УДК 512.742.72

АНИМАЦИЯ ТОЧЕК ЭКСПОНЕНЦИРОВАНИЯ КРИВОЙ ЭДВАРДСА

О. В. Цыганкова[1, a], Р. И. Цыганков[1]

[1] *Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Физико-технический институт*

Аннотация

В работе рассматривается ряд новых свойств полных кривых Эдвардса над простым полем. Предлагается простой метод нахождения точек заданного порядка, метод нахождения порядка точки на полной кривой Эдвардса, метод реконструкции точек kP скалярного произведения. Впервые представлена анимация последовательно соединенных точек скалярного произведения $kP^{(i)}$ для 6-ти генераторов $P^{(i)}$ кривой Эдвардса порядка 28 над полем F_{19}.

Ключевые слова: эллиптические кривые в форме Эдвардса, порядок кривой, порядок точки.

Введение

Эллиптические кривые в форме Эдвардса сегодня являются наиболее быстрыми и перспективными для использования в асимметричных криптосистемах. В сравнении с кривыми в форме Вейерштрасса, полные кривые Эдвардса выигрывают в быстродействии арифметики экспоненцирования точки кривой на $50-60\%$ [1, 2, 3]. Наличие аффинных координат нейтральной точки группы и универсальность закона сложения еще в большей степени ускоряет программную реализацию криптоалгоритмов. В сегодняшних, явно устаревших, стандартах криптосистем (в том числе стандарте США FIPS-186-2) еще используются кривые над простым полем, рассчитанные в 1997 году [4]. Внедрение новой технологии полных кривых Эдвардса в современные стандарты криптосистем даст большой экономический выигрыш [3]. В данной работе мы предлагаем простой метод нахождения точек заданного порядка на полной кривой Эдвардса, определяем условие делимости на 2 для точек полной кривой Эдвардса большого порядка (более 4-го), предлагаем 2 утверждения о порядках точек кривой доказанные в работе [2], и, на основе взаимосвязи точек семейства — метод реконструкции точек kP скалярного произведения. Впервые представлена завораживающая анимация реконструкции точек kP скалярного произведения.

1. Методы нахождения точек заданного порядка

Полные кривые Эдвардса определенные в [5]

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

подходят для использования в криптосистемах, если их порядок $N = 4n$, где n — большое простое число ($n > 2^{190}$). Если порядок генератора кривой $\mathrm{Ord}P = 4n$, то генератор криптосистемы $G = 4P$ имеет порядок n. Точки 8-го порядка отсутствуют согласно теореме 3, [5] если $(1-d)$ — квадратичный невычет.

Утверждение 1. *На полной кривой Эдвардса (1) порядка $4n$ существуют точки деления на 2 для всех точек, кроме точек $\langle P\rangle$ максимального порядка и точек $\pm F$ четвертого порядка.*

Если случайная точка кривой Q имеет порядок $2n$, то обе точки деления на 2 $\{Q/2, Q/2+D\}$ имеют максимальный порядок $4n$. Если точка Q имеет порядок n, то порядки точек деления на 2 $\{Q/2, Q/2+D\}$ равны n и $2n$, соответственно.

Теперь для нахождения порядка точек кривой Эдвардса не требуется вычислять скалярное произведение nQ. Если у случайной точки кривой (x_Q, y_Q) величина $(1-y_Q^2)$ – квадратичный невычет, то $\mathrm{Ord}(Q) = 4n$. В противном случае порядок точки равен n или $2n$. Получить такую точку можно непосредственно, меняя местами координаты x_Q и y_Q. В [2] доказана теорема 2: *Для любой не базовой точки (x_1, y_1) кривой (1) справедливо равенство* $\left(\frac{1-x_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right) = \left(\frac{1-d}{p}\right)$. После этого генератор G порядка n находится одним удвоением $G = 2Q$.

Утверждение 2. *Для кривой Эдвардса порядка $4n$ любое семейство из 8 точек (x_1, y_1), (y_1, x_1), лежащих на одной окружности, содержит 4 точки порядка $4n$, 2 точки порядка $2n$ и 2 точки порядка n.*

Замечание. Приведенные выше свойства кривой Эдвардса не должны снижать сложности вычисления дискретного логарифма в группе точек $\langle G\rangle$ простого порядка n. Действительно, согласно утверждению 2, из 8-ми точек каждого семейства на колесе точек рис. 2 лишь 2 обратных точки имеют порядок n подгруппы $\langle G\rangle$. Поэтому, как и для кривых в канонической форме, сложность DLP [2] здесь снижается лишь вдвое за счет обратных точек. Тем не менее,

[a] cig@pti.kpi.ua

эти свойства могут послужить основой для поиска новых методов решения проблемы дискретного логарифма.

2. Взаимосвязь семейств точек больших порядков. Реконструкция точек kP кривой Эдвардса

На основе симметрии восьми точек полной кривой Эдвардса $(\pm x_1, \pm y_1)$, $(\pm y_1, \pm x_1)$ семейства точек, лежащих на одной окружности, и формул (2)

$$\begin{aligned} P+D &= (x_1,y_1)+(-1,0) &&= (-x_1,-y_1) = P^* \\ P+F &= (x_1,y_1)+(0,1) &&= (-y_1,x_1) \\ P-F &= (x_1,y_1)+(0,-1) &&= (y_1,-x_1). \end{aligned} \tag{2}$$

связывающих эти точки, можно построить алгоритм нахождения всех точек скалярного произведения kP точки P, если известен сегмент 1/8 части всех точек. Этот метод предложен в работе [2]. Проиллюстрируем примером.

Пример. Рассмотрим кривые Эдвардса с модулем $p = 19$, для которого выполняются оба условия теоремы 3 [2]. При $d \in \{-1, 2, 2^{-1}\}$ имеем суперсингулярные кривые с порядком $N_E = p + 1 = 20$. Исключим также кривые с порядком, кратным 8, для которых $(1 - d)$ — квадратичный вычет. Получаем две кривые с параметрами $d = 8$ и $d^{-1} = 12$, которые дают пару кривых кручения с порядками 28 и 12 (для них $t = \pm 8$). Точки первой из них представлены на рис. 1.

Обозначим $P = (2, 9)$, $Q = (3, 5)$, $R = (4, 8)$, $S = (5, 3)$, $T = (8, 4)$, $U = (9, 2)$ — точки первого квадранта. Здесь точками максимального порядка 28 являются точки P, Q, R, для которых значения $(1 - y^2)$ являются квадратичными невычетами. Всех таких точек $\varphi(28) = 12$, по 3 точки в каждом квадранте. Кроме них, имеется 6 точек 14-го и 6 точек 7-го порядков. Удвоение точек P, Q, R дает точки 14-го порядка $2P = (-8, 4) = -T^*$, $2Q = (-9, 2) = -U^*$, $2R = (5, -3) = -S$. Итак, в первом квадранте имеем одну точку S 14-го порядка и 2 точки и U 7-го порядка.

Циклическую группу точек кривой kP можно представить в виде последовательности точек на окружности в порядке роста скалярного числа $k = 0, 1, 2, \ldots, N_E - 1$ по часовой стрелке. Для нашего примера такая точечная окружность представлена на рис. 2. Назовем этот график колесом Бессалова т.к. идея принадлежит ему [6]. Точки колеса Бессалова, соединенные диаметральными линиями, связаны как P и $P^* = P + D$. Для любой не базовой точки семейство из 8 связанных линиями точек на рис. 2 лежат на одной окружности на графике кривой рис. 1.

Знание около 1/8 части всех точек позволяет реконструировать все другие точки кривой. Пусть точка P порождает все точки кривой и известны 4 точки: $P = (2, 9)$, $2P = (-8, 4)$, $4P = (-5, 3)$, $7P = -F = (0, -1)$. В силу свойства $(x_1, y_1) + (-y_1, -x_1) = (0, -1) = -F$, легко находятся точки $6P = (-9, -2)$,

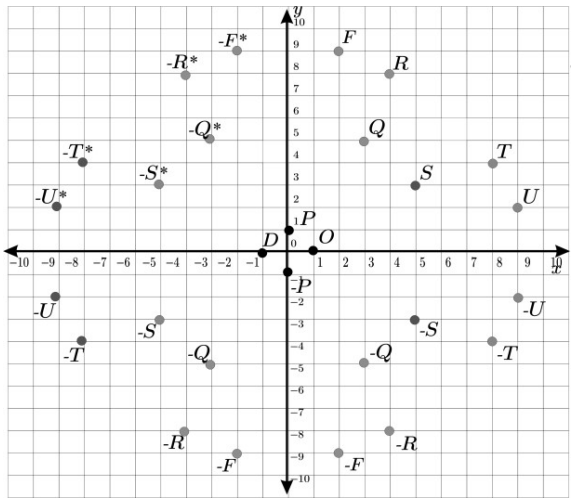

Рис. 1. График полной Эдвардса при $p = 19$, $d = 8$, $N_E = 28$

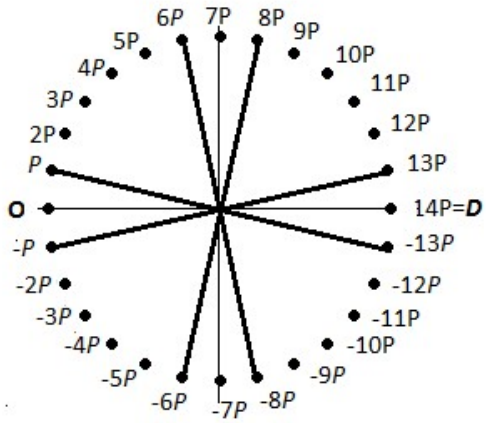

Рис. 2. Колесо точек циклической кривой порядка $N_E = 28$

$5P = (-4, 8)$, $3P = (-3, 5)$, меняя местами координаты $x \leftrightarrow y$ и их знаки соответственно точек P, $2P$ и $4P$. Координаты точек kP при $k = 0 \ldots 14$ представлены в таблице 1.

Для определения координат точек правее точки 4-го порядка мы используем свойство $P + D = P^* = (-x_1, -y_1)$ или $P - P^* = D = 14P$. Например, точка $13P$, вертикально симметричная точке P и равная $-P^*$, имеет координаты $(-x_1, y_1)$. В таблице 1 хорошо видна симметрия (антисимметрия) координат точек верхней половины рис. 2: все y-координаты симметричны относительно точки $7P$, тогда как x-координаты обратны по знаку. Точки нижней половины колеса Бессалова рис. 2 обратны точкам верхней половины с инверсией знака y-координаты. Например, точка $17P = 28P - 11P = -11P = (3, -5)$.

Итак, при известных 4-х точках (причем одна из них базовая $-F$) мы без вычислений получили координаты всех 28 точек kP кривой Эдвардса. Этот метод годится для кривой любого порядка, при этом предвычисления состоят в расчете координат точек kP для $k = 2, 3, \ldots, (n-1)/2$, что составляет практически 1/8-ю часть порядка кривой. Возвращаясь

Табл. 1. Координаты точек kP полной кривой Эдвардса при $d = 8$, $N_E = 28$

kP	O	P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$
x_k	1	2	–8	–3	–5	–4	–9	0	9	4	5	3	8	–2	–1
y_k	0	9	4	5	3	8	–2	–1	–2	8	3	5	4	9	0

к графику кривой на рис. 1, мы находим в таблице 1 все ее точки как скалярное произведение kP. Точки первого квадранта $Q = (3, 5) = 11P$, $R = (4, 8) = 9P$ имеют порядок 28, точка $S = (5, 3) = 10P$ имеет порядок 14, а две точки $U = (9, 2) = -8P$ и $T = (8, 4) = 12P$ — порядок 7. Это отвечает выводам предыдущего анализа.

Заметим, что существует лишь 2 точки максимального порядка, порождающие известный генератор G подгруппы точек простого порядка n — это точки P и P^*, для которых $2P^* = 2P$, $G = 4P$. Все четные точки колеса рис. 2 при переходе к порождающей точке P^* сохраняют свои координаты, а нечетные P^*, $3P^*$, $5P^*$, ... меняют знаки обеих координат.

График точек кривой на рис. 1 является точечным и, естественно, не отвечает термину «кривая Эдвардса».Если предварительно соеденить прямыми линиями точки скалярного произведения kP,$k = 1, 2, 3, \ldots, N = 28$, то получится интересная анимация этого графика кусочно-ломаной кривой. Всего имеется $\varphi(28) = 12$ точек 28-го порядка, которые могут «нарисовать» 6 различных графиков (обратные точки дают один рисунок). Это точки $P^{<1>} = (2, 9)$, $P^{<2>} = (3, 5)$, $P^{<3>} = (4, 8)$, $P^{<4>} = (-4, 8)$, $P^{<5>} = (-3, 5)$, $P^{<6>} = (-2, 9)$. Нарисованные этими 6-ю генераторами графики представлены на рис. 3.

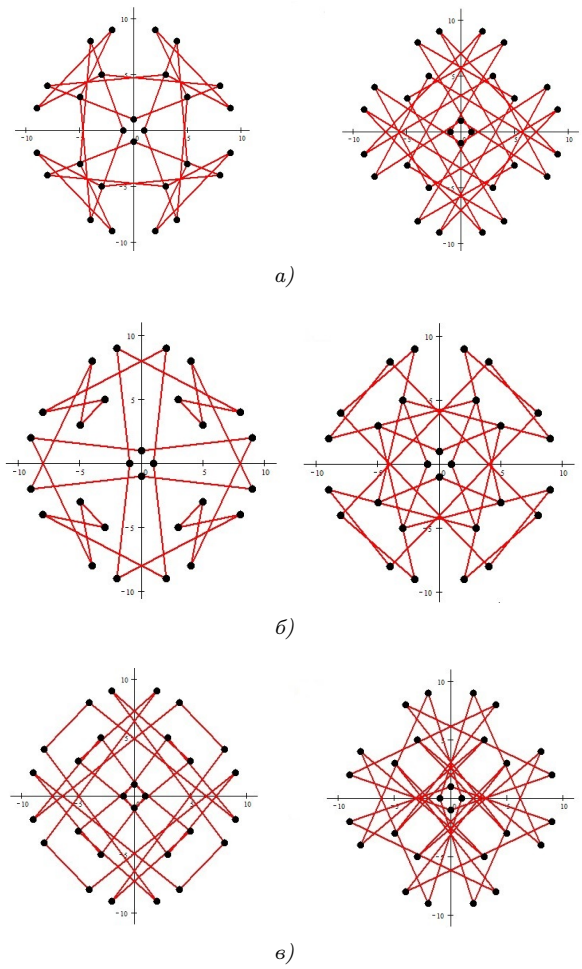

Рис. 3. Последовательно соединенные точки скалярного произведения $kP^{<i>}$ для 6 генераторов $P^{<i>}$ кривой Эдвардса порядка 28 над полем F_{19}

Выводы

В данной работе предложено новый более простой метод нахождения порядка кривой и реконструкции всех точек полной кривой формы Эдвардса. Наглядно представлено новую анимацию соединения точек полной кривой в форме Эдвардса.

Перечень использованных источников

1. Бессалов А. В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника. — 2011. — № 167. — С. 203–208.
2. Bessalov A. V., Tsygankova O. V. Interrelation of families of points of high order on the Edwards curve over a prime field // Problems of Information Transmission. — 2015. — Vol. 4, no. 51. — P. 391–397.
3. Бессалов А. В., Циганкова О. И. Производительность групповых операций на скрученной кривой Эдвардса над простым полем // Радиотехника. — 2015. — № 181. — С. 58–63.
4. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування: монографія. — 2012. — № 181. — С. 870.
5. Бессалов А. В., Циганкова О. И. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой // Проблемы передачи информации. — 2017. — Т. 53, № 1. — С. 101–111.
6. Бессалов А. В., Циганкова О. И. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем // Захист інформації. — 2015. — Т. 17, № 1. — С. 73–80.