УДК 621.391.15 : 519.7

А.В. БЕССАЛОВ, Л.В.КОВАЛЬЧУК, Н.В. КУЧИНСКАЯ

ОЦЕНКА ЭФФЕКТИВНОСТИ ДИФФЕРЕНЦИАЛЬНОГО СЛОЖЕНИЯ ТОЧЕК КРИВЫХ В ОБОБЩЕННОЙ ФОРМЕ ЭДВАРДСА

Введение

Наряду с бесспорным приоритетом аспектов безопасности значимую роль в современных криптосистемах играет быстродействие. Если на заданном уровне безопасности удастся вдвое сократить время, например, на вычисление цифровой подписи, следует ожидать и пропорционального снижения стоимости этой процедуры («время – деньги»). Потому временные затраты на вычисления – важная составляющая эффективности криптосистемы.

В большинстве алгоритмов криптосистем на эллиптических кривых основной и наиболее трудоемкой является экспоненцирование точки P или скалярное произведение kP (где число $k < ordP = n$). Сегодня известно множество методов его вычисления [1,2]. Мы остановились на одном из наиболее изящных – методе дифференциального сложения точек Монтгомери [3], обеспечивающего гарантированную защиту от некоторых атак побочного канала. Вместе с тем недавно (2017) предложен новый метод реализации дифференциального сложения точек на кривых в форме Эдвардса [4], имеющий, как и для кривых в форме Монтгомери, рекордно низкую сложность вычислений. Прежние сравнительные оценки эффективности вычислений для кривых Эдвардса и других типов кривых [5 – 9] с учетом результатов работы [4] могут быть улучшены. Одной из целей данной статьи является сравнительная оценка скорости экспоненцирования точки на основе алгоритма Монтгомери для кривых в форме Эдвардса и Вейерштрасса. Последние получили наибольшее распространение в современных стандартах асимметричной криптографии, которые, очевидно, требуют обновления.

В разделе 1 работы даны определения и свойства 3-х классов кривых в обобщенной форме Эдвардса [7]. Во 2-м разделе рассматривается алгоритм Монтгомери дифференциального сложения точек для кривой в форме Монтгомери [3] с оценкой стоимости вычислений на одном шаге рекуррентного цикла. В разделе 3 дан вывод новых формул дифференциального сложения-вычитания и удвоения точек для кривой в обобщенной форме Эдвардса, который не приведен в [4], с первой оценкой стоимости вычислений. В разделе 4 обсуждаются аспекты выбора и оптимизации параметров кривой в обобщенной форме Эдвардса для ее криптографических приложений и стандартизации. Здесь же приведены формулы сложения произвольной точки с одной из 4-х особых точек, которые необходимы для построения завершенной арифметики кривых при неполном законе сложения точек. Наконец, в 5-м разделе дан краткий сравнительный анализ трех полученных в [4] оценок стоимости вычислений, и оценивается потенциальный выигрыш в скорости вычисления скалярного произведения kP на кривых Эдвардса по сравнению с кривыми в форме Вейерштрасса, равный 3.09.

1. Классификация кривых в обобщенной форме Эдвардса

Эллиптическая кривая *в обобщенной форме Эдвардса* [7] определяется уравнением

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

В отличие от уравнения этой кривой в [6] здесь мы параметр a умножаем на y^2 вместо x^2. Если квадратичный характер $\chi(ad) = -1$, кривая (1) изоморфна *полной кривой* Эдвардса [5] с одним параметром d

$$E_d: x^2 + y^2 = 1 + dx^2y^2,\ \chi(d) = -1,\ d \neq 0,1. \qquad (2)$$

При $\chi(ad)=\chi(a)=\chi(d)=1$ имеет место изоморфизм кривой (1) с *квадратичной кривой Эдвардса* [7]

$$E_d:\ x^2+y^2=1+dx^2y^2,\ \chi(d)=1,\ d\neq 0,1. \tag{3}$$

с одним параметром d, определенным, в отличие от (2), как квадрат. Это отличие ведет к кардинально различным свойствам кривых (2) и (3) [7], которые резюмируются ниже. Несмотря на это, в пионерской статье [6] эти классы кривых объединены общим термином *кривые Эдвардса.*

Наконец, при $\chi(a)=\chi(d)=-1$ кривая (1) попадает в класс *скрученных кривых Эдвардса*. Это единственный случай, оправдывающий введение нового параметра a в уравнение кривой (1) в работе [6].

В работе [7] модифицированный универсальный закон сложения точек кривой (1) имеет вид

$$(x_1,y_1)+(x_2,y_2)=\left(\frac{x_1x_2-ay_1y_2}{1-dx_1x_2y_1y_2},\frac{x_1y_2-x_2y_1}{1+dx_1x_2y_1y_2}\right) \tag{4}$$

При совпадении двух точек получим из (4) закон удвоения точек

$$2(x_1,y_1)=\left(\frac{x_1^2-ay_1^2}{1-dx_1^2y_1^2},\frac{2x_1y_1}{1+dx_1^2y_1^2}\right) \tag{5}$$

Форма (4), (5) модифицированных законов сложения позволяет сохранить общепринятую горизонтальную симметрию (относительно оси x) обратных точек. Определяя обратную точку как $-P=(x_1,-y_1)$, получим согласно (4) координаты нейтрального элемента группы точек $O=(x_1,y_1)+(x_1,-y_1)=(1,0)$. Кроме нейтрального элемента О на оси x всегда лежит точка $D_0=(-1,0)$ второго порядка, для которой в соответствии с (5) $2D_0=(1,0)=O$. В зависимости от свойств параметров a и d из (1) можно получить еще 2 особые точки 2-го порядка и 2 точки 4-го порядка:

$$D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right),\ \pm F_1=\left(\infty,\pm\frac{1}{\sqrt{d}}\right) \tag{6}$$

где знак "∞" мы ставим при делении на 0. Они возникают при $\chi(ad)=1$ и $\chi(d)=1$ соответственно.

В зависимости от свойств параметров a и d кривые в обобщенной форме (1) разбиваются на 3 непересекающиеся (неизоморфных) класса [7]:

- *полные кривые Эдвардса* с условием С1: $\chi(ad)=-1$;
- *скрученные кривые Эдвардса* с условиями С2.1: $\chi(a)=\chi(d)=-1$;
- *квадратичные кривые Эдвардса* с условиями С2.2: $\chi(a)=\chi(d)=1$.

Перечислим основные свойства этих классов кривых.

1. Порядок N_E кривой (1) делится на 4. В отношении точек 2-го порядка первый класс полных кривых Эдвардса над простым полем является классом *циклических* кривых (с одной точкой 2-го порядка), скрученные же и квадратичные кривые Эдвардса образуют классы *нециклических* кривых (по 3 точки 2-го порядка). Максимальный порядок точек кривых двух последних классов равен $N_E/2$.

2. Класс полных кривых Эдвардса не содержит особых точек.

3. Скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения на основе преобразования параметров: $\tilde{a} = ca,\ \tilde{d} = cd,\ \chi(c) = -1.$

4. Скрученные кривые Эдвардса содержат лишь две особые точки 2-го порядка $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty \right)$, а квадратичные кривые Эдвардса, кроме них – еще две особые точки 4-го порядка $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}} \right)$.

5. В классах скрученных и квадратичных кривых Эдвардса замена $a \leftrightarrow d$ дает изоморфизм $E_{a,d} \sim E_{d,a}$

6. Полные и квадратичные кривые Эдвардса изоморфны кривым с параметром $a = 1$: $E_{a,d} \sim E_{1,d/a}$.

7. Скрученные кривые Эдвардса при $p \equiv 1 \bmod 4$ не имеют точек 4-го порядка и имеют порядок $N_E = 4n$ (n - нечетное).

8. Для точек нечетного порядка закон сложения точек (4) кривой (1) полный (не образует особых точек).

Заметим, что в расширении F_{p^2} простого поля F_p все 3 класса кривых Эдвардса, заданных над простым полем, приобретают свойства квадратичных кривых (3).

2. Алгоритм Монтгомери вычисления скалярного произведения точки эллиптической кривой

Весьма эффективный алгоритм Монтгомери [3] вычисления точки $Q = kP$ скалярного произведения успешно решает 2 задачи: противодействие атаке побочного канала типа «оценка парциальных вычислительных затрат» и повышение скорости экспоненцирования точки. Пусть число k представлено в двоичной форме $k = (k_{m-1}, k_{m-2}, ..., k_0)_2$, где $k = \sum_{i=0}^{m-1} k_i 2^i$, $k_i \in \{0,1\}$, тогда классический алгоритм удвоений-сложений точек на каждом шаге (или одном бите m-битного числа k) последовательно удваивает предыдущий результат и, если $k_i = 1$ складывает его с точкой P. Так как в среднем при числе m удвоений число сложений равно $m/2$, измерение времени вычислений на каждом шаге алгоритма позволяет мониторящему канал противнику организовать известную атаку побочного канала. Полезной для него информацией является также различие вычислительной сложности сложения и удвоения точки. В работе [3] Питер Монтгомери предложил алгоритм дифференциального сложения точек ($dADD$) в котором на каждом шаге алгоритма выполняются обе операции: сложения и удвоения точек. Очевидно, в этом случае атака подобного типа становится бессмысленной.

Алгоритм 1 Монтгомери (*dADD*)

Вход: $P_2 \leftarrow O$ (O – нейтральный элемент группы точек);

$P_1 \leftarrow P$ (P – базовая точка)

для $i \in m-1..0$

если $k_i = 1$: $P_2 \leftarrow P_1 + P_2$,

$P_1 \leftarrow 2P_1$;

если $k_i = 0 : P_1 \leftarrow P_1 + P_2$,

$$P_2 \leftarrow 2P_2.$$

Выход: $Q = P_2$.

Идея этого алгоритма проста: на каждом шаге цикла разность точек $P_1 - P_2 = P$ остается фиксированной точкой P. В качестве простого примера примем значение $k = (10111)_2 = 23_{10}$. Тогда получим в цикле пары точек $\{P_1, P_2\}$: $\{2P, P\}$, $\{3P, 2P\}$, $\{6P, 5P\}$, $\{12P, 11P\}$, $\{24P, 23P\}$. На выходе – точка $Q = 23P$.

Далее Монтгомери для специфической кривой вида

$$M_{A,B} : By^2 = x^3 + Ax^2 + x \tag{7}$$

получившей позже название кривой в форме Монтгомери, удалось получить лаконичные выражения для координат суммы точек при известной их разности, а также координат удвоенной точки.

Пусть $P_i = (x_i, y_i), i = \overline{0,4}$. Обозначим $P_0 = P_1 - P_2 = P$, $P_3 = P_1 + P_2$, $P_4 = 2P_1$. Для координат сложения, вычитания и удвоения точек кривой (7) в работе [3] получены выражения:

$$x_0 x_3 = \frac{(x_1 x_2 - 1)^2}{(x_1 - x_2)^2}, \tag{8}$$

$$x_4 = \frac{\left(x_1{}^2 - 1\right)^2}{4x_1\left((x_1 + 1)^2 + ex_1\right)}, e = (A + 2). \tag{9}$$

Характерно, что x-координаты точек P_0, P_3, P_4 зависят лишь от x-координат складываемых точек. Поэтому в [3] введены проективные координаты $(X : Z)$ для рекуррентных вычислений без инверсий с восстановлением y-координаты на финальном шаге процедуры. Согласно (8) и (9) они имеют вид:

$$X_3 = Z_0 (X_1 X_2 - Z_1 Z_2)^2,$$

$$Z_3 = X_0 (X_1 Z_2 - X_2 Z_1)^2,$$

$$X_4 = \left(X_1^2 - Z_1^2\right)^2$$

$$Z_4 = 4X_1 Z_1 \left((X_1 + Z_1)^2 + X_1 Z_1\right)^2 \tag{10}$$

Если M – ввычислительная стоимость умножения элементов поля, S – стоимость возведения в квадрат, U – стоимость умножения на константу e, то, игнорируя незначительные затраты на сложение в поле, получим из (10) стоимость сложения точек $C(P_1 + P_2) = 6M + 2S$, стоимость удвоения точек $C(2P_1) = 2M + 4S + 1U$ Поскольку базовая точка $P = P_0 = (X_0 : Z_0)$ является фиксированной, можно принять $Z_0 = 1$ (т.е. точка P является аффинной), при этом $C(P_1 + P_2) = 5M + 2S$, а суммарная стоимость равна

$C(P_1+P_2,2P_1)=7M+6S+1U$. Для минимизации вычислений Монтгомери представил формулы (10) в виде:

$$X_3=\left[(X_1-Z_1)(X_2+Z_2)+(X_1+Z_1)(X_2-Z_2)\right]^2,$$

$$Z_3=X_0\left[(X_1-Z_1)(X_2+Z_2)+(X_1+Z_1)(X_2-Z_2)\right]^2,$$

$$X_4=(X_1-Z_1)^2(X_1+Z_1)^2,$$

$$Z_4=4X_1Z_1\left((X_1+Z_1)^2+eX_1Z_1\right). \qquad (11)$$

При вычислении X_4 учтем бесплатный промежуточный результат, который используется при расчете Z_4

$$4X_1Z_1=(X_1+Z_1)^2-(X_1-Z_1)^2.$$

Тогда $C(P_1+P_2)=3M+2S$, $C(2P_1)=2M+2S+1U$. Суммарная стоимость этих двух операций равна $C(P_1+P_2,2P_1)=5M+4S+1U$. Этот результат для кривых в форме Монтгомери (7) и на сегодняшний день является рекордом минимальной вычислительной сложности выполнения 2-х операций – сложения и удвоения точек.

Примечание. Проективные координаты, использующие некоторые аффинные точки, называют смешанными проективными координатами (mixed projective coordinates).

3. Проективные координаты Фарашахи-Хоссейни для кривых в обобщенной форме Эдвардса

Поскольку эллиптические кривые в форме Монтгомери (7) и Эдвардса (1) бирационально эквивалентны [6], следует ожидать близких результатов оценки вычислительной сложности для кривых в форме (1). Если операции (4), (5) выполнять в классических проективных координатах $(X:Y:Z)$, то полученные в [6] оценки для кривых (1) составляют $C(P_1+P_2)=10M+1S+2U$, $C(2P_1)=3M+4S+1U$. Суммарная стоимость этих двух операций при этом равна $C(P_1+P_2,2P_1)=13M+5S+3U$, что более чем вдвое проигрывает кривым (7). Одной из очевидных причин этого является использование в расчетах обеих координат X и Y кривой (1) вместо одной X-координаты кривой (7) (Z-координаты во всех случаях заменяют инверсию).

Авторы работы [4] нашли эффективное решение этой проблемы. В уравнении (1) обе координаты представлены последним слагаемым $w(x,y)=dx^2y^2$, а это позволяет предположить, что по аналогии с методом дифференциального сложения точек Монтгомери (при $w(x,y)=x$), можно выразить формулы сложения-вычитания и удвоения точек кривой Эдвардса с помощью одной интегральной координаты w. В основе такой идеи лежит бирациональная эквивалентность кривых (7) и (1) с рациональным преобразованием координат $\frac{x}{y}\to y$, $\frac{x-1}{x+1}\to x$ [6]. В разделе 4 работы [4] приводятся итоговые формулы дифференциального сложения точек для кривых в форме (1) без их выводов. В связи с их нетривиальностью мы ниже даем подробный вывод этих формул. Как отмечалось в разделе 1, мы используем формулы (4), (5) с заменой $x\leftrightarrow y$ в [4].

Сложение-вычитание точек

Пусть $P_i=(x_i,y_i)$, $w_i=w(P_i)=dx_i^2y_i^2, i=\overline{0,3}$. Обозначим $P_0=P_1-P_2$, $P_3=P_1+P_2$, $w_0=w(P_0)$, $w_3=w(P_3)$. Тогда согласно (4)

$$P_0=(x_0,y_0)=\left(\frac{x_1x_2+ay_1y_2}{1+dx_1x_2y_1y_2},\frac{-x_1y_2+x_2y_1}{1-dx_1x_2y_1y_2}\right),$$

$$P_3=(x_3,y_3)=\left(\frac{x_1x_2-ay_1y_2}{1-dx_1x_2y_1y_2},\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}\right).$$

Отсюда

$$w_0w_3=(dx_0y_0x_3y_3)^2=d^2\left[\left(\frac{(x_1x_2)^2-(ay_1y_2)^2}{1-w_1w_2}\right)\left(\frac{(x_2y_1)^2-(x_1y_2)^2}{1-w_1w_2}\right)\right]^2 \qquad (12)$$

Сомножитель числителя преобразуем как

$$I=\left(\left((x_1x_2)^2-(ay_1y_2)^2\right)\left((x_2y_1)^2-(x_1y_2)^2\right)\right)=$$

$$=x_1^2y_1^2x_2^4-a^2x_2^2y_2^2y_1^4-x_2^2y_2^2x_1^4+a^2x_1^2y_1^2y_2^4=$$

$$=x_1^2y_1^2\left(x_2^4+a^2y_2^4\right)-x_2^2y_2^2\left(x_1^4+a^2y_1^4\right).$$

Так как

$$\left(x_i^2+ay_i^2\right)=1+w_i, i=1,2,$$

тогда

$$\left(x_i^4+ay_i^4\right)=(1+w_i)^2-2ad^{-1}w_i, i=1,2,$$

и можно получить

$$I=d^{-1}\left[w_1\left((1+w_2)^2-2ad^{-1}w_2\right)\right]-d^{-1}\left[w_2\left((1+w_1)^2-2ad^{-1}w_1\right)\right]=$$

$$=d^{-1}\left[w_1+w_1w_2^2-w_2-w_2w_1^2\right]=d^{-1}\left(w_1-w_2\right)\left(1-w_1w_2\right).$$

С учетом этого равенство (6) принимает вид

$$w_0w_3=d^2\frac{I^2}{(1-w_1w_2)^4}=\frac{(w_1-w_2)^2}{(1-w_1w_2)^2}. \qquad (13)$$

Удвоение точек

Пусть $P_1=(x_1,y_1)$, $P_4=2P_1$, $w_1=w(P_1)$, $w_4=w(2P_1)$.

Согласно (5) и принятых обозначений

$$2P_1=\left(\frac{x_1^2-ay_1^2}{1-dx_1^2y_1^2},\frac{2x_1y_1}{1+dx_1^2y_1^2}\right)=\left(\frac{x_1^2-ay_1^2}{1-w_1},\frac{2x_1y_1}{1+w_1}\right),$$

$$w_4 = d\left(\left(\frac{x_1^2 - ay_1^2}{1-w_1}\right)\left(\frac{2x_1y_1}{1+w_1}\right)\right)^2 = 4w_1\left(\frac{\left(x_1^2 - ay_1^2\right)^2}{\left(1-w_1^2\right)^2}\right).$$

В последней формуле сомножитель в числителе преобразуется к виду

$$\left(x_1^2 - ay_1^2\right)^2 = \left(x_1^2 + ay_1^2\right)^2 - 4ax_1^2y_1^2 = \left(1+w_1\right)^2 - 4ad^{-1}w_1.$$

В итоге

$$w_4 = \frac{4w_1\left(\left(1+w_1^2\right)^2 - cw_1\right)}{\left(1-w_1^2\right)^2},\ c = 4ad^{-1} \qquad 14)$$

Формулы (13) и (14) с целью вычисления инверсий Z представляются в проективных координатах $(W:Z)$ как:

$$W_3 = Z_0\left[\left(W_1 - Z_1\right)\left(W_2 + Z_2\right) - \left(W_1 + Z_1\right)\left(W_2 - Z_2\right)\right]^2,$$

$$Z_3 = W_0\left[\left(W_1 - Z_1\right)\left(W_2 + Z_2\right) + \left(W_1 + Z_1\right)\left(W_2 - Z_2\right)\right]^2,$$

$$W_4 = 4W_1Z_1\left(\left(W_1 + Z_1\right)^2 - cW_1Z_1\right),\ c = 4ad^{-1},$$

$$Z_4 = \left(W_1 - Z_1\right)^2\left(W_1 + Z_1\right)^2. \qquad (15)$$

Нельзя не заметить, что они мало отличаются от формул (11) для координат $(X:Z)$ кривой в форме Монтгомери после обращения $X \leftrightarrow W^{-1}$. Как и для кривой (7), с учетом $Z_0 = 1$, стоимость вычислений сложения и удвоения точек на одном шаге алгоритма Монтгомери $dADD$ минимальна и равна $C\left(P_1 + P_2, 2P_1\right) = 5M + 4S + 1U$.

Следует отметить, что проективные координаты Фарашахи-Хоссейни для кривых (1) оказались также очень перспективными при вычислении изогений нечетных степеней в задачах постквантовой криптографии [10].

4. Специфические свойства приемлемых для криптосистем кривых в обобщенной форме Эдвардса

Из краткого обзора свойств кривых в форме (1) в разделе 1 следует, что кривые классов нециклических скрученных $\left(\chi(a) = \chi(d) = -1\right)$ и квадратичных $\left(\chi(a) = \chi(d) = 1\right)$ кривых Эдвардса содержат соответственно 2 и 4 особых точки 2-го и 4-го порядков (6). В литературе по эллиптической криптографии существует мнение, что это ограничивает применение этих кривых при необходимости выполнения групповых операций с точками четных порядков, так как бесконечная координата особой точки не лежит в конечном поле.

Один из авторов данной статьи в работе [7] ввел соответствующие групповые операции с особыми точками (6):

$$\left(x_1, y_1\right) + \left(\sqrt{\frac{a}{d}}, \infty\right) = \left(\sqrt{\frac{a}{d}} \cdot x_1^{-1}, \frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right),$$

$$(x_1, y_1) + \left(-\sqrt{\frac{a}{d}}, \infty\right) = \left(-\sqrt{\frac{a}{d}} \cdot x_1^{-1}, -\frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right)$$

$$(x_1, y_1) + \left(\infty, \frac{1}{\sqrt{d}}\right) = \left(-\frac{1}{\sqrt{d}} \cdot y_1^{-1}, \frac{1}{\sqrt{d}} \cdot x_1^{-1}\right),$$

$$(x_1, y_1) + \left(\infty, -\frac{1}{\sqrt{d}}\right) = \left(\frac{1}{\sqrt{d}} \cdot y_1^{-1}, -\frac{1}{\sqrt{d}} \cdot x_1^{-1}\right).$$

Все найденные суммы, полученные с помощью правил предельного перехода, удовлетворяют уравнению (1) при подстановке, т.е. являются точками кривой. Эти формулы снимают теоретические ограничения в задаче построения арифметики группы точек в условиях неполноты закона сложения (4).

Вместе с тем, разумеется, наличие особых точек (6) в криптоалгоритмах нежелательно в связи с проблемами программирования и снижением скорости выполнения алгоритмов. Однако, в большинстве криптопримитивов точки четных порядков не используются. В их отсутствие закон сложения точек является полным (свойство 8 раздела 1).

Наиболее целесообразным следует считать выбор для криптосистемы кривой (1) порядка $N_E = 4n$ (n - простое) с минимальным кофактором 4. Такой кофактор при $p \equiv 1 mod 4$ имеют порядки половины всех полных кривых Эдвардса (2) и всех скрученных кривых Эдвардса (1) ($\chi(a) = \chi(d) = -1$) [7].

Циклические полные кривые (2) содержат точки порядков 2, 4, n, $2n$, $4n$. Подкласс нециклических скрученных кривых Эдвардса при $p \equiv 1 \bmod 4$ содержат точки порядков 2, n, $2n$. В криптосистеме базовой является точка $P, ordP = n$. Такая точка в подклассе скрученных кривых Эдвардса находится наиболее просто – с помощью единственной групповой операции удвоения случайной точки. Это существенно упрощает задачу нахождения генератора (базовой точки P) на этапе вычисления общесистемных параметров криптосистемы. Для точек циклической группы $\langle P \rangle$ закон сложения точек (4) кривой (1) является полным. Отмеченные преимущества (минимальный кофактор порядка кривой 4, минимальный набор порядков точек 2, n $2n$, простое вычисление базовой точки P) позволяют рекомендовать данный подкласс скрученных кривых Эдвардса при проектировании и стандартизации криптосистем. Это не исключает применение для этих целей и полных кривых Эдвардса с порядком $N_E = 4n$.

Операция скалярного произведения kP является основной в большинстве алгоритмов эллиптической криптографии. Наиболее безопасным к атакам побочного канала является алгоритм Монтгомери дифференциального сложения точек с рекордным быстродействием для кривых в форме Монтгомери и Эдвардса с использованием проективных координат Фарашахи-Хоссейни.

Дальнейшего снижения вычислительных затрат при вычислении скалярного произведения kP на скрученной кривой Эдвардса можно достичь путем минимизации константы $c = 4ad^{-1}$ в формуле (15) для координаты W_4. Если принять $p \equiv 5 \bmod 8$, можно зафиксировать $d = 2$ как минимальный квадратичный невычет простого поля F_p, тогда $c = 2a$ После этого методом наращивания квадратичных невычетов a можно найти кривую приемлемого порядка $N_E = 4n$ ($n-$ простое). Решение этой задачи позволяет получить минимальную оценку стоимости вычислений на одном шаге алгоритма Монтгомери $C(P_1 + P_2, 2P_1) = 5M + 4S$.

5. К оценке эффективности метода дифференциального сложения точек Монтгомери на кривых Эдвардса

В работе [4] получены 3 оценки стоимости вычислений для кривых (1)

$$C_1(P_1+P_2,2P_1)=5M+4S+1U,$$

$$C_2(P_1+P_2,2P_1)=3M+7S+1U,$$

$$C_3(P_1+P_2,2P_1)=3M+6S+3U.$$

Две последние оценки C_2 и C_3 получены из первой путем модификаций расчетных формул. Кроме того, оценка C_3 справедлива лишь для некоторого семейства класса полных кривых Эдвардса. Если воспользоваться известной оценкой $1S=2/3M$ [5], то получим $C_1=7.67M+1U$, $C_2=7.67M+1U$, $C_3=7M+3U$. При этом, мы видим, что две первые оценки равнозначны, а последняя может быть полезной для полных кривых Эдвардса лишь при очень малых значениях констант, для которых $U<0,17M$.

В предыдущих наших работах [7,8,9] проводился сравнительный анализ скорости вычисления скалярного произведения kP в проективних координатах $(X:Y:Z)$ для кривых в формах Эдвардса и Вейерштрасса. Использование классического метода последовательных удвоений и сложений точек обеспечивает максимальный выигрыш первых в быстродействии до 1.61 раза. Для кривых в форме Вейерштрасса стоимости вычислений составляют $C_W(P_1+P_2)=12M+2S$, $C_W(2P_1)=7M+5S$ [7]. Так как алгоритм сложений и удвоений точек Монтгомери можно реализовать для любого типа кривой, то для кривой в форме Вейерштрасса стоимость одного бита вычисления kP составит $C_W(P_1+P_2,2P_1)=19M+7S$. Тогда, с учетом оценки $1S=2/3M$, имеем $C_W(P_1+P_2,2P_1)=23.67M$. Если константой $c=4ad^{-1}$ в (15) можно пренебречь (это достигается методом, описанным в разделе 4), потенциальный выигрыш в скорости вычислений для кривой в форме Эдвардса (1) составит $\frac{C_W}{C_1}=\frac{23.67}{7.67}=3.09$.

Заключение

Проведенный в статье анализ позволяет заключить, что алгоритм дифференциального сложения точек Монтгомери с его реализацией на скрученных кривых Эдвардса в проективных координатах Фарашахи-Хоссейни является на сегодня наиболее быстрым и безопасным к атакам побочного канала методом экспоненцирования точки кривой. Его можно рекомендовать при проектировании криптосистем и новых стандартов допостквантовой эллиптической криптографии.

Список литературы

1. Menezes A., van Oorshot P,C., Vanstone S.A Handbook of Applied Cryptography. CRC press, New York, 2006.
2. Washington L,C. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.
3. Montgomery, P.L. Speeding the Pollard and elliptic curve methods of factorization. Math. Comp. 48(177), P. 243–264 (1987).
4. Farashahi, R.R., Hosseini, S.G.: Differential addition on twisted Edwards curves. In: Pieprzyk, J., Suriadi, S. (eds.) Information Security and Privacy. pp. 366-378. Springer International Publishing, Cham (2017).
5. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves// Advances in Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.

6. Bernstein Daniel J., Birkner Peter, Joye Marc, 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.

7. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. - 272с.

8. Бессалов А.В., Дихтенко А.А.,Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, №4, 2011. С.33-36.

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

10.Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. Center for Information Security Technologies (CIST), Korea University, Seoul,Republic of Korea, 2018.