МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Станкевіч Андрій Олександрович

УДК 004.056.55

ДОСЛІДЖЕННЯ ТЕ РАЕЛІЗАЦІЯ ПРОТОКОЛУ ДІФФІ-ГЕЛЛМАНА НА ЕЛІПТИЧНИХ КРИВИХ

122 – Комп’ютерні науки

Автореферат
магістерської кваліфікаційної роботи на здобуття освітньої кваліфікації
«Магістр комп’ютерних наук»

Миколаїв – 2021

Магістерська кваліфікаційна робота є рукопис.

Робота виконана в Чорноморському національному університеті імені Петра Могили Міністерства освіти і науки України на кафедрі інтелектуальних інформаційних систем

Науковий керівник: д.т.н., професор кафедри інженерії програмного забезпечення Фісун Микола Тихонович

Рецензент: к.т.н., доцент (б.в.з.) кафедри інженерії програмного забезпечення Горбань Гліб Валентинович

Захист відбудеться «23» лютого 2021 р. о 9^{30} год. на засіданні екзаменаційної комісії (ауд. 2-403) у Чорноморському національному університеті імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

З магістерською кваліфікаційною роботою можна ознайомитися в бібліотеці Чорноморського національного університету імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

Автореферат представлений «16» лютого 2021 р.

Секретар
екзаменаційної комісії,
к.пед.н., доцент Н. М. Болюбаш

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження визначається підвищеними вимогами до інформаційних систем щодо захисту конфіденційності та цілісності інформації, що передається по незахищеному каналу зв'язку.

Метою магістерської кваліфікаційної роботи є дослідження протоколу Діффі-Геллмана на еліптичних кривих, реалізація даного протоколу.

Об'єктом дослідження є криптографічний захист інформації під час її передачі в телекомунікаційних мережах.

Предметом дослідження є протокол Діффі-Геллмана на еліптичних кривих (ECDH).

Практичне значення даної магістерської кваліфікаційної роботи полягає у можливості застосування реалізації ECDH для забезпечення захисту інформації.

Апробація результатів дослідження: Станкевіч А. О., Фісун М. Т. "Протокол Діффі-Геллмана на еліптичних кривих і його застосування", Інтелектуальні інформаційні системи: матеріали всеукр. наук.-практ. конф., м. Миколаїв, 9-12 лют. 2021 р. Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2021. С. 164-166.

Магістерська кваліфікаційна робота складається із вступу, 5 розділів та висновків. Загальний обсяг роботи складає 89 сторінок, 37 рисунків, 10 таблиць та 45 посилань на літературні джерела.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі магістерської кваліфікаційної роботи обґрунтовано актуальність обраної теми, сформульовано мету і задачі дослідження, визначено предмет та об’єкт дослідження.

У першому розділі розглядаються асиметричні алгоритми для формування спільного ключа (DH, RSA та ECDH) та механізми захисту передачі інформації у TLS.

Головним обмеженням симетричних алгоритмів шифрування є необхідність у захищеному каналі зв’язку для передачі симетричного ключа, що могло би стати суттєвою перепоною у впровадженні захисту при передачі даних у телекомунікаційних мережах. Вирішенням даної проблеми є використання асиметричних алгоритмів шифрування (зокрема RSA), DH або ECDH. Оскільки асиметричні алгоритми шифрування значно повільніші ніж асиметричні з відповідним рівнем безпеки, асиметричні шифри використовуються лише для передачі сесійних ключів або попереднього секрету для їх формування.

RSA. Асиметричний алгоритм шифрування, що базується на проблемі розкладання великих чисел на прості множники. RSA став першим алгоритмом, що придатний для формування цифрового підпису. За останні роки було розроблено низку ефективних методів розкладання на множники цілих чисел, що змушує постійно збільшувати розмір ключів RSA.

DH. Оригінальний метод запропонований У. Діффі та М. Геллманом у 1976 році. До публікації алгоритму авторами він вже використовувався, але не публікувався, оскільки був засекречений. DH використовує проблему дискретного логарифму в мультиплікативній групі скінченного поля. Проблема дискретного логарифму полягає у пошуку такого цілого x, що

$$g^x \equiv a \pmod{p} \qquad (1)$$

де p - велике просте число;

g, a - цілі числа.

Загалом для проблеми дискретного логарифмування в мультиплікативній групі скінченного поля також розроблено низку методів, що змушує використовувати розмір ключів, що відповідає ключам RSA.

ECDH. Модифікація DH, що використовує групу точок еліптичної кривої (ЕК) над скінченним полем. У ECDH замість операцій піднесення у степінь за модулем використовується операція множення точки ЕК на число. Для еліптичних кривих проблема дискретного логарифму є більш складною ніж для мультиплікативної групи скінченного поля, тому ECDH має набагато менший розмір ключа. Співвідношення розміру ключів для різних протоколів DH/ECDH та алгоритму шифрування RSA наведено у табл. 1.

Таблиця 1

Співвідношення довжини ключа для різних алгоритмів

Симетричні алгоритми	DH	RSA	ECDH
80	1024	1024	160-223
112	2048	2048	224-255
128	3072	3072	256-383
192	7680	7680	384-511
256	15360	15360	512+

Ефімерний та статичний DH(ECDH). Існують два варіанти DH/ECDH статичний та ефімерний (DHE/ECDHE). Використання статичного DH/ECDH означає, що учасник протоколу використовує одну і ту саму пару приватний-публічний ключ для кожного нового з’єднання. Використання статичного ключа на стороні сервера має певні недоліки. Відповідно до принципу прямої секретності (forward security) компрометація довготривалих ключів не має призводити до компрометації сесійних ключів і відповідно до розкриття минулих сесій. По-друге,

якщо єдиний ключ використовується для шифрування трафіку усіх користувачів, то “ціна” такого ключа може перевищити потенційні витрати на здобуття приватного ключа і тому створює додаткові стимули для цього. Саме з цих причин доцільним є використання змінних ключів. Недоліком DHE/ECDHE є додаткові витрати пов’язані з генерацією пари ключів для кожної сесії.

Для шифрування RSA також можливо використовувати ефімерні ключі. Проте час генерації пари відкритий-закритий ключ RSA займає набагато більше часу ніж генерація ключів з відповідним рівнем безпеки для DHE/ECDHE. Саме тому варіант гібридних криптосистем з RSA та симетричним алгоритмом поступається місцем зв’язці DHE/ECDHE + симетричний алгоритм. У специфікації TLS v1.3 затверджено, що в якості процедури узгодження ключів дозволяється використовувати лише DHE, ECDHE (у версії TLS v1.2 передбачається також використання RSA) .

У другому розділі розглянуто DH, поняття скінченного поля та операції в ньому, поняття еліптичної кривої та операції над точками еліптичної кривої, ECDH та вибір безпечних параметрів еліптичних кривих.

Застосування еліптичних кривих в якості криптографічного примітиву було запропоновано незалежно Н. Кобліцем та В. Міллером в 1985 році, зокрема було запропоновано ECDH. Відмінність ECDH від DH полягає в тому, що операція піднесення до степеня за модулем простого числа замінюються на операцію множення на скаляр у групі точок еліптичної кривої над скінченним полем

Еліптична крива визначається як кубічна крива від двох змінних. За допомогою заміни змінних будь-яка кубічна крива над полем, характеристика якого не дорівнює 2 або 3 може бути представлена у вигляді:

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

де a, b - коефіцієнти.

Запис у вигляді (2.26) називається формою Вейєрштрасса. Множина точок координати яких є елементами поля K (де коефіцієнти також належать полю K)

разом з “точкою на нескінченності” O (що не має координат в K) і слугує нейтральним елементом (аналогом нуля) утворюють групу точок еліптичної кривої. При цьому коефіцієнти a, b належать також цьому полю K.

Операції в групі точок еліптичної кривої. Для того щоб множина точок, що належать еліптичній кривій разом з точкою O утворювали групу, необхідно ввести операцію (умовно її називають +), що ставить у відповідність двом елементам множини деяку точку на цій же множині - їх “суму”. При цьому виконуються умови:

1. Існування нейтрального елемента O: A + O = A
2. Існування протилежного елемента: для будь-якого A існує B, що A + B = O
3. Комутативність: A + B = B + A
4. Асоціативність: (A + B) + C = A + (B + C)

Для еліптичних кривих операція “+” визначається графічним та відповідним йому аналітичним способом.

Графічний спосіб: якщо пряма, що не паралельна осі ординат перетинає еліптичну криву у трьох точках A, B, C, то вважається, що A + B + C = O. Якщо пряма дотикається до кривої в певній точці, то вважається, що пряма проходить через дану точку двічі та через деяку третю точку. Сума симетричних відносно осі абсцис точок рівна O.

Таким чином можна визначити операцію додавання, існує доведення факту, що множина точок еліптичної кривої з O та дана операція утворюють групу.

Існує аналітичний спосіб виконання операції додавання у групі точок еліптичної кривої (що відповідає графічному методу). Сума точок A та B визначається наступним чином. Якщо A≠B кутовий коефіцієнт прямої:

$$m = \frac{y_A - y_b}{x_a - x_b} \tag{3}$$

де x_a, y_A координати точки A;

x_b, y_b координати точки B.

Якщо A=B, то коефіцієнт дотичної:

Координати результуючої точки (R=A+B):

$$m=\frac{3x^2+a}{2y} \tag{4}$$

$$x_R=m^2-x_a-x_b \tag{5}$$

$$y_R=y_A+m(x_R-x_A) \tag{6}$$

Еліптична крива може бути визначена на довільному полі. Проте в криптографічних цілях використовуються еліптичні криві над скінченними полями.

ЕК над скінченним полем F_p (де p>3) у формі Вейєрштрасса складається з точок з координатами у полі F_p, що задовольняють рівнянню (2.26), включаючи O. При цьому коефіцієнти a, b також належать даному полю.

Формули додавання точок (табл. 2.1) при переході з R уF_p зберігаються: додавання, віднімання, множення, піднесення в степінь виконуються за модулем p, операція ділення - шляхом множення на обернений мультиплікативний елемент.

Множенням точки G на скаляр k називають:

$$kG=\sum_{i=1}^{k} G \tag{7}$$

Операція множення точки еліптичної кривої на скаляр k, за умови ефективної реалізації, потребує не більше ніж $2\log_2 k$ додавань і є ефективно обчислюваною операцією навіть для великих значень k.

Дискретний логарифм в групі ЕК. Незважаючи на те, що множення точки на число є практично обчислюваною, обернена задача, що полягає у знаходженні для двох заданих точок G та P такого k, що:

$$G\cdot k=P \tag{8}$$

є досить складною. Немає ефективного алгоритму для її розв'язання (виключаючи слабкі ЕК, що будуть розглянуті далі). Дана задача схожа на задачу дискретного логарифмування в мультиплікативній групі поля. Проте на відміну від дискретного логарифму в мультиплікативній групі дана задача вважається більш складною. Саме це сприяло появі ECDH.

Формування спільного ключа у ECDH. Нехай є 2 сторони A та B, що обмінюються повідомленнями, а сторона C може прочитати будь-яке повідомлення, що передає сторона A або B.

Одна зі сторін (нехай A) обирає деяке велике просте число p (задає скінченне поле), а також коефіцієнти еліптичної кривої a, b (для кривої у формі Вейєрштрасса) та базову точку G. Для базової точки G визначається її порядок n - найменше додатне число, що:

$$nG = O \tag{9}$$

Порядок точки n можна розуміти як кількість різних точок, що можуть бути отримані багатократним додаванням G. Числа p, a, b, G, n - часто називають параметрами ЕК. Ці параметри підготовлюються заздалегідь. Зокрема для TLS визначається перелік кривих, що використовуються в ECDH. Крім параметрів ЕК, A генерує випадкове число x з відрізку [2; n - 1]. Сторона A передає стороні B повідомлення, що містить параметри кривої (p, a, b, G, n) та публічний ключ Z_1, що визначається наступним чином:

$$Z_1 = xG \tag{10}$$

Друга сторона B генерує випадкове число y на відрізку [2; n - 1] та відповідає повідомленням, що містить одне значення Z_2, що обчислюється наступним чином:

$$Z_2 = yG \tag{11}$$

Сторона A обчислює спільний ключ K_1:

Сторона В обчислює спільний ключ K_2:

$$K_1 = xZ_2 = x \cdot (y \cdot G) = xy \cdot G = yG \quad (12)$$

$$K_2 = yZ_1 = y \cdot (x \cdot G) = yx \cdot G = xy \cdot G \quad (13)$$

Таким чином сторони А і В отримали одну й ту ж точку. Як правило кожна із сторін використовує абсцису обчисленої точки в якості спільного секретного ключа. Інформація, що передавалась між сторонами: параметри кривої (p, a, b, G, n) та кратні точки Z_1, Z_2 визначення за якими чисел x або y є складною обчислюваною задачею.

Існують окремі класи ЕК для яких задача дискретного логарифмування може бути розв'язана досить ефективно. Відповідно до цього не можна використовувати "слабкі" ЕК для реалізації ECDH та деяких інших алгоритмів, що опираються на складність задачі дискретного логарифмування (DLP). Можна виділити наступні класи ЕК (перелік не є вичерпним), що небезпечно використовувати при реалізації криптографічних систем, що залежать від DLP.

Сингулярні ЕК. ЕК називається сингулярною, якщо вона містить принаймні одну особливу точку. Особлива точка ЕК це точка в якій обидві частинні похідні дорівнюють нулю або не існують. Графічно особлива точка — це точка в якій не можна провести дотичну до кривої (наприклад, точки самоперетину тощо).

Для ЕК, що представлена у формі Вейєрштрасса критерієм визначення сингулярності є знаходження дискримінанта:

$$\Delta = -16\left(4a^3 + 27b^2\right) \quad (14)$$

Якщо виконується умова:

$$\Delta = 0 \quad (15)$$

то ЕК є сингулярною. Сингулярність ЕК залежить від того над яким полем вона визначена. У випадку, якщо ЕК визначена над скінченним полем F_p потрібно перевірити рівність:

$$\Delta = 0 \pmod{p} \tag{16}$$

Якщо рівність виконується ЕК є сингулярною.

Особливістю сингулярних кривих є те, що DLP для сингулярної кривої над полем F_p може бути зведена до DLP в мультиплікативній групі цього ж поля. Оскільки для ECDH використовуються набагато менші значення модулю p ніж для DH з тим же рівнем безпеки (табл. 1), то це є причиною виключення сингулярних кривих під час реалізації ECDH.

Суперсингулярні та аномальні ЕК. Позначимо через |E| - кількість точок ЕК над скінченним полем F_p включаючи O. Кількість точок n для заданих a, b, p (параметри кривої) може бути обчислена за допомогою алгоритму Шуфа. Варто уникати ЕК для яких виконується одна з рівностей:

$$|E| = p+1 \tag{17}$$

$$|E| = p \tag{18}$$

Крім того рекомендується перевіряти умову:

$$\exists m 0 < m < 33 : p^m = 1 \pmod{n} \tag{19}$$

Якщо таке m існує, то DLP на ЕК може бути зведено до DLP для алгебраїчного розширення поля F_p степені m.

ЕК з порядком, що не є простим числом. Як зазначалось, порядком точки G називають найменше ціле n таке, що задовольняє рівність (2.30).

Нехай n представлено у вигляді добутку взаємно простих чисел відмінних від одиниці:

$$n = \prod_{l_i \neq 1}^{\square} l_i \qquad (20)$$

Тоді DLP у групі порядку n може бути зведено до DLP у підгрупах порядку l1, l2, l3, …, ln.

У третьому розділі наведено реалізацію даного криптографічного протоколу. Реалізація включає такі основні елементи: функцію для розв’язання лінійного діофантового рівняння (ЛДР) та функцію для обчислення оберненого мультиплікативного елемента за модулем вказаного числа (шляхом пошуку розв’язку відповідного ЛДР); клас, що представляє елементи скінченного поля (ResidueMember); клас, що представляє еліптичну криву (EC) та точку кривої (ECPoint); клас, що реалізує ECDH. На базі даної реалізації можуть бути розроблені інші криптографічні алгоритми засновані на ЕК.

У спеціальній частині розглянуто дотримання вимог гігієни праці на робочому місці та заходи в умовах виникнення вибуху.

У методичній частині У методичній частині розроблено практичну роботу з теми “Програмування алгоритмів розгалудженої структури на алгоритмічній мові С++”.

ЗАГАЛЬНІ ВИСНОВКИ

Недоліком симетричних алгоритмів шифрування є необхідність передачі ключа шифрування іншій стороні. Для цього повинен існувати певний захищений канал зв’язку між учасниками. Вирішенням даної проблеми є протокол Діффі-Геллмана та його модифікація — протокол Діффі-Геллмана на еліптичних кривих.

Елптичні криві можуть бути визначені над різними полями, проте саме скінченне поле простого порядку та скінченне поле характеристики 2 використовуються при реалізації криптографічних алгоритмів, що опираються на DLP. Оскільки складність розв’язання DLP для групи точок ЕК є набагато вищою ніж складність деяких інших обчислюваних задач, що використовуються у криптографії, то це дозволяє використовувати меншу довжину ключа у ECDH в порівнянні з іншими алгоритмами.

Окремою проблемою є вибір криптографічно стійких параметрів ЕК. При невдалому виборі параметрів (що було розглянуто) можливе суттєве послаблення стійкості ECDH.

У методичній частині розроблено практичну роботу з теми “Програмування алгоритмів розгалудженої структури на алгоритмічній мові С++”.

У спеціальній частині з охорони праці та безпеки життєдіяльності у надзвичайних ситуаціях розглянуто дотримання вимог гігієни праці на робочому місці та заходи в умовах виникнення вибуху.

АНОТАЦІЯ

Станкевіч Андрій Олександрович. Дослідження та реалізація протоколу Діффі-Геллмана на еліптичних кривих. – На правах рукопису.

Магістерська кваліфікаційна робота на здобуття освітньої кваліфікації «Магістр комп'ютерних наук». – Чорноморський національний університет імені Петра Могили, Миколаїв, 2020.

Дана магістерська кваліфікаційна робота присвячена проблемі захисту інформації, а саме протоколу Діффі-Геллмана на еліптичних кривих.

Метою є дослідження протоколу Діффі-Геллмана на еліптичних кривих (ECDH) та аспектів пов'язаних з їх застосуванням.

Об'єктом дослідження є криптографічний захист інформації під час її передачі в телекомунікаційних мережах.

Предметом дослідження є протокол Діффі-Геллмана на еліптичних кривих.

Фахова частина магістерської кваліфікаційної роботи складається з наступних розділів: проблема захисту інформації при передачі даних через телекомунікаційні мережі, дослідження ECDH, програмна реалізація ECDH.

Задачі, які були виконані в процесі роботи:

- аналіз останніх наукових публікацій;
- аналіз предметної області, дослідження недоліків симетричних алгоритмів шифрування та роль ECDH;
- порівняння ECDH та інших асиметричних алгоритмів шифрування/узгодження ключа;
- дослідження еліптичних кривих;
- дослідження слабких класів еліптичних кривих з точки зору DLP;
- програмна реалізація ECDH.

У методичній частині розроблено практичну роботу з теми "Програмування алгоритмів розгалудженої структури на алгоритмічній мові С++".

У спеціальній частині з охорони праці та безпеки життєдіяльності у надзвичайних ситуаціях розглянуто дотримання вимог гігієни праці на робочому місці та заходи в умовах виникнення вибуху.

Робота складається з 89 сторінок, 37 рисунків, 10 таблиць та 45 посилань на літературні джерела.

Ключові слова: *протокол Діффі-Геллмана на еліптичних кривих, протокол узгодження ключів, еліптична крива, груповий закон, задача дискретного логарифмування, модульна арифметика, криптосистема з відкритим ключем.*

ABSTRACT

Stankevich Andrii. Research and implementation of Diffie-Hellman protocol –

On the rights of the manuscript.

Master's qualification work for the educational qualification "Master of Computer Science". - Petro Mohyla Black Sea National University, Mykolaiv, 2020.

This master's qualification work is devoted to the problem of information security, namely the Diffie-Gellman protocol on elliptic curves.

The aim is to study the Diffie-Gellman protocol on elliptic curves (ECDH) and aspects related to their application.

The object of the study is the cryptographic protection of information during its transmission in telecommunications networks.

The subject of the study is the Diffie-Gellman protocol on elliptic curves.

The professional part of the master's qualification work consists of the following sections: the problem of information protection in data transmission over telecommunications networks, ECDH research, software implementation of ECDH.

Tasks that were performed in the process:

- analysis of the latest scientific publications;
- subject analysis, study of the shortcomings of symmetric encryption algorithms and the role of ECDH;
- comparison of ECDH and other asymmetric key encryption / matching algorithms;
- study of elliptic curves;
- study of weak classes of elliptic curves from the point of view of DLP;
- program implementation of ECDH.

In the methodical part the practical work on the topic "Programming of algorithms of branched structure in algorithmic language C ++" is developed.

The special part on labor protection and life safety in emergencies considers compliance with the requirements of occupational health in the workplace and measures in the event of an explosion.

The work consists of 89 pages, 37 figures, 10 tables and 45 references.

Keywords: *elliptic curve Diffie-Hellman protocol, key agreement protocol, elliptic curve, group law, discrete logarithm problem, modular arithmetic, public key cryptography*.