curves [Електронний ресурс] – Режим доступу: http://clc.am/FSw3kQ

20. Pierrick G. Pairing-friendly curves [Електронний ресурс] – Режим доступу: https://www.cosic.esat.kuleuven.be/ecc2013/files/pierrick_gaudry_2.pdf

21. Boneh D. Rubin K. Finding composite order ordinary ellsptic curves using the Cocks-Pinch method [Електронний ресурс] – Режим доступу: https:// https://eprint.iacr.org/2009/533.pdf.

22. Nanjo Y.,Ghammam L. Efficient optimal ate pairing at 128-bit security level [Електронний ресурс] – Режим доступу: https://hal.archives-ouvertes.fr.

23. Lauter K., Naehrig M. Attractive subfamilies of BLS curves for implementing high-security pairings [Електронний ресурс] – Режим доступу: http://clc.am/DBZqNQ

24. Costello C. Fast formulas for computing cryptographic pairings [Електронний ресурс] – Режим доступу - http://clc.am/L2ucAA.

25. Miller V.S. The weil pairing, and its efficient calculation [Електронний ресурс] – Режим доступу - clc.am/IGKjxg.

26. Beuchat J., Okamato E. High-speed software implementation of the optimal ate pairing over Barreto-Naehrig curves [Електронний ресурс] – Режим доступу - https://eprint.iacr.org/2010/354.pdf

27. Shirase M., Okamato E. Some efficient algorithm for the final exponentiation of η_T pairing [Електронний ресурс] – Режим доступу - https://eprint.iacr.org/2006/431.pdf.

28. Криптографічна бібліотека MIRACL [Електронний ресурс] – Режим доступу - https://github.com/miracl.

29. Леонтьєв В. С. Аналіз методів спарювання точок еліптичних кривих / Леонтьєв В. С., Неласа Г. В. // Комп'ютерна інженерія і кібербезпека : досягнення та інновації : матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.). — Кропивницький: ЦНТУ, 2018. — 317 С.

Додаток А

РЕАЛІЗАЦІЯ КОРОТКОГО ПІДПИСУ БЛС ЗА ДОПОМОГО КРИПТОГРАФІЧНОЇ БІБЛІОТЕКИ MIRACL

```
#include <iostream>
#include <ctime>

#define MR_PAIRING_BN
#define AES_SECURITY 128
#include "pairing_3.h"
int main()
{
	PFC pfc(AES_SECURITY); //ініціалізація еліптичної кривої призначеної для спарювання
	G2 Q,V;
	G1 S,R;
	int lsb;
	Big s,X;
	time_t seed;
	time(&seed);
    irand((long)seed);
// Генерація відкритого та закритого ключів
	pfc.random(Q); // Обираємо довільну точку Q, яка є генератором підгрупи G2
	pfc.random(R); // Обираємо довільну точку R, яка є генератором підгрупи G1
	pfc.random(s);    // Обираємо випадковий секретний ключ s
	V=pfc.mult(Q,s);  // Обчислюємо відкритий ключ Q^s

// Підпис
	pfc.hash_and_map(R,(char *)"Test Message to sign"); // хешуємо повідомлення
	S=pfc.mult(R,s); // Обчислюємо R^s
	lsb=S.g.get(X);   // підпис це молодший біт та координата x на еліптичній кривій

// Верифікація
	if (!S.g.set(X,1-lsb)) { // спочатку відновлюємо повну точку S
		cout << "Signature is invalid" << endl;
		exit(0);
	}

	G1 *g1[2]; // створюємо масиви з 2 елементів, що містять точки підгруп G1 та G2
	G2 *g2[2];
	g1[0]=&S; g1[1]=&R;
	g2[0]=&Q; g2[1]=&V;

	if (pfc.multi_pairing(2,g2,g1)==1) // обчислюємо спарювання.
//За властивістю альтернативності e(P,P)=1
		cout << "Signature verifies" << endl;
	else
		cout << "Signature is bad" << endl;

	 return 0;
   }
```

Додаток Б

РЕАЛІЗАЦІЯ СПАРЮВАННЯ ТЕЙТА ЗІ СТУПЕНЕМ ВКЛАДУ K=2 ЗА ДОПОМОГО КРИПТОГРАФІЧНОЇ БІБЛІОТЕКИ MIRACL

```
BOOL tate(ECn& P,ECn& Q,Big& q,ZZn& r){
    int i,nb,qnr;
    ZZn2 res;
    ZZn a,d;
    Big p,x,y,n;
    ECn A;
    p=get_modulus();
    normalise(P);
    normalise(Q);
    extract(Q,a,d);
    qnr=get_mip()->qnr;
    if (qnr==-2){
        a=a/2;
           d=d/4;    }
    A=P; n=q-1;
    nb=bits(n); res=1;
    for (i=nb-2;i>=0;i--){
        res*=res;
        res*=g(A,A,a,d);
        if (bit(n,i)) res*=g(A,P,a,d);
    }
    if (A != -P || res.iszero()) return FALSE;
    res=conj(res)/res;
    r=powl(real(res),(p+1)/q);
    if (r==1) return FALSE;
    return TRUE;
   }
ECn hash_and_map(char *ID,Big cof){
    ECn T;
    Big a=H1(ID);
    while (!is_on_curve(a)) a+=1;
    T.set(a);
    T*=cof;
    return T;
}
int main(){
    ifstream common("curve.ecs");      // параметри еліптичної кривої
    miracl* mip=&precision;
    ECn P,Q;
    ZZn res;
    Big q,r,y,B,cof;
    int nbits,A,qnr;
       clock_t time1;
       mip->IOBASE=16;
    modulo(q);
    qnr=mip->qnr;
    ecurve(qnr*qnr*A,qnr*qnr*qnr*B,q,MR_PROJECTIVE);

    ecurve(A,B,q,MR_PROJECTIVE);
    Q = hash_and_map((char *)"point 1",cof);
    P = hash_and_map((char *)"point 2",cof);
    cout << "Q=" << sA << endl;
    cout << "P=" << Server << endl;
       time1 = clock();
    if (!tate(P,Q,r,res)) cout << "Trouble" << endl;
       cout << "Швидкість: ";
       time1 = clock() - time1;
       printf("%f", (double)time1 / CLOCKS_PER_SEC);
    return 0;}
```

Додаток В

РЕАЛІЗАЦІЯ СПАРЮВАННЯ ТЕЙТА ЗІ СТУПЕНЕМ ВКЛАДУ K=4 ЗА ДОПОМОГО КРИПТОГРАФІЧНОЇ БІБЛІОТЕКИ MIRACL

```
#include <iostream>
#include <fstream>
#include <string.h>
#include "ecn.h"
#include <ctime>
#include "ecn2.h"
#include "zzn4.h"

using namespace std;
Miracl precision(16,0);
#define HASH_LEN 20
#define PROJECTIVE

void extract(ECn& A,ZZn& x,ZZn& y)
{
    x=(A.get_point())->X;
    y=(A.get_point())->Y;
}

#ifdef PROJECTIVE
void extract(ECn& A,ZZn& x,ZZn& y,ZZn& z)
{
    big t;
    x=(A.get_point())->X;
    y=(A.get_point())->Y;
    t=(A.get_point())->Z;
    if (A.get_status()!=MR_EPOINT_GENERAL) z=1;
    else                                   z=t;
}
#endif

BOOL tate(ECn& P,ECn2 Q,Big& q,Big *cf,ZZn2 &Fr,ZZn2& r){
    int i,nb;
    ECn A;
    ZZn4 w,res;
    ZZn4 a[2];
    ZZn2 Qx,Qy;

    Q.get(Qx,Qy);
    Qx=txd(Qx);
    Qy=txd(txd(Qy));
    res=1;
    A=P;
    nb=bits(q);
    for (i=nb-2;i>=0;i--) {
        res*=res;
        res*=g(A,A,Qx,Qy);
        if (bit(q,i))
                    res*=g(A,P,Qx,Qy);
    }
    if (!A.iszero() || res.iszero()) return FALSE;
    w=res;
       w.conj();
    res=w/res;
    res.mark_as_unitary();
    a[0]=a[1]=res;
    a[0].powq(Fr);
    res=pow(2,a,cf);
```

```
    r=real(res);
    if (r.isunity()) return FALSE;
    return TRUE;
}
ECn hash_and_map(char *ID,Big cof)
{
    ECn Q;
    Big x0=H1(ID);

    while (!is_on_curve(x0)) x0+=1;
    Q.set(x0);
    Q*=cof;
    return Q;
}
void set_frobenius_constant(ZZn2 &X){
    Big q=get_modulus();
    switch (get_mip()->pmod8){
    case 5:
         X.set((Big)0,(Big)1); // = (sqrt(-2)^(q-1)/2
         break;
    case 3:                    // = (1+sqrt(-1))^(q-1)/2
         X.set((Big)1,(Big)1);
         break;
   case 7:
         X.set((Big)2,(Big)1);  // = (2+sqrt(-1))^(q-1)/2
    default: break;
    }
    X=pow(X,(q-1)/2);
}
int main(){
    ifstream common("curve2.ecs");      // параметри еліптичної кривої
    miracl* mip=&precision;
    ECn P;
    ECn2 Q;
    ZZn2 res,Fr;
    Big q,r,B,cof;
    Big cf[2];
    clock_t time1;

    int bits,A;
    time_t seed;
    common >> bits >> q >> A >> B >> cof >> r;
    mip->IOBASE=16;
    time(&seed);
    irand(1L);

    ecurve(A,B,q,MR_PROJECTIVE);
    set_frobenius_constant(Fr);
    mip->IOBASE=16;
    mip->TWIST=MR_QUADRATIC;
    Q=hash2((char *)"Server");
    P=hash_and_map((char *)"Alice",cof);
       cout << "P: " << P << endl;
       cout << "Q: " << Q << endl;
       time1 = clock();
       if (!tate(P,Q,r,cf,Fr,res)) cout << "Trouble" << endl;
       time1 = clock() - time1;
       cout << "Time speed: ";
       printf("%f", (double)time1 / CLOCKS_PER_SEC);
        return 0;
    }
```

Додаток Г

РЕАЛІЗАЦІЯ СПАРЮВАННЯ ЕЙТА ЗІ СТУПЕНЕМ ВКЛАДУ K=4 ЗА ДОПОМОГО КРИПТОГРАФІЧНОЇ БІБЛІОТЕКИ MIRACL

```
#include <iostream>
#include <fstream>
#include <string.h>
#include "ecn.h"
#include <ctime>
#include "ecn2.h"
#include "zzn4.h"

using namespace std;
Miracl precision(16,0);
#define HASH_LEN 20
#define AFFINE

void extract(ECn& A,ZZn& x,ZZn& y){
    x=(A.get_point())->X;
    y=(A.get_point())->Y;
}

BOOL ate_pairing(ECn2& P,ECn Q,Big& T,Big *cf,ZZn2 &Fr,Big &e,Big q,ZZn2& r)
{
    int i,nb;
    ECn2 A;
    ZZn4 w,res,a[2];
    ZZn Qx,Qy;
    Big carry,ex[2],p=get_modulus();

    extract(Q,Qx,Qy);
    res=1;
    A=P;
    nb=bits(T);
    for (i=nb-2;i>=0;i--) {
        res*=res;
        res*=g(A,A,Qx,Qy);
        if (bit(T,i))
            res*=g(A,P,Qx,Qy);
    }
    w=res;
    w.powq(Fr); w.powq(Fr);
    res=w/res;
    res.mark_as_unitary();
    if (e.isone()){
        ex[0]=cf[0];
        ex[1]=cf[1];
    }
    else {
        carry=mad(cf[1],e,(Big)0,p,ex[1]);
        mad(cf[0],e,carry,p,ex[0]);
    }
    a[0]=a[1]=res;
    a[0].powq(Fr);
    res=pow(2,a,ex);
    r=real(res);
    if (r.isunity()) return FALSE;
    return TRUE;
}
ECn hash_and_map(char *ID,Big cof)
{
    ECn Q;
    Big x0=H1(ID);
```

```
    while (!is_on_curve(x0)) x0+=1;
    Q.set(x0);
    Q*=cof;
    return Q;
}
void set_frobenius_constant(ZZn2 &X){
    Big q=get_modulus();
    switch (get_mip()->pmod8)
    {
    case 5:
         X.set((Big)0,(Big)1); // = (sqrt(-2)^(q-1)/2
         break;
    case 3:                    // = (1+sqrt(-1))^(q-1)/2
         X.set((Big)1,(Big)1);
         break;
    case 7:                    // = (2+sqrt(-1))^(q-1)/2
         X.set((Big)2,(Big)1);
         break;
    default: break;
    }
    X=pow(X,(q-1)/2);
}
int main(){
    ifstream common("curve3.ecs");      // параметри еліптичної кривої
    miracl* mip=&precision;
    ECn Q;
    ECn2 P;
    ZZn2 res,Fr;
    ZZn ww;
    ZZn4 w;
    Big a,q,r,B,cof,t1;
    Big cf[2];
    clock_t time1;
    int bitz,A;
    time_t seed;

    common >> bitz;
    mip->IOBASE=16;
    common >> q >> A >> B >> cof >> r >> cf[0] >> cf[1];
    Big t=q+1-cof*r;
    Big cof2=(q*q+1)/r+(q*q-2*q)/r;
    t1=q-cof*r;
    time(&seed);
    irand((long)seed);

    ecurve(A,B,q,MR_AFFINE);
    set_frobenius_constant(Fr);
    mip->IOBASE=16;
    mip->TWIST=TRUE;
    P=hash2((char *)"Server",cof2);
    Q=hash_and_map((char *)"Alice",cof);
    a=rand(r);
       cout << "P: " << P << endl;
       cout << "Q: " << Q << endl;
       cout << "Time speed: ";
       time1 = clock();
    if (!power_pairing(P,Q,t1,cf,Fr,a,r,res)) cout << "Trouble" << endl;
       time1 = clock() - time1;
       printf("%f", (double)time1 / CLOCKS_PER_SEC);

    return 0;
   }
```

Додаток Д

РЕАЛІЗАЦІЯ СПАРЮВАННЯ ЕЙТА ЗА ДОПОМОГОЮ НОВОГО КЛАСУ PFC (PAIRING-FRIENDLY CURVE) ПРИ СТУПЕНЯХ ВКЛАДУ K=2,6,12,18,24

```
#include <iostream>
#include <ctime>

// Вибір кривої та рівня захищеності
//#define MR_PAIRING_CP      // рівень безпеки AES-80
//#define AES_SECURITY 80

//#define MR_PAIRING_MNT   // рівень безпеки AES-80
//#define AES_SECURITY 80

//#define MR_PAIRING_BN    // рівень безпеки AES-128
//#define AES_SECURITY 128

#define MR_PAIRING_KSS    // рівень безпеки AES-192
#define AES_SECURITY 192

//#define MR_PAIRING_BLS    // рівень безпеки AES-256
//#define AES_SECURITY 256

#include "pairing_3.h"

int main()
{
	PFC pfc(AES_SECURITY);  // ініціалізація еліптичної кривої призначеної для спарювання
	Big order=pfc.order();
	miracl* mip=get_mip();

	G2 Q;
	G1 P;
	GT g;
	time_t seed;
	clock_t time1;

	time(&seed);
	irand((long)seed);
	pfc.random(P);
	pfc.random(Q);
	cout << order << endl;

	pfc.precomp_for_mult(P);
	pfc.precomp_for_mult(Q);
	cout << "P: " << P.g << endl;
	cout << "Q: " << Q.g << endl;
	time1 = clock();
	g=pfc.pairing(Q,P);
	cout << "Time speed: ";
	time1 = clock() - time1;
	printf("%f", (double)time1 / CLOCKS_PER_SEC);

	return 0;
}
```