КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1(21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.4864
УДК 004.056.55

Щур Наталія Олександрівна
старший викладач кафедри комп'ютерної інженерії та кібербезпеки
державний університет «Житомирська політехніка», Житомир, Україна
ORCID ID: 0000-0002-1182-4799
thalitana@gmail.com

Покотило Олександра Андріївна
старший викладач кафедри комп'ютерної інженерії та кібербезпеки
державний університет «Житомирська політехніка», Житомир, Україна
ORCID ID: 0000-0002-1587-235X
kik_poa@ztu.edu.ua

Байлюк Єлизавета Максимівна
старший викладач кафедри комп'ютерної інженерії та кібербезпеки
державний університет «Житомирська політехніка», Житомир, Україна
ORCID ID: 0000-0002-4961-7816
liza.bailiuk@gmail.com

КРИПТОГРАФІЯ НА ЕЛІПТИЧНИХ КРИВИХ ТА ЇЇ ПРАКТИЧНЕ ЗАСТОСУВАННЯ

Анотація. Еліптичні криві є одним із найперспективніших інструментів для побудови сучасних криптографічних алгоритмів. Безпека криптографії на еліптичних кривих ґрунтується на складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої над скінченним полем. Криптографія на еліптичних кривих дає змогу реалізувати захищений обмін даними між різними сторонами, використовуючи алгоритми шифрування та підписування на основі еліптичних кривих. Еліптичні криві дозволяють досягти еквівалентного рівня безпеки з меншими розмірами ключів порівняно з іншими асиметричними криптографічними алгоритмами. У статті описано математичний апарат еліптичних кривих, що використовуються для криптографічних цілей, наведено основні операції в групі точок еліптичних кривих, такі як додавання точок, подвоєння точки та скалярне множення точки на число. Розглянуто кроки і принципи роботи алгоритму обміну ключами Діффі-Хеллмана (ECDH) та схеми цифрового підпису (ECDSA) на еліптичних кривих. Проведено огляд стандартів, що встановлюють рекомендації та вимоги щодо використання еліптичних кривих у криптографічних системах. Проаналізовано переваги криптографії на еліптичних кривих порівняно із традиційними асиметричними алгоритмами, такі як менші розміри ключів, швидкість обчислень та ефективне використання ресурсів. Розглянуто потенційні загрози та вразливості криптографічних алгоритмів на основі еліптичних кривих. Здійснено огляд основних сфер практичного застосування криптографічних алгоритмів на еліптичних кривих, зокрема таких як захист мережевого з'єднання, криптовалютні операції, обмін повідомленнями, Інтернет речей, державні установи. Наведено приклади популярних стандартизованих кривих (Curve25519, Curve448, secp256k1), що були перевірені та рекомендовані спеціалізованими організаціями, зокрема такими як NIST.

Ключові слова: криптографія на еліптичних кривих; асиметричні криптосистеми; алгоритм обміну ключами Діффі-Хеллмана; цифровий підпис на еліптичних кривих; ECC; ECDH; ECDSA

ВСТУП

Безпека інформаційних систем є одним із пріоритетних напрямків розвитку сучасних технологій. Важливим засобом, що використовується для захисту інформації в комп'ютерних системах, є криптографічні перетворення.

Криптографія на еліптичних кривих (Elliptic Curve Cryptography, ECC) – це сучасне сімейство криптосистем із відкритим ключем, що базується на алгебраїчних структурах еліптичних кривих над скінченними полями та на складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem, ECDLP). ECC використовує властивості еліптичних кривих для створення криптографічних протоколів та алгоритмів, які можуть гарантувати високий рівень безпеки за відносно невеликої довжини ключа. ECC реалізує всі основні функції асиметричних криптосистем такі як шифрування, підписи та обмін ключами.

Постановка проблеми. Поява квантових комп'ютерів ставить під загрозу деякі класичні криптографічні протоколи, оскільки вони можуть ефективно розв'язувати складні математичні задачі, які лежать в основі більшості криптосистем. Крім того, традиційні асиметричні криптографічні алгоритми, такі як RSA та DSA, можуть стикатися з проблемами щодо ефективності та безпеки при використанні ключів великої довжини. Тому виникає потреба у застосуванні криптографічних алгоритмів, які були б стійкими до квантових атак, ефективнішими з точки зору продуктивності та забезпечували б високий рівень безпеки для комунікації та обміну даними.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження криптосистем на еліптичних кривих зробили такі зарубіжні вчені як N. Koblitz [1], V. Miller [2], A. Menezes [3], S. Vanstone [4], D. Bernstein [5], T. Lange [6], L. Washington [7], H. Edwards [8] та інші.

Різні методи криптографічного захисту інформаційних ресурсів, засновані на особливостях перетворень в групі точок еліптичних кривих висвітлювали такі вітчизняні науковці як Юдін О.К., Вадясов К.А. [9], Чевардін В.Є., Пономарьов О.А. [10]. Дослідженню властивостей еліптичних кривих у формі Едвардса присвячено праці Бессалова А.В. [11], Циганкової О.В. [12], Беспалова О.Ю., Н.В. Кучинської [13], Ковальчук Л.В. [14], Скуратовського Р.В. [15].

Перспективи розвитку цифрових підписів на основі властивостей груп точок еліптичної кривої розглянуто в працях Ільєнко А.В., Ільєнко С.С., Мазур Я.С., Прокопенко О.В. [16], Нікуліщева Г.І. [17].

Сучасні напрями застосування еліптичних кривих в криптографії розглянуто у роботах Мелешко О.О., Ковальського О.О. [18], R. Harkanson, Y. Kim [19].

Незважаючи на вивченість предмету, не усі сфери практичного застосування ECC мають достатнє висвітлення у науковій літературі, що стало підґрунтям для вибору теми нашого дослідження.

Мета статті. Метою статті є розглянути криптографію на еліптичних кривих як альтернативу традиційним асиметричним криптографічним методам та дослідити сучасні тенденції практичного застосування ECC. Основні завдання дослідження полягають у огляді теорії еліптичних кривих у контексті криптографії, описі найпоширеніших криптографічних алгоритмів, які використовують еліптичні криві, таких як ECDH та ECDSA, розгляді прикладів практичного застосування криптографії на еліптичних кривих у різних сферах.

ISSN 2663 - 4023

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Криптографія на еліптичних кривих вивчає асиметричні криптосистеми, засновані на еліптичних кривих над скінченими полями. Використання еліптичних кривих у криптографії було незалежно запропоновано Нілом Кобліцом та Віктором Міллером у 1985 році. Ніл Кобліц припустив, що ECC забезпечуватиме кращий захист порівняно із звичайними асиметричними алгоритмами, оскільки задача дискретного логарифмування в групі точок еліптичної кривої є складнішою для розв'язання ніж стандартна задача дискретного логарифмування [1]. Віктор Міллер дослідив математичні властивості еліптичних кривих та дійшов висновку, що еліптичні криві можна застосувати до протоколу обміну ключами Діффі-Хеллмана [2].

У спрощеному вигляді еліптична крива описується рівнянням (форма Вейєрштрасса):

$$y^2 = x^3 + ax + b \quad (1)$$

Залежно від значень параметрів a і b еліптичні криві можуть приймати на площині різні форми. Так як $y = \pm\sqrt{x^3 + ax + b}$, то графік кривої симетричний відносно *Ox*.

Дискримінант рівняння: $D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$:

- $D < 0$ – три різних дійсних корені (рис.1, графік 1);
- $D = 0$ – три дійсних корені, два з яких однакові (рис.1, графік 2 – сингулярна крива, такі криві виключають з розгляду);
- $D > 0$ – один дійсний корінь та два комплексних (рис.1, графік 3).

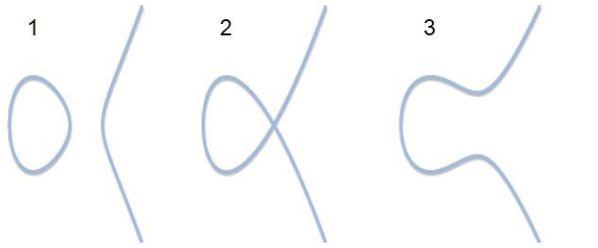

Рис. 1. Варіанти еліптичних кривих при $D < 0$, $D = 0$ *та* $D > 0$

У багатьох реальних криптосистемах використовуються еліптичні криві над простим скінченним полем $F(p)$, що описуються рівнянням:

$$y^2 \equiv x^3 + ax + b \ (mod\ p), \quad (2)$$

де $(x,\ y)$ – точки еліптичної кривої, $a,\ b$ – параметри еліптичної кривої, p – просте число ($p \neq 2,\ p \neq 3$). При цьому параметри кривої a та b мають задовольняти умову: $4a^3 + 27b^2 \neq 0 \ (\mathrm{mod}\ p)$.

Точка належить еліптичній кривій, якщо пара чисел $(x,\ y)$ задовольняє рівнянню (2). Множину точок еліптичної кривої позначають через $E_p(a,\ b)$. Також у множину точок еліптичної кривої включається нескінченно віддалена точка O. Кількість усіх точок кривої називається *порядком кривої*.

Множина $E_p(a,\ b)$ разом із введеною точкою на нескінченності O утворює адитивну абелеву групу щодо операції додавання точок (виконуються такі властивості як замкнутість, комутативність, асоціативність, існування оберненого та нейтрального елементів), що являється важливим чинником для застосування в криптографії.

ISSN 2663 - 4023

Нехай $P(x,\ y)$ – точка еліптичної кривої. *Оберненою точкою* до $P(x,\ y)$ називають точку еліптичної кривої, що симетрична відносно осі *Ox* та позначають її $-P(x,\ -y)$. Варто зауважити, що $-P$ має належати $E_p(a,\ b)$.

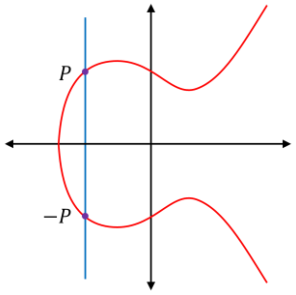

Рис. 2. Обернена точка еліптичної кривої

Додавання точок. Якщо через дві різні точки $P(x_1,\ y_1)$ та $Q(x_2,\ y_2)$, які належать $E_p(a,\ b)$ провести пряму, то вона обов'язково перетне криву в третій точці R. Сумою двох точок P та Q буде точка $-R = P + Q$, обернена до третьої точки перетину еліптичної кривої і прямої, що проходить через задані точки.

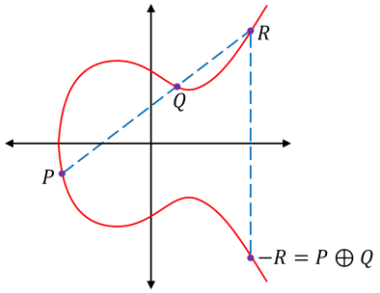

Рис. 3. Додавання точок еліптичної кривої

Координати $-R(x_3,\ y_3)$ визначаються за формулами:

$$x_3 = \lambda^2 - x_1 - x_2 (mod\ p),\ y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p), \quad (3)$$

де $\lambda = \frac{y_2 - y_1}{x_2 - x_1} (mod\ p)$ – кутовий коефіцієнт січної, що проведена через точки $P(x_1,\ y_1)$ та $Q(x_2,\ y_2)$.

Подвоєння точки. Якщо дві точки $P(x_1,\ y_1)$ та $Q(x_2,\ y_2)$ співпадають, то $P + Q = P + P$, що рівнозначно подвоєнню точки $2P = -R$. При $P = Q$ січна перетворюється на дотичну, тому точка $2P$ є оберненою до точки R.

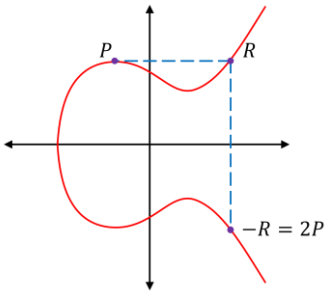

Рис. 4. Подвоєння точки еліптичної кривої

Координати $-R(x_3,\ y_3)$ визначаються за формулами:

$$x_3 = \lambda^2 - 2x_1\ (mod\ p),\ y_3 = \lambda(x_1 - x_3) - y_1(mod\ p), \quad (4)$$

де $\lambda = \frac{3x_1^2+a}{2y_1}(mod\ p)$ – кутовий коефіцієнт дотичної, що проведена через точку $P(x_1,\ y_1)$.

Скалярне множення точки на число. Із попередніх операцій додавання точок та подвоєння точки випливає операція скалярного множення точки на число:

$$2P = P + P$$
$$3P = P + P + P$$
$$\dots$$
$$mP = P + P + P + \dots + P.$$

Скалярне множення є аналогом піднесення до степеню в звичайних асиметричних алгоритмах. Прямою задачею є обчислення $mP\ = Q$. Зворотна задача полягає у тому, що знаючи точки P та Q, знайти m важко. Дану задачу називають задачею дискретного логарифмування у групі точок еліптичної кривої або ж ECDLP. Для ретельно підібраних параметрів еліптичних кривих та скінченних полів ECDLP не має ефективного рішення.

Точка $G \in\ E_p(a, b)$ називається *базовою точкою* підгрупи точок еліптичної кривої $E_p(a, b)$, якщо будь-яка точка P цієї підгрупи може бути подана у вигляді $P = mG$, де $m = 1,\ 2, \dots n$, де n – порядок підгрупи. Для базової точки G має місце рівність $nG = O$.

Пара ключів в ECC складається із закритого (приватного) і відкритого (публічного) ключів. Приватний ключ використовується для розшифрування або підпису повідомлень, тоді як публічний ключ використовується для шифрування або перевірки підпису. Закритий ключ є випадковим цілим числом, що генерується в діапазоні розміру поля кривої (зазвичай 256-бітне ціле число). Тільки власник закритого ключа повинен знати це число і тримати його в таємниці. Відкритий ключ обчислюється шляхом операції скалярного множення базової точки на значення закритого ключа. Тобто відкритим ключем є точка еліптичної кривої, яка є парою цілих координат (x, y), що належать кривій. Завдяки унікальним характеристикам цієї точки її можна стиснути до однієї координати + 1 біт (парний або непарний). У результаті стиснутий відкритий ключ є 257-бітним цілим числом та відповідає 256-бітному закритому ключу.

Розглянемо докладніше роботу найвідоміших криптографічних алгоритмів на базі еліптичних кривих. *Алгоритм обміну ключами Діффі-Хеллмана на еліптичних кривих* (Elliptic Curve Diffie-Hellman, ECDH) дозволяє двом сторонам отримати спільний секретний ключ, використовуючи незахищений від прослуховування, але захищений від модифікації канал зв'язку [20, с. 8]. Припустимо, користувачі A і B мають намір обмінятися ключами за алгоритмом Діффі-Хеллмана, суть якого полягає в наступному:

1. Абоненти A і B спільно обирають просте число p та параметри еліптичної кривої a та b.
2. У групі точок еліптичної кривої $E_p(a,\ b)$ також обирається спільна базова точка $G = (x, y)$, що має дуже великий порядок n.
3. Абонент A обирає $x < n$, обчислює $X_A = xG$ та відправляє його B.
4. Абонент B обирає $y < n$, обчислює $Y_B = yG$ та відправляє його A.
5. Користувач A обчислює закритий ключ за формулою $K_A = xY_B$.
6. Користувач B обчислює закритий ключ за формулою $K_B = yX_A$.

Отриманий спільний секретний ключ $K_A = K_B$ можна використовувати для подальшого шифрування повідомлень із використанням симетричного алгоритму.

Алгоритм цифрового підпису на еліптичних кривих (Elliptic Curve Digital Signature Algorithm, ECDSA) – це варіант алгоритму цифрового підпису (DSA), який використовує

еліптичні криві [20, с. 4]. Як відомо, цифровим підписом повідомлення є блок даних невеликого розміру, одержаний в результаті криптографічного перетворення повідомлення з використанням особистого (закритого) ключа відправника. Обов'язковою складовою цифрового підпису є хеш-функція H, яка призначена для того, щоб стиснути повідомлення M довільної довжини до двійкового хеш-значення $h(M)$ фіксованої довжини.

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

Обирається закритий ключ d – випадкове ціле число, таке що $0 < d \leq n - 1$. Обчислюється відкритий ключ $Q = dG$. Для формування підпису використовується закритий ключ, а для перевірки – відкритий ключ.

Підписування повідомлення складається з наступних кроків:

1. Вибирається випадкове ціле число k – разовий секретний ключ, де $0 < k \leq n - 1$.
2. Обчислюється $(x_1, y_1) = kG$
3. Обчислюється $r = x_1 \, mod \, n$. Якщо $r = 0$, то повертаємося до кроку 1.
4. Обчислюється $s = k^{-1}(z + dr) mod \, n$. Якщо $s = 0$, то повертаємося 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 $w = s^{-1} \, mod \, n$.
2. Обчислюється $u_1 = z \cdot w \, mod \, n$ та $u_2 = r \cdot w \, mod \, n$.
3. Обчислюється $(x_1, y_1) = u_1 G + u_2 Q$.
4. Якщо $(x_1, y_1) = O$ – підпис недійсний.
5. Якщо $r \equiv x_1 mod \, n$ – підпис дійсний.

Окрім форми Вейєрштрасса, еліптичні криві можуть бути представлені і в інших формах. Наприклад, у формі Монтгомері рівняння еліптичної кривої має наступний вигляд:

$$by^2 = x^3 + ax^2 + x, \tag{5}$$

де $a \neq \pm 2$ і $b \neq 0$.

З міркувань продуктивності ECC також використовує криві у формі Едвардса, які є еліптичними кривими наступного вигляду:

$$x^2 + ay^2 = 1 + dx^2y^2, \tag{6}$$

де $d \neq 1$ і $a \neq d$.

Кожна **крива Едвардса** біраціонально еквівалентна еліптичним **кривим у формі Вейєрштрасса** та у формі Монтгомері, що означає, що можна ефективно користуватися усіма цими формами без втрати інформації про криву.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Хоча ECC стала проривом серед криптосистем, вона не знайшла широкого практичного застосування до початку 2000-х років. На сьогоднішній день використання еліптичних кривих для вирішення криптографічних завдань закріплено в численних міжнародних та американських стандартах, зокрема таких як:

- ANSI X9.62 (1999 рік) та ANSI X9.63 (2001 рік) – це стандарти, розроблені Американським Національним Інститутом Стандартів (ANSI) та комітетом X9. Обидва стандарти визначають схеми підпису та обміну ключами на еліптичних кривих і широко

застосовуються у фінансовій галузі для захисту фінансових операцій, зокрема для автентифікації платіжних транзакцій [21], [22];

- FIPS 186-3 (2009 рік), FIPS 186-4 (2013 рік) та нова редакція FIPS 186-5 (2023 рік) – стандарти, прийняті Національним інститутом стандартів і технологій США (NIST), що визначають алгоритми цифрового підпису, зокрема ECDSA, а також надають список рекомендованих для використання кривих та їх параметрів [23];
- ISO/IEC 15946-4 (2004 рік) та ISO/IEC 15946-5 (2022 рік) – це міжнародні стандарти, що є складовими частинами серії стандартів ISO/IEC 15946, схвалених Міжнародною організацією по стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). ISO/IEC 15946-4 встановлює вимоги та рекомендації для генерації та перевірки електронних підписів на основі еліптичних кривих [24], а ISO/IEC 15946-5 визначає методи щодо генерації еліптичної кривої над скінченним полем [25].

Державні стандарти України, що визначають застосування еліптичних кривих для криптографічного захисту даних, буде розглянуто в окремому розділі цієї статті. Також важливо зазначити, що нормативні документи та стандарти з криптографії на еліптичних кривих постійно оновлюються. Тому, окрім згаданих стандартів, існує безліч інших документів та рекомендацій, що слугують основою для розробки та впровадження безпечних систем криптографічного захисту інформації на основі еліптичних кривих.

До основних переваг ECC відносять:

1. *Менші розміри ключів.* ECC забезпечує той самий рівень захисту, що й інші асиметричні алгоритми, використовуючи ключі значно меншого розміру (табл.1). Наприклад, 256-бітні ключі ECC забезпечують захист, еквівалентний 3072-бітним ключам RSA [27]. Водночас невеликі розміри ключів значно полегшують процедуру керування ключами, їх зберігання та передачу.

Таблиця 1

Порівняння довжини ключів звичайних асиметричних алгоритмів та криптосистем на еліптичних кривих

Ступінь захисту (на кожен біт ключа)	*Мінімальна довжина ключа (в бітах)*	
	RSA/DSA/DH	**ECC**
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

2. *Швидкість операцій*. Оскільки використовуються ключі невеликої довжини, то обчислення на еліптичних кривих відбуваються досить швидко. Це забезпечує високу швидкодію обробки даних та підвищує продуктивність систем, особливо в ситуаціях, де потрібно здійснювати багато криптографічних перетворень. У контексті серверних технологій це допомагає пришвидшити TLS-рукостискання, що призводить до надзвичайно швидкого завантаження вебсторінки та підвищення безпеки.

3. *Висока ефективність*. Менша довжина ключа також призводить до того, що пристрої вимагають менше процесорної потужності для виконання криптографічних операцій, що робить ECC ідеальним рішенням для мобільних пристроїв, систем Інтернету речей та інших пристроїв з обмеженою обчислювальною потужністю.

Однак, як і будь-яка криптографічна система, ECC не повністю захищена від атак, а вдосконалення обчислювальних технологій вимагають постійної пильності для гарантії безперервної безпеки ECC. Розглянемо деякі види можливих атак на ECC:

1. Атака грубою силою (brute force attack) є найпростішою атакою на будь-яку криптографічну систему, включаючи ECC. У цій атаці зловмисник намагається знайти приватний ключ, шляхом перебору всіх можливих комбінацій. Хоча ECC вимагає довжини ключа принаймні 128 біт для запобігання атакам грубої сили, прогрес у обчислювальній потужності може зробити цей захист недостатнім у майбутньому. Тому важливо використовувати ключі достатньої довжини та правильно обирати параметри кривих.

2. Атака по бічному каналу (side-channel attack), коли зловмисник намагається здобути інформацію про ключ шляхом моніторингу фізичних параметрів криптосистеми, таких як споживання енергії чи електромагнітне випромінювання, під час виконання криптографічних операцій. Для захисту від таких атак можуть використовуватися методи, які зменшують витрати енергії або випромінювання під час обчислень, такі як шумові імпульси.

3. Квантова атака (quantum-based attack) з використанням квантових обчислювальних систем. Квантові комп'ютери потенційно можуть зламати певні алгоритми ECC, такі як ECDSA та ECDH, ефективно розв'язуючи задачу дискретного логарифмування в групі точок еліптичної кривої за допомогою алгоритму Шора. Це створює значну загрозу безпеці ECC, тому докладаються зусилля для розробки постквантових криптографічних алгоритмів, стійких до квантових атак.

Варто зауважити, що різні криві можуть забезпечувати різний рівень криптографічного захисту, різну продуктивність (швидкодію), а також можуть використовувати різні алгоритми і різну довжину ключа. Вибір конкретної еліптичної кривої залежить від потреб і вимог конкретної системи. Рекомендується використання стандартизованих кривих з метою реалізації сумісності з іншими системами і протоколами. Прикладами таких кривих є NIST P-256, Curve25519, BrainpoolP256r1, secp256k1, Ed25519 [26].

Мережеве з'єднання

Криптосистеми на еліптичних є важливим елементом сучасних реалізацій багатьох протоколів безпеки, зокрема протоколу TLS, що використовується для передачі даних між вузлами комп'ютерної мережі. TLS дозволяє здійснювати автентифікацію сторін, забезпечувати конфіденційність даних, контролювати їх цілісність за допомогою кодів автентифікації повідомлень [28].

На початку встановлення безпечного з'єднання клієнт та сервер узгоджують версію протоколу, наприклад TLS 1.2, TLS 1.3. Після чого сервер обирає набір параметрів шифрування (cipher suites), які підтримуються клієнтом та відповідають усім необхідним вимогам.

Розглянемо приклад такого набору параметрів шифрування як **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**, який визначає наступне:

- для обміну ключами використовується ECDHE – алгоритм Діффі-Хеллмана на еліптичних кривих (остання літера «E» означає «ефемерний»). Ефемерний криптографічний ключ є тимчасовим ключем, створеним спеціально для використання в межах однієї операції обміну ключами. Сам по собі алгоритм Діффі-Хеллмана нестійкий до атаки типу «людина посередині» та зазвичай реалізується разом із засобами автентифікації, що включають у себе використання цифрових сертифікатів;

- для забезпечення автентифікації даних на етапі встановлення з'єднання застосовується алгоритм цифрового підпису ECDSA. Варто зауважити, що ECDSA була введена до специфікації TLS 1.2 у 2008 році.
- повідомлення шифруються симетричним алгоритмом AES зі 128-бітним ключем в режимі GCM (лічильник Галуа);
- в якості алгоритму хешування використовується SHA-256.

Зазначимо, що одним з найбільш поширених застосувань TLS є протокол HTTPS – більш просунута і безпечна версія HTTP. Аналогічним чином, електронна пошта з протоколом SMTPS фактично є SMTP у поєднанні із TLS, а FTPS – протокол для безпечної передачі файлів – це також FTP разом із TLS.

Криві NIST, рекомендовані для використання в TLS, такі: P-256, P-384, P-521. Окрім цих кривих NIST, існує також кілька інших кривих, які вважаються безпечними для використання в TLS, зокрема Curve25519 і Curve448. Ці криві все частіше використовуються в реалізаціях TLS, особливо в його нових версіях. Зокрема крива Curve25519 визначена над простим полем $p = 2^{255} - 19$ і є кривою Монтгомері, що означає, що її можна представити рівнянням:

$$y^2 = x^3 + 486662x^2 + x \ (mod\ p), \quad (7)$$

Еліптична крива Curve448 визначена над простим полем $p = 2^{448} - 2^{224} - 1$ і задається рівнянням:

$$x^2 + y^2 = 1 - 39081x^2y^2 \ (mod\ p), \quad (8)$$

Однією з ключових відмінностей між Curve25519 та Curve448 є розміри ключів. Тоді як Curve25519 має розмір ключа 256 біт, Curve448 має розмір ключа 448 біт. Рекомендується надавати перевагу Curve448 перед Curve25519, якщо потрібен вищий рівень безпеки, але варто мати на увазі, що Curve448 приблизно в три рази повільніше за Curve25519.

Криптовалюта

Найвідомішою і найпоширенішою криптовалютою у світі є біткоїн – криптографічно безпечна децентралізована система однорангових (Peer To Peer, P2P) електронних платежів, яка дозволяє здійснювати транзакції з використанням віртуальної валюти. Біткоїн заснований на технології блокчейн, що являє собою розподілену базу даних для зберігання інформації про усі транзакції учасників системи у вигляді ланцюжка блоків. При цьому кожен блок містить свій власний унікальний ідентифікатор, що пов'язує його з попереднім блоком ланцюжка.

Верифікацію транзакцій між учасниками мережі дозволяє здійснювати алгоритм цифрового підпису ECDSA [29]. Для роботи цього алгоритму використовується варіант еліптичної кривої відомий як secp256k1, який належить до сімейства стандартів, пропонованих для використання в криптографії (Standards for Efficient Cryptography, SEC).

У випадку біткоїнів еліптична крива secp256k1 задається рівнянням:

$$y^2 = x^3 + 7 \ (mod\ p), \quad (9)$$

де p – дуже велике просте число $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

Стандартом secp256k1 також визначена базова точка $G = (x, y)$, що належить заданій кривій (9) та має дуже великий порядок n (близький до 2^{256}). Основне використання secp256k1 полягає у генерації ключів, підписуванні та перевірці підпису. Кроки формування та перевірки цифрового підпису за алгоритмом ECDSA описано вище, а даними для підписування будуть транзакції, які передають право власності на біткоїни.

Обмін повідомленнями

ECC часто використовується в системах наскрізного шифрування (End-to-End Encryption, E2EE) голосових викликів, відеодзвінків і миттєвих повідомлень. Наскрізне шифрування означає, що повідомлення шифруються на пристрої відправника та можуть бути розшифровані лише на пристрої одержувача. Технологія E2EE гарантує, що ніхто, навіть сервер, який з'єднує користувачів, не зможе отримати доступ до повідомлень.

Одним із популярних прикладів E2EE, що використовує апарат еліптичних кривих, є криптографічний протокол Signal, розроблений Open Whisper Systems у 2013 році і вперше представлений в додатку TextSecure з відкритим вихідним кодом, який пізніше було об'єднано в додаток Signal. Кілька додатків з закритим вихідним кодом, наприклад, такі як WhatsApp, стверджують, що реалізували цей протокол, який, за їхніми словами, шифрує розмови більше мільярда людей у всьому світі. Розробники Facebook Messenger також стверджують, що вони пропонують цей протокол для додаткових секретних сеансів зв'язку.

Протокол Signal [30] об'єднує розширений протокол узгодження ключів Діффі-Хелмана на еліптичних кривих (X3DH) та алгоритм Double Ratchet для шифрування. X3DH встановлює початковий спільний секретний ключ між двома сторонами, які взаємно автентифікують одна одну на основі відкритих ключів. До або після угоди про ключ X3DH сторони можуть порівнювати свої ідентифікаційні відкриті ключі через певний автентифікований канал. Наприклад, вони можуть порівнювати відбитки відкритих ключів вручну або скануючи QR-код.

Надсилання та отримання зашифрованих повідомлень відбувається за алгоритмом Double Ratchet. Для кожного надісланого або отриманого повідомлення Double Ratchet генерує новий набір ключів. Відкритий текст шифрується за допомогою симетричного алгоритму AES-256 у режимі CBC. Автентифікація та хешування у протоколі Signal відбувається за допомогою HMAC-SHA256. Для асиметричних криптографічних перетворень рекомендовано використовувати еліптичні криві Curve25519 або Curve448.

Інтернет речей

Інтернет речей (Internet of Things, IoT) являє собою мережу підключених до Інтернету пристроїв, що аналізують, обробляють та передають дані. За допомогою цієї технології існує можливість керувати кількома пристроями віддалено. Ця галузь стрімко розвивається, проте на даний момент головною проблемою IoT є вразливість до кібератак. Зі збільшенням кількості підключених «розумних» пристроїв, ростуть ризики несанкціонованого доступу до IoT-системи.

Для того, щоб пристрої, що працюють відповідно до технології IoT могли повноцінно функціонувати і безпечно взаємодіяти між собою, між ними необхідно встановити захищене з'єднання. З цією метою, як правило, використовують «легкі» криптографічні алгоритми, оскільки вони вимагають менше обчислювальних ресурсів і пам'яті, ніж звичайні алгоритми. Так звана «легковагова» криптографія на еліптичних кривих являє собою спеціалізовану реалізацію ECC, розроблену для пристроїв IoT з обмеженими ресурсами. За рахунок використання ключа меншого розміру або вибору спеціальних параметрів кривої, алгоритми, які використовуються для обміну ключами (ECDH) та цифрових підписів (ECDSA) можна оптимізувати для пристроїв IoT.

Впровадження полегшених криптографічних перетворень часто включає компроміси між безпекою та ефективністю. Наприклад, зменшення розміру ключа або використання спрощених алгоритмів може підвищити ефективність, але може знизити безпеку. Незважаючи на це, на сьогоднішній день питання застосування ECC для IoT залишається актуальним. Низка досліджень [31]-[33] присвячена проектуванню і

впровадженню криптографії на еліптичних кривих для підтримки безпечної роботи таких складових IoT як бездротові сенсорні мережі (WSN), радіочастотні ідентифікатори (RFID), «розумні» будинки та міста тощо.

ECC є важливою технологією для захисту пристроїв і комунікацій IoT, оскільки вона може надавати надійну безпеку з мінімальними витратами ресурсами. Однак правильна реалізація та оптимальний вибір параметрів роботи алгоритмів на еліптичних кривих мають вирішальне значення для реалізації довгострокової безпеки системи.

ECC в Україні

В Україні основним документом, що регулює процедури формування та перевірки цифрового підпису є Національний стандарт ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка» [34]. Цей стандарт встановлює механізм цифрового підпису, оснований на властивостях груп точок еліптичних кривих над скінченними полями, та правила застосування цього механізму до повідомлень, що пересилаються каналами зв'язку і обробляються у комп'ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства.

Національний стандарт ДСТУ 4145-2002 регламентує використання еліптичних кривих над скінченним полем $GF(2^m)$. Згідно зі стандартом визначено допустимі основні поля і рекомендовані незвідні многочлени, що їм відповідають. Дозволено використовувати еліптичні криві з параметрами, що наведені в окремому додатку стандарту. Національний стандарт також встановлює алгоритми перевірки правильності вибору рівняння еліптичної кривої та базової точки. ДСТУ 4145-2002 досить гнучкий і щодо вибору параметрів безпеки (наприклад, для нього можна обирати функцію хешування, генератор псевдовипадкових чисел тощо).

На сьогоднішній день низка державних установ, зокрема і банки України ефективно використовують цифровий підпис на основі стандарту ДСТУ 4145-2002 для здійснення банківських операцій у корпоративних та інших телекомунікаційних мережах. Закони України прирівнюють за юридичною силою електронні документи, підписані цифровим підписом, до документів із власноручним підписом, що дозволяє виконувати юридично значущі дії шляхом електронного документообігу.

Також 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» [35]. Цей алгоритм призначений для шифрування коротких повідомлень довжиною до 616 біт.

Як і стандарт цифрового підпису ДСТУ 4145-2002, новий алгоритм використовує криптографічні перетворення у групі точок еліптичних кривих, використовуючи замість кривих у формі Вейєрштрасса криві у формі Едвардса. Це дає суттєві переваги у швидкодії більш ніж у 3 рази. Новий стандарт розроблений з урахуванням усіх найсучасніших вимог до стійкості криптографічних алгоритмів.

Стандарт ДСТУ 9041-2020 узгоджений з усіма діючими в Україні національними стандартами. Його характерними особливостями є відносно невелика довжина ключа, найсучасніший математичний апарат, а також новий алгоритм генерації псевдовипадкових послідовностей, який, на відміну від аналогічного алгоритму генерації з ДСТУ 4145-2002, використовує виключно національні криптографічні алгоритми та не містить посилань на відповідні пострадянські стандарти, термін дії яких вже практично вичерпався.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Криптографія на еліптичних кривих – це важлива платформа для побудови сучасних криптографічних алгоритмів з відкритим ключем. ECC використовується для захисту мережевого з'єднання, формування секретних ключів для TLS-серверів та їх клієнтів. ECC дозволяє створювати цифрові підписи, які підтверджують автентичність транзакції та надають високий рівень безпеки в екосистемі криптовалют. Мобільні додатки використовують криптографічні протоколи на базі еліптичних кривих для захисту голосових викликів, відеодзвінків і миттєвих повідомлень. ECC відіграє важливу роль у захисті зв'язку, забезпеченні цілісності даних та механізмів автентифікації для пристроїв IoT. Алгоритми і протоколи ECC широко застосовуються в нашій країні та закріплені в державних стандартах ДСТУ 4145-2002 та ДСТУ 9041-2020.

ECC є досить новим поколінням криптосистем з відкритим ключем, які побудовані на зрозумілих математичних перетвореннях і забезпечують більш серйозний захист, ніж класичні криптосистеми з відкритим ключем. На даний момент не існує алгоритмів субекспоненційної складності для знаходження дискретного логарифму у групі точок еліптичних кривих над скінченними полями, що дозволяє гарантувати стійкість ECC на теперішній час.

Однак, криптографія на еліптичних кривих також має свої проблеми та виклики. Наприклад, проектування безпечних криптосистем на основі еліптичних кривих потребує додаткових знань та компетенцій у порівнянні з більш традиційними алгоритмами криптографії. Адже вибір правильних параметрів кривих є критично важливим для безпеки ECC. Також із часом алгоритми на еліптичних кривих можуть втратити криптостійкість до атак із використанням квантових обчислень. Алгоритм Шора, використовуючи гіпотетичний квантовий комп'ютер, може зламати алгоритм на основі ECC за короткий проміжок часу. Зважаючи на це, перспективи подальших дослідження полягатимуть у аналізі забезпечення стійкості ECC перед квантовими атаками, у розгляді нових квантовостійких алгоритмів, протоколів та рішень, які можуть посилити безпеку та ефективність криптосистем на еліптичних кривих.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177), 203. https://doi.org/10.1090/s0025-5718-1987-0866109-5.
2 Miller, V.S. Use of elliptic curves in cryptography. *Lecture notes in computer science*, 417–426. https://doi.org/10.1007/3-540-39799-x_31.
3 Menezes, A. (1993). Introduction to public key cryptography. *Elliptic curve public key cryptosystems*. Boston, 1–14. https://doi.org/10.1007/978-1-4615-3198-2_1.
4 Vanstone , S. (1997). Elliptic curve cryptosystem – The answer to strong, fast public-key cryptography for securing constrained environments. *Information security technical report, 2*(2), 78–87. https://doi.org/10.1016/s1363-4127(97)81331-3.
5 Bernstein, D. J., Lange, T. (2014). Hyper-and-elliptic-curve cryptography. *LMS journal of computation and mathematics*, 17, 181–202. https://doi.org/10.1112/s1461157014000394 (date of access: 05.05.2023).
6 Lange, T. (2011). Edwards curves. *Encyclopedia of cryptography and security*, 380–382. https://doi.org/10.1007/978-1-4419-5906-5_243.
7 Washington, L. C. (2008). Elliptic curves: number theory and cryptography. 2nd ed. Boca Raton, FL : Chapman & Hall/CRC.
8 Edwards, H. M. (2007). A normal form for elliptic curves. Bulletin of the american mathematical society, 44(03), 393–423. https://doi.org/10.1090/s0273-0979-07-01153-6.
9 Юдін, О., Вадясов, К. (2010). Method of elliptic curves imposition in cryptographic protection tasks of graphic information. *Science-based technologies, 6*(2). https://doi.org/10.18372/2310-5461.6.5202.

10 Чевардін, В.Є., Пономарьов, О.А. (2020). Перспективи розвитку криптосистем на основі перетворень в групі точок еліптичних кривих. *Збірник наукових праць ВІТІ, 1*. https://viti.edu.ua/files/zbk/2020/12_1_2020.pdf.

11 Бессалов, А.В. (2017). Эллиптические кривые в форме Эдвардса и криптография: монография. Киев: изд-во «Политехника».

12 Циганкова, О.В. (2021). Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса: дис... канд. техн. Наук.

13 Беспалов, О. Ю., Кучинська, Н. В. (2017). Крива Едвардса над кільцем лишків як декартів добуток кривих Едвардса над скінченими полями. *Прикладная радиоэлектроника.* 2017, 16(3-4), 170-175. http://nbuv.gov.ua/UJRN/Prre_2017_16_3-4_13.

14 Ковальчук, Л.В., Бессалов, А.В., Беспалов, О.Ю. (2015). Порівняльний аналіз алгоритмів генерації базової точки на кривій Едвардса. У Безпека інформації у інформаційно-телекомунікаційних системах (с. 32-33).

15 Skuratovskii, R. (2020). Supersingular edwards curves and edwards curve points counting method over finite field. *Journal of numerical and applied mathematics*, *1*(133), 68–88. https://doi.org/10.17721/2706-9699.2020.1.06.

16 Ільєнко, А.В., Ільєнко, С.С., Мазур, Я.С., Прокопенко, О.В. (2021). Перспективи використання еліптичної криптографії для забезпечення цілісності та конфіденційності інформації. *Вісник Університету «Україна» Серія Інформатика, обчислювальна техніка та кібернетика*, *2*(23). https://visn-it.uu.edu.ua/index.php/visn-icct/article/view/61.

17 Нікуліщев, Г.І. (2013). Протокол сліпого електронного цифрового підпису на еліптичних кривих над скінченим векторним полем. *Радіоелектроніка, інформатика, управління*, (2). https://doi.org/10.15588/1607-3274-2013-2-12.

18 Meleshko, O.O., Kovalskiy, O.O. (2014). Elliptic curve cryptography. *Science-based technologies*, *22*(2). https://doi.org/10.18372/2310-5461.22.6815.

19 Harkanson, R., Kim, Y. (2017). Applications of elliptic curve cryptography: a light introduction to elliptic curves and a survey of their applications. *CISRC'17: twelfth annual cyber and information security research conference*, Oak Ridge Tennessee USA. https://doi.org/10.1145/3064814.3064818.

20 Blake, I. F., Smart, N. P., Seroussi, G. (2009). Advances in elliptic curve cryptography. Cambridge University Press,.

21 (1999). ANSI X9.62. Public key cryptography for the financial services industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, Washington.

22 (2001). 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.

23 (2013). FIPS 186-5. Digital Signature Standard (DSS). National Institute of Standards and Technology, U.S. Department of Commerce, Washington. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.

24 (2004). ISO/IEC 15946-4. Information technology. Security techniques. Cryptographic techniques based on elliptic curves. Part 4: Digital signatures giving message recovery, Geneva.

25 (2022). ISO/IEC 15946-5. Information technology. Security techniques. Cryptographic techniques based on elliptic curves. Part 5: Elliptic curve generation, Geneva, 2022.

26 SafeCurves: choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to/.

27 Saho, N.J.G., Ezin, E.C. (2020). Comparative study on the performance of elliptic curve cryptography algorithms with cryptography through RSA algorithm, CARI. https://hal.science/hal-02926106/document?ref=panther-protocol-blog.

28 Nir, Y., Josefsson, S., Pegourie-Gonnard, M. (2018). Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS) versions 1.2 and earlier. RFC Editor. https://doi.org/10.17487/rfc8422.

29 Grunspan, C., Pérez-Marco, R. (2020). The mathematics of bitcoin. *EMS newsletter*, *3*(115), 31–37. https://doi.org/10.4171/news/115/8.

30 Signal. Technical information. Specifications and software libraries for developers. https://www.signal.org/docs/.

31 HU, X., HUANG, H., ZHENG, X., LIU, Y., XIONG, X. (2021). Low-power Reconfigurable Architecture of Elliptic Curve Cryptography for IoT. *IEICE Transactions on Electronics*. https://doi.org/10.1587/transele.2021ecp5009.

32 Lee, Y. K., Sakiyama, K., Batina, L., Verbauwhede, I. (2008). Elliptic-Curve-Based Security Processor for RFID. *IEEE Transactions on Computers*, *57*(11), 1514–1527. https://doi.org/10.1109/tc.2008.148.

33 Simon Francia, A., Solis-Lastra, J., Papa Quiroz, E. A. (2022). Elliptic Curves Cryptography for Lightweight Devices in IoT Systems. У *Emerging Research in Intelligent Systems* (с. 71–82). Springer International Publishing. https://doi.org/10.1007/978-3-030-96043-8_6.

34 ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ, Держстандарт України.
35 ДСТУ 9041-2020. Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Nataliia Shchur
Senior Lecturer of the Department of Computer Engineering and Cybersecurity
Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
ORCID ID: 0000-0002-1182-4799
thalitana@gmail.com

Oleksandra Pokotylo
Senior Lecturer of the Department of Computer Engineering and Cybersecurity
Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
ORCID ID: 0000-0002-1587-235X
kik_poa@ztu.edu.ua

Yelyzaveta Bailiuk
Senior Lecturer of the Department of Computer Engineering and Cybersecurity
Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
ORCID ID: 0000-0002-4961-7816
liza.bailiuk@gmail.com

ELLIPTIC CURVE CRYPTOGRAPHY AND ITS PRACTICAL APPLICATION

Abstract. Elliptic curves are one of the most promising tools for constructing modern cryptographic algorithms. The security of elliptic curve cryptography is based on the complexity of solving the discrete logarithm problem in the group of points of the elliptic curve over a finite field. Elliptic curve cryptography enables two parties communicating over public channel using elliptic curve encryption and signing algorithms. Elliptic curves allow to achieve the same level of security with small key sizes than other asymmetric cryptographic algorithms. The article describes the mathematical apparatus of elliptic curves used for cryptographic purposes, the basic operations in the group of points of elliptic curves, such as addition of points, doubling of a point, and scalar multiplication of a point by a number are given. The steps and principles of the Diffie-Hellman key exchange algorithm (ECDH) and the digital signature scheme (ECDSA) on elliptic curves are considered. An overview of standards establishing recommendations and requirements for the use of elliptic curves in cryptographic systems is provided. The advantages of elliptic curve cryptography compared to traditional asymmetric algorithms, such as smaller key sizes, computational speed, and efficient use of resources, are analyzed. Potential threats and vulnerabilities of cryptographic algorithms based on elliptic curves are discussed. The main practical application areas of cryptographic algorithms on elliptic curves, including network security, cryptocurrency operations, message exchange, the Internet of Things, and government institutions are investigated. Examples of popular standardized curves (Curve25519, Curve448, secp256k1) that have been tested and recommended by specialized organizations such as NIST are given.

Keywords: elliptic curve cryptography; asymmetric cryptosystems; Diffie-Hellman key exchange algorithm; elliptic curve digital signature; ECC; ECDH; ECDSA

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203. https://doi.org/10.1090/s0025-5718-1987-0866109-5.
2 Miller, V.S. Use of elliptic curves in cryptography. Lecture notes in computer science, 417–426. https://doi.org/10.1007/3-540-39799-x_31.
3 Menezes, A. (1993). Introduction to public key cryptography. Elliptic curve public key cryptosystems. Boston, 1–14. https://doi.org/10.1007/978-1-4615-3198-2_1.
4 Vanstone , S. (1997). Elliptic curve cryptosystem – The answer to strong, fast public-key cryptography for securing constrained environments. Information security technical report, 2(2), 78–87. https://doi.org/10.1016/s1363-4127(97)81331-3.
5 Bernstein, D. J., Lange, T. (2014). Hyper-and-elliptic-curve cryptography. LMS journal of computation and mathematics, 17, 181–202. https://doi.org/10.1112/s1461157014000394 (date of access: 05.05.2023).

6 Lange, T. (2011). Edwards curves. Encyclopedia of cryptography and security, 380–382. https://doi.org/10.1007/978-1-4419-5906-5_243.
7 Washington, L. C. (2008). Elliptic curves: number theory and cryptography. 2nd ed. Boca Raton, FL : Chapman & Hall/CRC.
8 Edwards, H. M. (2007). A normal form for elliptic curves. Bulletin of the american mathematical society, 44(03), 393–423. https://doi.org/10.1090/s0273-0979-07-01153-6.
9 Iudin, O., Vadiasov, K. (2010). Method of elliptic curves imposition in cryptographic protection tasks of graphic information. Science-based technologies, 6(2). https://doi.org/10.18372/2310-5461.6.5202.
10 Chevardin, V.Ie., Ponomarov, O.A. (2020). Perspektyvy rozvytku kryptosystem na osnovi peretvoren v hrupi tochok eliptychnykh kryvykh. Zbirnyk naukovykh prats VITI, 1. https://viti.edu.ua/files/zbk/2020/12_1_2020.pdf.
11 Bessalov, A.V. (2017). Эllyptycheskye kryvыe v forme Эdvardsa y kryptohrafyia: monohrafyia. Kyev: yzd-vo «Polytekhnyka».
12 Tsyhankova, O.V. (2021). Metody pidvyshchennia shvydkodii asymetrychnykh kryptosystem z vykorystanniam eliptychnykh kryvykh u formi Edvardsa: dys... kand. tekhn. Nauk.
13 Bespalov, O. Yu., Kuchynska, N. V. (2017). Kryva Edvardsa nad kiltsem lyshkiv yak dekartiv dobutok kryvykh Edvardsa nad skinchenymy poliamy. Prykladnaia radyoэlektronyka. 2017, 16(3-4), 170-175. http://nbuv.gov.ua/UJRN/Prre_2017_16_3-4_13.
14 Kovalchuk, L.V., Bessalov, A.V., Bespalov, O.Iu. (2015). Porivnialnyi analiz alhorytmiv heneratsii bazovoi tochky na kryvii Edvardsa. U Bezpeka informatsii u informatsiino-telekomunikatsiinykh systemakh (c. 32-33).
15 Skuratovskii, R. (2020). Supersingular edwards curves and edwards curve points counting method over finite field. Journal of numerical and applied mathematics, 1(133), 68–88. https://doi.org/10.17721/2706-9699.2020.1.06.
16 Ilienko, A.V., Ilienko, S.S., Mazur, Ya.S., Prokopenko, O.V. (2021). Perspektyvy vykorystannia eliptychnoi kryptohrafii dlia zabezpechennia tsilisnosti ta konfidentsiinosti informatsii. Visnyk Universytetu «Ukraina» Seriia Informatyka, obchysliuvalna tekhnika ta kibernetyka, 2(23). https://visn-it.uu.edu.ua/index.php/visn-icct/article/view/61.
17 Nikulishchev, H.I. (2013). Protokol slipoho elektronnoho tsyfrovoho pidpysu na eliptychnykh kryvykh nad skinchenym vektornym polem. Radioelektronika, informatyka, upravlinnia, (2). https://doi.org/10.15588/1607-3274-2013-2-12.
18 Meleshko, O.O., Kovalskiy, O.O. (2014). Elliptic curve cryptography. Science-based technologies, 22(2). https://doi.org/10.18372/2310-5461.22.6815.
19 Harkanson, R., Kim, Y. (2017). Applications of elliptic curve cryptography: a light introduction to elliptic curves and a survey of their applications. CISRC17: twelfth annual cyber and information security research conference, Oak Ridge Tennessee USA. https://doi.org/10.1145/3064814.3064818.
20 Blake, I. F., Smart, N. P., Seroussi, G. (2009). Advances in elliptic curve cryptography. Cambridge University Press,.
21 (1999). ANSI X9.62. Public key cryptography for the financial services industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, Washington.
22 (2001). 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.
23 (2013). FIPS 186-5. Digital Signature Standard (DSS). National Institute of Standards and Technology, U.S. Department of Commerce, Washington. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.
24 (2004). ISO/IEC 15946-4. Information technology. Security techniques. Cryptographic techniques based on elliptic curves. Part 4: Digital signatures giving message recovery, Geneva.
25 (2022). ISO/IEC 15946-5. Information technology. Security techniques. Cryptographic techniques based on elliptic curves. Part 5: Elliptic curve generation, Geneva, 2022.
26 SafeCurves: choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to/.
27 Saho, N.J.G., Ezin, E.C. (2020). Comparative study on the performance of elliptic curve cryptography algorithms with cryptography through RSA algorithm, CARI. https://hal.science/hal-02926106/document?ref=panther-protocol-blog.
28 Nir, Y., Josefsson, S., Pegourie-Gonnard, M. (2018). Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS) versions 1.2 and earlier. RFC Editor. https://doi.org/10.17487/rfc8422.
29 Grunspan, C., Pérez-Marco, R. (2020). The mathematics of bitcoin. EMS newsletter, 3(115), 31–37. https://doi.org/10.4171/news/115/8.
30 Signal. Technical information. Specifications and software libraries for developers. https://www.signal.org/docs/.

31 HU, X., HUANG, H., ZHENG, X., LIU, Y., XIONG, X. (2021). Low-power Reconfigurable Architecture of Elliptic Curve Cryptography for IoT. IEICE Transactions on Electronics. https://doi.org/10.1587/transele.2021ecp5009.

32 Lee, Y. K., Sakiyama, K., Batina, L., Verbauwhede, I. (2008). Elliptic-Curve-Based Security Processor for RFID. IEEE Transactions on Computers, 57(11), 1514–1527. https://doi.org/10.1109/tc.2008.148.

33 Simon Francia, A., Solis-Lastra, J., Papa Quiroz, E. A. (2022). Elliptic Curves Cryptography for Lightweight Devices in IoT Systems. U Emerging Research in Intelligent Systems (s. 71–82). Springer International Publishing. https://doi.org/10.1007/978-3-030-96043-8_6.

34 DSTU 4145-2002. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Tsyfrovyi pidpys, shcho gruntuietsia na eliptychnykh kryvykh. Formuvannia ta pereviriannia. Kyiv, Derzhstandart Ukrainy.

35 DSTU 9041-2020. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm shyfruvannia korotkykh povidomlen, shcho gruntuietsia na skruchenykh eliptychnykh kryvykh Edvardsa.