УДК 681.3.06

С.И. ЗБИТНЕВ В.Ю. КОВТУН О.Е. ИЛЯСОВА
staszb@ukr.net vladislav.kovtun@gmail.com illasova@ukr.net

АРИФМЕТИЧЕСКИЕ ОПЕРАЦИИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ НАД ДВОИЧНЫМ ПОЛЕМ В ПРОЕКТИВНЫХ КООРДИНАТАХ

Введение

Массовое создание, внедрение и эксплуатация информационных систем привели к возникновению спектра новых проблем в сфере безопасности личности, общества и государства. Внимание к этим проблемам закономерно. Если коммерческая организация допускает утечку более 20% важной внутренней информации, то она в 60 случаях из 100 банкротится [18]. Утверждают также [19], 93% компаний, лишившихся доступа к собственной информации на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей несостоятельности немедленно.

Потребность в обеспечении безопасности связана с тем, что существует множество субъектов и структур, весьма заинтересованных в чужой информации и готовых заплатить за это высокую цену. Так, стоимость устройств подслушивания, продаваемых только в США, составляет в среднем около 900 млн. долл. в год. Суммарный урон, нанесенный организациям, против которых осуществлялось прослушивание, составляет ежегодно в США около 8 млрд. долл. А ведь существуют и, соответственно, приобретаются устройства для несанкционированного доступа к информации и по другим каналам: проникновение в информационные системы, перехват и дешифровка сообщений и т.д. В результате, по данным SANS Institute, средний размер убытка от одной атаки в США на корпоративную систему для банковского и ИТ-секторов экономики составляет около полумиллиона долларов [21]. Примерная структура последствий неэффективного обеспечения информационной безопасности в американских организациях такова [20]: кража конфиденциальной информации — 20-25% от общего годового ущерба; фальсификация финансовой информации — 21-25%; заражение вредоносными программами — 11-12%; нарушение доступа к Web-сайтам — 1-11%; срыв работы информационной системы — 4-10%; незаконный доступ сотрудников к информации — 4-9%; другие виды ущерба — 14-33%.

Не вызывает сомнений, что мероприятия по защите критически важных информационных систем должны соответствовать многочисленным международным, национальным, корпоративным, нормативным и методическим документам [1-3]. К их числу следует отнести и украинский стандарт ДСТУ 4145-2002, в основу которого положены криптографические преобразования на эллиптических кривых (ЭК). Популярность этого математического аппарата обусловлена возможностью применения малой длины ключа и блока преобразований. Наряду с этим, остается актуальным вопрос минимизации вычислительной сложности.

Методы реализации и характеристики криптопреобразований на ЭК зависят от следующих параметров [4]:

1. Видов поля $GF(q)$, над которым задается ЭК: $GF(p)$ или $GF(2^m)$, где p - простое, m - целое;

2. Представления элементов поля в расширенном поле Галуа $GF(2^m)$ (полиномиальное или нормальное);

3. Видов ЭК $E(GF(q))$ (случайная кривая, кривая Коблица);

4. Представления точек ЭК (аффинного или проективного).

Последнее, позволяет повысить производительность, без ущерба безопасности криптосистем, т.е. не уменьшает сложность решения задачи дискретного логарифма в группе точек ЭК, и поэтому, является одним из основных подходов к уменьшению сложности преобразований в группе точек ЭК. Предварительный анализ известных выражений для операций над точками ЭК в различных координатных системах [1-3, 5, 7-9, 12, 13] показывает, что большинство из них могут быть улучшены.

Целью настоящей работы является анализ существующих способов представления точек ЭК, изложение позиций по их усовершенствованию и применению.

Статья состоит из нескольких разделов. В первом разделе рассматриваются арифметические операции над известными представлениями точек эллиптической кривой и их вычислительные сложности. Во втором разделе рассматриваются усовершенствованные арифметические операции с точки зрения сложности. В третьем разделе сравниваются улучшенные арифметические операции с известными. Даются рекомендации по применению различных представлений.

1. Арифметика точек ЭК в известных представлениях

Арифметика в аффинных координатах [1-3, 5]

Рассмотрим ЭК $E\left(GF\left(2^m\right)\right)$, которая описывается усеченной формой уравнения Вейерштрасса:

$$y^2 + xy = x^3 + ax^2 + b, \tag{1}$$

где $a, b \in GF\left(2^m\right)$ при $b \neq 0$.

Напомним, что вычисление точки пересечения выполняется методом секущих Диофанта [16]. При пересечении кривой порядка 3 кривой порядка 1 в общем случае будет три точки пересечения. На рис. 1 приведена демонстрация применения метода секущих Диофанта.

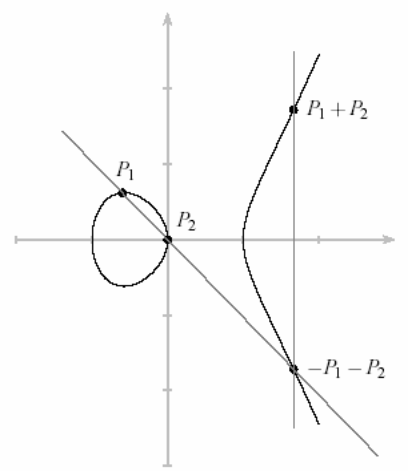

Рис. 1. Иллюстрация операции сложения и инвертирования точек эллиптической кривой

Дана ЭК $E\left(GF\left(2^m\right)\right)$ заданная уравнение (1) и $P_1\left(x_1, y_1\right)$, $P_2\left(x_2, y_2\right)$ точки на ней, причем $P_1 \neq P_2$, тогда точка $P_3\left(x_3, y_3\right) = P_1 + P_2$ вычисляется:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, \tag{2}$$

$$y_3 = (x_1 + x_3)\lambda + x_3 + y_1, \tag{3}$$

где

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}, \text{ если } P_1 \neq P_2, \tag{4}$$

$$\lambda = \frac{y_1}{x_1} + x_1, \text{ если } P_1 = P_2, \tag{5}$$

Вычислительная сложность операции сложения и удвоения точек, соответственно, составит:

$$I_{add}(Af) = I_{inv} + 2I_{mul} + I_{sqr} + 9I_{add}, \tag{6}$$

$$I_{dbl}(Af) = I_{inv} + 2I_{mul} + I_{sqr} + 7I_{add}, \tag{7}$$

где I_{inv} - сложность операции инвертирования элемента в поле; I_{mul} - сложность операции умножения в поле; I_{sqr} - сложность операции возведения в квадрат в поле; I_{add} - сложность операции сложения в поле.

Известно, что наиболее вычислительно сложной операцией является инверсия элемента поля. Одним из возможных способов исключения операции инвертирования при сложении и удвоении точки, является переход к проективным координатам [1-5].

Арифметика в проективных координатах [6]

На сегодняшний день в литературе по имплементации криптографических преобразований в группе точнее эллиптической кривой описано несколько видов проективных координат.

Арифметика в стандартных проективных координатах [1-3, 5, 7, 8]

Проективной точке $(X:Y:Z)$, $Z \neq 0$, ставится в соответствие точка с аффинными координатами

$$\left(\frac{X}{Z}, \frac{Y}{Z}\right). \tag{8}$$

Уравнение кривой в стандартных проективных координатах имеет вид:

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3. \tag{9}$$

Для заданных точек $P_1(X_1:Y_1:Z_1)$, $P_2(X_2:Y_2:Z_2)$, причем точки P_1 и P_2 не принадлежат одному классу смежности, координаты результирующей точки $P_3(X_3:Y_3:Z_3) = P_1 + P_2$, определяются соотношениями:

$$\begin{aligned} X_3 = {} & (X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1)^2 Z_1Z_2 + (Y_1Z_2 + Y_2Z_1)\times \\ & \times (X_1Z_2 + X_2Z_1)^2 Z_1Z_2 + (X_1Z_2 + X_2Z_1)^4 + aZ_1Z_2(X_1Z_2 + X_2Z_1)^3, \end{aligned} \tag{10}$$

$$\begin{aligned} Y_3 = {} & (X_1Z_2 + X_2Z_1)^2 (X_1Z_2Y_2Z_1 + X_2Z_1Y_1Z_2) + \\ & X_3(X_1Z_2 + X_2Z_1 + Y_1Z_2 + Y_2Z_1)Z_1Z_2 \end{aligned}, \tag{11}$$

$$Z_3 = (X_1Z_2 + X_2Z_1)^3 Z_1Z_2, \tag{12}$$

Обозначим $E = Y_1 \cdot Z_2$, $F = Y_2 \cdot Z_1$, $I = X_1 \cdot Z_2$, $J = X_2 \cdot Z_1$, $B = E + F$, $A = I + J$, $C = Z_1 \cdot Z_2$, $D = C \cdot B$. С учетом введенных обозначений (10)-(11) примут вид:

$$X_3 = (A^2 + A \cdot B) \cdot D + a \cdot Z_3 + B^4, \tag{13}$$

$$Y_3 = B^2 \cdot (F \cdot I + E \cdot J) + X_3 \cdot (A + B), \tag{14}$$

$$Z_3 = B^2 \cdot D. \tag{15}$$

В случае если точки P_1 и P_2 принадлежат одному классу смежности, выражения для вычисления координат результирующей точки имеют вид:

$$X_3 = X_1Z_1(Y_1Z_1 + X_1^2)^2 + (X_1Z_1)^2(Y_1Z_1 + X_1^2) + a(X_1Z_1)^3, \tag{16}$$

$$Y_3 = X_1^3 + X_3(Y_1Z_1 + X_1^2 + X_1Z_1), \tag{17}$$

$$Z_3 = (X_1 Z_1)^3. \tag{18}$$

Введем обозначения $A = Y_1 \cdot Z_1 + C$, $B = X_1 \cdot Z_1$, $C = X_1^2$. С учетом введенных обозначений выражения (16)-(18) примут вид:

$$X_3 = A \cdot B \cdot (A + B) + a \cdot Z_3, \tag{19}$$

$$Y_3 = X_3 \cdot (A + B) + C \cdot X_1, \tag{20}$$

$$Z_3 = B^2 \cdot B. \tag{21}$$

Сложность операции сложения и удвоения, соответственно, составит:

$$I_{add}(StdPrj) = 14 I_{mul} + 3 I_{sqr} + 8 I_{add}, \tag{22}$$

$$I_{dbl}(StdPrj) = 8 I_{mul} + 2 I_{sqr} + 3 I_{add}. \tag{23}$$

Арифметика в проективных координатах Якоби [1-3, 5, 7, 12, 13]

Проективной точке $(X : Y : X)$, $Z \neq 0$, ставится в соответствие точка с аффинными координатами:

$$\left(\frac{X}{Z^2}, \frac{Y}{Z^3} \right). \tag{24}$$

Уравнение кривой в проективных координатах Якоби представляется в виде:

$$Y^2 + XYZ = X^3 + aX^2 Z^2 + bZ^6. \tag{25}$$

Для заданных точек $P_1(X_1 : Y_1 : Z_1)$, $P_2(X_2 : Y_2 : Z_2)$, причем точки P_1 и P_2 не принадлежат одному классу смежности, координаты результирующей точки $P_3(X_3 : Y_3 : Z_3) = P_1 + P_2$, определяются соотношениями:

$$\begin{gathered} X_3 = \left(Y_1 Z_2^3 + Y_2 Z_1^3\right)^2 + Z_1 Z_2 \left(Y_1 Z_2^3 + Y_2 Z_1^3\right)\left(X_1 Z_2^2 + X_2 Z_1^2\right) + \\ \left(X_1 Z_2^2 + X_2 Z_1^2 + a Z_1 Z_2\right)\left(X_1 Z_2^2 + X_2 Z_1^2\right)^2, \end{gathered} \tag{26}$$

$$\begin{gathered} Y_3 = X_1 Z_2^2 \left(Y_1 Z_2^3 + Y_2 Z_1^3\right)\left(X_1 Z_2^2 + X_2 Z_1^2\right)^2 + X_3 \left(Y_1 Z_2^3 + Y_2 Z_1^3 + Z_3\right) + \\ + Y_1 Z_2^3 \left(X_1 Z_2^2 + X_2 Z_1^2\right)^3, \end{gathered} \tag{27}$$

преобразуем (26) и (27) к виду описанном в стандарте [3]:

$$X_3 = aZ_3^2 + \left(Y_1 Z_2^3 + Y_2 Z_1^3\right)\left(Y_1 Z_2^3 + Y_2 Z_1^3 + Z_3\right) + \left(X_1 Z_2^2 + X_2 Z_1^2\right)^3, \tag{28}$$

$$\begin{gathered} Y_3 = X_3 \left(Y_1 Z_2^3 + Y_2 Z_1^3 + Z_3\right) + \\ + \left(X_2 \left(Y_1 Z_2^3 + Y_2 Z_1^3\right) + Y_2 Z_1 \left(X_1 Z_2^2 + X_2 Z_1^2\right)\right) Z_1^2 \left(X_1 Z_2^2 + X_2 Z_1^2\right)^2, \end{gathered} \tag{29}$$

$$Z_3 = Z_1 Z_2 \left(X_1 Z_2^2 + X_2 Z_2^2\right). \tag{30}$$

Обозначим $A = Y_1 \cdot Z_2^3 + E \cdot Z_1^2$, $B = X_1 \cdot Z_2^2 + X_2 \cdot Z_1^2$, $C = B \cdot Z_1$, $E = Y_2 \cdot Z_1$. С учетом введенных обозначений выражения (28)-(30) преобразуются к виду:

$$X_3 = A \cdot (A + Z_3) + B^2 \cdot B + a \cdot Z_3^2, \tag{31}$$

$$Y_3 = X_3 \cdot (A + Z_3) + C^2 \cdot (A \cdot X_2 + B \cdot E), \tag{32}$$

$$Z_3 = C \cdot Z_2. \tag{33}$$

В случае если точки P_1 и P_2 принадлежат одному классу смежности, выражения для вычисления координат результирующей точки имеем вид:

$$X_3 = \left(X_1 + cZ_1^2\right)^4, \tag{35}$$

$$Y_3 = X_3 \left(Y_1 Z_1 + X_1^2 + Z_3\right) + X_1^4 Z_3, \tag{36}$$

$$Z_3 = X_1 \cdot Z_1^2. \tag{37}$$

Введем обозначения $A = X_1^2$, $B = Z_1^2$, $c = b^{1/4}$. С учетом введенных обозначений выражения (35)-(37) примут вид:

$$X_3 = \left(X_1 + c \cdot B\right)^4, \tag{38}$$

$$Y_3 = A^2 \cdot Z_3 + X_3 \cdot \left(Z_3 + Y_1 \cdot Z_1\right), \tag{39}$$

$$Z_3 = X_1 \cdot B. \tag{40}$$

Сложность операции сложения и удвоения, соответственно, составит:

$$I_{add}\left(JacPrj\right) = 15I_{mul} + 5I_{sqr} + 8I_{add}. \tag{41}$$

$$I_{dbl}\left(JacPrj\right) = 5I_{mul} + 5I_{sqr} + 4I_{add}. \tag{42}$$

Арифметика в проективных координатах Лопеса-Дахаба [8]

Проективной точке $(X:Y:Z)$, $Z \neq 0$, ставится в соответствие точка с аффинными координатами

$$\left(\frac{X}{Z}, \frac{Y}{Z^2}\right). \tag{43}$$

Уравнение кривой в проективных координатах Лопеса-Дахаба имеет вид:

$$Y^2 Z + XYZ = X^3 Z + aX^2 Z^2 + bZ^4. \tag{44}$$

Для заданных точек $P_1(X_1 : Y_1 : Z_1)$, $P_2(X_2 : Y_2 : Z_2)$, причем точки P_1 и P_2 не принадлежат одному классу смежности, координаты результирующей точки $P_3(X_3 : Y_3 : Z_3) = P_1 + P_2$, определяются соотношениями:

$$X_3 = A^2 + I \cdot \left(D + a \cdot C^2\right) + A \cdot D, \tag{45}$$

$$Y_3 = Z_3 \cdot \left(X_3 + I \cdot E\right) + A \cdot B \cdot \left(F \cdot Z_3 + X_3 \cdot I\right), \tag{46}$$

$$Z_3 = D^2, \tag{47}$$

где $E = Y_2 \cdot Z_1^2$, $A = Y_1 \cdot Z_2^2 + E$, $F = X_1 \cdot Z_2$, $B = F + X_2 \cdot Z_1$, $C = Z_1 \cdot Z_2$, $D = B \cdot C$, $I = B^2$.

В случае если точки P_1 и P_2 принадлежат одному классу смежности, выражения для вычисления координат результирующей точки имеют вид:

$$X_3 = B^2 + A, \tag{48}$$

$$Y_3 = A \cdot Z_3 + X_3 \cdot \left(a \cdot Z_3 + Y_1^2 + A\right), \tag{49}$$

$$Z_3 = B \cdot C, \tag{50}$$

где $A = b \cdot C^2$, $B = X_1^2$, $C = Z_1^2$.

Сложность операции сложения и удвоения, соответственно, составит:

$$I_{add}\left(LDPrj\right) = 15I_{mul} + 6I_{sqr} + 8I_{add}, \tag{51}$$

$$I_{dbl}\left(LDPrj\right) = 5I_{mul} + 5I_{sqr} + 4I_{add}. \tag{52}$$

Арифметика в проективных координатах Чудновского [12, 13]

Отличительной особенностью представления точек в координатах Чудновского от Якобиановых, является сопоставление точки в аффинном представлении, точки вида $\left(X : Y : Z : Z^2 : Z^3\right)$, $Z \neq 0$. При сложении точек, такое представление позволяет сэкономить несколько операций возведения в квадрат.

Сложности операции сложения и удвоения, соответственно, составит:

$$I_{add}\left(ChudPrj\right) = 15I_{mul} + 3I_{sqr} + 8I_{add}, \tag{53}$$

$$I_{dbl}\left(ChudPrj\right) = 6I_{mul} + 5I_{sqr} + 4I_{add}. \tag{54}$$

Арифметика в модифицированных проективных координатах Якоби [9, 5, 12]

Отличительной особенностью представления точек в координатах Якоби является сопоставление точки в аффинном представлении точки $\left(X:Y:Z:Z^2\right),\ Z\neq 0$. При сложении точек, такое представление позволяет сэкономить несколько операций возведения в квадрат.

Сложности операции сложения и удвоения, соответственно, составит:

$$I_{add}\left(JacPrjMdf\right)=15I_{mul}+3I_{sqr}+8I_{add}, \tag{55}$$

$$I_{dbl}\left(JacPrjMdf\right)=5I_{mul}+5I_{sqr}+4I_{add}. \tag{56}$$

Арифметика в модифицированных проективных координатах Лопеса-Дахаба [9, 12, 13]

Отличительной особенностью представления точек в координатах Лопеса-Дахаба является сопоставление точки в аффинном представлении точки $\left(X:Y:Z:Z^2\right),\ Z\neq 0$, что позволяет сэкономить одну полевую операцию возведения в квадрат. Для заданных точек $P_1(X_1:Y_1:Z_1)$, $P_2(X_2:Y_2:Z_2)$, причем точки P_1 и P_2 не принадлежат одному классу смежности, координаты результирующей точки $P_3(X_3:Y_3:Z_3)=P_1+P_2$, определяются соотношениями (45)-(47).

В случае если точки P_1 и P_2 принадлежат одному классу смежности, выражения для вычисления координат результирующей точки определяются соотношениями (48)-(50).

Сложность операции сложения и удвоения, соответственно, составит:

$$I_{add}\left(LDPrjMdf\right)=15I_{mul}+5I_{sqr}+8I_{add}, \tag{57}$$

$$I_{dbl}\left(LDPrjMdf\right)=5I_{mul}+5I_{sqr}+4I_{add}. \tag{58}$$

Арифметика в смешанных координатах

В работах [8, 13] предлагается оригинальный способ сложения точек, в котором одна из точек представлена в аффинных, а другая в проективных координатах $P_1\left(X_1:Y_1:Z_1\right)$, $P_2\left(X_2:Y_2:1\right)$.

Для сложения точки в стандартных проективных координатах, $P_1(X_1:Y_1:Z_1)$, $P_2(X_2:Y_2:1)$ в аффинных координатах, причем они не принадлежат одному классу смежности, выражения (19)-(21) примут вид:

$$X_3=A\cdot C\cdot\left(A+B\right)+B^4+a\cdot Z_3, \tag{59}$$

$$Y_3=X_3\cdot\left(A+B\right)\cdot Z_1+B^2\cdot\left(F\cdot Y_1+E\cdot X_1\right), \tag{60}$$

$$Z_3=C\cdot B^2, \tag{61}$$

где $E=Y_2\cdot Z_1$, $F=X_2\cdot Z_1$ $A=Y_1+E$, $B=X_1+F$, $C=Z_1\cdot B$.

Сложность операции сложения в смешанных стандартных проективных координатах составляет:

$$I_{add}^{mix}\left(StdPrj\right)=12I_{mul}+2I_{sqr}+8I_{add}. \tag{62}$$

В случае, когда одна из точек представлена в проективных координатах Якоби $P_1\left(X_1:Y_1:Z_1\right)$, а другая в аффинных координатах, $P_2\left(X_2:Y_2:1\right)$, причем они не принадлежат одному классу смежности, выражения (31) – (33) примут вид:

$$X_3=a\cdot E+A\cdot\left(A+Z_3\right)+B^2\cdot B, \tag{63}$$

$$Y_3=X_3\cdot\left(A+Z_3\right)+E\cdot\left(X_2\cdot Y_1+D\cdot X_1\right), \tag{64}$$

$$Z_3=B\cdot Z_1, \tag{65}$$

где $C = Z_1^2, D = Y_2 \cdot Z_1,\ A = Y_1 + C \cdot D,\ B = X_1 + X_2 \cdot C,\ E = Z_3^2$.

Сложность операции сложения в смешанных проективных координатах Якоби составляет:

$$I_{add}^{mix}(JacPrj) = 11I_{mul} + 3I_{sqr} + 8I_{add}. \quad (66)$$

Далее рассмотрим сложение в проективных координатах Лопаса-Дахаба точки $P_1(X_1 : Y_1 : Z_1)$ и точки представленной в аффинных координатах $P_2(X_2 : Y_2 : 1)$, причем они не принадлежат одному классу смежности, выражения (45) – (47) [8] примут вид:

$$X_3 = A^2 + D + B^2 \cdot (C + a \cdot E), \quad (67)$$

$$Y_3 = D \cdot (X_2 \cdot Z_3 + X_3) + Z_3 \cdot (X_3 + Y_2 \cdot Z_3), \quad (68)$$

$$Z_3 = C^2, \quad (69)$$

где $A = Y_1 + Y_2 \cdot E,\ B = X_1 + X_2 \cdot Z_1,\ C = Z_1 \cdot B,\ D = A \cdot C,\ E = Z_1^2$.

Сложность операции сложения в смешанных проективных координатах Якоби составляет:

$$I_{add}^{mix}(LDPrj) = 10I_{mul} + 4I_{sqr} + 8I_{add}. \quad (70)$$

При сложении в смешанных координатах Чудновского, точек $P_1(X_1 : Y_1 : Z_1 : Z_1^2 : Z_1^3)$ и $P_2(X_2 : Y_2 : 1 : 1 : 1)$, используются выражения (63)-(65). Отличие этих координат состоит в экономии одной операции возведения в квадрат за счет предвычислений.

Сложность операции сложения в смешанных проективных координатах Чудновского составляет:

$$I_{add}^{mix}(ChudnPrj) = 11I_{mul} + 2I_{sqr} + 8I_{add}. \quad (71)$$

Для сложения точки в модифицированных проективных координатах Якоби $P_1(X_1 : Y_1 : Z_1 : Z_1^2)$ и в аффинных координатах $P_2(X_2 : Y_2 : 1 : 1)$, используются выражения (64)–(66).

Сложность операции сложения в смешанных модифицированных проективных координатах Якоби составляет:

$$I_{add}^{mix}(JacPrjMdf) = 11I_{mul} + 3I_{sqr} + 8I_{add}. \quad (72)$$

Сложение точек проективных модифицированных координатах Лопеса-Дахаба $P_1(X_1 : Y_1 : Z_1 : Z_1^2)$ и в аффинных координатах $P_2(X_2 : Y_2 : 1 : 1)$ выполняется аналогично проективным координатам Лопеса-Дахаба согласно выражений (67)-(69).

В этом случае сложность операции сложения составит:

$$I_{add}^{mix}(LDPrjMdf) = 10I_{mul} + 4I_{sqr} + 8I_{add}. \quad (73)$$

2. Операции сложения проективных координат с пониженной вычислительной сложностью

Анализируя арифметические операции в существующих проективных координатах, авторами был проведен вывод выражений для вычисления координат результирующей точки. Полученные результаты, выгодно отличаются от приведенных в открытой печати [1-3, 7-10, 12], и содержат на несколько полевых операций меньше. Рассмотрим операции сложения с уменьшенной сложностью.

Сложение точек в проективных координатах Якоби

Преобразуем выражение (27) Y-координаты к виду:

$$\begin{gathered} Y_3 = X_3\left(Y_1Z_2^3 + Y_2Z_1^3 + Z_3\right)+ \\ +\left(X_2Z_1^2\left(Y_1Z_2^3 + Y_2Z_1^3\right)+ Y_2Z_1^3\left(X_1Z_2^2 + X_2Z_1^2\right)\right)\left(X_1Z_2^2 + X_2Z_1^2\right)^2. \end{gathered} \tag{74}$$

Введем обозначения $L = Z_2^2$, $E = Y_1 \cdot L \cdot Z_2$, $F = Y_2 \cdot K \cdot Z_1$, $I = X_1 \cdot L$, $J = X_2 \cdot K$, $A = E + F$, $B = I + J$, $C = Z_1 \cdot Z_2$, $K = Z_1^2$, $M = B^2$. В новых обозначениях выражения (74), (28) и (30) примут вид:

$$X_3 = A \cdot \left(A + Z_3\right)+ M \cdot B + a \cdot Z_3^2, \tag{75}$$

$$Y_3 = X_3 \cdot \left(A + Z_3\right)+ M \cdot \left(A \cdot J + B \cdot F\right), \tag{76}$$

или преобразовав $\left(A \cdot J + B \cdot F\right)$ из (76), имеем

$$Y_3 = X_3 \cdot \left(A + Z_3\right)+ M \cdot \left(E \cdot J + F \cdot I\right), \tag{78}$$

$$Z_3 = C \cdot B. \tag{79}$$

Сложность операции сложения в проективных координатах полученных авторами составит:

$$I_{add}\left(JacPrj*\right) = 15I_{mul} + 4I_{sqr} + 8I_{add}. \tag{80}$$

Сложение точек в проективных координатах Лопеса-Дахаба

Преобразуем выражения (2) и (3) к проективному виду:

$$\begin{gathered} X_3 = \left(Y_1Z_2^2 + Y_2Z_1^2\right)^2 + Z_1Z_2\left(Y_1Z_2^2 + Y_2Z_1^2\right)\left(X_1Z_2 + X_2Z_1\right)+ \\ + Z_1Z_2\left(X_1Z_2 + X_2Z_1 + aZ_1Z_2\right)\left(X_1Z_2 + X_2Z_1\right)^2, \end{gathered} \tag{81}$$

$$\begin{gathered} Y_3 = \left(X_1Z_2 + X_2Z_1\right)^3\left(Z_1Z_2\right)^2\left(Y_1Z_2^2X_2Z_1 + Y_2Z_1^2X_1Z_2\right)+ \\ + X_3\left(Z_1Z_2\left(Y_1Z_2^2 + Y_2Z_1^2\right)\left(X_1Z_2 + X_2Z_1\right)+ Z_3\right), \end{gathered} \tag{82}$$

$$Z_3 = \left(Z_1Z_2\right)^2\left(X_1Z_2 + X_2Z_1\right)^2. \tag{83}$$

Обозначим $E = Y_1 \cdot Z_2^2$, $F = Y_2 \cdot Z_1^2$, $A = F + E$, $I = X_1 \cdot Z_2$, $J = X_2 \cdot Z_1$, $B = I + J$, $C = Z_1 \cdot Z_2$, $D = B \cdot C$, $K = A \cdot D$, $L = B^2 \cdot D$. В рамках введенных обозначений конечные формулы представим в виде:

$$X_3 = A^2 + K + L + a \cdot Z_3, \tag{84}$$

$$Y_3 = X_3 \cdot \left(K + Z_3\right)+ L \cdot C \cdot \left(F \cdot I + E \cdot J\right), \tag{85}$$

$$Z_3 = D^2. \tag{86}$$

Сложность операции сложения составит:

$$I_{add}\left(LDPrj*\right) = 14I_{mul} + 5I_{sqr} + 8I_{add}. \tag{87}$$

Сложение точек в смешанных координатах Лопеса-Дахаба и аффинных

В смешанных координатах Лопеса-Дахаба выражения для вычисления координат точек (84)-(87) упростятся:

$$X_3 = A^2 + D + C \cdot B^2 + a \cdot Z_3, \tag{88}$$

$$Y_3 = Z_3 \cdot \left(X_2 \cdot D + Y_2 \cdot Z_3\right)+ X_3 \cdot \left(D + Z_3\right), \tag{89}$$

$$Z_3 = C^2, \tag{90}$$

где $A = Y_1 + Y_2 \cdot Z_1^2$, $B = X_1 + X_2 \cdot Z_1$, $C = Z_1 \cdot B$, $D = A \cdot C$.

Сложность операции сложения в смешанных координатах составит:

$$I_{add}^{mix}\left(LDPrj*\right) = 10I_{mul} + 4I_{sqr} + 8I_{add}. \tag{90}$$

Сложение точек в проективных координатах Чудновского

В качестве отправной точки примем выражения (31)-(33). Обозначим $E = Y_1 \cdot Z_2^3$, $F = Y_2 \cdot Z_1^3$, $I = X_1 \cdot L$, $J = X_2 \cdot K$, $A = E + F$, $B = I + J$, $C = Z_1 \cdot Z_2$, $K = Z_1^2$, $L = Z_2^2$, $M = B^2$. Согласно введенным обозначениям, формулы для вычисления результирующей точки примут вид:

$$X_3 = A \cdot (A + Z_3) + M \cdot B + a \cdot Z_3^2, \tag{91}$$

$$Y_3 = X_3 \cdot (A + Z_3) + M \cdot (E \cdot J + F \cdot I), \tag{92}$$

$$Z_3 = C \cdot B. \tag{93}$$

Сложность операции сложения точек в координатах:

$$I_{add}(ChudPrj*) = 14I_{mul} + 2I_{sqr} + 8I_{add}. \tag{94}$$

Сложение точек в модифицированных проективных координатах Якоби

Введем обозначения $E = Y_1 \cdot L \cdot Z_2$, $F = Y_2 \cdot K \cdot Z_1$, $I = X_1 \cdot L$, $J = X_2 \cdot K$, $A = E + F$, $B = I + J$, $C = Z_1 \cdot Z_2$, $K = Z_1^2$, $L = Z_2^2$, $M = B^2$. Воспользуемся введенными обозначениями и выражениями (31)-(33). В результате (31)-(33) преобразуются к виду:

$$X_3 = A \cdot (A + Z_3) + M \cdot B + a \cdot Z_3^2, \tag{95}$$

$$Y_3 = X_3 \cdot (A + Z_3) + M \cdot (E \cdot J + F \cdot I), \tag{96}$$

$$Z_3 = C \cdot B. \tag{97}$$

Сложность операции сложения составит:

$$I_{add}(JacPrjMdf*) = 15I_{mul} + 2I_{sqr} + 8I_{add}. \tag{98}$$

Сложение точек в модифицированных проективных координатах Лопеса-Дахаба

Воспользуемся ранее полученными выражениями (45)–(47), с учетом введенных обозначений $E = Y_1 \cdot Z_2^2$, $F = Y_2 \cdot Z_1^2$, $A = F + E$, $I = X_1 \cdot Z_2$, $J = X_2 \cdot Z_1$, $B = I + J$, $C = Z_1 \cdot Z_2$, $D = B \cdot C$, $K = A \cdot D$, $L = B^2 \cdot D$, формулы (45)–(47) примут вид:

$$X_3 = A^2 + K + L + a \cdot Z_3, \tag{99}$$

$$Y_3 = X_3 \cdot (K + Z_3) + L \cdot C \cdot (F \cdot I + E \cdot J), \tag{100}$$

$$Z_3 = D^2. \tag{101}$$

Сложность операции сложения составит:

$$I_{add}(LDPrjMdf*) = 14I_{mul} + 3I_{sqr} + 8I_{add}. \tag{102}$$

3. Сравнение

В сводной таблице 1 приведены полученные сложности арифметических операций на ЭК. Строки, помеченные символом (*) содержат результаты, полученные авторами.

С целью сравнения сложности преобразований в различных координатах, выразим вычислительную сложность операции инверсии и возведения в квадрат через сложность операции умножения в поле, следующим образом $I_{inv} \approx 10{,}5I_{mul}$, $I_{sqr} \approx 0{,}11I_{mul}$ [8]. Операция сложения не учитывалась в силу своей малой вычислительной сложности, что не приводит к существенному влиянию на результирующую сложность.

Таблица 1.

Система координат	Общее сложение				Общее сложение (смешанные координаты)				Удвоение			
	/	^2	*	Σ*	/	^2	*	Σ*	/	^2	*	Σ*
Аффинная, (x, y)	1	1	2	12,6	-	-	-		1	1	2	12,6
Стандартная проективная, [8], $(X/Y, Y/Z)$	-	3	14	14,3	-	2	12	12,2	-	2	8	8,22
Проективная Якоби, [8], $(X/Z^2, Y/Z^3)$	-	5	15	15,5	-	3	11	11,3	-	5	5	5,55
Проективная Якоби*, $(X/Z^2, Y/Z^3)$	-	4	15	15,4	-	3	11	11,3	-	5	5	5,55
Модифицированная проективная Якоби, [8], $(X/Z^2, Y/Z^3)$	-	3	15	15,3	-	3	11	11,3	-	5	5	5,55
Модифицированная проективная Якоби*, $(X/Z^2, Y/Z^3)$	-	2	15	15,2	-	3	11	11,3	-	5	5	5,55
Проективная Чудновского, $(X/Z^2, Y/Z^3)$	-	3	15	15,3	-	2	11	11,2	-	5	6	6,55
Проективная Чудновского*, $(X/Z^2, Y/Z^3)$	-	2	14	14,2	-	2	11	11,2	-	5	6	6,55
Проективная Лопес-Дахаб, [8], $(X/Z, Y/Z^2)$	-	6	15	15,7	-	4	10	10,4	-	5	5	5,55
Проективная Лопес-Дахаб*, $(X/Z, Y/Z^2)$	-	5	14	14,5	-	4	10	10,4	-	5	5	5,55
Модиф. проективная Лопес-Дахаб, $(X/Z, Y/Z^2)$	-	5	15	15,5	-	4	10	10,4		5	5	5,55
Модиф. проективная Лопес-Дахаб*, $(X/Z, Y/Z^2)$	-	3	14	14,3	-	4	10	10,4	-	4	5	5,44

* - авторская оптимизация.

Заключение

Из данных приведенных в таблице 1 следует, что операция сложения в проективных координатах Чудновского, стандартных проективных координатах, а также полученные авторами выражения для сложения в модифицированных координатах Лопеса-Дахаба, являются наиболее эффективными. Если рассматривать весь комплекс операций с точками на кривой, а именно, операции необходимые для выполнения скалярного умножения точек, тогда лидирующие позиции занимают арифметические операции в координатах Лопес-Дахаба, согласно выражениям полученных авторами.

Внешне, полученный авторами выигрыш в несколько полевых операций кажется незначительным, однако он становится ощутимым при выполнении большого количества операций скалярного умножения. Примером может служить процессинговый центр банка по работе с электронными транзакциями. Известно, что каждая транзакция содержит авторскую электронную подпись, которую необходимо проверить. Так, при проверке электронной подписи на 1 млн. транзакций, выигрыш от применения выражений предложенных авторами в проективных координатах Лопеса-Дахаба, составит 44,8 тыс. транзакций.

В дальнейшем

Использование проективных координат позволяет уйти от операции инвертирования, время выполнения которой является наиболее значимой и составляет $I_{inv} \approx 10{,}5 I_{mul}$ [8], в то время как граничное условие является $I_{inv} \geq 3 I_{mul}$ [14]. Следовательно, использование проективных координат будет актуальным и в ближайшем будущем.

В последующих работах будет рассмотрен подход [9, 13], основанный на комбинировании различных координат, с целью уменьшения количества операций умножения и инвертирования при сложении и удвоении точек ЭК.

Список литературы. 1. ДСТУ 4541-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка. 2. IEEE P1363 / D9 (Draft Version 9). Standard Specifications for Public Key Cryptography, 1999. 3. AMERICAN NATIONAL STANDARD X9.62-1998 (Draft version), Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). 4. *D. Johnson, A. Menezes, S. Vanstone*. The elliptic curve digital signature. Certicom research 2001. Canada. 5. Анализ методов представления точек эллиптической кривой над двоичными полями/ *Ю.В. Стасев, В.Ю. Ковтун, О.А. Смирнов, Я.Ю. Стасева*// Системы обработки информации. – 2002. – Вып. 5(21). 6. Elliptic curves. J.S. MILNE. University of Michigan. 1996. 7. *Agnew, G. B., Mullin, R. C. and Vanstone, S. A.* On the development of a fast elliptic curve cryptosystem. Advances in Cryptology EuroCrypt'92. 8. *Darell Hankrson, Julio Lopez Hernandez, Alfred Menezes*. Software implementation of elliptic curve cryptography over binary fields. Advances in Cryptology Crypto '99. 9. *H. Cohen, A. Miyaji, T. Ono*. Efficient elliptic curve exponentiation using mixed coordinates. 10. *J.Lopez and R.Dahab*, Improved algorithms for elliptic curve arithmetic's in $GF\left(2^n\right)$, Selected Areas in Cryptography –SAC'98, LNCS 1556, 1999, 201-212. 11. Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three. *N.P. Smart, E.J. Westwood*. Computer Science Department University of Bristol. United Kingdom. 12. *D.V. Chudnovsky, G.V. Chudnovsky* "Sequence of number generated by addition in formal group and new primality and factorization test", Advanced in Applied Math., 8 (1986), 385-434. 13. *Збитнев С.И.* Проективная геометрия – не все так гладко // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2002. Вып. 126. 14. *Вишенько В.В., Ковтун В.Ю., Пєвнєв В.Я., Смирнов А.А.* Модифікований алгоритм скалярного добутку точок еліптичної кривої над двійковими полями.// Вісник ЖДТУ.-2003.-№2(26).-Т.1/Технічні науки.-С.187-192. 15. *И.Р. Шафаревич.* Основы алгебраической геометрии. –М. -1972, с. 568. 16. Ю.П. Соловьев. Рациональные точки на эллиптических кривых// Соросовский образовательный журнал. 1997. №10, с. 138-143. 17. *Степанов* С.А. Арифметика алгебраических кривых. М.: Наука, 1999. 18. А. Ездаков, О. Макарова, Как защитить информацию. Сети, 1997, № 8. 19. *В. Сабынин*, Специалисты, давайте говорить на одном языке и понимать друг друга. Информост - Средства связи, № 6. 20. *П. Сэйер*. Lloyd страхует от хакеров. Computerworld Россия, 2000, № 30. 21. *Л. Хмелев.* Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем. Труды научно-технической конференции "Безопасность информационных технологий", Пенза, июнь 2001.

УДК 681.3.06:519.248.681

Арифметические операции на эллиптической кривой над двоичным полем в проективных координатах / С.И. Збитнев, В.Ю. Ковтун, О.Е. Илясова // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2004. Вып. 0000. С. 00-00.

В работе проводится анализ арифметических операций на эллиптической кривой в проективных координатах. Предлагаются улучшенные выражения для вычисления результатов арифметических операций в проективных координатах, а также даются рекомендации по их применению.

Табл. 1. Библиогр.: 21 назв.

УДК 681.3.06:519.248.681

Арифметичні операції на еліптичній кривій над двійковим полем у проективних координатах / С.І. Збітнєв, В.Ю. Ковтун, О.Є. Ілясова // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2004. Вип. 000. С. 00-00.

У роботі проводиться аналіз арифметичних операцій на еліптичній кривій у проективних координатах. Пропонуються покращенні вирази для обчислення результатів арифметичних операцій у проективних координатах, також даються рекомендації щодо їх застосування..

Табл. 1. Бібліогр.: 21 назви.

UDC 681.3.06:519.248.681

Arithmetic operations on elliptic curve over binary field in projective coordinates/ S.I. Zbitnev, V.Jur. Kovtun, O.E. Ilysova // Radiotekhnika: all-Ukr. Sci. Interdep. Mag. 2003. N 000 C. 00-00

At this paper analyse arithmetic operations on elliptic curve in projective coordinates are considered. Efficient expressions for arithmetic computing in projective coordinates are proposed and recommendations for their usage are given too.

1 tab., Ref.: 21 items