УДК 004.056 **DOI:10.30837/rt.2019.3.198.15**

В.А. КУЛІБАБА

ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИПТОПЕРЕТВОРЕНЬ НА ЕЛІПТИЧНИХ КРИВИХ ТА КРИВИХ ЕДВАРДСА

Вступ

Останнім часом все більш гостро постає проблема швидкодії асиметричних криптографічних механізмів і, передусім, цифрових підписів. Це питання постає через те, що неминучим є збільшення для забезпечення криптографічної стійкості в умовах постійно зростаючих можливостей порушників довжин параметрів. Реальна поява квантового комп'ютера ставить перед дослідниками нові задачі: розробити, стандартизувати та впровадити нові механізми захисту інформації, стійкі, в тому числі, в постквантовий період. Проте, в так званий перехідний період до появи цих нових стандартів будуть використовуватися механізми цифрового підпису, в основі яких лежить математика еліптичних кривих. Новим запропонованим математичним апаратом є криві Едвардса, які мають певні переваги перед еліптичними кривими [2, 6]. Метою даної статті є огляд та порівняння криптографічних перетворень в групі точок еліптичних кривих та кривих Едвардса, а також попередня оцінка криптографічної стійкості кривих Едвардса.

Криві Едвардса та їх переваги

В оригінальному вигляді [2] криві Едвардса були запропоновані у вигляді

$$x^2 + y^2 = e^2(1 + x^2 y^2) \tag{1}$$

Закон складання точок для кривої у формі Едвардса визначений як

$$P_1(x_1, y_1) + P_2(x_2, y_2) = P_3\left(\frac{x_1 y_2 + x_2 y_1}{e(1 + x_1 x_2 y_1 y_2)}, \frac{y_1 y_2 - x_1 x_2}{e(1 - x_1 x_2 y_1 y_2)}\right) \tag{2}$$

Також було введено поняття так званого нейтрального елемента $0 = (0, e)$. Операція знаходження зворотної точки ЕК визначається як

$$-P(x_p, y_p) = P(-x_p, y_p) \tag{3}$$

на відміну кривих в класичній формі, де

$$-P(x_p, y_p) = P(x_p, -y_p) \tag{4}$$

Операція подвоєння точки із (2) визначається як

$$2P(x, y) = \left(\frac{2xy}{e(1 + x^2, y^2)}, \frac{y^2 - x^2}{e(1 - x^2 y^2)}\right) \tag{5}$$

Проте, як зазначається в [5], криві в оригінальній формі Едвардса мають ряд вагомих недоліків і не можуть бути застосовані в криптографічних додатках.

Для практичного застосування в криптографії в [1] обгрунтовано модифікацію кривих Едвардса. Зокрема, для циклічності групи точок кривої та видалення особливих точок було введено додатковий коефіцієнт *d*, такий, що символ Лагранжа $\left(\frac{d}{p}\right) = -1$, тобто *d* э квадратичним невичетом, а також на нього накладено обмеження $d(1 - de^4) \neq 0$. Рівняння кривої в модифікованому вигляді має вид

$$x^2 + y^2 = e^2(1 + dx^2 y^2) \tag{6}$$

Аналогічно з (2) закон складання точок кривої Едвардса визначається як

$$P_1(x_1, y_1) + P_2(x_2, y_2) = P_3(\frac{x_1y_2 + x_2y_1}{e(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{e(1 - dx_1x_2y_1y_2)}), \quad (7)$$

А операція подвоєння точки визначається як

$$2P(x, y) = \left(\frac{2xy}{e(1 + dx^2, y^2)}, \frac{y^2 - x^2}{e(1 - dx^2y^2)} \right) \quad (8)$$

Операція знаходження оберненої точки визначається згідно (3).

Порівняння складності перетворень в групі точок еліптичних кривих в класичному вигляді та кривих Едвардса

Груповий закон у проективних координатах для класичних еліптичних кривих.

Особливістю проективного базису для класичних ЕК є те, що при використанні проективних координат необхідно виконувати більше операцій множення, але немає операції ділення за модулем (інверсії), що дає виграш у швидкодії. Після виконання скалярного множення в проективному базисі необхідно зробити зворотне перетворення на афінні координати [6].

Проективний аналог короткого афінного рівняння Вейєрштраса (4) визначається [6]:

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in F(q). \quad (9)$$

Еліптична крива, що задається в проективних координатах, складається з усіх точок $R = (X, Y, Z)$ рівняння (9) так, що трійка (X, Y, Z) є розв'язком рівняння.

У проективних координатах груповий закон задається наступним чином:

1) точка $(0_F, 1_F, 0_F)$ є одиничним елементом 0_E відносно операції «+»;

2) точка $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на кривій E, що задана в проективних координатах, тоді обернена точка $-R = (X, -Y, Z)$;

3) нехай $R_1 = (X_1, Y_1, Z_1)$ і $R_2 = (X_2, Y_2, Z_2)$ є дві різні точки на E – такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (0_F, 1_F, 0_F)$, тоді сума R_1 та R_2 є $R_3 = (X_3, Y_3, Z_3)$. Координати X_3, Y_3 і Z_3 можуть бути обчислені як

$$\begin{aligned} X_3 &= -su, \\ Y_3 &= t(u + s^2X_1Z_2) - s^3Y_1Z_2, \\ Z_3 &= s^3Z_1Z_2, \end{aligned} \quad (10)$$

де $s = X_2Z_1 - X_1Z_2$, $t = Y_2Z_1 - Y_1Z_2$, і $u = s^2(X_1Z_2 + X_2Z_1) - t^2Z_1Z_2$; якщо $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на E, тоді її подвоєння є $2R = (X_3, Y_3, Z_3)$.

Координати точки $2R - (X_3, Y_3, Z_3)$ можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -su, \\ Y_3 &= t(u + s^2X) - s^3Y, \\ Z_3 &= s^3Z, \end{aligned} \quad (11)$$

де $t = 3X^2 + aZ^2$, $s = 2YZ$, а також $u = 2s^2X - t^2Z$.

Згідно [1] повні криві Едвардса визначені як

$$x^2 + y^2 = 1 + dx^2y^2; d(1 - d) \neq 0; \left(\frac{d}{p}\right) = -1, \quad (12)$$

а також було введено обмеження $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$.

Для повної кривої Едвардса (12) закон складання точок визначено у вигляді [4]

$$P(x_1, y_1) + Q(x_1, y_2) = Z\left(\frac{x_1 ч_2 + y_1 y_2}{1 - dx_1 x_2 y_1 y_2}, \frac{x_1 y_1 + x_2 y_2}{1 + dx_1 x_2 y_1 y_2}\right) \tag{13}$$

$$2P(x, y) = \left(\frac{x_1^2 - y_1^2}{1 - dx_1^2 y_1^2}, \frac{2x_1 y_1}{1 + dx_1^2 y_1^2}\right) \tag{14}$$

Так як в афінних координатах присутнє знаходження оберненого елемента в полі, то прийнято переходити до проективних координат. Це пояснюється тим, що [4] операція інверсії в полі з обчислювальної точки зору є найбільш складною. Причому, заміна $x = \frac{x}{z}, y = \frac{y}{z}$ дозволяє перейти в проективні координати. В такому випадку рівняння кривої має вигляд

$$(X^2 + Y^2)Z^2 = Z^4 + dX^2 Y^2, X = xZ, Y = yZ\,. \tag{15}$$

Закон складання точок в проективних координатах має вигляд

$$P(X_1, Y_1, Z_1) + Q(X_2, Y_2, Z_2) = (X_3, Y_3, Z_3)\,.$$

Після підстановки [4] маємо:

$$y_3 = \frac{Y_3}{Z_3} = \frac{\left(\frac{X_1 Y_2}{Z_1 Z_2} + \frac{X_2 Y_1}{Z_1 Z_2}\right)\left(1 - d\frac{X_1 X_2 Y_1 Y_2}{Z_1^2 Z_2^2}\right)}{\left(1 + d\frac{X_1 X_2 Y_1 Y_1}{Z_1^2 Z_2^2}\right)\left(1 - d\frac{X_1 X_2 Y_1 Y_2}{Z_1^2 Z_2^2}\right)} = \frac{Z_1 Z_2 (Z_1^2 Z_2^2 - dX_1 X_2 Y_1 Y_2)(X_1 Y_2 + X_2 Y_1)}{(Z_1^2 Z_2^2 + dX_1 X_2 Y_1 Y_2)(Z_1^2 Z_2^2 - dX_1 X_2 Y_1 Y_2)} \tag{16}$$

$$x_3 = \frac{X_3}{Z_3} = \frac{Z_1 Z_2 (Z_1{}^2 Z_2{}^2 + dX_1 X_2 Y_1 Y_2)(X_1 X_2 - Y_1 Y_2)}{(Z_1{}^2 Z_2{}^2 + dX_1 X_2 Y_1 Y_2)(Z_1{}^2 Z_2{}^2 - dX_1 X_2 Y_1 Y_2)}\ . \tag{17}$$

Нехай $A = Z_1 Z_2; B = A^2; C = X_1 X_2; D = Y_1 Y_2; E = dCD; F = B - E; G = B + E$, тоді координати точок виражаються через

$$\begin{aligned} Y_3 &= A \cdot F((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D) \\ X_3 &= A \cdot G \cdot (D - C) \\ Z_3 &= F \cdot G \end{aligned} \tag{18}$$

Після підрахунку елементарних операцій в полі маємо, що $V_E = 10M + 1S + 1U$ операцій в полі. При цьому можна прийняти[5], що $1S \approx \frac{2}{3}M$.

За аналогічною методикою виконуються оцінки подвоєння точок:

$$x_3 = \frac{X_3}{Z_3} = \frac{\left(\left(\frac{X_1}{Z_1}\right)^2 - \left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + \left(\frac{Y_1}{Z_1}\right)^2\right)}{\left(2 - \left(\frac{X_1}{Z_1}\right)^2 - \left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + \left(\frac{Y_1}{Z_1}\right)^2\right)} = \frac{\left(X_1^2 - Y_1^2\right)\left(X_1^2 + Y_1^2\right)}{\left(2Z_1^2 - X_1^2 - Y_1^2\right)\left(X_1^2 + Y_1^2\right)} \tag{19}$$

$$y_3 = \frac{Y}{Z} = \frac{2\frac{X_1 Y_1}{X_1}\left(2-\left(\frac{X_1}{Z_1}\right)^2-\left(\frac{Y_1}{Z_1}\right)^2\right)}{\left(2-\left(\frac{X_1}{Z_1}\right)^2-\left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2+\left(\frac{Y_1}{Z_1}\right)^2\right)} = \frac{2X_1Y_1(X_1^2+Y_1^2)}{(2Z_1^2-X_1^2-Y_1^2)(X_1^2+Y_1^2)} \quad (20)$$

Після виконання заміни [3, 5] та підрахунку кількості операцій складність подвоєння точки на ЕК в формі Едвардса оцінюється як $T_E = 3M + 4S$. За аналогічною методикою оцінюється складність виконання операцій додавання та подвоєння точок в проективних координатах для еліптичних кривих в канонічній формі.

Зведені дані щодо складності операцій наведено в табл. 1, де для спрощення використано такі співвідношення [5]: 1S = 0.67M та $1U$ = 0.5M.

Таблиця 1

Порівняння складності операцій множення і додавання точок ЕК
в кривих Едвардса та канонічних кривих

	Криві у формі Вейерштрасса		Криві у формі Едвардса	
	Додавання	Множення	Додавання	Множення
1	*12M+2S*	*7M+5S*	*10M+1S+1U*	*3M+4S*
2	*13.33M*	*10.33M*	*11.57M*	*5.67M*

Як зазначено в роботі [5], криві у формі Едвардса мають значний виграш у складності виконання операцій в групі точок еліптичної кривої, приріст швидкодії сягає 1,5 рази, що, безумовно, є важливим з точки зору практичних застосувань.

Порівняльний аналіз стійкості класичних ЕК та ЕК Едвардса та складності атак

Відомо [6], що найбільш універсальною атакою на асиметричні крипто перетворення є атаки типу «повне розкриття», яка зводиться до дискретного логарифмування в групі точок еліптичної кривої, а також для електронного підпису до атаки «повне розкриття» на основі підписаних даних. Тому в якості основної загрози будемо розглядати загрозу визначення особистого ключа *d* шляхом дискретного логарифмування у відповідних групах кривих.

Нехай порушникові відомо порядок базової точки еліптичної кривої, відкритий ключ Q, а також всі загальносистемні параметри, включаючи модуль перетворення q. Він також знає, що особистий та відкритий ключі пов'язані між собою співвідношенням

$$Q_i = d_i \cdot G(\mathrm{mod} q) . \quad (21)$$

У [3] показано, що еліптичні криві Едвардса, які є придатними до застосувань у крипторгафії, є ізоморфними до ЕК у формі Вейерштрасса, до них можуть бути застосовані ті ж самі методи криптоаналізу, тобто дискретного логарифмування в групі точок.

За цієї умови для знаходження особистого ключа d скористаємося методом ро-Поларда як одним з найбільш ефективних [4]. Суть його полягає у наступному.

Нехай для деякого кінцевого набору W є відображення $F: W \to W$. Сама послідовність формується за правилом $w_0 \in W, w_{k+1} = F(w_k)$. Далі, нехай n – порядок базової точки G, а відкритий ключ Q є точкою на цій кривій. Тоді для знаходження секретного параметра *d* Поллардом було введено інтерполяційну функцію

$$F(Y) = \begin{Bmatrix} G+Y, 1 \le Y(x) \le n \\ 2Y, n/3 \le Y(x) \le 2n/3 \\ Q+Y, 2n/3 \le Y(x) \le n \end{Bmatrix}. \quad (22)$$

Правило розбиття за інтервалами може бути обрано інше, а замість *x*-координати точки використовувати *y*-координату. Як можна зазначити, у 2/3 випадків використовується додавання точок, а в 1/3 – подвоєння.

Існує також альтернативна форма завдання рекурентних співвідношень для обчислення наступної точки:

$$Y_k = \alpha_k G + \beta_k Q,$$
$$\alpha_{k+1} = \begin{cases} \alpha_k, Y_k \in S_1 \\ 2\alpha_k, Y_k \in S_2 \\ \alpha_k + 1, Y_k \in S_3 \end{cases} \qquad (23)$$
$$\beta_{k+1} = \begin{cases} \beta_k + 1, Y_k \in S_1 \\ 2\beta_k, Y_k \in S_2 \\ \beta_k, Y_k \in S_3 \end{cases}$$

Використання (22) чи (23) дозволяє побудувати дві послідовності, збіг значень в яких $Y_i = Y_j$ при різних індексах дозволяє створити колізію та визначити особистий ключ [6]:

$$d = \frac{\alpha_j - \alpha_i}{\beta_i - \beta_j} G (\mathrm{mod}\, n). \qquad (24)$$

Також показано, що ймовірність знаходження колізії при *k* спробах складає [6]:

$$P(n,k) = 1 - \frac{n}{n} \cdot \left(\frac{n-1}{n}\right) \cdot \left(\frac{n-2}{n}\right) \ldots \left(\frac{n(k-1)}{n}\right) = 1 - \left(1 - \frac{1}{n}\right) \cdot \left(\frac{2}{n}\right) \ldots \left(\frac{n(k-1)}{n}\right). \qquad (25)$$

При $k << n$ маємо

$$P_k = 1 - e^{-\frac{k(k-1)}{2n}} \qquad (26)$$

Тому (26) дає можливість також обчислити *k* необхідних елементів послідовності (22), щоб отримати колізію з необхідною ймовірністю.

Тепер оцінимо складність обчислення послідовності довжиною *k* для кривих у формі Вейерштрасса та у формі Едвардса.

Побудування послідовності довжиною *k* потребує *k -1* викликів функції F(Y). Позначимо складність виконання однієї операції додавання точок ЕК як I_+, а складність подвоєння точки на ЕК як I_*. Так як послідовність $w_0 \in W, w_{k+1} = F(w_k)$ можна вважати випадковою, маємо

$$I_{sum} = (k-1)\left(\frac{1}{3} I_* + \frac{2}{3} I_+\right). \qquad (27)$$

Підставимо із табл. 1 значення для різних кривих та оцінимо складність генерації послідовності довжиною *k* для ЕК у формі Едвардса та канонічних кривих.

Для канонічних кривих:

$$I_{sum.canonocal} = (k-1)\left(\frac{1}{3} \cdot 10.33M + \frac{2}{3} \cdot 13.33M\right) = (k-1) \cdot 12.33M$$

Для кривих Едвардса:

$$I_{sum.edwards} = (k-1)\left(\frac{1}{3} \cdot 5,67M + \frac{2}{3} \cdot 11.57M\right) = (k-1) \cdot 9.603M$$

Тобто, побудування послідовності точок для криптоаналізу методом ро-Полларда є більш ефективним для кривих Едвардса, ніж для кривих в канонічному вигляді. Слід зазначити, що оскільки в (22) було прийнято, що множення точок виконується тільки в третині випадків, тобто коли $n/3 \le Y(x) \le 2n/3$, а для випадку додавання точок різниця в складності операцій не настільки суттєва, як у випадку множення, то приріст швидкості крипто аналізу складає приблизно 22 %, проте для інших алгоритмів, які більш активно використовують множення точок ЕК, він може бути суттєво вищим. Таким чином, дійне збільшення швидкодії також дозволяє збільшити швидкодію, а значить зменшити складність криптоаналізу, тобто розв'язання дискретного порівняння в групі точок кривих Едвардса. Вказаний факт необхідно враховувати при переході від використання точок еліптичних кривих до кривих Едвардса.

Висновки та рекомендації

1. Еліптичні криві Едвардса, як новий вид представлення еліптичних кривих, має суттєві переваги, основними серед яких є швидкодія. В цьому випадку можливість прискорити виконання підпису у 1,5 рази є дуже привабливою, проте, на наш погляд, потребує подальшого дослідження в частині стійкості проти атак як з використанням класичних обчислювальних пристроїв, так і після появи квантового комп'ютера.

2. Проведений аналіз також дозволив дійти висновку, що для кривих Едвардса можливе прискорення порівняно с канонічними кривими виконання алгоритмів крипто аналізу, яке залежить від кількості використання у конкретному алгоритмі операцій множення точок ЕК. Також слід враховувати, що застосування механізмів, які базуються на ЕК, можливе тільки обмежено, адже після появи квантового комп'ютера їх використання вже не забезпечить необхідного рівня стійкості.

3. Проблемним також є питання впровадження реалізацій, що використовують криві Едвардса в існуючу інфраструктуру відкритих ключів. На наш погляд, доцільним є розгляд питання щодо вдосконалення моделей, методів та засобів побудови крипто стійких загальносистемних параметрів для криптографічних перетворень в групах точок еліптичних кривих в напрямку підвищення їх стійкості, а також обґрунтування можливостей використання таких параметрів у постквантовий період. Вказане дозволить, насамперед, зосередитися на стандартизації нових криптографічних механізмів постквантового періоду.

Список літератури:

1. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin : Springer, 2007. PP. 29–50.

2. Edwards H.M. A normal form for elliptic curves // Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, PP. 393-422

3. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary, Dawson Ed. Twisted Edwards Curves Revisited // ASIACRYPT. 5350. New York: Springer, 2008. PP. 326-343

4. Балагура Д.С. Методы оценки сложности криптоанализа для криптографических приложений в группе точек эллиптической кривой, учитывающие вероятность коллизий / Д.С. Балагура, Ю.И. Горбенко // Радиотехника. 2005. Вып. 142. С. 205 – 214.

5. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография: монография. Киев : ІВЦ «Видавництво «Політехника»», 2017. 272с.

6. Горбенко І. Д. Прикладна криптологія : підручник / І. Д. Горбенко, Ю. І. Горбенко ; вид. 2-ге. Харків : Форт, 2013. 878 с.

7. Горбенко Ю.І., Єсіна М.В., Кулібаба В.А. Сутність та умови здійснення атаки на зв'язаних ключах відносно ектронних підписів IBS-1 та IBS-2 ДСТУ ISO/IEC 14888-3 // Системи обробки інформації. 2016. № 7. С. 113-118. (http://www.hups.mil.gov.ua/periodic-app/article/16934)

Харківський національний
університет імені В.Н. Каразіна;

Надійшла до редколегії 06.09.2019