МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра комп'ютерної алгебри та дискретної математики

(повна назва кафедри (предметної, циклової комісії)

Дипломна робота

на здобуття ступеня вищої освіти «бакалавр»

(освітньо-кваліфікаційний рівень)

на тему Криптосистема і цифровий підіс ЕльГамаля на еліптичнній кривій
ElGamal cryptosystem and digital signature on an elliptic curve

Виконав: студент заочної форми навчання
спеціальності 123 Комп'ютерна інженерія
(шифр і назва напрямку підготовки, спеціальності)
Кричун Олександр Сергійович
(прізвище, ім'я, по-батькові)
Керівник док. ф-м.наук проф. Варбанець П.Д.
(науковий ступінь, вчене звання, прізвище та ініціали, підпис
Рецензент канд. ф-м. наук доц. Варбанець С.П.
(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рекомендовано до захисту:
Протокол засідання кафедри
№ від «» 2021 р.

Завідувач кафедри

(підпис) Варбанець П.Д. (прізвище, ініціали)

Захищено на засіданні ЕК №
Протокол № від «» 2021 р.
Оцінка / /
(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

(підпис) Н.Ф.Казакова (прізвище, ініціали)

Одеса – 2021

АНОТАЦІЯ

У даній дипломній роботі розглядується криптосистема с відкритим ключем ЕльГамаль, цифровий підпис ЕльГамаль, щоб построїти їхні аналоги на еліптичний кривій

Об’єктом дослідження є комбінування досліджень еліптичних кривих, криптосистеми і цифрового підпису ЕльГамаль

Метою роботи є збудувати аналогу криптосистеми та аналогу цифровогого підпису ЕльГамаль на еліптичний кривій завдяки чому покращити крипостійкість звичайной криптосистеми і цифрового підпису ЕльГамаль

Ключові слова: криптосистема ЕльГамаль, цифровий підпис ЕльГамаль, еліптична крива, дискретний логарифм.

АННОТАЦИЯ

В данной дипломной работе рассматривается криптосистема с открытым ключом ЕльГамаль, цифровая подпись, чтобы построить их аналоги на эллиптических кривых.
Объектом нашего исследования является комбинирование исследований эллиптических кривых, криптосистемы и цифровой подписи ЭльГамаль на эллиптической кривой благодаря чему улучшить криптостойкость обычной криптосистемы и цифровой подписи ЭльГамаль
Ключевые слова: криптосистема ЭльГамаль, цифровая подпись ЭльГамаль, эллиптическая кривая, дискретный логарифм.

ABSTRACT

This thesis examines ElGamal public key cryptosystem, digital signature to build their analogues on elliptic curves.

The object of our study is the combination of elliptic curves research, ElGamal cryptosystem and digital signature on the elliptic curve by which to improve the crypto stability of conventional cryptosystem and ElGamal digital signature

Keywords: ElGamal cryptosystem, ElGamal digital signature, elliptic curve, discrete logarithm.

ЗМІСТ

ВСТУП

У третій чверті XX століття в криптографії з'явився новий тип передачі секретних повідомлень, який дозволяє досить просто створювати і обмінювати ключі шифрування і розшифрування між двома або більшою кількістю абонентів, що беруть участь в секретному спілкуванні. При цьому не потрібно безпосереднє спілкування самих абонентів. Такі криптосистеми називаються криптосистемами з відкритим ключем. Незабаром, Н.Кобліц і В.Міллер вдосконалили новий підхід в передачі повідомлень за відкритими каналами зв'язку, використовуючи так звані еліптичні криві над кінцевим полем. Вивченню криптосистем на еліптичний кривих присвячена наша дипломна робота. Оскільки неможливо пояснити все, розроблене в цій області, ми приділяємо увагу тільки криптосистемі ElGamal на еліптичних кривих, яка відіграє важливу роль в криптографії.

1 КРИПТОСИСТЕМА ELGAMAL

Спочатку пригадаємо суть криптосистеми ElGamal над кільцем класів залишків за модулем числа p.

Нехай є абоненти A, B, C ,. . . , Які хочуть передавати один одному зашифровані повідомлення, але не мають ніяких захищених каналів зв'язку. Ми розглянемо шифр, запропонований Ель-Гамалем (Taher ElGamal), який вирішує цю задачу, на відміну від інших, тільки однією пересилкою повідомлення. Фактично тут використовується схема Діффі-Хеллмана, щоб сформувати загальний секретний ключ для двох абонентів, які передають одне одному повідомлення, і потім повідомлення шифрується шляхом множення його на цей ключ. Для кожного наступного повідомлення секретний ключ обчислюється заново. Перейдемо до точного опису методу. Для всієї групи абонентів вибираються деяке велике просте число p і число g, такі, що різні ступені g різні числа по модулю p. Числа p і g передаються абонентам у відкритому вигляді (вони можуть вживатися всіма абонентами мережі)

Потім кожен абонент групи вибирає свою секретну число x, $1 < x < p-1$, і обчислює відповідне йому відкрите число h, $h = g^x \bmod p$. В результаті отримуємо таблицю 1.1

Таблиця 1.1 – Секретні та відкриті ключі абонентів

Абонент:	**Секретний ключ:**	**Відкритий ключ:**
A	X_a	h_a
B	X_b	h_b
C	X_c	h_c

Покажемо тепер, як A передає повідомлення m абоненту B. Будемо припускати, що повідомлення представлено у вигляді числа $m < p$.

1) Крок 1.

А формує випадкове число k, $1 \le k \le p-2$, обчислює числа:

$$r = g^k \bmod p$$

$$e = m \cdot h_b^k \bmod p$$

і передає пару чисел (r, e) абоненту B.

Крок 2.

B, отримавши (r, e), обчислює:

$$m' = e \cdot r^{p-1x_b} \bmod p$$

Властивості шифру ElGamal:

1) абонент B отримав повідомлення, тобто $m_0 = m$;
2) опонент, знаючи p, g, h_b, r і e, не може обчислити m.

Доведення. Підставимо в $m' = e \cdot r^{p-1x_b} \bmod p$ значення e з $e = m \cdot h_b^k$:

$$m' = m \cdot h_b^k \cdot r^{p-1x_b} \bmod p.$$

Тепер замість r підставимо $r = g^k \bmod p$, а замість h_b - $h = g^x \bmod p$:

$$m' = m \cdot (gx_b)^k \cdot (g^k)^{p-1x_b} \bmod p =$$
$$= m \cdot g^{x_b k + k(p-1) - kcx_b} \bmod p = m \cdot g^{k\,(p-1)} \bmod p.$$

По теоремі Ферма:

$$g^k(p-1)) \bmod p = 1^k \bmod p = 1,$$

і, таким чином, ми отримуємо першу частину твердження. Для доказу другої частини зауважимо, що противник не може обчислити k в рівності $r = g^k \bmod p$, так як це завдання дискретного логарифмування. Отже, він не може обчислити m в рівність $e = m \cdot h_b^k \bmod p$, так як m було помножено на

невідоме йому число. Противник також не може відтворити дії законного одержувача повідомлення (абонента B), так як йому не відомо секретне число x_b (обчислення x_b на підставі $h = g^x \bmod p$ - також завдання дискретного логарифмування).

Приклад.

Передамо повідомлення m = 15 від A до B. Виберемо параметри. Нехай

p = 23 = 2 · 11 + 1 (q = 11). Візьмемо p = 23, g = 5 Нехай абонент B вибрав для себе секретне число $x_b = 13$ і обчислив по $h = g^x \bmod p$.

$$h_b = 5^{13} \bmod 23 = 21.$$

Абонент A вибирає випадково число k, наприклад k = 7, і обчислює по $r = g^k \bmod p$ і $e = m \cdot h_b^k \bmod p$:

$$r = 5^7 \bmod 23 = 17,\ e = 15 \cdot 21^7 \bmod 23 = 15 \cdot 10 \bmod 23 = 12.$$

Тепер A посилає до B зашифроване повідомлення у вигляді пари чисел (17, 12). B обчислює по:

$$m' = e \cdot r^{p-1x_b} \bmod p$$

$$m' = 12 \cdot 17^{23\text{-}1\text{-}13} \bmod 23 = 12 \cdot 17^9 \bmod 23 = 12 \cdot 7 \bmod 23 = 15$$

Ми бачимо, що B зміг розшифрувати передане повідомлення. Зрозуміло, що за аналогічною схемою можуть передавати повідомлення всі абоненти в мережі. Зауважимо, що будь-який абонент, що знає відкритий ключ абонента B, може посилати йому повідомлення, зашифровані за допомогою відкритого ключа h_b. Але тільки абонент B, і ніхто інший, може розшифрувати ці повідомлення, Використовуючи відомий тільки йому секретний ключ x_b. Відзначимо також, що обсяг шифру в два рази перевершує обсяг повідомлення, але потрібна тільки одна передача даних (за умови, що таблиця з відкритими ключами заздалегідь відома всім абонентам).

2 ЕЛІПТИЧНІ КРИВІ

2.1 Теорія еліптичних кривих

Тепер наведемо деякі факти з теорії еліптичних кривих Еліптичні криві давно вивчалися в математиці, але їх використання з криптографічною метою було вперше запропоновано Коблицем (Neal Koblitz) і Міллером (Victor Miller) в 1985 році. П'ятнадцять років інтенсивних досліджень цих систем підтвердили їх корисні властивості і привели до відкриття багатьох ефективних методів їх реалізації. З 1998 року використання еліптичних кривих для вирішення криптографічних завдань, таких як цифровий підпис, було закріплено в стандартах США ANSI X9.62 і FIPS 186-2.

Основна перевага криптосистем на еліптичний кривих полягає в тому, що у порівнянні зі «звичайними» криптосистемам вони забезпечують суттєво більш високу стійкість при рівній трудомісткості, або, навпаки, істотно меншу трудомісткість при рівній стійкості. Це пояснюється тим, що для обчислення обернених функцій на еліптичний кривих відомі тільки алгоритми з ростом трудомісткості, тоді як для звичайних систем запропоновані субекспоненціальні методи. В результаті той рівень стійкості, який досягається, скажімо, в RSA при використанні 1024-бітних модулів, в системах на еліптичних кривих реалізується при розмірі модуля 160 біт, що забезпечує більш просту як програмну, так і апаратну реалізацію. Детальне вивчення еліптичних кривих вимагає знань вищої алгебри, особливо алгебраїчної геометрії. Ми, однак, постараємося викласти матеріал без залучення складних алгебраїчних конструкцій і в обсязі, достатньому для розуміння принципів побудови і роботи відповідних криптосистем.

Математичні основи:

Крива третього порядку E, що задається рівнянням виду E: $Y^2 = X^3 + Ax + b$ називається еліптичною кривою.

Оскільки Y = $\pm\sqrt{x^3 + Ax}$ +b, графік кривої симетричний відносно осі абсцис. Щоб знайти точки його перетину з віссю абсцис, необхідно вирішити кубічне рівняння:

$$X^3 + Ax + b = 0$$

Це можна зробити за допомогою відомих формул Кардано. Дискримінант цього рівняння

$$D=(\frac{a}{3})^3 + (\frac{b}{2})^2$$

Якщо D <0, то $X^3 + Ax + b = 0$ має три різних дійсних корені α, β, γ; якщо D = 0, то $X^3 + Ax + b = 0$ має три дійсних кореня, скажімо, α, β, β, принаймні два з яких рівні; нарешті, якщо D> 0, рівняння $X^3 + Ax + b = 0$ має один дійсний корінь α і два комплексно сполучених. Вид кривої у всіх трьох випадках представлений на рисунках нижче. Крива, представлена на рисунках. $X^3 + Ax + b = 0$, називається сингулярною. В її точці сингулярності (β, 0) є дві дотичні. Сингулярні криві ми будемо виключати з нашого розгляду. Тому при завданні кривої за допомогою параметрів a і b Потрібні виконання умови D ≠ 0, що еквівалентно умови:

$$4a^3 + 27b^2 \neq 0$$

Отже, нехай еліптична крива E задана рівнянням E: $Y^2 = X^3 + Ax + b$ з обмеженням на коефіцієнти $4a^3 + 27b^2 \neq 0$. Визначимо операцію композиції точок на кривій. Візьмемо будь-які дві точки $P = (x_1, y_1)$,

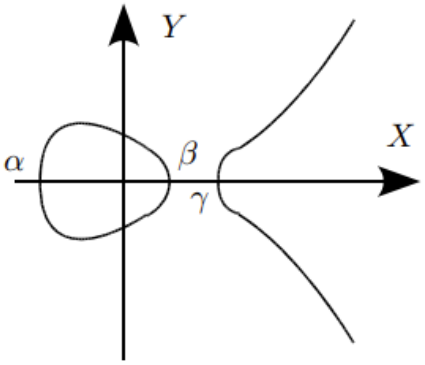

Рис.1 Еліптична крива D <0

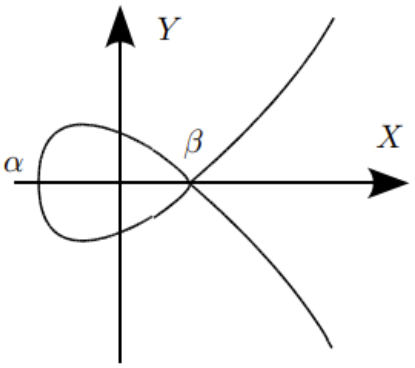

Рис.2 Еліптична крива D = 0

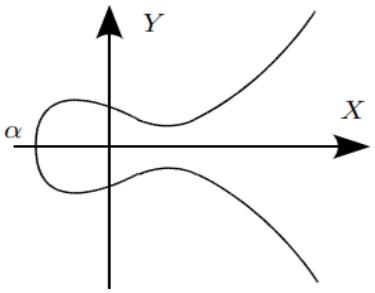

Рис. 3. Еліптична крива D> 0

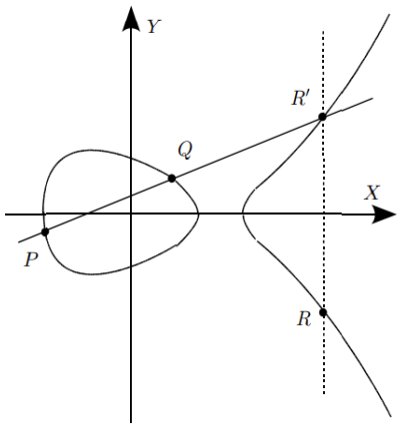

Рис. 4. Композиція точок R = P + Q

Q = (x_2,y_2) ∈ E і проведемо через них пряму (рис.4). Ця пряма обов'язково перетне криву в третій точці, яку позначимо через R_0. (Третя точка обов'язково існує. Справа в тому, що кубічне рівняння, отримане після підстановки рівняння прямої в E: $Y^2 = X^3 + Ax + b$, має два дійсних кореня, відповідних точкам P і Q, отже, його третій корінь, відповідний R_0, також дійсний.) Точку R = (x_3,y_3) отримаємо шляхом зміни знака ординати точки R_0. Будемо позначати описану операцію композиції точок наступним чином: R = P + Q. Нехай точка P ∈ E має координати (x, y). Тоді точку з координатами (x, -y) будемо позначати -P. Будемо вважати, що вертикальна пряма, що проходить через P і -P, перетинає криву в нескінченно віддаленій точці O, тобто P + (-P) = O. За угодою P + O = O + P = P. Як ми побачимо надалі, точка O буде грати роль нуля в операціях на еліптичній кривій. Тепер уявімо, що точки P і Q (рис.4) зближуються одна з одною і, нарешті, зливаються в одну точку P = Q = (x_1,y_1).Тоді композиція R = (x_3,y_3)= P + Q = P + P буде отримана шляхом проведення дотичної в точці P і відображення її другого перетину з кривою R_0 відносно осі абсцис (рис.5). Будемо використовувати наступне позначення: R = P + P = [2] P.

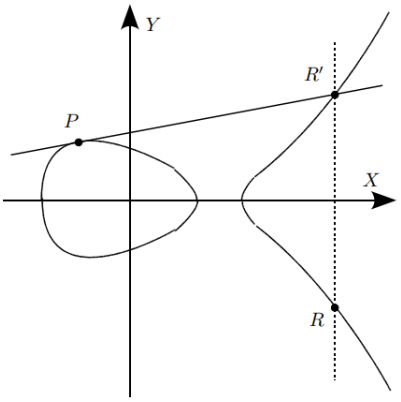

Рис.5 Подвоєння R = P + P = [2] P

Виведемо формули для визначення координат результуючих точки R = (x_3,y_3) на основі координат вихідних точок P = (x_1,y1)і Q = (x_2, y_2).Розглянемо спочатку випадок, коли P ≠ ± Q, R = P + Q (рис.4). Позначимо через k кутовий коефіцієнт прямої, що проходить через P і Q. Очевидно, що

$$k=\frac{y_2-y_1}{x_2-x_1}$$

Тоді рівняння прямої буде мати вигляд Y -y_1 = k (X -x_1), звідки:

$$Y = y_1 + k\,(X - x_1).$$

Підставимо знайдений вираз для змінної Y в рівняння кривої E: $Y^2 = X^3 + Ax + b$.

Отримаємо:

$$(y_1 + k\,(X - x1))^2 = X^3 + aX + b$$

зводячи в квадрат і гуртуючи подібні члени, отримаємо кубічне рівняння:

$$X^3 - k\,2X^2 + \ldots = 0$$

Відомо, що сума коренів кубічного рівняння дорівнює коефіцієнту при X^2, взятому з протилежним знаком (теорема Вієта для кубічних рівнянь), тобто:

$$x_1 + x_2 + x_3 = k^2,$$

звідки:

$$x_3 = k^2 - x_1 - x_2$$

Підставивши знайдене значення x_3 в рівняння прямої $Y = y_1 + k (X - x_1)$, знайдемо ординату точки R', $y_{'3} = y_1 + k (x_3 - x_1)$, і , Змінивши знак, отримаємо:

$$y_3 = k (x_1 - x_3)- y1.$$

Отже, ми знайшли координати R точки яка нас цікавить.

Тепер розглянемо випадок, коли P = Q і результуюча точка R = [2] P (рис.5.). Диференціюючи обидві частини E: $Y^2 = X^3 + Ax + b$ по X, отримаємо:

$$2YY' = 3X^2 + a$$

Кутовий коефіцієнт дотичної дорівнює значенню похідної в точці P

$$k = \frac{3x_1^2 + a}{2y_1}$$

Подальші міркування аналогічні першому випадку, і координати точки R визначаються за тими ж формулами $x_3 = k^2 - x_1 - x_2$ і $y_3 = k (x_1 - x_3)$-

y_1. Зауважимо, що якщо ордината точки P дорівнює нулю , то дотична проходить паралельно осі ординат і [2] P = O.

Використовуючи отримані формули для обчислення композиції і прийняті угоди відносно точки в нескінченності, можна довести такі властивості точок на еліптичній кривій:

1) P + Q = Q + P для всіх точок P, Q ∈ E
2) P + (Q + S) = (P + Q) + S для всіх точок P, Q, S ∈ E
3) існує нульовий елемент O (точка в нескінченності), такий, що P + O = O + P = P для всіх P ∈ E
4) для кожної точки P ∈ E існує точка -P ∈ E, така, що P + (-P) = O

Перераховані властивості точок збігаються з властивостями цілих чисел при використанні операції додавання. Тому композицію точок часто називають додавання точок, а операцію [2] P - подвоєння точки. Продовжуючи аналогію з додавання чисел, зручно ввести такі позначення. Для цілого m

[m] P = P + P + ...P [0] P = 0

[-m] P = - (P + P + ... + P).

Тепер ми готові до того, щоб зробити останній крок, необхідний для криптографічного використання еліптичних кривих. Ми бачимо, що при обчисленнях композиції точок на кривій використовуються тільки операції додавання, віднімання, множення і ділення чисел. Це означає, що всі Наведені вище тотожності збережуться, якщо ми будемо виконувати обчислення з цілими числами по модулю простого числа p. В цьому випадку додавання і множення чисел виконуються по модулю p, різниця u - v обчислюється як u + (p - v) mod p, а розподіл u / v виконується шляхом множення u на v^{-1} mod p (простота модуля гарантує, що для будь-якого додатного числа v <p існує число $v^{-1,}$ таке, що vv^{-1} mod p = 1).

$$E: Y^2 = X^3 + aX + b \pmod p.$$

У рівнянні E: $Y^2 = X^3 + aX + b \pmod p$ змінні X, Y і коефіцієнти a, b приймають цілочисельні значення, а всі обчислення виконуються по модулю p. Відповідно до $4a^3 + 27b^2 \neq 0$ в a, b накладається обмеження

$$(4a^3 + 27b^2) \bmod p \neq 0.$$

Безліч $E_p(a, b)$ складається з усіх точок (x, y), $0 \leq x, y < p$, задовольняють рівняння E: $Y^2 = X^3 + aX + b \pmod p$, і точки в нескінченності O. Кількість точок в $E_p(a, b)$ будемо позначати $\#E_p(a, b)$. Ця величина має важливе значення для криптографічних додатків еліптичних кривих.

Приклад.

Розглянемо криву

$$E_7(2, 6): Y^2 = X^3 + 2X + 6 \pmod 7.$$

Перевіримо умову $(4a^3 + 27b^{2)} \bmod p \neq 0$.

$$4 * 2^3 + 27 \cdot 6^2 = 4 \cdot 1 + 6 \cdot 1 = 3 \neq 0 \pmod 7$$

Отже, подана крива несингулярна. Знайдемо якусь (випадкову) точку в $E_7(2,6)$. Нехай x = 5 Тоді:

$$Y^2 = 5^3 + 2 * 5 + 6 = 6 + 3 + 6 = 1 \pmod 7$$

і $y = 1 \pmod 7$ або $y = -1 = 6 \pmod 7$. Ми знайшли відразу дві точки: (5, 1) і (5,6). Знайдемо ще пару точок шляхом обчислення композиції. Спочатку знайдемо [2](5, 1). Використовуючи $k = \frac{3x_1^2 + a}{2y_1}$, $x_3 = k^2 - x_1 - x_2$ і $y3 = k (x_1 - x_3) - y_1$, Обчислюємо:

$$k = \frac{3 * 5^2 2}{2 * 1} = \frac{5}{6} = 5 * 6 = 2 \pmod 7$$

$$x_3=2^2\text{-}5\text{-}4=2 \pmod 7$$

$$y_3= 2 * (5\text{-}2)\ 1 = 2 * 3\text{-}1 = 5 \pmod 7$$

Ми отримали [3] (5, 1) = (2, 5). Отже, ми знайшли чотири точки.

Скажімо кілька слів про властивості безлічі точок $E_p(a, b)$. Цілком очевидно, що ця безліч кінченна, так як в неї входять тільки точки з цілочисельними координатами $0 \le x, y < p$. Існує пряма аналогія між $E_p(a, b)$ і безліччю ступенів цілих чисел, що обчислюються за модулем p. Так, $E_p(a, b)$ має генератор, тобто таку точку G, що ряд G, [2] G [3] G ,. . . [N] G, де $n = \#E_p(a, b)$, містить всі точки безлічі $E_p(a, b)$, причому [n] G = O. Число точок на кривій, при належному виборі параметрів p, a і b, може бути простим числом, $\#E_p(a, b) = q$. У цьому випадку будь-яка точка (крім O) є генератором всієї безлічі точок. Така крива краща у багатьох відношеннях і завжди може бути знайдена за достатньо приємлемий час. Якщо з якихось причин таку криву знайти не вдалося і $\#E_p(a, b) = h_q$, де q - знову просте число, то в $E_p(a, b)$ існує підмножина з q точок (тобто потужності q), генератором якого може служить будь-яка точка $G \ne O$, така, що [q] G = O. В подальшому, без втрати спільності, ми будемо вважати, що працюємо з таким підмножинами потужності q (а при виборі кривої будемо прагнути отримати $q = \#E_p(a, b)$). Основна криптографічна операція на еліптичній кривій – m - кратна композиція, тобто обчислення

$$Q [m] P = P + P + ... + P$$

Ця операція виконується дуже ефективно і вимагає не більш ніж 2log m композицій точок. Підхід до її реалізації абсолютно той самий, що і до піднесення до степеню. Наприклад, щоб Отримати точку Q = [21] P, Обчислюємо [2] P [4] P [8] P [16] P, кожен раз подвоюючи попередню точку, і складаємо P + [4] P + [16] P = Q (всього 4 подвоєння і 2 складання). Зворотне завдання, яке за традицією називається дискретним

логарифмування на еліптичній кривій, формується таким чином. Знаючи точки P і Q, знайти таке число m, що [m] P = Q. Ця задача виявляється дуже важкою. Якщо ретельно вибрати параметри кривої (як описується в наступному розділі), то найкращі відомі в даний час алгоритми для знаходження m вимагають O $(\sqrt{q})$операцій на кривій, де q - потужність підмножини точок, якій належать точки P і Q. Всі обчислення на кривій проводяться по модулю p, тобто з числами довжини t ≈ log p біт. Для криптографічних додатків log q ≈ log p, тому O $(\sqrt{q})$= O $(2^{t/2})$ означає експоненціальні зростання трудомісткості при збільшенні довжини чисел.

Шифр ElGamal на еліптичній кривій

Для користувачів деякої мережі вибираються загальна еліптична крива $E_p(a, b)$ і точка G на ній, такі, що G, [2] G [3] G ,. . . [Q] G різні точки і [q] G = O для деякого простого числа q.

Кожен користувач U вибирає число cU, 0 <cU <q, яке зберігає як свій секретний ключ, і обчислює точку на кривій DU = $[c_U]$ G, яка буде його відкритим ключем. Параметри кривої і список відкритих ключів передаються всім користувачам мережі. Припустимо, користувач A хоче передати повідомлення користувачу B. Будемо вважати, що повідомлення представлено у вигляді числа m <p. A робить наступне:

1) обирає випадкове число k, 0 <k <q
2) обчислює R = [k] G, P = [k] D_B = (x, y)
3) шифрує e = mx mod p
4) посилає B шифротекст (R, e)

Користувач B, після отримання (R, e)

1) обчислює Q = [cB] R = (x, y)
2) дешифрує m` = ex^{-1} mod p

Дамо обґрунтування протоколу. Для цього достатньо показати, що

$$cB] R = [c_B]([k] G) = [k] ([c_B]G) = [k] D_B$$

тобто, Q = P. Тому m` = m. Координата x точки Q залишається секретною для опонента, так як він не знає числа k. Опонент може спробувати обчислити k з точки R, але для цього йому потрібно вирішити проблему дискретного логарифмування на кривій, що вважається неможливим.

Найбільш вірогідним варіантом використання представленого протоко лу буде передача в якості числа m секретного ключа для блокового або поток ового шифру. В цьому випадку розумно вибирати параметри кривої так, щоб log q приблизно удвічі перевищував довжину ключа шифру.

Ми виклали загальну схему роботи криптосистеми на еліптичних крив их над полем F_p. У цій криптосистемі важливе місце грає група точок Ep на е ліптичній кривій (разом з точкою O), і зокрема, її порядок N_p (тобто число ел ементів < E_p).

Приведемо деякі факти про структуру групи точок на еліптичній кривій.

2.2 Структура групи точок еліптичної кривої

Нехай E_p

Нехай еліптична крива, визначена над полем Ep рівнянням $y_2=x_3+ax+b$ Відносно операції (+) безліч точок цією кривою разом з точкою O утворює групу. Щоб помітити структуру цієї групи розглянемо декілька прикладів.

Приклад.

$$E_p: y^2 \equiv x^3+x \pmod{17}$$

Ось її точки:

x:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
y:	0	±6	-	±9	0	-	±1	-	-	-	-	±4	-	0	±2	-	±7

також O.

Порядок E_p дорівнює 16

Візьмемо дві точки на E_p: P= (11,4), Q=(6,1) і обчислимо дві точки S=P(+)Q и T=P(+)P=[2]P.

Так як $x_1 \neq \pm x_2$, то знаходимо число λ по формулі $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ (дріб розглядається як элемент поля F_{17}). Маємо $\lambda = \frac{1+4}{6-11} = 5*(-5)^{-1} = -1 \equiv 16$. .

Зараз маємо: . .

$$x_3 = \lambda^2 - x_1 - x_2 = 1,\ y_s(x_1 - x_2) - y_1 = -(11-1) - (-4) = -6, .$$

тобто .

$$S=(1,-6) .$$

Координати точки [2]P обчисленням по формулам .

$$x_t = \lambda^2 - 2x_1,\ y_t = \lambda (x_1 - x_3) - y_1, \text{ де } \lambda = \frac{3x_{1+}^2 + a}{2y_1}.$$

Має $\lambda = \frac{3+11^2+1}{2*(-4)} = +14$. Тобто, x_t= -13, y_t= 0, T= (4,0) Зазначимо, що обидві точки S и T знаходяться на еліптичній кривій .

Приклад. .

$$y^2 \equiv x^3 + x \pmod{17}. .$$

Знайти точки цієї кривої и обчислити порядок точки P(1,6)

Будуємо точки кривої $y^2 \equiv x^3 + x \pmod{17}$

x: 0 1 -1 2 -2 3 -3 4 -4 5 -5 6 -6 7 -7 8 -8

y: 0 ±6 ±7 - - - - - - - - - … -

x=0, f(x)=0, => y=0

x=1, f(1)=2, => $(\frac{2}{17})$=1 => y= ± 6

x= -1, f(-1)= -2 => $(-\frac{2}{17})$= 1 => 1 => y = ± 7

x= 2, f(2) = 10 => $(\frac{10}{17}) = (\frac{-7}{17}) = (\frac{7}{17}) = (\frac{7}{17}) = -1^{\frac{7-1}{2}*\frac{17-1}{2}}(\frac{17}{7}) = (\frac{3}{7}) = (\frac{-4}{7})$ = -1

x= -2, f(-2)= -10 => $(\frac{-10}{17}) = (\frac{10}{17})$ = -1

Знайдемо порядок точки (1,6)

Для цього будемо обчислювати точки [2]P, [3]P, … доки не з’явиться точка Q з координатами (1,-6). Ця точка співпадає з точкою –P, а потім P(+)(-P)=0. Тобто, якщо –P=[k]P, то порядок точок P дорівнює k+1.

Еліптична крива E_p, розглядається як абелева група відносно операції (+) (яка була описана вище), більш інтересна ніж мультиплікативна група класів відємностей по mod p, а тому знайшла своє застосування в криптографії. Окрім цього, група E_p не обов’язково є циклічною. Знову розглянемо приклад

Описати точки кривої $y^2 \equiv x^3 + 2x + 1 \pmod 5$ Маємо

x: 0 1 2 3 4

y: ±2 - ±1 - ±1

Разом з точкою O група E_p має порядок, а тому – циклічна. Кожен елемент групи звичайного порядку є утворювачем цієї групи точек, в зокрема, точка P(2,-1) породжує всю цю групу, тобто

$$E_p = \{0,P,[2]P,[3]P,[4]P,[5],[6]P\} \text{ (уже } [f]P=0)$$

А група кривої $y^2 \equiv x^3+ax+b$ в F_p має рішення тоді і тількі тоді

$$|F_p| = m_1+2m_2+1$$

Доповідь. Кожне x є F_p визначає не більш ніж два значення y, таких, що точка (x,y) належить кривій. Кожен корінь многочлена x^3+ax+b визначается тільки одним значенням y. Тому група точок кривої E_p має порядок

$$m_1+2m_2+1$$

Приблизно 75% кривих над полем F_p є циклічними. Це дозволяе нам будувати аналог криптосистеми ElGamal на еліптичних кривих, групи точок котрих циклічні.

Доведенно, що або група точок E_p є цикліною, або в ній присутні дві циклічні подгрупи порядків n_1 и n_2, причому n_2 ділить n_1 и ділить (p-1), так, що будь-який елемент з E_p є сумою (и при цому однозначна) вида R=[k]P + [l]Q, де P и Q породжоючі елементи вказаних циклічних груп. Якщо ж n_2X(p-

1), то

$$E_p = Z_n(+)Z_n$$

Нехай F_q – поле з q елементів. Для qp шукаємо $F_p=Z_p$ (класу від'ємностей по mod p)

Теорема 1

Нехай E - еліптична крива над кінцевим полем F_q. Тоді

$$E(Pq) \approx Z_n \text{ або } Z_{n1}(+) Z_{n2}$$

для деякого цілого числа $n \geq 1$, або для деяких цілих чисел n_1, $n_2 \geq 1$, причому n_1 ділиться на n_2.

Теорема 2

Нехай $q = p^n$ - степінь первісної p і нехай N= q + 1-a. Існує еліптична крива E, визначенна над P_q так, що $\#E(P_q) = N$ тоді і тільки тоді, коли $|a| \leq 2\sqrt{q}$ та a задоволняє одну з наступних умов:

1. gcd(a,p)=1
2. n парне $a=+-\sqrt{q}$
3. n парне, p ≡ 1 (mod 3), та $a= +-\sqrt{q}$
4. n непарне, p=2 или 3 та, $a=+-p^{(n+1)/2}$
5. n парне, p ≡ 1 (mod 4), та a= 0
6. n непарне та a = 0.

Нехай E - крива $y^2 = x^3 + x + 1$ над P_5. Щоб порахувати точки на E, ми створюємо список можливих значень x, потім $x^3 + x + 1$ (mod 5), потім квадратних коренів y з $x^3 + x + 1$ (mod 5).є

У результаті отримуємо точки на E_p

x=0 $y^2 \equiv 1$(mod5) $y_1=1$, $y_2= -1 \rightarrow (0,1); (0,-1)$

x=1 $y^2 \equiv 3$ (mod5) – немає рішень→ немає точок (1,x)

$x=-1 \equiv 4$ $y^2 \equiv -1$ (mod5) → y= ±2 → (-1,2), (-1,-2)

x=2 $y^2 \equiv 11 = 1$(mod5) → y= ±1→ (2,1), (2,-1)

$x=-2 \equiv 3$ $y^2 \equiv -9 \equiv 1 \rightarrow (3,1), (3,-1)$

Висновок $N_P = |E_P| = 8+1 = 9$

Обчислимо (3, 1) + (2, 4) на E. Нахил прямої через дві точки

$$\frac{4-1}{2-3} \equiv 2 \pmod 5$$

Таким чином лінія y = 2(x-3)+1 ≡ 2x. З'єднаємо ці точки підставив це в

$$y^2 = x^3+x+1$$

підстановка дає

$$0=x^3-4x^2+x+1$$

Сума коренів дорівнює 4, а корені 3 і 2 нам відомі. Тому залишившийся корінь -x = 4. Так як y = 2x, то y ≡ 3. Відображено через відображення по осі x дає суму:

$$(3,1)+(2,4) = (4,2).$$

Невеликі обчислення показують, що $E(P_5)$ циклічна, породжена (0, 1)

Нехай E_7 - еліптична крива $y^2 = x^3 + 2$ над з F_7. Тоді

$$E(P_7) = \{\infty, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\},$$

Легке обчислення показує, що всі ці точки P задоволняють 3P = ∞, тому група ізоморфна Z_3 (+) Z_3

Теорема 3

Пусть E - еліптична крива, визначуванна $y^2 = x^3 + Ax + B$ над Zq. Тоді

$$\#E(Fq) = p +1+ \sum_{X \in Z_p} \left(\frac{x^3+Ax+B}{p}\right)$$

Доведення.

Для даного x_0 існують дві точки (x, y) з x-координатою x_0 якщо $x_0^3+ Ax_0 + B$ - ненульовий квадрат в F_p, одна така точка, якщо $x_0^3+ Ax_0 + B$ дорівнює нулю, і ні однієї точки, якщо $x_0^3+ Ax_0 + B$ не квадрат. Отже, число точок з координатою x_0 дорівнює $1+ (\frac{x_0^3+Ax_0+B}{p})$. Додавання по всім $x_0 \in F_p$ и включення 1 для точки ∞, дає

$$|N_P|= 1+\sum_{x\epsilon p_q} \quad (1 + (\frac{x^3+Ax+B}{P_q}))$$

Приклад

Нехай E - крива $y^2 = x^3 + x + 1$ над Z_5, як у прикладі вище. Ненульові квадрати mod 5 є 1 и 4. Тому

$$\#E(P_5)= 5+1+\sum_{x=0}^{4} \quad (\frac{x^3+x+1}{5}) = 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + (\frac{4}{5}) =$$

$$=6+1-1+1+1+1=9$$

Можна вичислити кожен окремий узагальнений символ Лежандра (але ефективніше звести в квадрат усі елементи P_q і зберігати список квадратів. Німецький математик Х.Хассе довів наступну теорему Теорема (Хассе) Неха й E_p - еліптична крива над полем Z_p. Тоді її порядок Np задовольняє нерівності

$$|N_p – p -1|\leq 2\sqrt{p}$$

(Зазвичай через t визначали ухилення N_p від значення p+1, тобто

$$t= |Np-1|.$$

Наступний приклад показує як можливо застосувати теорему Хассе для визначення кривої E_p

Приклад

Нехай E_P – крива $y^2 = x^3 + 7x+ 1$ над Z_{101}. Можна показати, що точка (0, 1) має порядок 116, тому $N_{101} = \#E_{101}$ кратно 116. Теорема Хассе говорить, що

$$101 + 1 - 2\sqrt{101} \leq N_{101} \leq 101 + 1 + 2\sqrt{101},$$

що означає, що $82 \leq N_{101} \leq 122$. Единим кратним 116 в цьому діапазоні є 116, тому $N_{101} = 116$. Унаслідок, знаходимо, що група точок являється циклічною порядка 116, породжена (0,1)

Приклад (Наслідок Хасса)

Нехай E_p - еліптична крива $y^2 = x^3 -10x+ 21$ на Z_{557}. можливо показати, що точка (2,3) має порядок 189. З теореми Хасса випливає, що $511 \leq N_{557} \leq 605$.

Єдине кратне 189 в цьому діапазоні дорівнює 3 * 189 = 567. Тому $N_{557} = 567$.

Приклад

Нехай E - еліптична крива $y^2 = x^3 + 7x + 12$ на P_{103}. Точка (-1, 2) має порядок 13, а точка (19, 0) має порядок 2. Тому порядок N_{103} в $E(P_{103})$ кратний 26. З теореми Хассе випливає, що $84 \leq N_{103} \leq 124$.
Єдине кратне 26 в цьому діапазоні дорівнює 104, тому $N_{103} = 104$.

Припущення

Нехай E - еліптична крива над Z_q. Нехай $E(P_q)$ $Zn_1 \oplus Zn_2$ при n1|n2. Допустимо, що q не є одним з наступних:
3, 4, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 43, 61, 73, 181, 331, 547.
Тоді n_2 однозначно визначає n_1

Доведення

Зафіксуємо q та припустимо, що існують n_2, x, y (розглядаємо x, y як два ймовірних значення n_1) з

1. x,y,n_2
2. $2.(\sqrt{q}-1)^2 \leq n_2x \leq n_2y \leq (\sqrt{q}+1)^2$

(тому групи порядка n_2x і n_2y задовольняють обмеження теореми Хасса). Наша перша мета - показати, що якщо n_2, x, y, задовольняють (1) і (2), то $q \leq 4612$.

Нехай $d = \gcd(x, y)$. Тоді $n`_2 = dn_2$, $x` = x/d$, $y` = y/d$ також задовольняють (1), (2).

Тому можливо припустити, що $\gcd(x, y) = 1$. Так як $n_2y - n_2x > 0$

$$n_2 \leq n_2y n_2x \leq (\sqrt{q}+1)^2-(\sqrt{q}-1)^2=4\sqrt{q}$$

Так як $x, y | n_2$, то маємо $xy | n_2$, отже, $xy \leq n_2$. Тому

$$x^2 \leq xy \leq n_2 \leq 4\sqrt{q}$$

внаслідок маємо

$$(\sqrt{q}-1)^2 \leq n_2x \leq (4\sqrt{q})(4\sqrt{q})^{1/2}$$

Але $(\sqrt{q}-1)^2 > 8q^{3/4}$, тоді $q \geq 4613$. Отже, ми повинні мати $q \leq 4612$.

Значення $q \leq 4612$ можна перевірити на комп'ютері, щоб отримати набагато меньший список ймовірних значень q. Однак ми можемо прискорити пошук за допомогою наступних спостережень.

По перше, $(\sqrt{q}-1)^2 \leq n_2x \leq 4\sqrt{q}x$ припускає, що $x > (\sqrt{q}-2)/4$. По друге, $y^2 \leq n_2y \leq (\sqrt{q}+1)^2$. По третє, $xy^2 = (xy)y \leq n_2y \leq (\sqrt{q}+1)^2$. Нарешті, $n_1 | q - 1$, тому $x, y | q - 1$.

Отже, ми повинні шукати значення $q \leq 4612$, які є простими та такі, що $q - 1$ має дільники x, y с

1. $\gcd(x,y)=1$
2. $(\sqrt{q}-2)/4 < x < y < \sqrt{q}+1$
3. $xy^2 \leq (\sqrt{q}+1)^2$

Значення q, для яких існують такі x, y, знаходяться у списку в утвердженні теоремі, плюс п’ять значень q = 49, 81, 121, 169, 841. Отже, для всіх інших q, число n_2 не може мати двух можливих значень x, y для n_1, тому n_1 є визначено.

Нам треба виключити останні п’ять значень. Наприклад, розглянемо q = 49. Одно з рішень - x = 2, y = 3, n_2 = 18, що відповідає #E(P_q) = 36 і 54. Якщо #E(P_q) = $(\sqrt{q} - 1)^2$, то E(Pq) Z√q-1 ⊕ Z√q-1. Тому, якщо #E(P_{49}) = 36, то ми повинні мати $n_1 = n_2 = 6$. Це витікає з x = 2 після умноження на 3 (нагадем, що ми прибрали d = gcd(x, y) з x, y, щоб зробити їх відносно простими).

Множення y = 3 на d = 3 дає n_1 = 9, n_2 = 6, що не задовільнує $n_1|n_2$.

Тому рішення x = 2, y = 3 для q = 49 відпадає. Аналогічно, всі рішення для всіх п’яти значень q = 49, 81, 121, 169, 841 можуть бути виключенням.

Це завершує доказ.

Нехай F ∈ E(P_q). Ми хочемо знайти порядок F. Спочатку ми хочемо знайти ціле число k таке, що kF = ∞. Пусть #E(P_q) = N. По теоремі Лагранжа, F = ∞. Звісно, ми можливо можемо не знати N, но ми знаемо, що $q+1-2\sqrt{q} \le N \le q+1+2\sqrt{q}$. Ми можемо перебирати усі значення N у цьому діапазоні і побачити, які із них задовольняють NF = ∞. Це займє біля $4\sqrt{q}$ шагов. Однак можливо прискорити цей процес приблизно до $4q^{1/4}$ шагів за допомогу наступного алгоритму.

1. Обчисліть Q = (q + 1)F.
2. Виберіть ціле число m, при тому $m>q^{1/4}$. Обчисліть і збережіть точки jP для j = 0, 1, 2,...,m.
3. Обчисліть точки

Q+k(2mF) для k= -m,-(m-1), …, m

поки не найдеться збуг Q+k(2mF) = ±jP з точкою (чи її від’ємне значення) в збереженому списку.

4. Зробіть висновок, що (q +1+2mk ∓ j)F = ∞. Нехай M = q +1+2mk ∓ j.

5. Нехай $p_1,...,pr$ - различные простые коэффициенты M.

6. Обичсліть (M/pi)F для i = 1,...,r. Якщо (M/pi)F = ∞ для деякого i, замініть M на M/p_i та поверніться к кроку (5). Якщо (M/pi)F = ∞ для всіх i, то M - порядок точки F.

7. Якщо ми шукаемо $\#E(P_q)$, то повторюймо кроки (1)-(6) з випадковими вибраними точками в E(Pq) до того часу, поки найменше спільне кратне з порядків діле тільки одне ціле число N c q + 1 - $2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$.

Тоді N = #E(Pq).

3 КРИПТОСИСТЕМА «ElGamal» НА ЕЛІПТИЧНИХ КРИВИХ

Криптосистема ElGamal на еліптичних кривих.

Нехай E_p- еліптична крива над полем Z_p, p> 3 – просте число Аліса выбирає точку A на F_p . A в групі E_p є велике просте число, порядок групи E_p, Тобто p|N_p. Аліса обирає секретне число S є |N та обичслює точку Q=[s]. Теперь еліптична крива E_p(точніше група точок на E_p) точка P и точка Q=[s]P создають відкритий ключ Аліси (число s- це приватний секретний ключ Аліси).

Боб щоб відіслати повідомлення Алісі поступає наступним чином:

(1) Використовуючи хєш-функцію відображає своє повідомлення в точку M є E_p

(2) Обирає свій секретний ключ k – (це ціле число≤ порядку групи E_p) і обчислює точку M_1=[k]P:

(3) Обчислює точку M_2= M+[k]Q

(4) Відправляє точки M_1 і M_2 Алісі

Аліса розшифровує отриманне повідомлення, проводячі наступні обчислення:

Вона обчислює точку

$$M=M_2-[3]M_1.$$

Дійсно:

$$M_2-[s]M_1=(M+[k]Q)-[s]([k]P)=M+[ks]P-[sk]P=M$$

Щоб зломати цю криптосистему, потрібно вміти по точкам P і Q знаходити число S. А ця завдання еквівалетне завданню дискретного логарифму з додатковими труднощами, котрі доставляють координати точок P і Q. Так само як в стандартної криптосистеми ElGamal не рекомендується двічи використовувати одно й теж саме секретне число S.

Припустимо, що Аліса хоче відправити повідомлення Бобу. По-перше, Боб встановлює свій публічний ключ наступним чином. Він обирає еліптичну криву E над кінцевим полем F_q такую, що проблема дискретного логарифма тяжка для $E(F_q)$ Він также обирає точку P на E(знову ж таки, зазвичай вважается, що порядок P – велике просте число). Він обирає секретне ціле число S и обчислює B = sP. Еліптична крива E, кінцеве поле F_q , а точки P и B – відкритий ключ Боба. Вони обнародувані.

Закрытий ключ Боба - це ціле число s.

Щоб відправити повідомлення Бобу, Аліса робить наступне:

1. Завантажує відкритий ключ Боба.
2. Виражає свое повідомлення як точку $M \in E(F_q)$.
3. Вибирає секретне випадкове ціле число k і обчислює $M_1 = kP$.
4. Обчислює $M_2 = M + kB$.
5. Відправляє M_1, M_2 Бобу.

Боб розшифровує обчислюючи:

$$M = M_2 – sM_1.$$

Ця розшифровка працює, тому що

$$M_2 – sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

Ева що підслуховує знає загальнодоступну інформацію Боба и точки M_1. і M_2. Якщо вона може обчислювати дискретні логарифми, вона може використовувати P і B, щоб знайти s, котре вона потім може використовувати для розшифрування повідомлення як $M_2 – sM_1$. Окріме того, вона може використати P і M_1, щоб знайти k.

Тоді вона може обчислити $M = M_2 − kB$. Якщо вона не може обчислит и дискретні логарифми, то схоже, немає способу знайти M. Для Аліси важлив о використати різні випадкові k кожного разу, коли вона відправляє повідомл

ення Бобу. Припустимо, що Аліса використовує одно і те ж k для M і M` . Єва дізнается це, тому що, тоді $M_1=M_1$`. Потім вона обчислює M_2’ – M_2 =M’-M. Допустимо M – це об’ява об продажу , яке публікується на добу пізніше. Потім Єва впізнає M, тому вона обчислює M_2’ – M_2 =M’ –M. Виходить що знання одного відкритого тексту M дозволяє Єві вивести інший відкритий текст M' в цьому випадку.

У описаному алгоритмі шифрування на еліптичних кривих зазвичай в икористовують так званний хэш функції.

4 ЦИФРОВИЙ ПІДПИС «ElGamal»

4.1. Цифровий підпис Elgamal

Навідміну від класичного цифрового підпису вивчений нижче цифровий підпис від еліптичної кривої не може буду скопійованна електроними засобами.

1. Спочатку Аліса встановлює відкритий ключ як і вище, Аліса будує еліптичну криву E_p, вибирає точку A є E_p (A≠ 0) досить великого простого порядку p.
2. Аліса вибирає секретне число a є Z, |a|<N обчислює точку B=[a]A.
3. Вибирає функцію f:E_p→Z (наприклад, для A=(x,y)<E_p вваєжаємо f(a)=x). Функція f повинна бути такой, щоб ця функція мала обмеженне число праобразів. Для обранної нами функції f малось не більше двух праорбразів: якщо f(x,y)=x, то має (x,y) и (x,-y) є E_p.

4. Аліса дає відкриту інформацію(відкритий ключ): E_p, f, A и B=[a]A.

Порядок точки A не обов'язково приховувати. Тепер щоб підписати документ m, m<N, Аліса робить наступне:

(1) Хешування дозволяє надати документ цілим числом m (m повинно бути менше p)

(2) Вибирає випадкове k під умовою (k,N)=1 і обчислює точку R=[k]A є E_p

(3) Обчислює $s\equiv k^{-1}(m-af(R))(\mathrm{mod}\ N)$

Підписане повідомлення є тройка (m,R,s). Відмітимо, що m, g є |N, R є E_p. Ще важливо відмітити, що Аліса не робить підписуваний документ секретним.

Боб перевіряє підпис Аліси наступним чином

(1) Він використовує відкритий ключ Аліси

(2) Обчислює дві точки на Ep V_1= [f(R)]B+[s]R и V_2= [m]A

(3) Якщо V_1 і V_2 співпадають то підпис істинний.

(4) Ящко підпис вірний (тобто належить Алісі) то $V_1=V_2$ оскільки

$$V_1=[f(R)]B+[s]R= [f(R)][a]A+ [s][k]A=[f(R)a]A+[(ma)f(R)]A=[m]A=V_2$$

Дійсно, оскільки $sk\equiv m-af(R)(\mathrm{mod}\ N_p)$, то $sk-af(R)+N_P$. Тому

$$[sk]A=[m-af(R)]A+[N_p]A= [m-af(R)]A+O= [m-af(R)]A$$

Помітно що Аліса повинна тримати в секреті число A і k причому k слід кожного разу міняти підписуючу необхідний документ. Властивості хеш-функії

1. По заданому повідомленню m легко визначити H(m)

2. За значенням хеш функції у дуже важко знайти m за умови H(m)=y

3. Вірогідність того, що різним повідомленням m_1и m_2 віповідає одно і те ж значення H(m) (тобто хеш функція H вільна від колізій) Аліса висилає Бобу підписане повідомлення у формі

$$(m, R_h,s_h)$$

де $(H(m), R_h, S_h)$ вірний підпис. Для перевірки Боб поступає так:

1. Застосовує відкритий ключ Аліси;
2. Обчислює $V_1= [f(R_h)]B+[s_h]R_h$ и $V_2=[H(m)]A$
3. Якщо $V_1= V_2$, то заявляє що цифровий підпис вірний

Припустимо Аліса хоче підписати документ. Класичний спосіб - поставити свій підпис на листі бумаги, який є документом. Хоча, припустимо, що документ є электронним, наприклад, комп’ютерним файлом. Наївним рішенням буде від цифрувати підпис Аліси и додати її в файл, який містить документ. В цьому випадку зла Єва може скопіювати підпис и додати її в інший документ. Отже, необхідно зробити кроки для привязання підпису до документу таким чином, щоб його неможливо було використувати ща раз.

Тим не менш, хтось повинен перевірити, що підпис дійса, і вона повинна показати, що Аліса була людиною, що підписала документ. Одно з рішень проблеми залежить від складності дискретного логарифма. Спочатку, алгоритм був розроблений для мультиплікативної групи кінцевого поля. Фактично, це може бути застосовано з любою кінцевою групою.

Аліса спочатку повинна встановити відкритий ключ. Вона обирає еліптичну криву E над кінцевим полем F_q таку, щоб проблема дискретного логарифма була складною для E (F_q). Вона також обирае точку A ∈ E (F_q). Зазвичай вибір робиться так, щоб порядок N з A - велике просте число. Аліса також обирає секретне ціле число a і обчислює B = aA. Нарешті, вона обирає функцію

$$f : E(F_q) \rightarrow Z$$

Наприклад, якщо $F_q = F_q$, то вона може використати f(x, y) = x, де x враховується як ціле число, $0 \leq x<p$. Функція f не потребує особливих властивостей, за винятком того, що її зображення повинно бути великим и тільки невелика кількість вхідних даних виробляти будь-які вихідні дані (наприклад, для f(x, y) = x, не більш ніж дві точки (x, y) дають заданий вихід x).

Відкритою інформацією Аліси є E, Fq, f, A и B. Вона тримає у секреті a. Ціле число N не потрібно розкривати. Його секретність не впливає на наш аналіз безпеки системи. Щоб підписати документ, Аліса робить наступне:

1. Представляє документ у виді цілого числа m (якщо m>N, оберіть велику криву або використовувайте хеш-функцію).
2. Обирається випадкове ціле число k з gcd(k,N) = 1 і обчислюється R = kA.
3. Обчислює $s \equiv k^{-1}(m - af(R)) \pmod N$.

Підписане повідомлення має вігляд (m, R, s). Зверніть увагу, що m, s - цілі числа, а R – точка на E. Також зауважимо, що Аліса не намагається

зберегти документ m в таємниці. Якщо вона хоче це зробити, то їй потрібно використовувати яку-небудь форму шифрування. Боб перевіряє підпис наступним шляхом:

1. Завантажує відкриту інформацію Аліси.

2. Обчислює $V_1 = f(R)B + sR$ и V2 = mA.

3. Якщо $V_1 = V_2$, то вын оголошує підпис дійсним.

Якщо підпис дійсний, то $V_1 = V_2$, так як

$$V_1 = f(R)B + sR = f(R)aA + skA = f(R)aA + (m - af(R))A = mA = V_2.$$

Ми використали той факт, що $sk \equiv m - af(R)$, отже, $sk = m - af(R) + zN$ для деякого цілого числа z. Отже,

$$skA = (m - af(R))A + zNA = (m - af(R))A + \infty = (m - af(R))A$$

Тому конгруентність, яка визначає s, була взята з mod N.

Якщо Єва може обчислити дискретні логарифми, то вона може використати A і B для находження a.В цьому випадку вона може поставити підпис Аліси під будь-яким повідомленням. Альтернативний варіант, Єва може використовувати A і R для знахождення k. Оскільки вона знає s, f(R), m, вона може використати $ks = m - af(R) \pmod N$, щоб знайти a. Якщо $d = \gcd(f(R), N) = 1$, тоді $af(R) = m - ks \pmod N$ має d рішень для a. Поки d мале, Єва може перебирати всі варіанти, поки не не отримає B = aA. Потім вона може використати a, как яа і раніше, для підробки підпису Аліси на довільних повідомленнях.

Як ми тільки що побачили, Аліса повинна берегти a і k у секреті. Крім того, вона повинна використовувати різне випадкове k для кожного підпису. Припустимо, що вона підписує m и m, використовуючи одне й те саме k для отримання підписаних повідомлень (m, R, s) та (m, R, s). Єва зразу ж розпізнає, що k було використано двічі, оскільки R однакове для обох підписів. Нерівність для s, s дають наступне:

$$ks \equiv m - af(R) \pmod N$$

$$ks \equiv m - af(R) \pmod N.$$

Віднімання дає $k(ss) \equiv mm \pmod N$. Нехай $d = \gcd(ss, N)$.

Можливо, Єві не потрібно вирішувати задачі дискретного логарифма для того, щоб підробити підпис Аліси на іншому повідомленні m. Усе, що потрібно зробити Єві, це провести R, s так, щоб нерівність перевірки $V_1 = V_2$ було виконано. Це означає, що їй потрібно знайти R = (x, y) та s такі, що $f(R)B + sR = mA$.

Якщо вона обере деяку точку R (ціле число k обирати не потрібно), то їй потрібно вирішити дискретну логарифмічну задачу $sR = mA - f(R)B$ для цлого числа s. Якщо замість цього вона обирає s, то їй потрібно вирішити нерівність для R = (x, y). Ця нерівність, мабудь, щанйменше, таке ж складне, як і дискретна логарифмічна задача, хоча воно не було проаналізовано так ретельно. Більш того, ніхто не зміг виключити можливість використання деякої процедури, котра знаходить R та s одночасно. Існують методи використання Дійсного підписаного повідомлення для створення іншого дійсного підписаного повідомлення. Однак отрименні повідомлення навряд чи будуть осмисленими повідомленнями.

За загальною думкою, безпека системи ElGamal дуже близька до безпеки дискретних логарифмів для группы $E(F_q)$.

Недоліком системи ElGamal є те, що підписане повідомлення (m, R, s) приблизно в три рази довще, ніж оригінал (немає необхідності зберігати повну y-координату R, так як існує тільки два варианти y для даного x). Найбільш эфективним методом є вибір публічної хеш-функції H та підпис H(m). Криптографічна хеш-функція - це функцця, яка приймає вхідні данні довільної довжини, інколи повідомлення з міліардів біт, та видає на виході значення фіксованної довжини, наприклад, 160 бит. Хеш-функція H повинна мати наступні властивості:

1. З огладу на повідомлення m, значення H(m) може бути обчислено дуже швидко.
2. З огляду на y, знайти m, при якому H(m) = y, обчислювально нездійсненно (це говорить про те, що H стійке до перетворень).
3. Обчислювально неможливо знайти різні повідомлення m1 та m2.

з $H(m_1) = H(m_2)$. (Це доводить, що H не містить колізій).

Причина для (2) і (3) полягає в тому, щоб не дозволити Єві робити полвідомлення з потрібними хеш-значеннями або два повідомлення з однаковим хеш-значенням. Це допомагає запобігти підробці. Існує декілька популярних хеш-функцій, наприклад, MD5 (автор Ривест; видає 128-бітний результат) и Secure Hash Algorithm (від NIST; видаеє 160-бітний результат). Ми не будемо обговорювати їх тут. У недавній праці Wang, Yin та Yu [127] були знайдені слабкі місця в них, тому ця тема знаходиться в стані деякої невизначенності.

Якщо Аліса використовує хеш-функцію, то підписане повідомлення буде виглядати наступним чином

(m, RH, sH),

де $(H(m), R_H, s_H)$ - дійсний підпис. Щоб перевірити, що підпис (m, RH, sH) є дійсним, Боб робить наступне:

1. Завантажує відкриту інформацію Аліси.

2. Обчислює $V_1 = f(RH)B + sHRH$ та $V_2 = H(m)A$.

3. Якщо $V_1 = V_2$, віноголошує підпис дійсним.

Перевага полягає в тому, що дуже довге повідомлення m, що містить міліарди бітів, підпис, для якого потребується усього декілька тисяч додаткових бітів. До тих пір, дики дискретна проблема дискретного логарифма буде тяжкою для E(Fq), Ева не сможе поставити підпис Алісы на інше повідомлення. Використання хеш-функції також захищає від деяких інших підробок.

Недавній варіант схеми підпису ElGamal, створений ван Дуином, дуже эфективний в деяких аспектах. Наприклад, він дозволяє уникнути обчислення k^{-1}, а процедура перевірки потербує тільки двух обчислень цілого числа, помноженого на точку. Як і раніше, у Алісы є документ m, який вона хоче підписат. Щоб налаштувати систему, вона обирає еліптичну криву E над кінцевим полем F_q та точку $A \in E(F_q)$ великого простого порядка N. Вона також вибирає криптографічну хэш-функцию H. Вона обирає секретне ціле

число a і обчислює B = aA. Відкрита інформація - це (E, q, N, H, A, B). Секретна інформація - це a. Щоб підписати
m, Аліса робить наступне:

1. Обирає випадкове ціле число k mod N и обчислює R = kA.

2. Обчислює t = H(R, m)k + a (mod N).

Підписаний документ має вид (m, R, t).

Щоб перевірити підпис, Боб завантажує відкриту інформацію Аліси і перевіряє че є вона істинною

$$tA = H(R, m)R + B$$

Якщо це так, то підпис вважається дійсною, в іншому випадку вона не є дійсною

4.2 Алгоритм цифрового підпису

Стандарт цифрового підпису [1], [86] базується на алгоритмі цифрового підписи (DSA). В першій версії використовувались мультиплікативні групи кінцевих полів. В больш сучасній версії (ECDSA) використовуються еліптичні криві. Алгоритм являє собою варіант схеми підпису ElGamal здеякими модифікаціями. Ми покажемо алгоритм тут.

Аліса хоче підписати документ m, який є цілим числом (насправді, вона зазвичай підписує хеш документа). Аліса обирає еліптичну криву над кінцевим полем F_q таку, що $\#E(F_q) = fr$, де r - велике просте число та f - невелике ціле число, зазвичай 1, 2 або 4 (f повинно бути невелики для того, щоб зберегти алгоритм эфективним). Вона обирає базову точку G в $E(F_q)$ порядка r.Нарешті, Аліса обирає секретное ціле число a і обчислює Q = aG. Аліса оприлюднює публічно наступну інформацію:

$$Fq, E, r, G, Q.$$

(Немає необхідності тримати f у секреті; воно може бути виведено з q і r за допомогою теореми Хассе.

Щоб підписати повідомлення m Аліса робить наступне:

1. Обирає випадкове ціле число k при $1 \leq k<r$ та обчислює $R = kG =(x, y)$.

2. Обчислює $s = k^{-1}(m + ax) \pmod r$.

Підписаний документ має вид

$$(m, R, s).$$

Щоб перевірити підпис, Боб робить наступне.

1. Обчислює $u1 = s^{-1}m \pmod r$ та $u2 = s^{-1}x \pmod r$.

2. Обчислює $V = u_1G + u_2Q$.

3. Оголошує підпис дійсним, якщо $V = R$.

Якщо повідомлення підписано правильно, то виконується нерівність перевірки:

$$V = u_1G + u_2Q = s^{-1}mG + s^{-1}xQ = s^{-1}(mG + xaG) = kG = R.$$

Основна різниця між ECDSA і системою ElGamal полягає в процедурі перевірки. В системе ElGamal нерівність верифікації $f(R)B + sR = mA$ потребує трьох обчислень цілого числа, помноженого на точку.

Це найбільш «дорогі» частини алгоритма. В системі ECDSA тільки два вичислення цілого числа, помноженого на точку. Якщо потрібно багато перевірок, то повищена эфективність ECDSA дуже важлива.

Це такий самий тип покращення, що і в системі ван Дуина.

ВИСНОВКИ

В роботі досліджуються властивості точок еліптичних кривих над еліптичним полем F_p, $p>3$ – просте раціональне число, а також криптографічні застосуваня таких точок. В тому чіслі аналог криптосистеми ElGamal на еліптичних кривих і алгоритм цифрового підпису по ElGamal на еліптичний кривих. Розглянули питання пипання порядку группи точек еліптичних кривих, задачи по застосування теореми Хассе, отримані оцінки порядку E_p з ростом p. Розглянуті узагальнення проблем дискретного логарифма на E_p (метод великих і малих кроків і метод Поліга-Хелмана)

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях: Москва 2005, p.326.
2. Elliptic Curves Number Theory and Cryptography, C. Washington: N.Y.2008, p.524.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с.
4. Методична література кафедри комп’ютерної алгебри та дискретної математики