КІБЕРБЕЗПЕКА

УДК 004.9 DOI: https://doi.org/10.32515/2664-262X.2024.9(40).1.14-26

О.С. Улічев, канд. техн. наук, **К.О. Задорожний,** студ.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: askin79@gmail.com, kostazadoroznij9@gmail.com

Стандартизація еліптичних кривих: аналіз та впровадження в криптографічні протоколи

Використання еліптичних кривих у криптографії вважається одним із найбільш перспективних напрямків розвитку сучасних алгоритмів безпеки. Цей математичний підхід базується на складності вирішення задачі дискретного логарифмування у групі точок еліптичної кривої над скінченним полем. Застосування криптографії на еліптичних кривих дозволяє забезпечити безпеку обміну даними, використовуючи ефективні алгоритми шифрування та створення цифрових підписів (ЦП). У цьому дослідженні розглядається еліптичні криві для криптографічних цілей, а також наводяться основні операції у групі точок еліптичних кривих. Особлива увага приділяється алгоритмам обміну ключами Elliptic curve Diffie-Hellman (ECDH) та Elliptic Curve Digital Signature Algorithm (ECDSA). Також аналізуються стандарти, що регламентують використання еліптичних кривих у криптографічних системах, та розглядаються переваги цієї криптографічної парадигми порівняно з основними асиметричними алгоритмами. Досліджуються потенційні загрози та вразливості криптографічних алгоритмів на основі еліптичних кривих. Також наводяться приклади популярних стандартизованих кривих, рекомендованих відповідними організаціями, такими як NIST, що використовуються в реальних криптографічних застосуваннях.

криптографія на еліптичних кривих; асиметричні криптосистеми; цифровий підпис на еліптичних кривих; ECC (Elliptic Curve Cryptography, еліптична криптографія); ECDH; ECDSA; RFC

Постановка проблеми. У сучасному цифровому світі, де інформація відіграє ключову роль, безпека даних стає необхідністю. З розвитком інформаційних технологій та збільшенням обсягу цифрових даних, виникають нові виклики у забезпеченні конфіденційності, цілісності та доступності інформації. Це створює потребу у надійних методах захисту, серед яких одним з найбільш перспективних є криптографія на еліптичних кривих. Додатковим викликом класичним криптографічним алгоритмам стає розвиток квантових обчислень та квантових комп'ютерів. Застосування останніх ставлять під загрозу використання класичних асиметричних алгоритмів шифрування. Ситуація вимагає застосування інших підходів, зокрема шифрування, що базується на еліптичних кривих, а відтак - ґрунтовного дослідження алгоритмів шифрування на еліптичних кривих, їх оцінки та інтеграції даних алгоритмів в безпекові стандарти.

Аналіз останніх досліджень і публікацій. Ідею використання еліптичних кривих започаткували та внесли суттєвий внесок в дослідження питання ряд закордонних вчених, зокрема дослідженню питання присвячено роботи N.Koblitz[3,10], V.Miller[11], N. Saho, E. Ezin[18], I. Blake, N. Smart, G. Seroussi [4], та інші. Серед вітчизняних авторів, що досліджують різні аспекти й особливості застосування еліптичних кривих в захисті інформації та криптографічні методи, засновані на перетвореннях в групах точок еліптичних кривих, можна виділити наступних науковців Горбенко Ю., Горбенко І., Циганкова О., Щур, Н., Покотило, О., Байлюк, Є. Автори Горбенко Ю., Горбенко І.,

в своїй монографії [2], широко розглядають питання криптографії та цифрового підпису, зокрема приділяють увагу й використанню еліптичних кривих в цьому напрямку. Щур, Н. з співавторами в статті [27] зосереджують увагу на практичному застосуванні еліптичних кривих. Циганкова О., в статті [26], приділяє увагу дослідженню властивостей окремої групи кривих - еліптичних кривих у формі Едвардса. Сьогодні еліптична криптографія імплементована в ряд вітчизняних та закордонних стандартів, що стосуються криптографії та захисту інформації.

Постановка завдання. У цьому дослідженні ми розглянемо процес стандартизації еліптичних кривих, проведемо аналіз їх застосування в криптографічних протоколах та розглянемо можливості їх впровадження. Метою дослідження є виявлення переваг ECC у порівнянні з іншими криптографічними методами та розгляд потенційних викликів і вразливості цієї технології. Результати цього дослідження сприятимуть кращому розумінню принципів функціонування ECC та розробці ефективних криптографічних заходів для захисту цифрової інформації.

Виклад основного матеріалу.

Основні властивості ECC. Еліптична криптографія - це метод шифрування з відкритим ключем, що базується на теорії еліптичних кривих, він дозволяє створювати швидкі, компактні та ефективні криптографічні ключі. Одним з основних застосувань еліптичних кривих у криптографічних схемах є системи з відкритим ключем та ЦП.

Еліптичні криві [1] – це алгебраїчні криві, які описуються рівнянням третьої степені з двома змінними. Її можна описати за допомогою рівняння Вейєрштраса (1) :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

де $\{a1, a2, a3, a4, a5, a6\} \in K, \Delta \neq 0.$

Це рівняння має широке застосування, адже воно може використовуватися над будь-якими полями, включаючи скінченні. Цей факт робить еліптичні криві особливо цікавими для криптографії [1]. У галузі криптографії активно застосовуються еліптичні криві, визначені над двома типами кінцевих полів: полями характеристики $2(GF(2m))$ і простими полями непарних характеристик.

$$\begin{gathered}\Delta = -d_2^2 + d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6; \\ d_2 = a_1^2 + 4a_2; \\ d_4 = 2a_4 + a_1a_3; \\ d_6 = a_3^2 + 4a_6; \\ d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.\end{gathered} \quad (2)$$

Якщо скінченне поле K є простим - GF(p), то крива E змінюється на криву, яка характеризується наступним рівнянням:

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

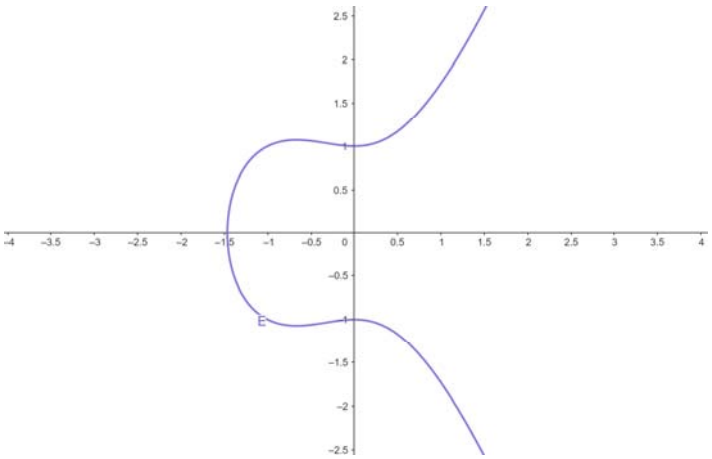

Рисунок 1 – Ілюстрація еліптичної кривої $y^2 = x^3 + 1x^2 + 1$

Джерело: [27]

У випадку, коли $K = GF(2^m)$, крива E перетворюється на криву, яка описується рівнянням:

$$2 + xy = x^3 + ax^2 + b, \quad (4)$$

де $a, b \in K$.

Далі розглянемо операції з точками на еліптичній кривій.

Припустимо, що крива E – еліптична крива, яка визначена над полем K, а P і Q є точками на цій кривій. Сума точок P та Q графічно визначається наступним способом [1].

1. Через точки P та Q провести пряму.
2. Показати, як виглядає перетин заданої прямої з еліптичною кривою у відношенні до вісі OY.

Графічно подвоєння точки P визначається таким способом:.

1. Провести дотичну до еліптичної кривої в точці P.
2. Подвоєною точкою P називається перетин заданої дотичної, який симетрично відображений відносно осі OY.

Вимоги до ЕСС. Для захисту від відомих атак, що базуються на проблемі дискретного логарифма у групі точок ЕК, важливо, щоб кількість точок ЕК була достатньою і ділилась на просте число n. Згідно зі стандартом ANSI X9.62, це число повинно перевищувати 2^160. Рівняння ЕК формується за допомогою специфічного методу, що використовує випадкові або псевдовипадкові коефіцієнти.

Ключовими параметрами під час будування еліптичних кривих над полем $GF(p)$ є:

1. Розмірність поля p , де p є простим числом.
2. Два елементи скінченного поля – a та b визначаються рівнянням еліптичної кривої E, яке має такий вигляд:

$$y^2 = x^3 + ax^2 + b, \quad (5)$$

де $a, b \in GF(p)$, та $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, p)$.

3. Два елементи поля $GF(p) - x_G$ та y_G , які визначають кінцеву точку $G = (x_G, y_G)$ - генератор групи.
4. Порядок q точки G , де $160\, q > 2^{160}$ та $q > 4\sqrt{p}$.
5. Співмножник $h = \#E/q$, де $\#E$ означає порядок групи точок ЕК.

Генерація основних параметрів. Один з методів створення криптографічно надійних параметрів полягає в наступному:

1. Коефіцієнти a та b вибираються специфічним чином за допомогою використання в обчисленнях випадкових або псевдовипадкових чисел. Припустимо E – еліптична крива $y^2 = x^3 + ax + b$ [3].
2. Підраховуємо $N = \#E$.
3. Робимо перевірку, що N має дільник, який являється великим простим числом $q(q > 2^{160}, q > 4\sqrt{p})$. В іншому випадку необхідно перейти на крок 1.
4. Перевіряємо, щоб q не ділився на $p^k - 1$ для кожного k ,$k, 1 \leq 100$. Якщо твердження хибне то, то необхідно повернутись на крок 1.
5. Перевірити, чи q не дорівнює p. У випадку невідповідності цій умові, необхідно повернутись до кроку 1.
6. Вибрати випадкову точку $G' \in E$і покласти $G = (N / q)G'$. Повторювати цей процес, доки $G \neq O$.

Методи шифрування в ECC. Одними із популярних сфер використання еліптичної криптографії, в яких криптостійкість ґрунтується на ECDLP або задачі дискретного логарифмування для еліптичних кривих, є шифрування з відкритим ключем та алгоритм електронно-цифрового підпису.

Розглянемо принципи роботи еліптичного варіанту протоколу обміну ключами Діффі-Хеллмана. Протокол Діффі-Хеллмана є методом обміну криптографічними ключами, який дозволяє двом учасникам, що не мають попередньої інформації один про одного, отримати загальний секретний ключ. Цей ключ використовується для шифрування даних, що обмінюються сторонами через незахищений канал зв'язку. Отриманий ключ може бути використаний для шифрування подальших сеансів зв'язку, що використовують шифр з симетричним ключем [4, с. 8].

Припустимо, що існує еліптична крива, яка забезпечує високий рівень криптостійкісті (несуперсингулярну, в якій генеруюча точка $G = (x; y)$ має великий порядок, тобто число n , при якому $nG = O$ є дуже великим простим числом), визначена параметрами a та b :

$$y^2 = x^3 + ax + b$$

Позначимо персону відправника та сторону отримувача як A та B відповідно, тоді обмін ключами між сторонами A та B проводиться наступним чином:

1. Учасник A обирає ціле число, яке має бути менше за n, $PrivateKey_A < n$. Це число є приватним ключем, а точка еліптичної кривої $PublicKey_A = PrivateKey_A \times G$ називається публічним ключем.
2. Сторона B обирає так само секретний ключ $PrivateKey_B$ та обчислює відкритий ключ $PublicKey_B = PrivateKeyv_B \times G$.
3. Учасник A генерує секретний ключ $K_A = k_A \times P_B$, а учасник B генерує секретний ключ $K_B = k_B \times P_A$.

Формули, що отримані в п.3 дають один й той самий результат, оскільки:

$k_A \times P_B = k_A \times (k_B \times G) = k_B \times (k_A \times G) = k_B \times P_A$

Отже тримані секретні ключі K_A та K_B еквіваленті, тому їх можна використовувати для подальшого шифрування повідомлень із використанням симетричного алгоритму.

Далі розглянемо ECDSA – це один із варіантів алгоритму ЦП (DSA), який використовує еліптичні криві [4, с. 4]. Цифровий підпис повідомлення - це блок даних

невеликого розміру, отриманий внаслідок криптографічного перетворення повідомлення за допомогою особистого (закритого) ключа відправника. Невід'ємною частиною цифрового підпису є хеш-функція *H*, яка призначена для того, щоб стиснути повідомлення *M* довільної довжини до фіксованого бінарного хеш-значення *h*(*M*).

Аналогічно до ECDH, обидві сторони спочатку мають узгодити параметри еліптичної кривої *a* та *b*, базову точку $G = (x,y)$, просте число *p*, та *n* (просте число), таке що $nG = O$. Якщо розмір n в бітах менше розміру в бітах хеш-значення повідомлення $h(M)$, то використовуються тільки ліві біти хеш-значення – z.

Вираховується закритий ключ d – це випадкове ціле число, таке що $0 < d \leq n - 1$. Вираховується відкритий ключ $Q = dG$. Для створення підпису використовується приватний ключ, а для його перевірки - публічний. Процес підписування повідомлення складається з таких етапів:

1. Обирається випадковим чином ціле число k – одноразовий секретний ключ, де $0 < k \leq n - 1$.
2. Обчислюється $(x1,y1) = kG$
3. Обчислюється $r = x1 \bmod n$. Якщо $r = 0$, то переходимо до п. 1.
4. Обчислюється $s = k - 1 (z + dr) \bmod n$. Якщо $s = 0$, то переходимо до п.1.
5. Підписом для повідомлення M є пара (r, s).

Для перевірки підпису одержувач, отримавши пару (r, s) та підтверджене значення відкритого ключа Q, виконує наступні дії:

1. Обчислюється $w = s - 1 \bmod n$.
2. Обчислюється $u1 = z \cdot w \bmod n$ та $u2 = r \cdot w \bmod n$.
3. Обчислюється $(x1,y1) = u1G + u2Q$.
4. Якщо $(x1,y1) = O$ – цифровий підпис не є дійсним.
5. Якщо $r \equiv x1 \bmod n$ – цифровий підпис є дійсним.

Окрім форми Вейєрштрасса (що є винятком), еліптичні криві можуть бути виражені і в іншій формі. Наприклад, в формі Монтгомері рівняння еліптичної кривої має такий вигляд:

$$by^2 = x^3 + ax^2 + x, \tag{6}$$

де $a \neq \pm 2$ і $b \neq 0$.

З міркувань ефективності ECC часто застосовує криві Едвардса, які являють собою еліптичні криві у формі:

$$x^2 + ay^2 = 1 + dx^2y^2, \tag{7}$$

де $d \neq 1$ і $a \neq d$.

Всі три форми еліптичних кривих – Едвардса, Вейєрштрасса та Монтгомері – біраціонально еквівалентні, що робить їх використання ефективним без втрати інформації про криву.

Переваги над мультиплікативною групою лишків за модулем p, де p - просте число. Незважаючи на існування таких криптосистем, як Діффі-Хеллман, Ель-Гамаль, RSA і багато інших, виникла потреба використання нового криптографічного примітиву.

З моменту виникнення раніше згаданих криптосистем (Діффі-Хеллман – 1976[5], RSA - 1978, Ель-Гамаль – 1985[7]) обчислювальні можливості виявилися значно покращеними. Частота процесорів зростала з кілогерців до гігагерців, кількість ядер збільшилась від одиниць до сотень, і з'явилися зручні інструменти для об'єднання процесорів у кластери. З іншого боку, через бажання зламати ці криптосистеми, багато дослідників шукали способи знайти більш ефективні алгоритми для розв'язання

проблем, на яких вони ґрунтуються. У 1993 році Ленстра [8] пропонує ефективний алгоритм розкладання великих чисел на множники - GNFS(General Number Field Sieve), який здатний розкласти число $n > 10^{100}$ за час:

$$\exp(((\frac{64}{9})^{\frac{1}{3}} + o(1))(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}). \quad (8)$$

Це стало головною проблемою криптосистем, що базуються на мультиплікативних групах лишків по модулю p, далі - $\mathbb{Z} * p$. Це зводить обчислювальну складність задач, які лежать в основі цих криптосистем, до суб'експоненційних, а не експоненційних. Важливо зауважити, що цей алгоритм(запропонований Ленстра) не лише теоретична загроза. Наприклад, у 2019 році[9] використовуючи цей алгоритм, було знайдено дискретний логарифм 795-бітного числа. У зв'язку з цим, рекомендований розмір ключів в оригінальному патенті RSA [6] складав 200 біт, у першій сертифікації від NIST - 512 біт, а наразі мінімальний рекомендований розмір становить 2048 біт. Також слід відзначити, що GNFS не можна застосувати до будь-яких скінчених циклічних груп, через це він не впливає на групу точок еліптичної кривої над скінченними полями. Через це найкращий відомий алгоритм для вирішення проблеми дискретного логарифма для групи точок еліптичних кривих (ECDLP) вимагає часу $O(\sqrt{q})$, де q - розмір групи. Тому розміри ключів, які забезпечують однаковий рівень безпеки для $\mathbb{Z} * p$ і для групи точок еліптичної кривої сильно відрізняються. Нижче приведена порівняльна характеристика безпеки ключа залежно від їхнього розміру для RSA/Diffie-Hellman і ECC:

Таблиця 1 – NIST рекомендовані розміри ключів

Розмір ключа RSA та Діффі-Хеллмана (біти)	Розмір ключа для еліптичних кривих (біти)	Симетричний розмір ключа (біти)
1024	160	80
2048	224	112
3072	256	128
7680	384	192
15360	521	256

Джерело: [18]

Як видно з вище наведеної таблиці, використання еліптичних кривих має значні переваги, оскільки ключі мають невелику довжину, що призводить до швидких обчислень на еліптичних кривих. Це сприяє високій швидкодії обробки даних та підвищує продуктивність систем, особливо у ситуаціях, коли потрібно провести велику кількість криптографічних операцій. Особливо це видно у сфері серверних технологій, де використання еліптичних кривих сприяє прискоренню TLS-рукостискання, що призводить до швидкого завантаження веб-сторінок та підвищення рівня безпеки. Важливо також зазначити, що менша довжина ключа призводить до того, що пристрої вимагають менше обчислювальних ресурсів для виконання криптографічних операцій, що робить ECC гарним рішенням для мобільних пристроїв, систем IoT та інших пристроїв з обмеженою обчислювальною потужністю.

Ще однією перевагою криптографії на еліптичних кривих (ECC) є можливість використання багатьох розробок з криптографії з відкритим текстом, що працює з групою за модулем $\mathbb{Z} * p$. Це пояснюється тим, що ECC використовує складну обчислювальну проблему, пов'язану із знаходженням дискретного логарифма (DLP). Для еліптичних кривих ця проблема відома як ECDLP і є аналогічною складній обчислювальній задачі у Діффі-Хеллмана і Ель-Гамаля. Крім того, еліптичні криві мають додаткову структуру, яку не має мультиплікативна група за модулем $\mathbb{Z} * p$, що

дозволяє створювати криптосистеми, неможливі для $\mathbb{Z}^*_p$. Такою додатковую структурою є можливість будувати спарювання точок еліптичних кривих, алгебраїчні решітки та ізогенії. Алгебраїчні решітки та ізогенії еліптичних кривих активно використовуються для розробки пост-квантових криптосистем з відкритим ключем.

Стандартизація еліптичних кривих у криптографії. Ідея використовувати еліптичні криві для криптографії з'явилась у 1985 році. Незалежно один від одного її запропонували два вчених: Ніл Кобліц та Віктор Міллер. Кобліц висунув теорію, що криптосистеми на основі еліптичних кривих (ECC) будуть стійкішими, ніж традиційними асиметричні алгоритмами. Це пов'язано із тим, що задача дискретного логарифмування в групі точок еліптичної кривої є складнішою для розв'язання, ніж стандартна задача дискретного логарифмування [10]. Міллер дослідив математичні властивості еліптичних кривих і зрозумів, що їх можна використовувати в протоколі обміну ключами Діффі-Хеллмана [5,11].

Хоча еліптична криптографія (ECC) існувала вже з 1980-х років, вона не знаходила широкого практичного застосування до початку 2000-х років. З того часу ECC стала революційною технологією в галузі криптографії. На даний момент використання еліптичних кривих для вирішення криптографічних задач визнано і закріплено в різних міжнародних та американських стандартах, у тому числі:

- ANSI X9.62 та ANSI X9.63 – були створені 1999 та 2001 року American National Standards Institute (ANSI) та комітетом X9. Ці стандарти описують алгоритми криптографії на основі еліптичних кривих (ECC) і описують протоколи ECDSA в ANSI X9.62 та ECIES, ECDH і ECMQV в ANSI X9.63. Ці стандарти визначають формати повідомлень, рекомендовані криві та методи підпису та обміну ключами на еліптичних кривих. Вони широко використовуються у фінансовій секторі для захисту фінансових операцій, включаючи підтвердження платіжних транзакцій [12], [13].

- IEEE 1363. Він включає в себе практично всі алгоритми з публічним ключем, в тому числі ECDSA (Elliptic curve digital signature algorithm), ECIES (Elliptic curve integrated encryption scheme), ECMQV (Elliptic curve Menezes-Qu-Vanstone) і ECDH. До того ж, у додатку цього стандарту містяться всі базові теоретико-числові алгоритми, необхідні для криптографії з публічним ключем [14].

- FIPS 186-3 (2009 рік), FIPS 186-4 (2013 рік) та FIPS 186-5 (2023 рік) – це стандарти, прийняті National Institute of Standards and Technology (NIST), що регламентують використання алгоритмів цифрового підпису (ЦП), зокрема ECDSA (алгоритм цифрового підпису на еліптичних кривих). Ці стандарти також надають список рекомендованих кривих та їх параметрів, що сприяє створенню безпечних і надійних систем цифрового підписування та забезпечує відповідність до сучасних вимог у сфері криптографічної безпеки [15].

- ISO/IEC 15946-4:2004 та ISO/IEC 15946-5:2022– це міжнародні стандарти, які входять до серії стандартів ISO/IEC 15946, прийнятих International Organization for Standardization (ISO) та International Electrotechnical Commission IEC). Стандарт ISO/IEC 15946-4 встановлює вимоги та рекомендації щодо генерації та перевірки електронних підписів на основі еліптичних кривих[16], тоді як ISO/IEC 15946-5 визначає методи створення еліптичної кривої над скінченним полем[17]. В окремому розділі цієї статті будуть розглянуті національні стандарти України, які регулюють використання еліптичних кривих для захисту криптографічної інформації

Паралельно із загальними стандартами, існують Request for Comments документи, далі просто RFC-документи, такі як RFC 7748 та RFC 8032, які описують використання конкретних еліптичних кривих, наприклад, Curve25519 та Ed25519, у протоколах обміну ключами та цифрового підпису.

Документ RFC 7748 визначає дві еліптичні криві над простими полями, такі як Curve25519 та Curve448, які пропонуються високий рівень практичної безпеки в криптографічних додатках, включаючи захист транспортного рівня (TLS). Ці криві призначені працювати на ~128-бітному та ~224-бітному рівні безпеки відповідно, і генеруються детерміновано на основі списку необхідних властивості [19].

А у документі RFC 8032 описана схема підпису еліптичної кривої Едвардса за допомогою алгоритму цифрового підпису (EdDSA). Цей алгоритм створено із рекомендованими параметрами для edwards25519 та edwards448 кривих [20].

Згадані RFC-документи важливі для визначення конкретних еліптичних кривих та їх параметрів, що можуть бути використані в криптографічних протоколах. Curve25519 використовується в протоколах обміну ключами, таких як Signal Protocol, і забезпечує ефективну та безпечну обмін ключами для забезпечення конфіденційності та цілісності даних. Аналогічно, Ed25519 є алгоритмом цифрового підпису, який базується на Curve25519 та забезпечує ефективність та високий рівень безпеки для підпису повідомлень.

Ці стандарти встановлюють загальноприйняті параметри для еліптичних кривих, роблячи їх доступними для широкого кола розробників та користувачів. Застосування стандартів у практиці демонструється в різних сферах, таких як криптовалютні системи (наприклад, Bitcoin, який використовує ECDSA), протоколи обміну даними (TLS/SSL, що використовує ECC), а також платіжні технології (Android Pay, Apple Pay), які використовують еліптичну криптографію для забезпечення безпеки та цифрового підпису.

Таким чином, стандартизація еліптичних кривих визначає єдині принципи для створення безпечних та ефективних криптографічних систем, що дозволяє їхню стандартизовану реалізацію та взаємодію в різних додатках та протоколах.

Аналіз сучасного стану стандартизації ЕСС в Україні. Головним документом, який встановлює правила для створення та перевірки цифрового підпису, є Національний стандарт ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що базується на використані еліптичних кривих. Формування та перевірка» [21]. Однак, варто зауважити, що цей стандарт залишається без оновлень з моменту його прийняття в 2002 році, незважаючи на рекомендації світових експертів про необхідність оновлення криптографічних стандартів кожні 4-5 років [26].

Національний стандарт ДСТУ 4145-2002 визначає механізм цифрового підписування, що ґрунтується на властивостях груп точок еліптичних кривих над полями $GF(2m)$. Він регламентує використання еліптичних кривих над скінченним полем $GF(2m)$ та встановлює правила застосування цього механізму до повідомлень, що пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення [21].

Відповідно до стандарту, використання еліптичних кривих з параметрами, наведеними в окремому додатку, дозволено лише згідно з визначеними алгоритмами перевірки правильності вибору рівняння еліптичної кривої та базової точки.

Хоча ДСТУ 4145-2002 є досить гнучким стандартом щодо вибору параметрів безпеки, у тому числі функції хешування та генератора псевдовипадкових чисел, він все ж відстає за сучасними стандартами криптографічної безпеки. Зокрема, існують обґрунтовані обговорення щодо вразливостей кривих над полями характеристики 2, які можуть бути використані для атак злому систем.

Нині близько 10% використання цифрового підпису в Україні ґрунтується на ДСТУ 4145-2002, що значно менше, ніж у випадку стандартів, що включають RSA та ECDSA. Це обумовлено, зокрема, відсталістю стандарту, а також існуючими вразливостями, які можуть порушити безпеку системи. Водночас, електронні

документи, підписані за допомогою цифрового підпису, мають юридичну силу, що дає певну правову базу для їх використання в електронному документообігу [26].

Також Чинний стандарт, прийнятий в Україні, не відповідає міжнародним стандартам щодо електронного підпису. Проблема недостатньої відповідності міжнародним стандартам у сфері електронного підпису висвітлена у пункті 4.11 Концепції, де особлива увага приділяється необхідності розробки механізмів для ефективної взаємодії України з іншими державами в рамках юридично значущого електронного документообігу. [23, с. 23], [2].

Очевидно, що ДСТУ 4145-2002 потребує оновлення з урахуванням сучасних вимог криптографічної безпеки та викликів, які ставлять перед ним розвиток технологій та методів кібератак.

У 2020 році в Україні запроваджено новий Національний стандарт ДСТУ 9041-2020 "Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса" [22] визначає методи шифрування коротких повідомлень до шістсот шістнадцяти біт. Новий алгоритм, порівняно зі стандартом цифрового підпису ДСТУ 4145-2002, використовує криптографічні перетворення у групі точок еліптичних кривих, застосовуючи криві у формі Едвардса, замість кривих у формі Вейєрштрасса. Це призводить до значного покращення швидкодії більш ніж у три рази. Новий стандарт розроблений з урахуванням усіх сучасних вимог до стійкості криптографічних алгоритмів та відповідає всім актуальним вимогам.

У додаток до цього, ДСТУ 9041-2020 відповідає міжнародним стандартам та враховує усі найсучасніші підходи до криптографічного захисту інформації. Стандарт узгоджений з усіма чинними національними стандартами в Україні. Його особливості включають відносно невелику довжину ключа, застосування передових математичних методів та новий алгоритм створення псевдовипадкових послідовностей. На відміну від аналогічного алгоритму у ДСТУ 4145-2002, цей новий підхід використовує виключно національні криптографічні алгоритми і не посилається на відповідні стандарти пострадянського періоду, чий термін дії вже майже минув.

У червні 2023 року було замінено стандарт ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017, IDT) на стандарт ДСТУ ISO/IEC 15946-5:2023 (ISO/IEC 15946-5:2022, IDT). Цей встановлює методи криптографії з відкритим ключем, які базуються на еліптичних кривих, описаних у ISO/IEC 15946-1. Він визначає методи генерації еліптичних кривих для впровадження механізмів на базі еліптичних кривих, що визначені у, ISO/IEC 14888-3, ISO/IEC 29192-4, ISO/IEC 11770-3, ISO/IEC 9796-3, ISO/IEC 18033-2 та ISO/IEC 18033-5. Цей документ застосовний до криптографічних методів, заснованих на еліптичних кривих, визначених над скінченними полями простого порядку ступеня (включаючи спеціальні випадки простого порядку та дві характеристики) [24].

У порівнянні зі стандартами ДСТУ 4145 і ДСТУ 9041, стандарт ДСТУ ISO/IEC 15946-5:2023 має кілька переваг. Він надає більш широкий набір параметрів для генерації кривих, що дозволяє вибирати криві з різними характеристиками залежно від конкретних потреб застосування. Крім того, цей стандарт використовує найсучасніші методи генерації еліптичних кривих, що забезпечує їхню стійкість та ефективність у сучасних криптографічних системах.

Атаки на ECC. Незважаючи на високий рівень стійкості, ECC, як і будь-яка криптографічна система, не є абсолютно захищеною від атак. З розвитком обчислювальних технологій зростає й потреба в постійному вдосконаленні методів захисту. Розглянемо деякі види можливих атак на ECC:

1. Атака грубою силою - це найпростіший метод атаки на будь-яку криптографічну систему, включаючи ECC, яка полягає у переборі всіх можливих

комбінацій для знаходження приватного ключа. Хоча ECC рекомендує використовувати ключі довжиною не менше сто двадцяти восьми біт для захисту від атак грубої сили, зростання обчислювальних потужностей може зробити цей захист вразливим у майбутньому. Тому важливо обирати ключі достатньої довжини та ретельно підбирати параметри кривих [27].

2. Атака по бічному: моніторинг фізичних параметрів криптосистеми (споживання енергії, електромагнітне випромінювання) під час виконання криптографічних операцій для отримання інформації про ключ. Якщо мінімізувати електричне споживання та випромінювання під час математичних операцій, наприклад, шумові імпульси, то це буде захистом від цієї атаки [27].

3. Квантова атака з використанням квантових обчислювальних систем. Використання квантових обчислювальних систем у квантовій атаці може становити загрозу для алгоритмів ECC, таких як ECDSA та ECDH, які ефективно розв'язують задачу дискретного логарифмування в групі точок еліптичної кривої за допомогою алгоритму Шора. Це може створити серйозні проблеми для безпеки ECC, тому зусилля спрямовані на створення постквантових криптографічних алгоритмів, що залишаються стійкими до квантових атак. Необхідно підкреслити, що різні еліптичні криві можуть мати різний рівень захисту від криптоаналізу, різну ефективність та використовувати різні методи та розміри ключів. [27].

Для вибору певної еліптичної кривої важливо враховувати потреби та вимоги конкретної системи. Рекомендується використовувати стандартизовані криві, щоб забезпечити сумісність з іншими протоколами та системами. Як приклад можна навести такі криві як NIST P-256, Curve25519, BrainpoolP256r1 [25].

Висновки. Криптографія на еліптичних кривих (ECC) на сьогодні є одною із основ для розробки сучасних криптографічних алгоритмів з відкритим ключем. ECC здобула визнання в криптографії, через забезпечення високого рівня безпеки за умови використання більш коротких довжин ключів (порівняно з іншими криптографічними підходами), високу швидкість, економію ресурсів та універсальність, що дає їй перевагу над іншими методами, такі як RSA та інші. Вона забезпечує безпечне мережеве з'єднання, генерує секретні ключі для TLS-серверів та їх клієнтів, а також використовується для створення цифрових підписів, які гарантують автентичність транзакцій у криптовалютних системах.

ECC також застосовується в мобільних додатках для шифрування голосових викликів, відеодзвінків та обміну повідомленнями. Окрім цього, ECC використовується для захисту зв'язку, забезпечення цілісності даних та автентифікації пристроїв IoT. Завдяки своїй стійкості та ефективності, ECC стає все більш популярним інструментом для забезпечення кібербезпеки.

Алгоритми і протоколи ECC включені до різних міжнародних та американських стандартів, таких як ANSI X9.62, ANSI X9.63, IEEE 1363, FIPS 186, та ISO/IEC 15946. Ці стандарти встановлюють формати повідомлень, рекомендовані криві та методи для підпису та обміну ключами на еліптичних кривих, забезпечуючи високий рівень безпеки та ефективності. Крім них є документи RFC, зокрема RFC 7748 та RFC 8032, які описують використання еліптичних кривих у протоколах обміну ключами та цифрового підпису. У нашій країні закріплені в таких державних стандартах як ДСТУ 4145-2002, ДСТУ 9041-2020 та ДСТУ 15946-2023.

Еліптична криптографія (ECC) представляє собою нове покоління криптосистем з відкритим ключем, що базується на зрозумілих математичних принципах і забезпечує більш високий рівень безпеки порівняно з традиційними системами. На сьогоднішній день не існує алгоритмів з субекспоненційною складністю для знаходження дискретного логарифму в групі точок еліптичних кривих над скінченними полями, що

забезпечує надійність ECC. Однак, криптографія на еліптичних кривих також стикається з викликами і проблемами. Розробка безпечних криптосистем на основі еліптичних кривих вимагає додаткових знань і експертизи порівняно з традиційними алгоритмами криптографії. Вибір вірних параметрів кривих є критично важливим для забезпечення безпеки ECC. Крім того, з часом алгоритми на еліптичних кривих можуть втратити свою криптостійкість через квантові обчислення. Алгоритм Шора, наприклад, може швидко зламати алгоритм на основі ECC за допомогою гіпотетичного квантового комп'ютера. Таким чином, майбутні дослідження в області криптографії на еліптичних кривих будуть спрямовані на аналіз забезпечення стійкості ECC перед квантовими атаками і розробку нових квантовостійких алгоритмів, протоколів і рішень, що підвищать безпеку та ефективність криптосистем на еліптичних кривих.

Список літератури

1. Дичка А. І. Модифікований метод багатократного скалярного множення точок еліптичної кривої у скінченних полях: магістерська дисертація. 2018 URL: https://ela.kpi.ua/bitstream/ 123456789/ 23653/1/Dychka_magistr.pdf
2. Горбенко Ю., Горбенко І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. Харків : Форт, 2010. 608 с.
3. Koblitz N. Elliptic Curve Cryptosystems. *Mathematics of Computation*. 1987. Vol. 48, № 177. P. 203-209.
4. Blake I. F., Smart N. P., Seroussi G. Advances in elliptic curve cryptography. Cambridge University. 2009.
5. Diffie W., Hellman M. E., New directions in cryptography. 1976. Vol. 22, No 6. P. 644-654. URL: https://ee.stanford.edu/~hellman/publications/24.pdf
6. Rivest R. L., Shamir A., Adleman L., A method for obtaining digital signatures and public-key cryptosystems, 1985. URL: https:// people.csail.mit.edu/rivest/Rsapaper.pdf
7. ElGamal T. Public key cryptosystem and a signature scheme based on discrete logarithms. 1985. URL: https://caislab.kaist.ac.kr/lecture/2010/ spring/cs548/basic/B02.pdf
8. Arjen K. Lenstra, H. W. Lenstra. The development of the number field sieve. Lecture Notes in Mathematics (LNM). 1993. Vol. 1554.
9. Dan Boneh, and Victor Shoup, A Graduate Course in Applied Cryptography, 2023. URL: http://toc.cryptobook.us/book.pdf
10. Koblitz, N. Elliptic curve cryptosystems. Mathematics of computation, 1987. Vol.48, № 177. P. 203. URL:https://doi.org/10.1090/s0025-5718-1987-0866109-5.
11. Miller, V.S. Use of elliptic curves in cryptography. Lecture notes in computer science. 2000. Vol. 218P. 417–426. URL:https://doi.org/10.1007/3-540-39799-x_31.
12. ANSI X9.62. Public key cryptography for the financial services industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, Washington. 1999
13. ANSI X9.63. Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography. American National Standards Institute, Washington. 2001.
14. IEEE P1363/D9(Draft Version 9). Standard Specifications for Public Key Cryptography, 1999
15. Digital Signature Standard (DSS). National Institute of Standards and Technology, U.S. Department of Commerce, Washington. URL:https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.
16. ISO/IEC 15946-4. Information technology. Security techniques. Cryptographic techniques based on elliptic curves. Part 4: Digital signatures giving message recovery, Geneva.
17. ISO/IEC 15946-5. Information technology. Security techniq
18. Saho, N.J.G., Ezin, E.C. Comparative study on the performance of elliptic curve cryptography algorithms with cryptography through RSA algorithm. 2020. CARI. URL:https://hal.science/hal02926106/document?ref=panther-protocol-blog
19. Elliptic Curves for Security RFC 7748. URL: https://datatracker.ietf.org/doc/html/rfc7748 (дата звернення: 15.03.2024)
20. Edwards-Curve Digital Signature Algorithm (EdDSA) RFC 8032. URL: https://datatracker.ietf.org/doc/html/rfc8032 (дата звернення: 15.03.2024)
21. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. [Чинний від 1 липня 2003 року]. Київ, Держстандарт України.
22. ДСТУ 9041-2020. Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. [Чинний від 01.11.2020 року]. Київ, Держстандарт України.

23. Забенько Ю. І., Ковтанюк Ю. С. Концепція планування життєвого циклу електронних документів. *Архіви України*. 2013. Вип. 4. С. 5-38.
24. ДСТУ ISO/IEC 15946-5:2023 Інформаційні технології. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих (ISO/IEC 15946-5:2022, IDT). [Чинний від 25 червня 2003 року]. Київ, Держстандарт України.
25. SafeCurves: [choosing safe curves for elliptic-curve cryptography]. URL: https://safecurves.cr.yp.to/
26. Циганкова,О.В. Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса: дис... канд. техн.: 28.04.2021/ Київ, 154 с.
27. Щур, Н., Покотило, О., Байлюк, Є. Криптографія на еліптичних кривих та її практичне застосування. *Кібербезпека: освіта, наука, техніка*. 2023. Вип. 1(21), С. 48–64. URL:https://doi.org/10.28925/2663-4023.2023.21.4864

References

1. Dychka, A. I. (2018). Modified method of multiple scalar multiplication of elliptic curve points in finite fields: master's thesis [Modyfikovanyj metod bahatokratnoho skaliarnoho mnozhennia tochok eliptychnoi kryvoi u skinchennykh poliakh]. *Master's thesis* URL: https://ela.kpi.ua/bitstream/123456789/23653/1/Dychka_magistr.pdf [in Ukrainian].
2. Horbenko, Yu. & Horbenko, I. (2010). Infrastruktury vidkrytykh kliuchiv. Elektronnyj tsyfrovyj pidpys. Teoriia ta praktyka : monohrafiia [Public key infrastructures. Electronic digital signature. Theory and practice]. Kharkiv: Fort [in Ukrainian].
3. N.Koblitz. (1987) Elliptic Curve Cryptosystems // Mathematics of Computation. Vol. 48, № 177. P. 203-209.
4. Blake, I. F., Smart, N. P., Seroussi, G.(2009) Advances in elliptic curve cryptography. Cambridge University.
5. Diffie W., Hellman M. E.. (1976) New directions in cryptography. URL: https://ee.stanford.edu/~hellman/publications/24.pdf
6. Rivest R. L., Shamir A., Adleman L..(1985) A method for obtaining digital signatures and public-key cryptosystems. URL: https:// people.csail.mit.edu/rivest/Rsapaper.pdf
7. ElGamal T.. (1985) Public key cryptosystem and a signature scheme based on discrete logarithms. URL: https://caislab.kaist.ac.kr/lecture/2010/ spring/cs548/basic/B02.pdf
8. Arjen K., Lenstra H.. (1993) The development of the number field sieve. Lecture Notes in Mathematics (LNM), Vol. 1554.
9. Boneh D., Shoup V./ (2023) A Graduate Course in Applied Cryptography. URL: http://toc.cryptobook.us/book.pdf
10. Koblitz, N.. (1987) Elliptic curve cryptosystems. Mathematics of computation, Vol.48, № 177. P. 203. URL:https://doi.org/10.1090/s0025-5718-1987-0866109-5.
11. Miller V.S. (2020) Use of elliptic curves in cryptography. Lecture notes in computer science, P. 417–426. URL:https://doi.org/10.1007/3-540-39799-x_31.
12. ANSI X9.62. Public key cryptography for the financial services industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, Washington. 1999
13. ANSI X9.63. Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography. American National Standards Institute, Washington. 2001.
14. IEEE P1363/D9(Draft Version 9). Standard Specifications for Public Key Cryptography, 1999
15. Digital Signature Standard (DSS). National Institute of Standards and Technology, U.S. Department of Commerce, Washington. URL:https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.
16. ISO/IEC 15946-4. Information technology. Security techniques. Cryptographic techniques based on elliptic curves. Part 4: Digital signatures giving message recovery, Geneva.
17. ISO/IEC 15946-5. Information technology. Security techniq
18. Saho, N.J.G., Ezin, E.C.. (2020) Comparative study on the performance of elliptic curve cryptography algorithms with cryptography through RSA algorithm. CARI. URL:https://hal.science/hal02926106/document?ref=panther-protocol-blog
19. Elliptic Curves for Security RFC 7748. URL: https://datatracker.ietf.org/doc/html/rfc7748
20. Edwards-Curve Digital Signature Algorithm (EdDSA) RFC 8032. URL: https://datatracker.ietf.org/doc/html/rfc8032
21. Informatsijni tekhnolohii. Kryptohrafichnyj zakhyst informatsii. Tsyfrovyj pidpys, scho gruntuiet'sia na eliptychnykh kryvykh. Formuvannia ta pereviriannia [Information Technology. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification] (2003). *DSTU 4145-2002 from July 1, 2003*. Kyiv: State Standard of Ukraine [in Ukrainian].
22. Informatsijni tekhnolohii. Kryptohrafichnyj zakhyst informatsii. Alhorytm shyfruvannia korotkykh povidomlen', scho gruntuiet'sia na skruchenykh eliptychnykh kryvykh Edvardsa [Information Technology. Cryptographic protection of information. Short Message Encryption Algorithm Based on

Twisted Edwards Elliptic Curves] (2020). *DSTU 9041-2020 from November 1, 2020*. Kyiv: Derzhstandart Ukrainy [in Ukrainian].
23. Zaben'ko, Yu. I. & Kovtaniuk, Yu. S. (2013). Kontseptsiia planuvannia zhyttievoho tsyklu elektronnykh dokumentiv [The concept of planning the life cycle of electronic documents]. *Arkhivy Ukrainy – Archives of Ukraine, 4,* 5-38 [in Ukrainian].
24. Informatsijni tekhnolohii. Kryptohrafichni metody na osnovi eliptychnykh kryvykh. Chastyna 5. Heneruvannia eliptychnykh kryvykh [Information technologies. Cryptographic methods based on elliptic curves. Part 5: Generation of elliptic curves] (2023). *DSTU ISO/IEC 15946-5:2023 from June 25, 2003.* Kyiv: Derzhstandart Ukrainy [in Ukrainian].
25. SafeCurves: [choosing safe curves for elliptic-curve cryptography]. URL: https://safecurves.cr.yp.to/
26. Tsyhankova,O.V. (2021). Metody pidvyschennia shvydkodii asymetrychnykh kryptosystem z vykorystanniam eliptychnykh kryvykh u formi Edvardsa [Methods of increasing the speed of asymmetric cryptosystems using elliptic curves in the form of Edwards]. *Candidate's thesis.* Kyiv [in Ukrainian].
27. Schur, N., Pokotylo, O. & Bajliuk, Ye. (2023). Kryptohrafiia na eliptychnykh kryvykh ta ii praktychne zastosuvannia [Elliptic curve cryptography and its practical application.]. *Kiberbezpeka: osvita, nauka, tekhnika – Cyber security: education, science, technology, 1(21),* 48–64. URL:https://doi.org/ 10.28925/2663-4023.2023.21.4864 [in Ukrainian].

Oleksandr Ulichev, PhD tech. sci., **Kostyantyn Zadorozhny**, student
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Standardization of elliptic curves: analysis and implementation in cryptographic protocols

The purpose of the article is to consider the current state of elliptic cryptography, the prerequisites for its use, as well as the requirements of modern standards related to the use of elliptic cryptography

The use of elliptic curves in cryptography is considered one of the most promising areas of development of modern security algorithms. This mathematical approach is based on the complexity of solving the discrete logarithm problem in a group of points of an elliptic curve over a finite field. The use of cryptography on elliptic curves allows you to ensure the security of data exchange using effective encryption algorithms and the creation of digital signatures (DI). This study examines elliptic curves for cryptographic purposes, and provides basic operations on the point group of elliptic curves. Special attention is paid to Elliptic curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) key exchange algorithms. The standards regulating the use of elliptic curves in cryptographic systems are also analyzed, and the advantages of this cryptographic paradigm compared to the main asymmetric algorithms are considered. Potential threats and vulnerabilities of cryptographic algorithms based on elliptic curves are investigated. Examples of popular standardized curves recommended by relevant organizations, such as NIST, used in real-world cryptographic applications are also provided.

Elliptic curve cryptography (ECC) is currently one of the foundations for the development of modern public-key cryptographic algorithms. ECC has gained recognition in cryptography for providing a high level of security with shorter key lengths (compared to other cryptographic approaches), high speed, resource savings, and versatility, giving it an advantage over other methods such as RSA and others. It provides a secure network connection, generates secret keys for TLS servers and their clients, and is also used to create digital signatures that guarantee the authenticity of transactions in cryptocurrency systems.

cryptography on elliptic curves, asymmetric cryptosystems, digital signature on elliptic curves, ECC (Elliptic Curve Cryptography), ECDH, ECDSA, RFC

Одержано (Received) 22.01.2024 *Прорецензовано (Reviewed) 08.03.2024*
Прийнято до друку (Approved) 25.03.2024