УДК 638.235.231

О. В. Циганкова

НОВІ АЛГОРИТМИ ЗНАХОДЖЕННЯ БАЗОВОЇ ТОЧКИ НА ЕЛІПТИЧНИХ КРИВИХ У ФОРМІ ЕДВАРДСА

Національний технічний університет України «КПІ ім. Ігоря Сікорського», Фізико-технічний інститут, місто Київ

Анотація. Перетворення еліптичних кривих, що використовують у національному стандарті цифрового підпису ДСТУ 4145 2002, відповідають сучасним вимогам. Однак, бурхливий розвиток обчислювальної техніки та значне підвищення інтересу до криптології в усьому світі, залучення величезної кількості спеціалістів, у тому числі математиків, до роботи у даній галузі, призвели до зростання об'єму досліджень, постійного виникнення нових, все більш потужних методів криптоаналізу і, як наслідок, до можливого зменшення терміну життя існуючих та нових алгоритмів. У даній статті розв'язано актуальну науково-практичну задачу дослідження властивостей еліптичних кривих у формі Едвардса над простим полем F_p, де $p \neq 2$, придатних для використання в алгоритмах асиметричних криптосистем, зокрема, в алгоритмах цифрового підпису (ЦП). На підставі проведених досліджень було знайдено та описано нові способи знаходження базової точки на кривих у формі Едвардса. З застосуванням цих методів запропоновано три нових алгоритми визначення базової точки для побудови криптосистеми на повних та скручених кривих у формі Едвардса. Також у статті проведено порівняльний аналіз швидкодії розроблених алгоритмів знаходження базової точки для побудови криптосистеми на кривих у формі Едвардса та швидкодії криптоалгоритмів на несуперсингулярних еліптичних кривих у формі Вейєрштрасса над полями характеристики 2, перетворення яких використовуються в криптоалгоритмах ЦП ДСТУ 4145 2002. За результатами проведеного аналізу встановлено, що швидкодія трьох запропонованих алгоритмів вища, від стандартного алгоритму цифрового підпису на кривих у формі Вейєрштрасса, для першого алгоритму у 180 раз, другого - у 16log (n) (де $n \in \mathbb{P}$) раз та третього алгоритму у 32log (n) (де $n \in \mathbb{P}$) раз відповідно. На підставі проведених досліджень, у статті доведено, що використання еліптичних кривих у формі Едвардса над простими полями, замість кривих Вейєрштрасса, дозволяють підвищити швидкість експоненціювання точки в асиметричних криптосистемах. Результати роботи можуть бути використані в задачах аналізу існуючих та при розробці нових алгоритмів і стандартів асиметричної криптографії.

Ключові слова: скручені криві Едвардса, повні криві Едвардса, порядок кривої, порядок точки, базова точка, квадратичний лишок, квадратичний нелишок, алгоритм цифрового підпису, криві Вейєрштрасса, швидкодія.

Аннотация. Преобразование эллиптических кривых, которые используют в национальном стандарте цифровой подписи ДСТУ 4145 2002, соответствуют современным требованиям. Однако, бурное развитие вычислительной техники и значительное повышение интереса к криптологии во всем мире, привлечения огромного количества специалистов, в том числе математиков к работе в данной области, привели к росту объема исследований, постоянного возникновения новых все более мощных методов криптоанализа и, как следствие, к возможному уменьшению срока жизни существующих и новых алгоритмов. В данной статье решена актуальная научно-практическая задача исследования свойств эллиптических кривых в форме Эдвардса над простым полем F_p, де $p \neq 2$, пригодных для использования в алгоритмах асимметричных криптосистем, в частности, в алгоритмах цифровой подписи (ЦП). На основании проведенных исследований было найдено и описано новые способы нахождения базовой точки на кривых в форме Эдвардса. С применением этих способов предложено три новых алгоритма определения базовой точки для построения криптосистемы на полных и скрученных кривых в форме Эдвардса. Также в статье проведен сравнительный анализ быстродействия разработанных алгоритмов нахождения базовой точки для построения криптосистемы на кривых в форме Эдвардса и быстродействия криптоалгоритмов на несуперсингулярних эллиптических кривых в форме Вейерштрасса над полями характеристики 2, преобразования которых используются в криптоалгоритмах ЦП ДСТУ 4145 2002. По результатам анализа установлено, что предложенных три алгоритма быстрее стандартного алгоритма цифровой подписи на кривых в форме Вейерштрасса - соответственно первый алгоритм в 180 раза, второй в 16log (n) (где n$\in \mathbb{P}$) раз и третий алгоритм в 32log (n) (где $n \in \mathbb{P}$) раз. На основании проведенных исследований, в статье доказано, что использование эллиптических кривых в форме Эдвардса над простыми полями, вместо кривых Вейерштрасса, позволяют повысить скорость експоненциювання точки в асимметричных криптосистемах. Результаты работы могут быть использованы в задачах анализа существующих и создание новых алгоритмов и стандартов асимметричной криптографии.

Ключевые слова: скрученные кривые Эдвардса, полные кривые Эдвардса, порядок кривой, порядок точки, базовая точка, квадратичный вычет, квадратичный невычет, алгоритм цифровой подписи, кривые Вейерштрасса, быстродействие.

Summary. Transformations on elliptic curves which are used in the national digital signature standard DSTU 4145 2002, satisfy modern requirements. However, the fast development of computer technologies and a significant interest in cryptology worldwide have led to an increase in research, the constant emergence of new powerful cryptanalysis methods and, as a consequence, to the possible shortening of the lifetime of existing and new algorithms. This article addresses the current scientific and practical problem of investigating the properties of elliptic curves in the Edwards form over a finite field F_p, p ≠ 2, suitable for use in asymmetric cryptosystem, in particular, digital signature algorithms. Based on the research completed, new ways of determination of a base point on Edwards curves were outlined and described. Three new algorithms were proposed for determination of the base point for constructing a cryptosystem on the full and twisted Edwards curves. In this work the comparative analysis of the performance of the developed algorithms of the Edwards curves base point determination and the performance of crypto-algorithms on the non-perpendicular elliptic curves in the Weierstrass form over the fields of characteristic 2 was carried out. The analysis shows that proposed algorithms are faster than the standard Weirstrass digital signature curve algorithm – respectively, the first algorithm – 180 times, the second–$16\log(n)$ $(n \in \mathbb{P})$times, and the third algorithm–$32\log(n)$ $(n \in \mathbb{P})$ times. It is proved that the use of elliptic curves in the form of Edwards over finite field F_p, instead of Weierstrass curves, can increase the speed of operations of adding points in asymmetric cryptosystems. The results of the work can be applied to the analysis of existing problems and creation of new algorithms and standards of asymmetric cryptography.

Keywords: complete Edwards curves, twisted Edwards curves, order of a curve, order of a point, base point, quadratic residue, quadratic nonresidue, digital signature algorithm, Weierstrass curves, exponential speed increase.
DOI: https://doi.org/10.31649/1999-9941-2020-47-1-39-47.

Вступ

Еліптичні криві у формі Едвардса (ЕКФЕ) над простим полем на сьогодні забезпечують найбільшу швидкість та є перспективними для використання в асиметричних криптосистемах. Найвища продуктивність, універсальність закону додавання, унікальна симетрія точок та наявність афінних координат нейтрального елемента групи – головні властивості ЕКФЕ, які були виявлені і обґрунтовані вже в першій роботі [1] фахівцями з криптографії. Важливим є також те, що ізоморфні криві завжди належать одному класу. Також в роботі [2] доведено, що продуктивність операції експоненціювання точки ЕКФЕ, порівняно з кривою у формі Вейєрштрасса, в середньому вище більш ніж в 1,5 рази. На підставі цього та згідно з доведеним ізоморфізмом ЕКФЕ та кривих Вейєрштрасса [1], криві у формі Едвардса можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

У данійстатті розглянуто три варіанта створення алгоритмів пошуку генератора криптосистеми(базової точки) на ЕКФЕ над простим полем. У розділі 1 визначено властивості повних та скручених ЕКФЕ згідно з новою запропонованою класифікації ЕКФЕ [3].Наведено властивості точок простого порядку та методи їх знаходження. У другому розділіописано алгоритм знаходження базової точки на кривих Вейєрштрасса та створено та описано нові алгоритми знаходження базової точки для побудови криптосистеми на повних та скручених ЕКФЕ. У третьому розділі зроблено порівняльний аналіз швидкодії алгоритмів на ЕКФЕ та на кривих, що використовуються в стандартах цифрового підпису (ЦП).

Актуальність

Перетворення еліптичних кривих, що використовують у національному стандарті цифрового підпису ДСТУ 4145 2002, відповідають сучасним вимогам. Однак, бурхливий розвиток обчислювальної техніки та значне підвищення інтересу до криптології в усьому світі, залучення величезної кількості спеціалістів, у тому числі математиків, до роботи у даній галузі, призвели до зростання об'єму досліджень, постійного виникнення нових, все більш потужних методів криптоаналізу і, як наслідок, до можливого зменшення терміну життя існуючих та нових алгоритмів. Це зумовлює актуальність дослідження властивостей ЕКФЕ над простими полями з метою застосування їх у сучасних більш ефективних криптосистемах на еліптичних кривих.

Мета

Метою дослідження є створення більш швидких за існуючі алгоритмів знаходження базової точки з застосуванням перетворень ЕКФЕ які можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

Задачі

1.Визначити необхідні властивості ЕКФЕ які можуть бути використані у створенні більш швидких алгоритмах знаходження базової точки.

2.Створитиалгоритми пошуку базової точки на повних та скручених ЕКФЕ.

3.Провести порівняльний аналіз швидкодії алгоритмів знаходження базової точки для побудови криптосистеми на ЕКФЕ та кривих у формі Вейєрштрасса.

Розв'язання задач

1. Визначення та властивості повних та скручених ЕКФЕ за новою класифікацією

Криву в узагальненій формі Едвардса визначено рівнянням:

$$E_{a,d}:\ x^2 + ay^2 = 1 + dx^2y^2,\quad a,d \in F_p^*, d \neq 1,\ a \neq d,\ p \neq 2. \tag{1}$$

Для форми кривої (1) маємо універсальний модифікований [3] закон додавання точок (2):

$$(x_1,y_1) + (x_2,y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2},\ \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right) \tag{2}$$

що не змінюється і у випадку коли$(x_1,y_1) = (x_2,y_2)$:

$$2(x_1,y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right). \tag{3}$$

Точка на ЕКФЕ визначена як $\boldsymbol{P} = (x,y)$,зворотна точка як $-\boldsymbol{P} = (x,-y)$, точки малих порядків: $\boldsymbol{O}, \boldsymbol{D}_0$ та $\pm\boldsymbol{F}_0$. На основі нової модифікації ЕКФЕ, введена арифметика для операцій у групі з особливими точками цих кривих, формули зв`язку точок малих порядків і формули, що пов'язують їх з іншими точками кривої. Точка другого порядку $\boldsymbol{D}_0 = (-1,0)$така, що $2\boldsymbol{D}_0 = \boldsymbol{O}$. Нейтральний елемент групи точок $\boldsymbol{O} = \boldsymbol{P} + (-\boldsymbol{P}) = (1,0)$. Залежно від властивостей параметрів *a* і *d,* наведено умови існування двох особливих точок 2-го порядку та умови існування двох або чотирьох точок 4-го порядку $\boldsymbol{F}$, для яких $\pm 2\boldsymbol{F} = \boldsymbol{D}$. Між точками існують залежності:

$(x,y) + (-1,0) = (-x,-y);$
$(x,y) - (0,1) = (-y,x);$
$(x,y) + (0,-1) = (y,-x);$
$(x,y) + (y,x) = (0,1).$

Із застосуванням нової модифікації, на базі аналізу квадратичності параметрів *a* і *d*кривої проведено аналіз ЕКФЕ над простими скінченними полями характеристики $p > 3$ та створено нову повну класифікаціюкривих в узагальненій формі Едвардса [3] (табл.1). За новою класифікацією ЕКФЕ розбиваються на три класи, що не перетинаються:

- *повні* ЕКФЕ з умовою: $\chi(ad) = -1$;
- *скручені*ЕКФЕ з умовами: $\chi(a) = \chi(d) = -1$;
- *квадратичні* ЕКФЕ з умовами: $\chi(a) = \chi(d) = 1$,

де $\chi(a) = \left(\frac{a}{p}\right)$ –символ Лежандра, показник квадратичності параметру.

Таблиця 1 - Нова класифікація ЕКФЕ над простими полями. Координати точок ЕКФЕ 2-го та 4-го порядків

		Параметри	Порядок кривої	Точки 2-го порядку	Точки 4-го порядку
Повні	***1.a***	$\chi(a) = 1$ $\chi(d) = -1$	$N_E = 4n$	$\boldsymbol{D}_0 = (-1,0)$	$\pm\boldsymbol{F}_0 = (0, \pm 1/\sqrt{a})$
	1.b	$\chi(a) = -1$ $\chi(d) = 1$			$\pm\boldsymbol{F}_0 = (0, \pm 1/\sqrt{d})$
Скручені	***2***	$\chi(a) = -1$ $\chi(d) = -1$	$N_E = 4n$	$\boldsymbol{D}_0 = (-1,0)$	$\pm\boldsymbol{F}_{1,2} = (\pm\sqrt[4]{a/d},$ $\pm\sqrt{-1/\sqrt{ad}})$ $p \equiv 3 mod 4$
Квадратичні	***3***	$\chi(a) = 1$ $\chi(d) = 1$	$N_E \geq 8n$	$\boldsymbol{D}_{1,2} = (\pm\sqrt{a/d}, \infty)$	$\pm\boldsymbol{F}_0 = (0, \pm 1/\sqrt{d})$ $\pm\boldsymbol{F}_1 = (\infty, \pm 1/\sqrt{d})$ $\pm\boldsymbol{F}_{2,3} = (\pm\sqrt[4]{a/d},$ $\pm\sqrt{-1/\sqrt{ad}})$

За результатами досліджень різних класів ЕКФЕ було зроблено висновки, що квадратичні ЕКФЕ мають чотири особливих точки та, як наслідок, великий мінімальний кофактор порядку кривої, що збільшує кількість операцій при пошуку генератора та ускладнює роботу з такими кривими. На підставі цього використовувати квадратичні ЕКФЕ в криптоалгоритмах недоцільно, хіба що для теоретичного аналізу, так як квадратичні криві зі скрученими утворюють пару квадратичного крутіння[3].

За аналізом властивостей класів повних та скручених ЕКФЕ було зроблено висновки, що повні та скручені ЕКФЕ можуть бути рекомендовані для використання в криптоалгоритмах, оскільки вони мають циклічну підгрупу групи точок, в якій всі точки не є особливими -це суттєво спрощує реалізацію алгоритмів ЦП та шифрування на ЕКФЕ. Повні та скручені криві мають мінімальний кофактор порядку кривої4. Також вони мають високу швидкість експоненціювання точки, завдяки чому прискорюється виконання алгоритмів ЦПта шифрування[3].На підставі цього розглянемо ЕКФЕ, які належать класам повних та скручених, за новою класифікацією, з метою створення алгоритмів пошуку генератора криптосистеми для використання у протоколах ЦП.

2 Алгоритми пошуку базової точки на повних та скручених ЕКФЕ

Важливою властивістю повних та скручених ЕКФЕ є те, що при $p \equiv 1 mod 4$ вони мають мінімальний парний кофактор порядку кривої 4: $N_E = 4n$ де $n \in \mathbb{P}$. Циклічна підгрупа скручених ЕКФЕ простого порядку n має такі ж самі корисні для криптографічних застосувань і стандартизації властивості,що і повні криві Едвардса[3]. В алгоритмі ЦП важливим кроком є знаходження генератора криптосистеми - тобто базової точки простого порядку n. Для створення алгоритму пошуку базової точки для побудови криптосистеми на повних та скручених кривих було розглянуто декілька варіантів знаходження точок простого порядку.

Один з алгоритмів знаходження базової точки на повних ЕКФЕ було створено на запропонованому методі знаходження точки максимального порядку $4n$ [5], розробленого на підставі 3-х теорем щодо властивостей точок повної ЕКФЕ:

Теорема 1Для будь-якої точки (x,y) повної кривої Едвардса, що не належить колу радіуса 1, існують 2 точки ділення на 2 $\{P, P+D\}$ тоді і тільки тоді, коли $\chi(1 - y^2) = 1$.

Доведення

Скористуємося методом заміни змінної. Якщо взяти лише точки, порядки яких більше 4, та у формулах зробимо заміну

$$X = x_1^2, Y = y_1^2, Z = Y/X, V = XY, X, Y \neq 0.$$

Зробимо заміну у знаменнику (2) на $(X + Y)$ та $(2 - X - Y)$ відповідно. Згідно з (1) та (3) для однієї точки P кривої $ordP > 4$ справедливі вирази:

$$Z^2 - 2x^{-1}Z + 1 = 0,$$
$$dV^2 - 2x^{-1}V + 1 = 0, x \neq 0,1. \quad (4)$$

Дискримінанти

$$\Delta_1 = 4x^{-2}(1 - x^2),$$
$$\Delta_2 = 4x^{-2}(1 - dx^2), \quad (5)$$

та розв'язок

$$Z_{1,2} = x^{-1}\left(1 \pm \sqrt{1 - x^2}\right),$$
$$V_{1,2} = (xd)^{-1}\left(1 \pm \sqrt{1 - dx^2}\right). \quad (6)$$

Необхідність. Подвоєння будь якої точки P з ненульовими координатами згідно з законом (2) породжує єдину точку $2P = (x, y)$, та координати точок P і $2P$ є розв'язок двох рівнянь (4) у полі $\boldsymbol{F}_p$. Необхідною умовою існування розв'язку першого з рівнянь (4), як слідує з (5), є те, що елемент поля $\chi(1 - x^2) = 1$. При виконанні цієї умови окрім точки P, для якої $2P = (x, y)$, існує ще одна точка $P^* = P + D = (-x_1, -y_1)$, для якої $2P^* = 2P + 2D = (x, y)$,так як $2D = 0$. При $\chi(1 - x^2) = -1$ рівняння (4) розв'язків в полі немає. Необхідність умови теореми 1 доведено.

Достатність. Для будь якої точки кривої (1), у якої $ordP > 4$, для якої має місце розв'язок (3), справедливо дві тотожності (4). Достатньо, щоб один з дискримінантів (5) був квадратичним лишком, тоді другий дискримінант теж буде квадратичним лишком. Нехай точка$P = (x, y)$ належить кривій (1) де $a = 1$. Тоді рівняння $x^2 + y^2 = 1 + dx^2y^2$можна записати як $(1 - y^2) = x^2(1 - dy^2)$. Звідси вочевидь випливає, що для будь-якої точки (x, y) кривої вирази$(1 - y^2)$ та $(1 - dy^2)$є обидва квадратичними лишками або нелишками. У першому випадку існує дві точки ділення на 2, а в іншому випадку – не існує. Теорему 1 доведено[6].

Теорема 2 Необхідною і достатньою умовою існування 4-х точок 8-го порядку повної кривої Едвардса є $\chi(1 - d) = 1$.

Доведення

Необхідність. Нехай $Ord(P) = 8$, тоді $2P = F$. Відповідно з формулою (2) для координат $P = (x, y)$ маємо:

$$\frac{2xy}{(1 + dx^2y^2)} = 1, \quad \frac{y^2 - x^2}{(1 - dx^2y^2)} = 0.$$

Звідси $y^2 = x^2 \implies dx^4 - 2x^2 + 1 = 0 \implies x^2 = 1 \pm \sqrt{1 - d}$.

Тобто умова $\chi(1 - d) = 1$ теореми є необхідною умовою існування координат $x = \pm y$.

Достатність. Доведемо, що умова теореми завжди породжує рівно 4 точки 8-го порядку. Так як додаток $(1+\sqrt{1-d})(1-\sqrt{1-d})=d,$ то одне з значень у рівності $x^2=1\pm\sqrt{1-d}$ є квадратичним лишком, а друге – нелишком. Якщо вибирати двійковим квадрат з цієї альтернативи $(1+(-1)^{\kappa}\sqrt{1-d}),\ \kappa\in\{0,1\},$ отримуємо 4 точки $(\pm x,\pm y)$ 8-го порядку. Теорему 2 доведено [8].

Теорема 3Для будь-якої точки(x,y) повної кривої Едвардса, що не належить колу радіуса 1, справедлива рівність $\chi(1-x^2)\cdot\chi(1-y^2)=\chi(1-d).$

Доведення

Для точки (x,y) з урахуванням (1) де $a=1$ запишемо додаток

$(1-y^2)(1-x^2)=1+x^2y^2-x^2-y^2=y^2-dy^2=(1-d)x^2y^2.$

Тоді з останнього співвідношення випливає, що додаток $(1-y^2)(1-x^2)$ є квадратичним нелишком при $\chi(1-d)=-1$, та навпаки, що і доводить твердження теореми 3[6].

Метод знаходження точки максимального порядку полягає у тестуванні значення символу Лежандра або квадратичного характеру виразу $(1-y^2)$. Якщо виконується умова $\chi(1-d)=-1$, то відповідно до теореми 2, крива не має точок 8 порядку і порядок кривої $N_E=4n$,де $n\in\mathbb{P}$. Таким чином якщо $\chi(1-y^2)=-1$, то $\chi(1-x^2)=1$ і навпаки, що дає можливість знайти точку максимального порядку одним тестуванням характеру квадратичності $(1-y^2)$координати випадкової точки кривої. Практично $1/2$ випадкових точок кривої мають порядок $4n,1/4$ – порядок $2n$ та $1/4$– порядок n [4].

На базі методу знаходження точки максимального порядку, створено Алгоритм 1(рис.1) обчислення генератора криптосистеми, тобто точки простого порядку *n*на повній ЕКФЕ.

***Алгоритм* 1**:

умови: ЕКФЕ має вигляд (1), де $\chi(ad)=-1, N_E=4n, n\in\mathbb{P}, p\equiv 1mod4.$

1. знаходиться випадкова координата x точки $P=(x,y);$
2. якщо $x=0,$ або $\pm1,$ або $\pm\frac{1}{\sqrt{d}}$,то перейти до кроку1;
3. обчислюється $z=(1-x^2)(1-dx^2)^{-1}modp;$
4. якщо $\chi(z)\neq1,$ то перейти до кроку 1;
5. обчислюється $y=\sqrt{z}modp;$
6. якщо $\chi(1-y^2)\neq1,$ то $x\leftrightarrow y; P\leftarrow(y,x);$
7. обчислюється $G=2P;$

вихід: точка $G=(x_G,y_G)$, така, що Ord(*G*) = *n*.

$$\begin{matrix} N_E=4n \\ \forall P=(x,y) \\ OrdP>4 \\ p\equiv 1mod4 \end{matrix}\Bigg\| \begin{matrix} if\ \chi(1-y^2)=1 \Longrightarrow\ 2P\ \Longrightarrow\ G \\ \\ if\ \chi(1-y^2)=-1 \Longrightarrow x\leftrightarrow y\Rightarrow\chi(1-y^2)=1\Longrightarrow 2P\Longrightarrow G \end{matrix}$$

Рисунок 1–Алгоритм 1 находження базової точки на повних ЕКФЕ

Згідно з властивостями порядків точок повної ЕКФЕ над полями F_p, де $p\equiv1mod4$, подвоєння точки максимального порядку $4n$ створює точку, порядок якої дорівнює $2n$. Подвоєння точки порядку $2n$створює точку простого порядкуn.На підставі цієї властивості порядків точок повної ЕКФЕ розроблено Алгоритм 2 (рис.2) знаходження точки простого порядку.

***Алгоритм* 2**:

умови: ЕКФЕ має вигляд за формулою (1) де $\chi(ad)=-1, N_E=4n, n\in\mathbb{P},\ p\equiv1mod4.$

1. знаходиться випадкова координата x точки $P=(x,y);$
2. якщо $x=0,$ або $\pm1,$ або $\pm\frac{1}{\sqrt{d}}$, то перейти до кроку1;
3. обчислюється$z=(1-x^2)(1-dx^2)^{-1}modp;$
4. якщо $\chi(z)\neq1,$ то перейти до кроку 1;

5. обчислюється $y = \sqrt{z} mod p;$
6. обчислюється $G = 4P$;

вихід: точка $G = (x_G, y_G)$, така, що Ord(G) = n.

$$\begin{cases} N_E = 4n \\ p \equiv 1 \bmod 4 \\ OrdP > 4 \end{cases} \quad \forall P \Longrightarrow 4P \Longrightarrow G.$$

Рисунок 2– Алгоритм 2 знаходження базової точки на повних ЕКФЕ

Для скрученої ЕКФЕ знаходження точки простого порядку прискорюється удвічі завдяки одному подвоєнню випадкової точки. На підставі цього створено найшвидший Алгоритм 3(рис.3).

***Алгоритм* 3**:

умови: ЕКФЕ має вигляд за формулою (1) де $\chi(a) = \chi(d) = -1, N_E = 4n, n \in \mathbb{P},\ p \equiv 1 mod 4.$

1. знаходиться випадкова координата x точки $P = (x, y)$;
2. якщо $x = 0$, або ± 1, або $\pm \frac{1}{\sqrt{d}}$, то перейти до кроку1;
3. обчислюється $z = (1 - x^2)(1 - dx^2)^{-1} mod p$;
4. якщо $\chi(z) \neq 1$, то перейти до кроку 1;
5. обчислюється $y = \sqrt{z} mod p;$
6. обчислюється $G = 2P$;

вихід: точка $G = (x_G, y_G)$, така, що Ord(G) = n.

$$\begin{cases} N_E = 4n \\ p \equiv 1 \bmod 4 \\ OrdP > 4 \end{cases} \quad \forall P \Longrightarrow 2P \Longrightarrow G.$$

Рисунок 3 – Алгоритм 3 знаходження базової точки на скручених ЕКФЕ

3 Порівняльний аналіз швидкодії алгоритмів знаходження базової точки для побудови криптосистеми на ЕКФЕ та кривих у формі Вейєрштрасса

Алгоритми знаходження базової точки на повних та скручених ЕКФЕ виглядають значно простішими та швидкими у порівняно зі стандартним алгоритмом на канонічній кривій. Необхідно провести порівняльний аналіз швидкодії цих алгоритмів.

Стандартний алгоритм ЦП на еліптичних кривих:

1. знаходиться випадкова точка $P = (x, y)$;
2. обчислюється скалярний добуток nP;
3. якщо $(nP) \neq \mathbf{0}$, то перейти до кроку 1;
4. якщо$(nP) = \mathbf{0}$, то $P = G$;

вихід: точка $G = (x_G, y_G)$.

Знаходження кількості операцій, які потрібно виконати при пошуку точки простого порядку на кривих Вейєрштрасса в стандартному алгоритмі [7]:

- пошук точки, стандартним методом, що належить кривій, потребує 8 кроків до успіху;
- обчислення скалярного добутку nP в проективних координатахпотребує $\log(n)$ подвоєння. Всього $5.67M\log(n)$ операцій. У середньому $0.5\log(n)$додавання точок;
- $0.5 \cdot 11.17M \log(n) = 5.58M \cdot \log(n)$,де M – кількість множень у полі;
- загальне число операцій у полі з урахуванням 4-х кроків (в середньому) до успішного результату:

$$S = 8 \cdot 4 \cdot (5.67 + 5.58)M \cdot \log(n) = 360M \cdot \log(n).$$

Знаходження кількості операцій в запропонованих алгоритмах 1, 2 та 3 виконувався таким же чином [6, 7].

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 1:

- пошук точки. Невдача: $\forall$ точка, якщо $x = 0, \pm 1, \pm\frac{1}{\sqrt{d}}$; та $\forall\, \chi(z) \neq 1$.

Якщо умови x виконуються $\Longrightarrow$ можна вважати, що z– виконуються. $\Longrightarrow p(\chi(z) \neq 1) = \frac{1}{2}$. Тому, імовірність успіху $\geq 1 - \frac{1}{2} - \frac{4}{n} \approx \frac{1}{2} \Longrightarrow$ середня кількість до успіху дорівнює 2 крокам.

- обчислення $(1 - y^2)$ потребує $0{,}67M$ операцій;
- обчислення символу Лежандра $\chi(1 - y^2)$ потребує $M\log(n)$;
- одне подвоєння точки потребує $0{,}67M$ операцій;
- сумарна кількість операцій у полі:

$S_1 = 2 \cdot (5.67 + 0.68 + \log(n)) \cdot M == 2 \cdot (6.34 + \log(n))M.$

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 2:

- пошук точки. Середня кількість до успіху дорівнює 2 крокам. (див. Алгоритм 1);
- обчислення $G = 4P$ потребує два подвоєння;
- сумарна кількість операцій у полі:

$$S_2 = 2 \cdot 2 \cdot 5.67M = 22.68M.$$

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 3:

- Пошук точки. Середня кількість до успіху дорівнює 2 крокам. (див. Алгоритм 1);
- Обчислення $G = 2P$ потребує одне подвоєння;
- Сумарна кількість операцій у полі:

$$S_3 = 11{,}34M.$$

Усі значення кількості операцій у групі, які потрібно виконати при пошуку точки простого порядку в алгоритмах пошуку базової точки,записано у таблиці 2.

Таблиця 2 - Кількості операцій при пошуку генератора криптосистеми

Алгоритми	**Кількість операцій у полі,** **де M– кількість множень у полі**
Стандартний алгоритм	$S = 360M \cdot \log(n)$
Алгоритм 1	$S_1 = 2 \cdot (6.34 + \log(n))M$
Алгоритм 2	$S_2 = 22{,}68M$
Алгоритм 3	$S_3 = 11{,}34M$

На підставі отриманих результатів можна зробити порівняльний аналіз швидкодії та отримати значення виграшу γ для усіх запропонованих алгоритмів.

$$\gamma_1 = \frac{S}{S_1} = \frac{360M \cdot \log(n)}{2 \cdot (6.34 + \log(n))M} \approx 180$$
$$\gamma_2 = \frac{S}{S_2} = \frac{360M \cdot \log(n)}{22{,}68M} \approx 16\log(n)$$
$$\gamma_3 = \frac{S}{S_3} = \frac{360M \cdot \log(n)}{11{,}34M} \approx 32\log(n)$$

За розрахунком значення виграшу нових алгоритмів порівняно зі стандартним алгоритмом, було отримано результати:

- виграш у швидкодії Алгоритму 1 порівняно зі стандартним алгоритмом у $\gamma_1 = \frac{5}{s_1} \approx 180$ разів;
- виграш у швидкодії Алгоритму 2 порівняно зі стандартним алгоритмом у $\gamma_2 = \frac{5}{s_2} \approx 16\log(n)$ разів.
- виграш у швидкодії Алгоритму 3 порівняно зі стандартним алгоритмом у $\gamma_2 = \frac{5}{s_3} \approx 32\log(n)$ разів.

Результати обчислень дають змогу зробити обґрунтовані висновки, що знаходження генератора на ЕКФЕ із застосуванням запропонованих алгоритмів порівняно зі стандартним алгоритмом істотно більш швидше і відповідно ефективніше.

Висновки

1. Устаттірозв'язано актуальну науково-практичну задачу дослідження властивостей еліптичних кривих у формі Едвардса, придатних для використання в алгоритмах асиметричних криптосистем, зокрема, в алгоритмах цифрового підпису, які дозволяють підвищити швидкодію експоненціювання точки в цих криптосистемах.

2. Проведені дослідження дозволили запропонувати три новихалгоритми визначення базової точки для побудови криптосистеми на повних та скручених ЕКФЕ,

3. За результатами досліджень зроблено висновки, що розроблені алгоритми визначення базової точки швидше стандартного алгоритму ЦПна кривих у формі Вейєрштрассау 180, $16\log(n)$ та $32\log(n)$(де$n \in \mathbb{P}$)разів відповідно. Результати роботи можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

Перелік посилань

[1] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

[2] Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015. С.58-63.

[3] Бессалов А.В., Цыганкова О.В. Классификация кривих в форме Эдвардса над простым полем. // Прикладная радиоелектроника, Том 14 № 3, 2015. С.197-203.

[4] Bessalov A.V.,Tsygankova O.V. New properties of the Edwards form elliptic curveover a primefield // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) №180 2015. pp.137-143.

[5] Bessalov A. V., Tsygankova O.V. Interrelation of families of points of highorderon the Edwards curve over a primefield // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397. sci-hub.tw/10.1134/S0032946015040080

[6] Бессалов А.В., Цыганкова О.В. Метод определения точек максимального порядка на кривой Эдвардса. // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, випуск 2(26), 2014. С.18-21.

[7] Bernstein Daniel J.,Birkner Peter, JoyeMarc, Lange Tanja, Peters Christiane. Twisted Edwards Curves.//IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.

[8] Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография: монографія //изд-во «Политехника», КПИ им. Игоря Сикорского, Киев. 2017. – 272с.

Стаття надійшла: 28.02.2020.

References

[1] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

[2] Bessalov A.V., Tsygankova O.V. Proyzvodytelnost hruppovykh operatsyi na skruchennoi kryvoi Edvardsa nad prostym polem. // Radyotekhnyka #181, 2015. S.58-63.

[3] Bessalov A.V., Tsygankova O.V. Klassyfykatsyia kryvykh v forme Edvardsa nad prostым polem. // Prykladnaia radyoelektronyka, Tom 14 № 3, 2015. S.197-203.

[4] Bessalov A.V., Tsygankova O.V. New properties of the Edwards form elliptic curveover a primefield // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) №180 2015. pp.137-143.

[5] Bessalov A.V., Tsygankova O.V. Interrelation of families of points of highorderon the Edwards curve over a primefield // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397. sci-hub.tw/10.1134/S0032946015040080

[6] Bessalov A.V., Tsygankova O.V. Metod opredelenyia tochek maksymalnoho poriadka na kryvoi Эdvardsa. // Spetsialni telekomunikatsiini systemy ta zakhyst informatsii. Zbirnyk naukovykh prats, vypusk 2(26), 2014. S.18-21.

[7] Bernstein Daniel J.,Birkner Peter, JoyeMarc, Lange Tanja, Peters Christiane. Twisted Edwards Curves.//IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.
[8] Bessalov A.V. Эllyptycheskye kryvыe v forme Эdvardsa y kryptohrafyia: monohrafiia // yzd-vo «Polytekhnyka», KPY ym. Yhoria Sykorskoho, Kyev. 2017. – 272s.

Відомості про автора
Циганкова Оксана Валентинівна - без ступеню, без звання, асистент кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського, Київ 02232 просп. Маяковського 71 кв. 2.

О. В. Цыганкова

НОВЫЕ АЛГОРИТМЫ НАХОЖДЕНИЯ БАЗОВОЙ ТОЧКИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В ФОРМЕ ЭДВАРДСА

Национальный технический университет Украины КПИ имени Игоря Сикорского, Киев

O.V. Tsygankova

NEW BASE POINT ALGORITHMS FOR EDWARDS ELLIPTIC CURVES

National Technical University of Ukraine "Igor Sikorsky KPI", Institute of Physics and Technology, Kiev

ДО ВІДОМА АВТОРІВ

Найновіші правила оформлення і подання статей знаходяться на сайті журналу
http://itce.vntu.edu.ua/