УДК 004.492.2

Петровский О. М., доцент, к.т.н.
Кікоть В. В., магістрант
Полтавський національний технічний університет імені Юрія Кондратюка

ЕЛІПТИЧНІ КРИВІ В ПОСТКВАНТОВІЙ КРИПТОГРАФІЇ ТА ВИТІСНЕННЯ RSA

Анотація. *У статті частково розглянуто криптографію загалом та необхідність переходу до постквантової криптографії. Мета роботи полягає у вивченні нового і цікавого напряму в криптографії, а саме постквантової криптографії. Проаналізовано стійкість криптосистем, заснованих на завданні дискретного логарифмування до атак зловмисників на засекречені дані. Також розглянуто методи застосування ізогенії для побудови криптосистем.*

Ключові слова: *криптографія, еліптичні криві, ізогенія, Microsoft SIDH, квантовий комп'ютер, постквантова криптографія.*

Вступ

Необхідність переходу до криптографії, стійкої до атаки на квантовому комп'ютері, вже офіційно анонсована NIST і NSA, з чого висновок досить-таки простий: варто відходити від старої доброї RSA і навіть, ймовірно, від улюблених багатьма еліптичних кривих і дізнаватися нові, не менш цікаві примітиви, здатні убезпечити конфіденційну інформацію. В цій статті ми розберемося в тонкощах криптографії на еліптичних кривих та простежимо новомодні віяння постквантової криптографії.

Декілька слів про криптографію. Що таке криптографія і для чого вона взагалі потрібна? Скажімо, Аліса і Боб хочуть обмінятися повідомленням, та так, щоб його зміст залишався в секреті. Очевидно, що у кожної зі сторін має бути свій ключ. І на цьому етапі можна виділити два підвиди криптосистем.

До першого з них відносяться симетричні криптосистеми. Тут один ключ може бути легко обчислений з іншого, а найчастіше вони і зовсім збігаються. Значущими плюсами таких криптосистем є простота реалізації і висока швидкість роботи за рахунок використання більш простих операцій. Однак, якщо один з ключів буде скомпрометований, будь-яка спроба захистити секретну інформацію втратить свій сенс.

Така проблема витончено вирішується в асиметричних криптосистемах за допомогою спеціальних алгоритмів. Однак тут ми стикаємося з трудомісткістю операцій, що може не дати бажаного результату для великого обсягу даних. У таких криптосистемах потрібно дуже постаратися, щоб з одного ключа обчислити інший, і, поки чийсь комп'ютер не володіє величезною потужністю, можна бути відносно спокійними за секретність даних, що захищаються.

Однак з урахуванням стрімкого зростання продуктивності обчислювальних пристроїв, виникає необхідність у збільшенні довжини ключа, ну а це може стати критичним фактором для пристроїв з обмеженою потужністю ... Ех, було б так здорово, якби з'явилася така структура, яка б дозволила скоротити розмір ключа при такому ж рівні стійкості ... І, на щастя, вона існує! Назва цього - еліптична крива.

Еліптичні криві

Для початку дамо визначення. Еліптична крива - це, перш за все, неособлива кубічна крива. Неособливою її називають, тому що до всіх її точок можна однозначно провести дотичну. Ну раз це крива кубічна, то і шукати відповіді вона повинна рівнянням третього ступеня, яке в узагальненій формі Вейерштрасса виглядає наступним чином:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Однак на практиці таку форму кривої можна зустріти нечасто. Розрізняють форми Лежандра, Монтгомері, Гессе і т.д. Використання тієї чи іншої форми може збільшити ефективність операцій над точками еліптичної кривої. Наприклад, у формі Монтгомері є можливість виконувати множення точки на число за фіксований час завдяки алгоритму Монтгомері.

Напевно багато хто стикався з формою Вейерштрасса, її називають канонічною для полів з характеристикою $char\ K\ \neq 2, 3$:

$$E(K) : y^2 = x^3 + ax + b$$

Важливою характеристикою еліптичної кривої є її дискриминант, який для форми Вейерштрасса обчислюється так: $\Delta = 4a^3 + 27b^2$

Дискримінант не повинен дорівнювати нулю, інакше крива вже не буде еліптичної, так як будуть існувати точки перегину, як на кривій

$y^2 = x^3 - 3x + 2$. (Рис. 1)

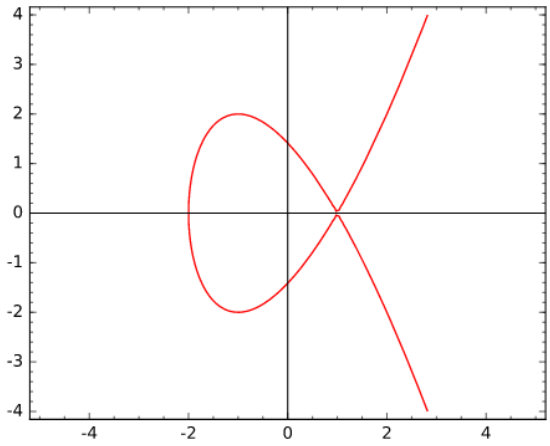

Рис. 1

Напевно багатьом знайоме зображення еліптичної кривої, яке можна побачити на малюнку нижче. Тут крива виду $y^2 = x^3 - 3x + 5$ задана над полем раціональних чисел. (Рис. 2)

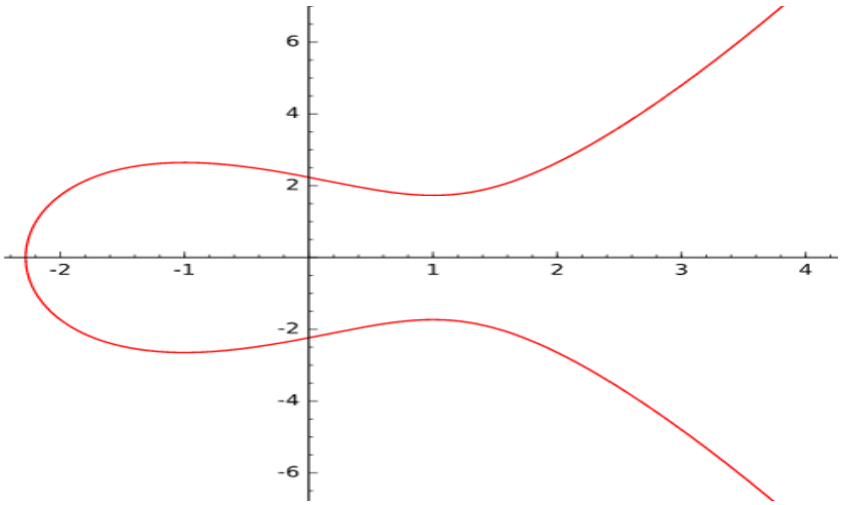

Рис. 2

Однак, при використанні раціональних чисел виникає складність з їх округленням, і, як наслідок, з неоднозначністю операцій шифрування і розшифрування. Тому в криптографії еліптичні криві задаються над кінцевим полем, де координати точок - це елементи поля. Графік кривої, звичайно, втратить свою колишню привабливість, плавні лінії заміняться на точки.(Рис. 3)

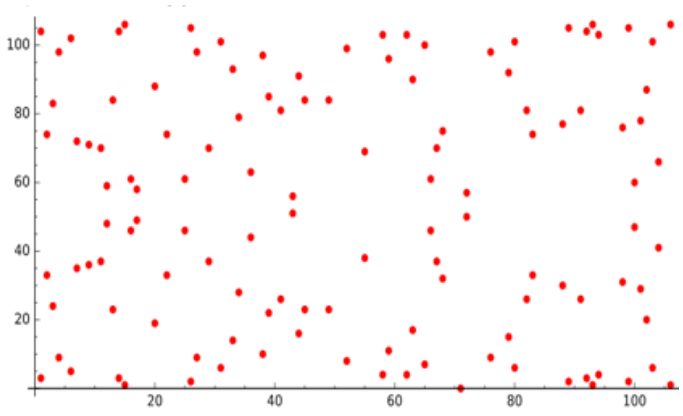

Рис. 3

Не можна не згадати ще одну характеристику еліптичних кривих, йдеться про j-інваріант, постійної величини. Його обчислення для еліптичної кривої в формі Вейерштрасса : $j = 1728 \frac{4a^3}{4a^3+27b^2}$

Властивості групи

Важливим моментом в криптографії на еліптичних кривих є те, що точки еліптичної кривої з абстрактної нескінченно віддаленою точкою утворюють абелеву групу. Візьмемо в якості групової операції додавання, тоді група - це така структура алгебри, яка має такі властивості:

•Замкнутість означає, що результат складання елементів групи теж є елементом групи. Переведемо в терміни еліптичної кривої: при додаванні точок еліптичної кривої виходить точка, що належить цій же кривій.

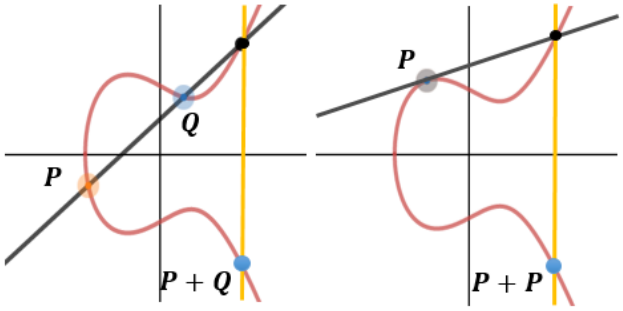

Рис. 4

Як видно з малюнку зверху (Рис. 4), геометричний сенс складання точок на еліптичній кривій полягає в наступному: необхідно провести січну через складаються точки і відобразити точку перетину цієї прямої з еліптичної кривої щодо осі Ox:

•Асоціативність означає незалежність результату складання від зміни порядку дії.

•У групі повинен існувати нейтральний елемент. Результат складання будь-якого елементу групи g і нейтрального буде дорівнює тому ж елементу. В еліптичних кривих роль нейтрального елемента грає нескінченно віддалена точка:

$$P_\infty : P_\infty + P = P + P_\infty = P$$

•До кожного елементу повинен існувати зворотний до нього (щодо основної операції). При додаванні елемента групи і зворотного до нього отримуємо нейтральний елемент.

•Властивість комутативності нам знайоме ще зі шкільної математики: від перестановки доданків сума не змінюється. Саме ця властивість і робить групу абелевою.

Стійкість

Тепер поговоримо про стійкість криптосистем, заснованих на завданні дискретного логарифмування. Нехай G- кінцева циклічна група, тобто, кожен її елемент представимо у вигляді ступеня одного-єдиного елемента – утворює $g: < g > = G = \{1, g^2, g^3, \dots, g^{q-1}\}$.

Залежно від вибору групи G існують різні методи розв'язання задачі дискретного логарифмування. Так, для вирішення завдання дискретного логарифмування в кінцевому полі, існують не тільки універсальні алгоритми (метод Поліга-Хеллмана, p-метод Полларда і ін.), які мають експонентну складність, але й спеціальні, що мають субекспоненціальну складність (метод бази розкладання , метод решета числового поля).

Якщо ж в якості утворює групи G взяти точку еліптичної кривої, то злодіям доведеться задовольнятися лише універсальними алгоритмами. Тому криптографія на еліптичних кривих «балує» користувачів меншою довжиною ключа.

Однак не всі еліптичні криві здатні забезпечити високий рівень стійкості в криптографічних протоколах. Першу небезпеку становлять суперсінгулярні криві. Їх перевага полягає в легкості обчислення числа точок, на відміну від несуперсінгулярних кривих. Є чимало чинників, за якими можна відрізнити суперсінгулярную криву від несуперсінгулярной, проте в даній статті не будемо загострювати на цьому увагу.

Дані криві уразливі до MOV атак, яка дозволяє зводити обчислення завдання дискретного логарифмування в групі точок еліптичної кривої над полем F_q^k до задачі дискретного логарифмування в кінцевому полі F_q^k. З огляду

на, що довжина ключа в криптографії на еліптичних кривих менше, і що для суперсінгулярних кривих значення k не є великим, реалізація даної атаки проходить вкрай успішно для зловмисника

Квантова загроза

Останнім часом широку популярність отримують квантові обчислення. Якщо в класичному комп'ютері найменша одиниця інформації представляється бітом, який може приймати значення або 0, або 1 в один час, то в квантовому цю роль виконують кубіти. Їх особливість полягає в тому, що кубіт може перебувати і в стані 0, і в стані 1 одночасно. Це і дає квантових комп'ютерів їх перевершує обчислювальну потужність. Наприклад, якщо ми розглядаємо чотири біта інформації, то з всіляких 16 станів ми можемо вибрати лише одне в один момент часу. 4 кубіта ж можуть перебувати в 16 станах одночасно, тобто в суперпозиції, і дана залежність зростає експоненціально з кожним новим кубітом.

Якщо в класичному комп'ютері логічні елементи отримують на вхід біти інформації, а на виході видають однозначно певний результат, то в квантовому комп'ютері в якості логічного елемента береться так званий квантовий гейт (quantim gate), який маніпулює значенням цілої суперпозиції.

Важливе явище, властиве кубітів, - це заплутаність. Наприклад, маємо два заплутаних кубіта. Вимірювання стану одного з них допоможе дізнатися інформацію про стан його пари без необхідності будь-якої перевірки.

Слід зазначити, що квантовий комп'ютер - це не заміна звичним нам класичним, так як вони швидше лише в виконанні обчислювальних операцій, де необхідно використовувати всілякі суперпозиції.

З одного боку, поява квантового комп'ютера - це круто. Серйозно. У багатьох сферах науки така машина принесе чимало користі (наприклад, при моделюванні), однак для криптографії такий значущий прорив буде критичний. А все тому, що в 1994 році Пітер Шор запропонував квантовий алгоритм, який

дозволяє розкласти число не за мільйони років, а за цілком доступний для огляду час.

Ізогенія

Почнемо з поняття: ізогенія - це раціональне відображення, що переводить точки однієї еліптичної кривої в точки ізогенної кривої, залишаючи нерухомою нескінченно віддалену точку. Нехай маємо дві ізогенні еліптичні криві $E1$ і $E2$. Ізогенними вони називаються, якщо вони задані над одним полем і мають однакове число точок.

Так ось, ізогенія - це, по суті, невеликий вжух, який бере точку кривої $E1$ на вхід, а на виході видає точку кривої $E2$. Ядром ізогенії називається безліч точок на кривій $E1$, які переходять в нескінченно віддалену точку кривої $E2$.

Для кожної ізогенії існує єдина дуальна ізогенія, що виконує зворотне перетворення. Тобто, якщо ізогенія має наступний вигляд: $\varphi: E1 \rightarrow E2$, то дуальна до неї: $\hat{\varphi}: E2 \rightarrow E1$. (Рис. 5)

Рис. 5

Якщо перемножити ізогенію і дуальну до неї, отримаємо точку кривої $E2$, помножену на ціле число l, яку називають ступенем ізогенії. Ізогенії простих ступенів можуть задавати перестановки на безлічі j-інваріантів ізогенних кривих. А послідовне накладення графів ізогенних еліптичних кривих дозволяє отримати просто космічно красиву зірку ізогенних кривих, як на малюнку нижче. (Рис. 6)

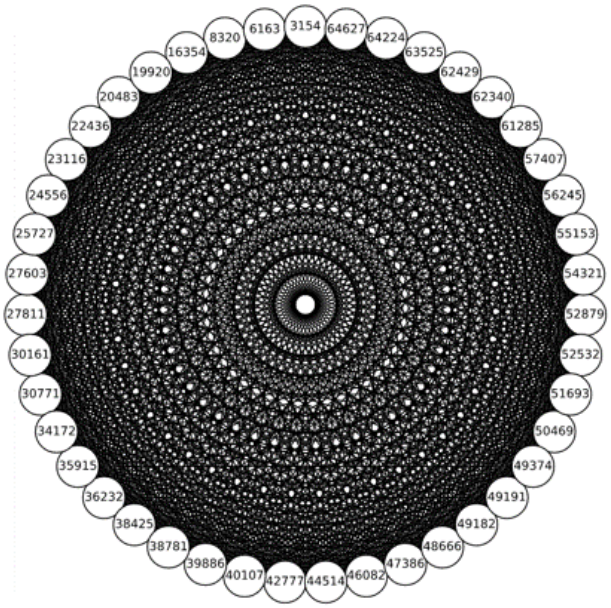

Рис. 6

Можливість застосування ізогенії для побудови криптосистем була запропонована порівняно недавно. У 2003 році автором E. Teske була опублікована робота, де ізогенії використовувалися в схемі з можливістю депонування ключів. У 2006 році А. Г. Ростовцева і А. Столбунова схема шифрування Ель-Гамаля була адаптована під ізогенії еліптичних кривих. У тому ж 2006 році для побудови хеш-функцій було запропоновано використовувати графи ізогенних суперсінгулярних кривих. Важливим і, можна сказати, переломним моментом в дослідженні ізогенії є робота, опублікована в 2010 році, де пропонується квантовий алгоритм, що вирішує завдання знаходження ізогеній несуперсінгулярних кривих за субекспоненціальний час. З цього моменту дослідження стали більше орієнтовані на суперсінгулярні криві. Так, в мережі вже можна знайти схеми шифрування з відкритим ключем, докази з нульовим розголошенням, схему незаперечного підпису і підпису наосліп.

Microsoft SIDH

Компанія Microsoft теж не залишилася осторонь і в 2016 році випустила бібліотеку SIDH (Supersingular Isogeny Key Exchange) з відкритим вихідним

кодом. Одним з переваг даної бібліотеки є можливість використання еліптичних кривих в формі Монтгомері, які захищають від атак за часом.

SIDH реалізована на мові C і підтримує використання Microsoft Visual Studio на ОС Windows і LNU GCC і clang на ОС Linux. У бібліотеці представлена реалізація базових арифметичних функцій з можливістю підтримки різних платформ, включаючи x64, x86 і ARM. Великим плюсом до продуктивності є оптимізована реалізація операцій на еліптичних кривих.

У бібліотеці реалізований протокол поділу ключа Діффі-Хеллмана на ізогеніях суперсінгулярних кривих.

Ця схема була запропонована авторами Jao і DeFeo. Спрощено її можна описати таким чином. Як параметри криптосистеми використовується загальновідома суперсінгулярная крива E_0 і зафіксовані на ній точки P_A, Q_A, P_B, Q_B.

Нехай Аліса хоче розділити з Бобом не життя, а закритий ключ. Для цього вона генерує випадкові числа m_A, n_A і будує ізогенію $\phi: E_0 \rightarrow E_A$, де ядро задається як $< m_A P_A + n_A Q_A >$.

Боб виконує ті ж дії, але тільки будує вже ізогенію $< m_B P_B + n_B Q_B >$, де в якості ядра вибирається $< m_B P_B + n_B Q_B >$.

Ізогенна ϕ_A і ϕ_B є секретними і кому попало не передаються. Однак, і Боб, і Аліса можуть без будь-яких наслідків розділити точки на своїх ізогенних кривих, до того ж, передані можуть бути і самі криві. Так і відбувається насправді. Аліса передає Бобу точки $\phi_A(P_B)$ і $\phi_A(Q_B)$, і саму криву E_A. Боб робить те ж саме: передає Алісі точки $\phi_B(P_A)$ і $\phi_B(Q_A)$ і криву E_B.

Отже, Аліса і Боб обмінялися даними, тепер підходимо до завершального і неймовірно красивого етапу, а саме, до отримання загального ключа. Знаючи образи точок P_A і Q_A на кривій E_B і випадкові числа m_B і n_B, Боб зможе легко побудувати ізогенію ϕ'_A, а Аліса, що володіє тим же об'ємом інформації, зможе побудувати ізогенію ϕ'_B. Витончене рішення полягає в тому, що ізогенії

ϕ'_A і ϕ'_B приведуть наших співрозмовників до кривої E_{AB}, і в якості ключа може бути взятий її j-інваріант.

Серед функцій в бібліотеці можна виділити і базові арифметичні, які допоможуть в реалізації своїх протоколів. Це, наприклад, j_inv, що обчислює j-інваріант еліптичної кривої, inv_3_way, що знаходить значення мультиплікативно зворотного, подвоєння точки і складання точок - xDBLADD, потроєння точки - xTPL і т.д.

Висновок

Безумовно, поки складно судити про необхідність постквантовой криптографії, коли потужного квантового комп'ютера, по суті, і немає ... Однак метушня в NSA і NIST не можуть не наводити на підозри. Про реальні мотиви такого поспіху нам залишається тільки здогадуватися. У будь-якому випадку, ніколи не завадить перестрахуватися і почати вивчення нового і цікавого напрямку в криптографії, тим більше, якщо це цілком здійсненно на практиці.

Список літератури

1. *Peter W. Shor "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" , 1995.*

2. *Guneysu, Tim Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems, 2012.*

3. *http://old.computerra.ru/features/284073/ - Эллиптическая криптография – [Електронний ресурс]-2006.*

4. *http://window.edu.ru/resource/758/20758 - Рациональные точки на эллиптических кривых – [Електронний ресурс] – 1997.*

Authors:
Oleksandr Petrovsky, Vladislav Kikot

ELLIPTIC CURVES IN POST-QUANTUM CRYPTOGRAPHY AND RSA DISPLACEMENT

Abstract. The article deals with cryptography in general and the need for transition to post-quantum cryptography. The purpose of the work is to study a new and interesting trend in cryptography, namely, post-quantum cryptography. The stability of cryptosystems based on the task of discrete logarithm to attacks by intruders on classified data is analyzed. Also, methods of using isogenesis for construction of cryptosystems are considered.

Keywords: cryptography, elliptic curves, isogenesis, Microsoft SIDH, quantum computer, post-quantum cryptography.

Авторы:
А.Н. Петровский, В.В. Кикоть

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ В ПОСТКВАНТОВИЙ КРИПТОГРАФИИ И ВЫТЕСНЕНИЕ RSA

Аннотация. В статье частично рассмотрена криптография в целом и необходимость перехода к постквантовой криптографии. Цель работы заключается в изучении нового и интересного направления в криптографии, а именно постквантовой криптографии. Проанализирована устойчивость криптосистем, основанных на задаче дискретного логарифмирования к атакам злоумышленников на засекреченные данные. Также рассмотрены методы применения изогении для построения криптосистем.

Ключевые слова: криптография, эллиптические кривые, изогения, Microsoft SIDH, квантовый компьютер, постквантовая криптография.