КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра математичної інформатики

Кваліфікаційна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою "Інформатика"
спеціальності 122 Комп'ютерні науки на тему:

ІМПЛЕМЕНТАЦІЯ КРИПТОСИСТЕМ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Виконав студент 4-го курсу
Солонко Нікіта Владиславович _____

(підпис)

Науковий керівник:
Член-кореспондент НАН України, професор
Анісімов Анатолій Васильович _____

(підпис)

Засвідчую, що в цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

(підпис)

Київ – 2023

РЕФЕРАТ

Обсяг роботи: 20 сторінок, 5 ілюстрацій, 0 таблиць, 12 використаних джерел.

TBD.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

ECC Elliptic curve cryptography;
EC Elliptic curve;
SIMD Single instruction multiple data;
DLP Discrete Logarithm Problem, задача дискретного логарифму;
GNFS General Number Field Sieve;

ВСТУП

Оцінка сучасного стану об’єкта дослідження

На даний момент, окрім того, що застосування еліптичних кривих у криптографії активно досліджується в академічних роботах, існує безліч прикладних реалізацій ECC, що використовуються повсюдно. Більш того, криптосистеми з відкритим ключем, що використовують еліптичні криві, потроху стають популярнішими за, найбільш розповсюджений зараз, RSA. Так, наприклад, нові версії ssh рекомендують використовувати ключі Ed25519, що побудовані на еліптичних кривих Едварда, замість RSA. Аналогічні рекомендації зараз дають такі сервіси як: GitLab, GitHub, Amazon Web Services, Google Cloud Platform і багато інших.

Актуальність роботи та підстави для її виконання

Як було зазначено раніше, криптосистеми з відкритим ключем побудовані на основі еліптичних кривих вже активно використовуються, але все ще перебувають у стані активного розвитку. Так, наприклад, стаття [1] в якій була запропонована одна з найбільш популярних зараз еліптичних кривих Ed25519 і алгоритм підпису/верифікації на її основі EdDSA була написана в 2012 році, що для криптографії недавно. Також зараз існує багато програмних реалізацій таких криптосистем, але, у зв’язку зі складністю їх імплементації, не всі вони є цілком безпечними. Варто зазначити, що з кожним роком архітектура обчислювальних систем розвивається: оптимізуються існуючі інструкції та додаються нові, що відкриває можливості як для оптимізації існуючих реалізацій, так і для написання нових - кращих. Наприклад, в архітектурі x64 апаратна підтримка SIMD обчислень з 512 бітними регістрами AVX-512 з’явилася в 2013 році, вже після виходу статті з описом Ed25519.

Мета й завдання роботи

Метою роботи є дослідження застосування еліптичних кривих у сучасній криптографії, і як результат дослідження імплементувати криптографічну бібліотеку для роботи з еліптичними кривими та порівняти її з існуючими реалізаціями.

Можливі сфери застосування

Оскільки програмна реалізація яку я розроблю у рамках цієї роботи не буде сертифікована, то її не варто буде застосовувати в реальних системах на які може бути здійснена атака, але вона може бути застосована у навчальних і академічних цілях. В перспективі така бібліотека може бути застосована всюди де потрібна безпечна комунікація, в умовах коли можливе прослуховування, або втручання в канали зв’язку, між сутностями які ще не узгодили симетричний ключ. Наприклад: TLS, HTTPS і так далі.

РОЗДІЛ 1. ЕЛІПТИЧНІ КРИВІ

1.1. Переваги над Z_p^*

Під Z_p^* мається увазі мультиплікативна група лишків за модулем p, де p - просте число.

Розглянемо мотивацію використання нового криптографічного примітиву, коли вже побудовано і імплементовано багато криптосистем на основі Z_p^*, таких як: Diffie-Hellman, ElGamal, RSA і багато інших. Проблема використання таких криптосистем полягає у тому, що вони були запропоновані давно: Diffie-Hellman [2] - 1976, RSA [3] - 1978, ElGamal [4] - 1985. З того часу кратно збільшились обчислювальні можливості. Частота ядер виросла з кГц до ГГц, кількість ядер збільшилась з одиниць до сотень, з'явилися зручні інструменти для об'єднання процесорів у кластери. Також, через бажання зламати дані криптосистеми, багато вчених шукали спосіб знайти більш ефективні алгоритми розв'язання проблем на які вони спираються. Таким чином у 1993 Ленстра [5] придумав ефективний алгоритм розкладання великих чисел на множники - GNFS(General Number Field Sieve), який може розкласти число $n > 10^{100}$ за час:

$$\exp\left(\left(\left(\frac{64}{9}\right)^{\frac{1}{3}} + o(1)\right)(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}\right)$$

Це стало основною проблемою криптосистем на основі Z_p^*, тому що він робить вирішення обчислювальних проблем, на які спираються ці криптосистеми субекспоненційним, замість експоненційних. Варто зазначити, що цей алгоритм не є чисто теоретичною загрозою. За його допомогою у 2019 році [6] було знайдено дискретний логарифм 795 бітного числа. Таким чином, в патенті RSA [3] рекомендований розмір ключів був 200біт, в першій NIST сертифікації -

512 біт, зараз же мінімальний рекомендований розмір - 2048 біт. Важливим також є те, що GNFS неможливо узагальнити на будь-які скінчені циклічні групи, тому він не зачіпає групу точок еліптичної кривої над скінченним полям (позначення буде наведено далі), по цій причині найкращий відомий алгоритм для вирішення проблеми дискретного логарифма для групи точок еліптичних кривих (ECDLP) займає час $O(\sqrt{q})$, де q - розмір групи. Через це розміри ключів що мають однакову безпеку для Z_p^* і для групи точок кліптичної кривої сильно відрізняються. Порівняльна характеристика безпеки ключа в залежності від розміру ключа RSA/Diffie-Hellman і ECC:

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Рисунок 1: https://www.globalsign.com/en/blog/elliptic-curve-cryptography

Як можна побачити з наведеної таблиці використання еліптичних кривих дає вагому перевагу, оскільки зменшує розмір ключа, що в свою чергу зменшує час потрібний на проведення операцій з ключем (що дає виграш у швидкодії), кількість затраченої енергії (що є вагомою перевагою для IoT), навантаження на мережу під час передачі ключа і загалом трафік.

Ще однією перевагою криптографії еліптичних кривих є те, що можна використати багато напрацювань з криптографії з відкритим що використовує Z_p^*. Оскільки ECC як складно обчислювальну проблему використовує

знаходження дискретного логарифма - DLP(у випадку еліптичних кривих вживають термін ECDLP), аналогічно до складно обчислювальної проблеми в Diffie-Hellman і ElGamal. До того еліптичні криві мають додаткову структуру, яку не має Z_p^*, що дозволяє побудувати неможливі для Z_p^* криптосистеми. Такою додатковую структурою є можливість будувати pairing(спарювання точок еліптичних кривих), lattices(алгебраїчні решітки), isogenies(ізогенії). Алгебраїчні решітки і ізогенії еліптичних кривих зараз активно використовуються для побудови пост-квантових криптосистем з відкритим ключем.

1.2. Загальний огляд еліптичних кривих

1.2.1. $E / \mathbb{R}$

Існує декілька форм задання еліптичних кривих. Почнемо з найбільш класичної:

Еліптичною кривою E називається множина точок, що є розв'язком рівняння: $y^2 = x^3 + a * x + b$.

Наведене рівняння називають рівнянням Веєрштрасса і, відповідно, дану форму задання еліптичної кривої називають формою Веєрштраса. Якщо еліптична крива задана над полем $\mathbb{F}$, будемо позначати це як $E / \mathbb{F}$

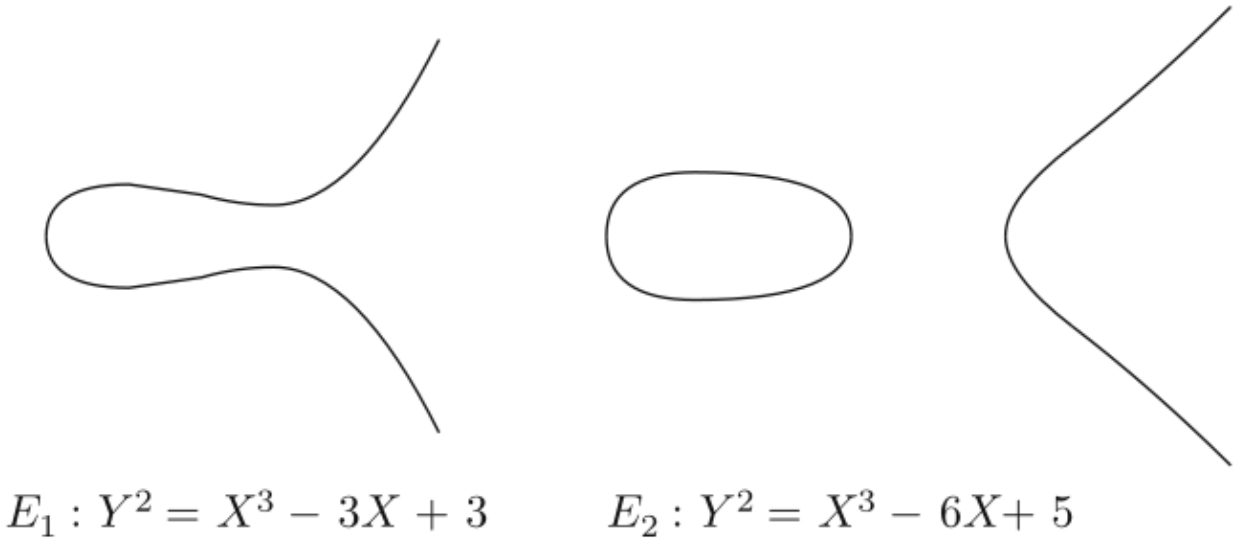

Рисунок 2: Ілюстрація 2 еліптичних кривих з [7]

Еліпітичні криві є не просто об'єктом вивчення аналітичної геометрії, а й ціким об'єктом алгебри, бо над точками еліптичної кривої можна проводити обчислення. Перед переходом до еліптичних кривих над скінченими полями, для більш інтуітивного розуміння, розглянемо як «додавати» точки еліптичної кривої над $\mathbb{R}$, бо це можна легко зобразити графічно. Позначемо операцію додавання точок еліптичної кривої як $\oplus$ і розглянемо її на прикладі з [7]. Для початку визначимо, що якщо $A = (x, y) \in E$, то $(-A) = (x, -y) \in E$. Нехай $E \,/\, \mathbb{R}$ - це еліптична крива задана рівнянням $y^2 = x^3 - 15x + 18$; Точки $P = (7, 16), Q = (1, 2)$ належать E, тоді пряма L що їх сполучає задається рівнянням: $y = \frac{7}{3}x - \frac{1}{3}$. Для того щоб знайти в яких точках L перетинає E ми можемо підставити замість y рівність з L в E і розв'язати рівняння відносно x. Для наведеного прикладу маємо:

$$\left(\tfrac{7}{3}x - \tfrac{1}{3}\right)^2 = x^3 - 15x + 18 \rightarrow x^3 - \tfrac{49}{9}x^2 - \tfrac{121}{9}x + \tfrac{161}{9} = 0$$

Отримане рівняння є рівнянням 3 степені, отже воно має 3 корені, 2 з яких нам вже відомі, залишається знайти 3 корінь. Найлегшим способом є поділити отриманий поліном на $(x - 7)(x - 1)$. Таким чином отримуємо 3

корінь $x = -\frac{23}{9}$. Підставляючи x в E отримуємо $y = -\frac{170}{27}$, а отже точку $R = \left(-\frac{23}{9}, -\frac{170}{27}\right)$. Далі відображаємо R відносно OX і маємо

$$P \oplus Q = -R = R' = \left(-\frac{23}{9}, \frac{170}{27}\right)$$

Назвемо це методом хорди. Наведене вище в графічному варіанті:

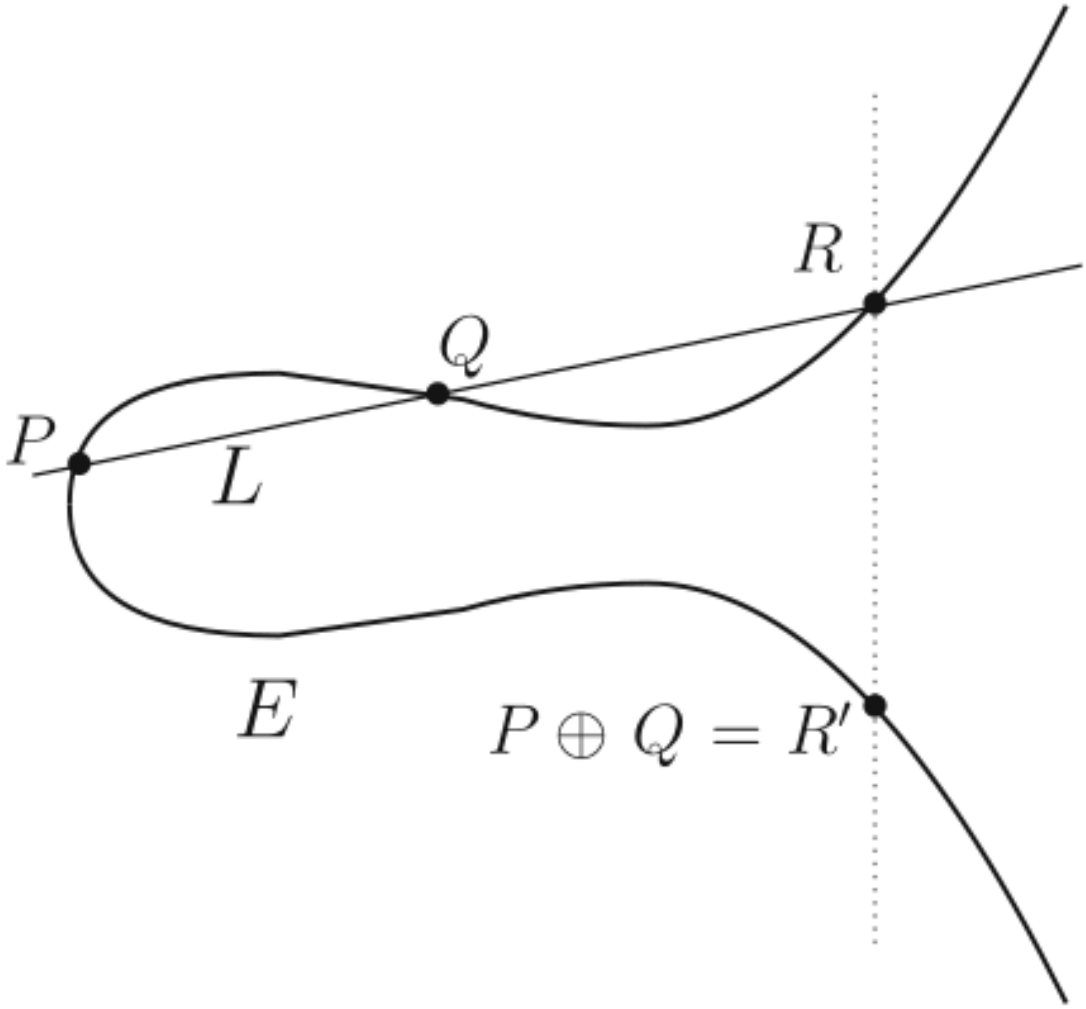

Рисунок 3: $P \oplus Q$ з [7]

Розглянемо випадок $P \oplus P = 2P = R'$. Для цього проведемо дотичну до E в точці P. Для цього потрібно діференціювати E по x. На прикладі, який розглядався раніше:

$$2y\frac{\mathrm{d}y}{\mathrm{d}x} = 3x^2 - 15 \to \frac{\mathrm{d}y}{\mathrm{d}x} = \frac{3x^2-15}{2y}$$

Підставляючи координати $P = (7, 16)$ отримуємо $L : y = \frac{33}{8}x - \frac{103}{8}$. Аналогічно попередньому прикладу знаходимо $R = \left(\frac{193}{64}, -\frac{223}{512}\right)$, а отже

$P \oplus P = R' = -R = \left(\frac{193}{64}, \frac{223}{512}\right)$

Назвемо це методом дотичної. Графічне зображення:

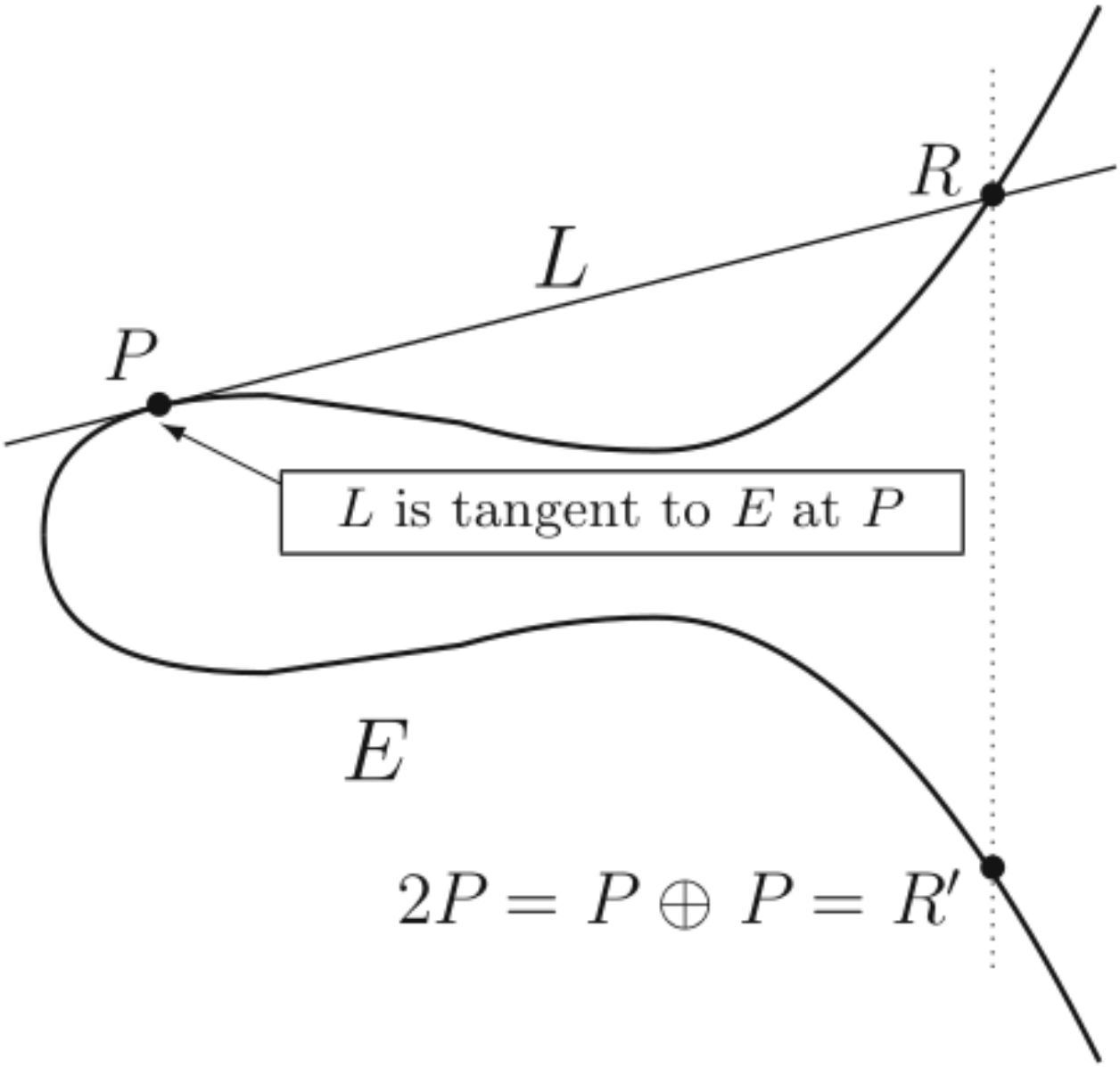

Рисунок 4: $P \oplus P$ з [7]

Залишиось розглянути останній випадок: $P \oplus (-P)$. Для цього введемо спеціальну точку, що називається точкою на нескінченості: $\mathcal{O}$, тоді $P \oplus (-P) = \mathcal{O}$. Графічно це виглядає наступним чином:

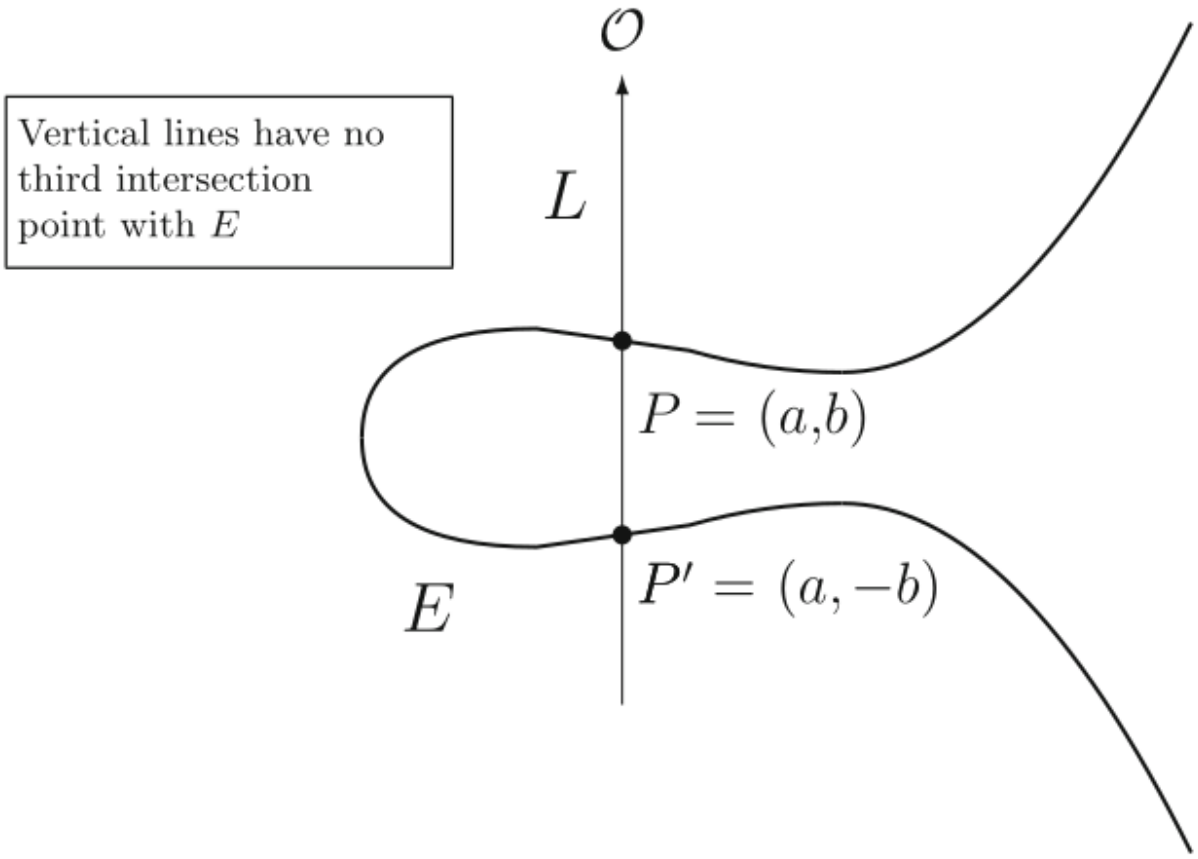

Рисунок 5: $P \oplus (-P) = \mathcal{O}$ з [7]

Формальний кінцевий алгоритм, що покриває всі, вищенаведені випадки, буде наведено у наступному підрозділі.

1.2.2. E / $\mathbb{F}_p$

Перейдемо до еліптичних кривих що застосовуються у криптографії - еліптичних кривих над скінченимими полями. Почнемо з визначення:

Нехай $p > 3$ - просте число. Тоді еліптичною кривою E визначеною над $\mathbb{F}_p$ є множина розв'язків рівняння $y^2 = x^3 + a * x + b$, де $a, b \in \mathbb{F}_p$ задовільняють умову $4a^3 + 27b^2 \neq 0$. Ця умова потрібна щоб впевнитись, що рівння $x^3 + ax + b = 0$ має тільки один корінь. У випадку, якщо попередня властивість не виконується, рівняння кривої буде мати 2, або 3 однакових кореня. Нехай у

такому випадку коренем рівняння кривої буде x_0, тоді точка $(x_0, 0)$ називається сингулярною і відповідна крива теж називається сингулярною.

Множиною точок еліптичною кривої $E \,/\, \mathbb{F}_p : y^2 = x^3 + ax + b; a, b \in \mathbb{F}_p$ є $E\big(F_p\big) = \big\{(x, y) : x, y \in \mathbb{F}_p \wedge y^2 = x^3 + ax + b\big\} \cup \{\mathcal{O}\}$.

Розглянемо приклад. Нехай $E : y^2 = x^3 + 1$ визначена на $\mathbb{F}_{11}$, тоді: $E(\mathbb{F}_{11}) = \{\mathcal{O}, (-1, 0), (0, \pm 1), (2, \pm 3), (5, \pm 4), (7, \pm 5), (9, \pm 2)\}$

Тепер розглянемо $\oplus$ для $E\big(\mathbb{F}_p\big)$. Для цього будемо спиратися на результати розгляду $(E(\mathbb{R}), \oplus)$, бо для $E\big(\mathbb{F}_p\big)$ алгоритм виглядає аналогічно до алгоритму для $E(\mathbb{R})$, але його не вдасться легко інтерпретувати геометрично. Розглядом геометричної інтерпретації обчислень над точками еліптичних кривих над скінченими полями займається алгебраїчна геометрія і це виходить за межі даної роботи. Нехай $P = \big(x_p, y_p\big) \vee \mathcal{O}, Q = \big(x_q, y_q\big) \vee \mathcal{O} \in E\big(\mathbb{F}_p\big)$:

- Якщо $P = \mathcal{O} \to P \oplus Q = Q$
- Інакше, якщо $Q = \mathcal{O} \to P \oplus Q = P$
- Інакше, якщо $Q = -P \to P \oplus Q = \mathcal{O}$ (варто зазначити що це покриває випадок коли $y_p = y_q = 0$)
- Інакше, якщо $P = Q$ використовуємо метод дотичної: $\lambda = \frac{3x_p + a}{2y_p}$
- Інакше $\lambda = \frac{y_q - y_p}{x_q - x_p}$
- $x = \lambda^2 - x_p - x_q; y = \lambda\big(x_p - x\big) - y_p \to P \oplus Q = (x, y)$

$\big(E\big(\mathbb{F}_p\big), \oplus\big)$ утворюють абелеву групу.

Якщо не буде вистачати об'єму розписати властивості.

Наведений вище алгоритм для еліптичних кривих загального вигляду має 2 основних недоліки:

1. Він не є достатньо швидким, як буде розглянуто далі існують спеціальні види еліптичних кривих, для яких його можна прискорити

2. Імплементація додавання точок еліптичної кривої має працювати за константний час, інакше можлива атака що викриває приватний ключ.
3. В цьому алгоритмі не вказано

1.2.3. Montgomery Curve

1.2.4. Edward Curve

1.2.5. Koblitz Curve

1.3. Характеристики еліптичних кривих

Hesse and SEA

1.3.1. ECDLP

1.3.2. CDH

1.3.3. DDH

1.4. Приклади еліптичних кривих у сучасній криптографії

1.4.1. secp256r1 (P256)

1.4.2. secp256k1 (Bitcoin curve)

1.4.3. Curve25519

??? 384 and 512

РОЗДІЛ 2. ЗАСТОСУВАННЯ У КРИПТОГРАФІЇ

2.1. Протоколи узгодження ключів

2.1.1. ECDH

2.2. Протоколи підпису і верифікації.

2.2.1. ECDSA

2.2.2. EdDSA

2.2.3. BLS

РОЗДІЛ 3. ІМПЛЕМЕНТАЦІЯ БІБЛІОТЕКИ

3.1. Core

SIMD

3.2. Algos

РОЗДІЛ 4. ПОРІВНЯННЯ З ІСНУЮЧИМИ БІБЛІОТЕКАМИ

Benchmarks

ВИСНОВКИ

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

[1] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang, “High-speed high-security signatures,” 2011. [Online]. Available: https://ed25519.cr.yp.to/ed25519-20110926.pdf

[2] W. Diffie, and M. E Hellman, “New directions in cryptography,” 1976. [Online]. Available: https://ee.stanford.edu/~hellman/publications/24.pdf

[3] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” 1985. [Online]. Available: https://people.csail.mit.edu/rivest/Rsapaper.pdf

[4] TAHER ELGAMAL, “Public key cryptosystem and a signature scheme based on discrete logarithms.” [Online]. Available: https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf

[5] Arjen K. Lenstra, and H. W. Lenstra, “The development of the number field sieve.”

[6] Dan Boneh, and Victor Shoup, *A Graduate Course in Applied Cryptography*, 2023. [Online]. Available: http://toc.cryptobook.us/book.pdf

[7] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An Introduction to Mathimatical Cryptography*, 2014.