УДК 681.3.06:519.248.681

И. Д. ГОРБЕНКО, д-р техн. наук, С. И. ЗБИТНЕВ, А. А. ПОЛЯКОВ

СЛОЖНОСТЬ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ В ГРУППАХ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ КРИПТОГРАФИЧЕСКИХ ОПЕРАЦИЙ

Введение

В 90-е годы разработаны и нашли широкое распространение методы и средства обеспечения целостности и подлинности информации, которые базируются на несимметричной криптографии. Необходимый уровень стойкости в них обеспечивается за счет выполнения арифметических операций над целыми числами в кольцах, полях и подполях (подгруппах). В то же время непрерывное развитие математических методов и средств криптоанализа требует постоянного увеличения величин модуля преобразования. На сегодня безопасным считается длина модуля 2048 и более битов. Однако увеличение длин преобразуемых чисел приводит к увеличению сложности преобразований, а также длин ключей и параметров. Разрешение этого противоречия наметилось за счет выполнения криптографических преобразований в группе точек эллиптической кривой (ЭК). Разработаны и нашли применения стандарты цифровой подписи X9.62 [1] и распределение ключей X9.63 [2]. При их использовании появилась возможность уменьшения длины параметров и ключей, а также уменьшения вычислительной сложности преобразований и, как следствие, повышение скорости преобразований. В то же время проблема дальнейшего уменьшения сложности криптографических преобразований в группах точек эллиптических кривых остается весьма актуальной.

Проведенный анализ показал, что выполнение операций сложения и умножения в группе точек эллиптической кривой может выполняться с использованием аффинных или проективных координат[3]. Представляется необходимым проведение подробных исследований и сравнительного анализа сложности арифметических операций (преобразований) с целыми числами большой разрядности (160 и более) с использованием аффинных и проективных координат. При этом первоочередным является проведение сравнительного анализа сложности операций и умножения в группе точек эллиптических кривых над полем $GF(2^m)$.

Целью настоящей статьи и является проведение сравнительного анализа сложности выполнения арифметических операций в группах точек эллиптических кривых в поле $GF(2^m)$ для $m = 160$ и более битов.

1. Сложность арифметических операций над элементами в поле $GF(2^m)$

Наиболее распространенные представления элементов в полях $GF(2^m)$ – полиномиальное и нормальное [3], но наиболее эффективным, позволяющим достичь большей производительности, является полиномиальное. Подробное сравнение проведено в [4] . Далее мы будем рассматривать только полиномиальное представление элементов поля $GF(2^m)$.

Основными операциями над элементами в поле $GF(2^m)$ являются операции сложения по модулю *2*, умножения по модулю $(f(x),2)$, вычитание (идентично сложению), возведение в квадрат (частный случай умножения), нахождение обратного элемента в поле. Ниже приведена сложность алгоритмов из [3] с учетом представления чисел в ЭВМ.

Сложение по модулю 2 (I_{sum}):

$$I_{sum}[x] = bl[x], \tag{1}$$

где x – дли блока преобразования в битах; $bl[x] = \left\lceil \frac{x}{32} \right\rceil$.

Умножение по модулю $(f(x),2)$ (I_{mul}):

$$I_{mul} = (5 + 1984 \cdot bl[x]) \cdot x \tag{2}$$

Возведение в квадрат по модулю $(f(x),2)$ (I_{sqr}):

$$I_{sqr} = x \cdot (5.5 + 993 \cdot bl[x]) + 468 \cdot bl[x] \tag{3}$$

Нахождение обратного элемента по модулю $(f(x),2)$ (I_{inv}):

$$I_{inv} = (x-1)\cdot I_{sqr} + 0.5\cdot x\cdot I_{mul} \tag{4}$$

2. Сущность и анализ сложности преобразований в аффинных координатах

Пусть в группе точек эллиптических кривых над полем $GF(2^m)$, вида $y^2 + xy = x^3 + ax^2 + b \bmod(f(x),2)$ заданы точки $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$. Суммой двух точек $P_1 + P_2$ называется точка, имеющая координаты (x_3, y_3), причем:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \bmod(f(x),2), \tag{5}$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \bmod(f(x),2), \tag{6}$$

где $\lambda = \dfrac{y_1 + y_2}{x_1 + x_2}$.

Подсчитав общее количество сложений, умножений и инверсий и подставив сложность соответствующих арифметических операций, получим:

$$I^{af}{}_{add} = (8 + x)\cdot I_{mul} + (x-1)\cdot I_{sqr} + 9I_{sum} \tag{7}$$

Существует частный случай сложение двух точек – удвоение. Пусть в группе точек эллиптических кривых над полем $GF(2^m)$ вида $y^2 + xy = x^3 + ax^2 + b \bmod(f(x),2)$ задана точка $P_1 = (x_1, y_1)$. Удвоением точки $2\cdot P_2$ называется точка, имеющая координаты (x_2, y_2), причем:

$$x_3 = \lambda^2 + \lambda + a \bmod(f(x),2), \tag{8}$$

$$y_3 = x_1^{\,2} + (\lambda + 1)\cdot x_3 \bmod(f(x),2), \tag{9}$$

где $\lambda = x_1 + \dfrac{y_1}{x_1}$.

Подсчитав общее количество сложений, умножений и инверсий и подставив сложность соответствующих арифметических операций, получим:

$$I^{af}{}_{double} = (5 + x)\cdot I_{mul} + x\cdot I_{sqr} + 5I_{sum} \tag{10}$$

3. Сущность и анализ сложности преобразований в проективных координатах

Пусть в группе точек эллиптических кривых над полем $GF(2^m)$ вида $Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6 \bmod(f(x),2)$ заданы точки $P_1 = (X_1, Y_1, Z_1)$ и $P_2 = (X_2, Y_2, Z_2)$. Суммой двух точек $P_1 + P_2$ называется точка, имеющая координаты (X_3, Y_3, Z_3), причем:

$$U_0 = X_1\cdot Z_2^{\,2}, \quad U_1 = X_2\cdot Z_1^{\,2}, \quad S_0 = Y_1\cdot Z_2^{\,3}, \quad S_1 = Y_2\cdot Z_1^{\,3}, \quad W = U_0 + U_1, \quad R = S_0 + S_1;$$
$$L = Z_1\cdot W, \qquad V = R\cdot X_2 + L\cdot Y_2,$$

$$Z_3 = L\cdot Z_2;\ T = R + Z_3, \qquad X_3 = a\cdot Z_3^{\,2} + T\cdot R + W^3, \qquad Y_3 = T\cdot X_3 + V\cdot L^2 \tag{11}$$

Подсчитав общее количество сложений, умножений и инверсий и подставив сложность соответствующих арифметических операций, получим:

$$I^{pr}{}_{add} = 22\cdot I_{mul} + 5\cdot I_{sqr} + 7I_{sum} \tag{12}$$

В проективных координатах также существует частный случай сложение двух точек – удвоение. Пусть в группе точек эллиптических кривых над полем $GF(2^m)$ вида

$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6 \bmod\left(f(x),2\right)$ задана точка $P_1 = (X_1, Y_1, Z_1)$. Удвоением точки $2 \cdot P_2$ называется точка, имеющая координаты (X_3, Y_3, Z_3). причем:

$$c = b^{2^{m-2}}, \qquad Z_2 = X_1 \cdot Z_1^{\,2}, \qquad X_2 = \left(X_1 + c \cdot Z_1^{\,2}\right)^4,$$
$$U = Z_2 + X_1^{\,2} + Y_1 \cdot Z_1, \qquad Y_2 = X_1^{\,4} \cdot Z_2 + UX_2. \tag{13}$$

Подсчитав общее количество сложений, умножений и инверсий и подставив сложность соответствующих арифметических операций, получим:

$$I^{pr}{}_{double} = 9 \cdot I_{mul} + 5 \cdot I_{sqr} + 4I_{sum} \tag{14}$$

С использованием выражений (7) и (12) определяем сложность сложения точек на ЭК, а с использованием выражений (10) и (14) - сложность удвоения на ЭК. При этом перевод из аффинных координат в проективные выполняется в виде [3]

$$X = x \ , \ Y = y, \ Z = 1. \tag{15}$$

Преобразование из проективных координат в аффинные выполняется в виде [3]

$$x = \frac{X}{Z^2}, \ y = \frac{Y}{Z^3} \tag{16}$$

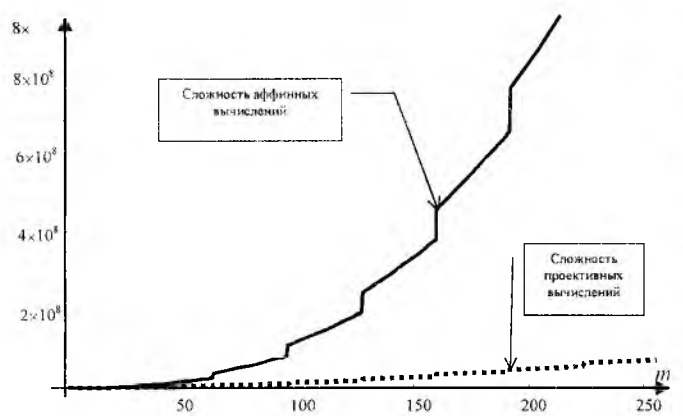

Рис. 1

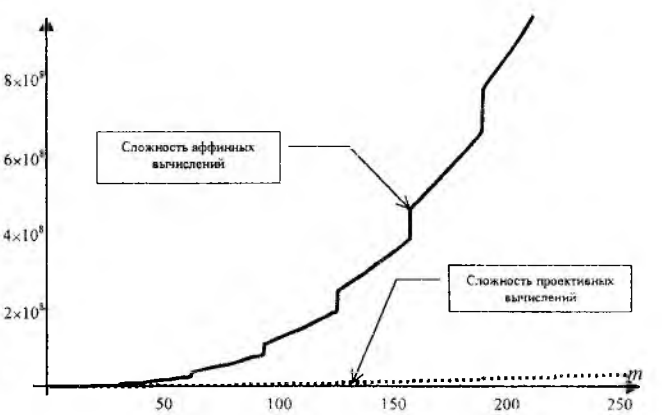

Рис. 2

В приведенных выражениях x, y - аффинные координаты, X, Y, Z – проективные координаты точек ЭК.

Графики сложности сложения и удвоения на эллиптической кривой в аффинных и проективных координатах (в зависимости от порядка расширенного поля m) приведены на рис.1, 2 соответственно.

Сложность сложения и удвоения точек на ЭК вычислена в числе тактов, необходимых для выполнения операций с длиной чисел в m бит. Зная число тактов выполнения операций сложения и удвоения можно определить время выполнения каждой из операций.

На рис. 3 и 4 приведены графики сложности сложения и удвоения для небольших значений m. Из графиков следует, что сложность вычислений в аффинных координатах меньше сложности вычислений в проективных координатах при $m \le 11$, а удвоение $m \le 5$.

Следует отметить, что на рис. 1-4 приведены значения сложности сложения и удвоения без учета преобразований из одних координат в другие. На практике выполняются операции умножения большого целого числа d на базовую точку G с координатами x_G и y_G, так, что

$$Q = d \cdot G(\bmod f(x), 2) \tag{17}$$

где Q - точка на ЭК (открытый ключ). Причем, значение (точка) Q вычисляется посредством многократного выполнения операций сложения и удвоения. После нахождения Q в проективных координ-

натах необходимо преобразовать его в аффинных координатах, что выполняется с использованием (16). Эта операция выполняется один раз.

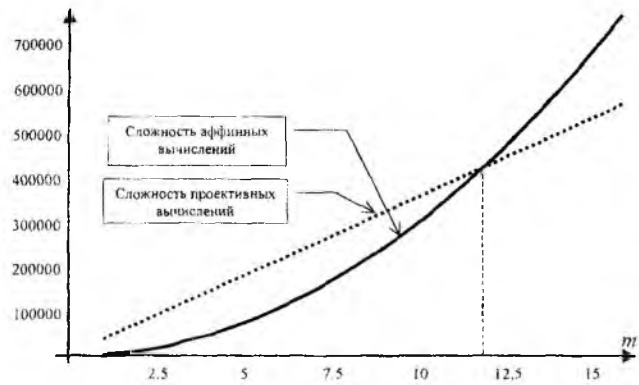

Рис. 3

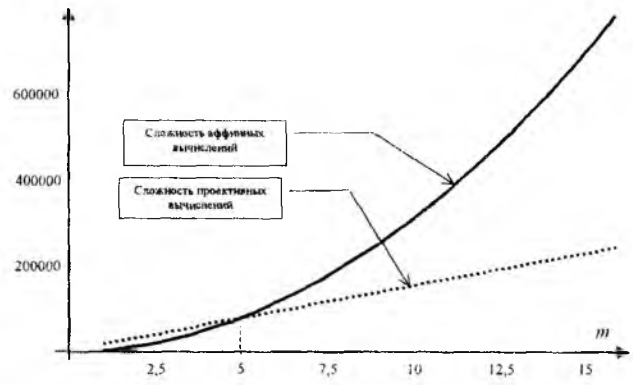

Рис. 4

В связи с тем, что основной операцией в криптографических преобразованиях является операция умножения (17), исследовалась сложность ее выполнения в аффинных и проективных координатах. На рис. 5-8 приведены зависимости сложности выполнения операции умножения (17) в зависимости от величины d при значения порядка расширения поля $m = 16, 32, 128, 256$, битов соответственно, причем, d изменялось в интервале от 1 до 2^m.

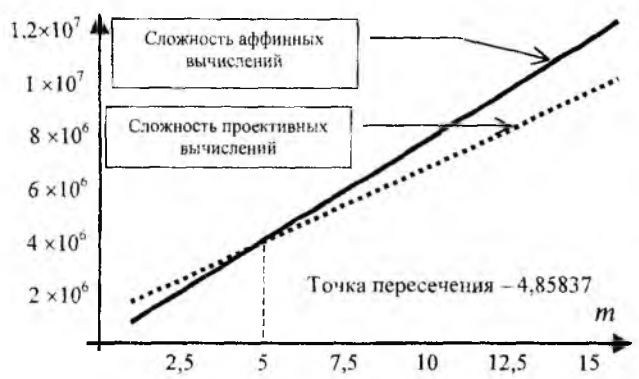

Рис. 5

Рис. 6

Рис. 7

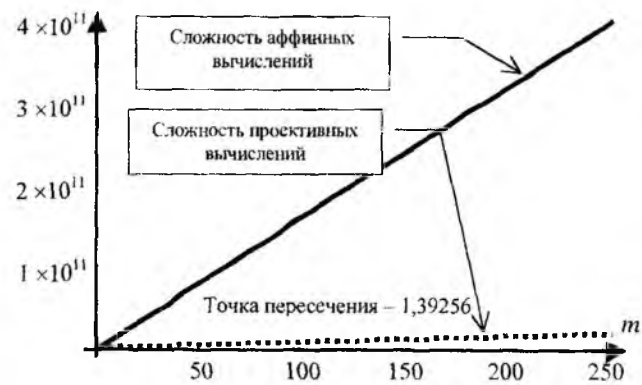

Рис.8

На рис. 9 и 10 приведены графики зависимости сложности умножений в аффинных и проективных координатах как функция величин d и m.

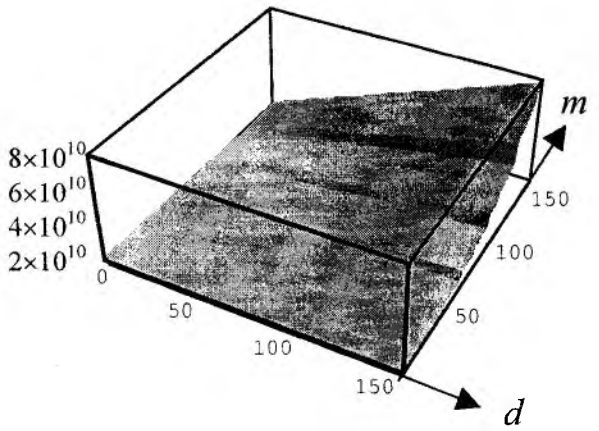

Рис. 9

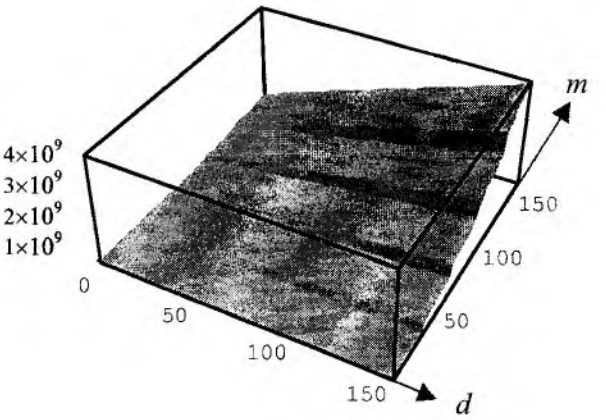

Рис. 10

Таблица 1

M	160	192	256
t_a	0,494	2,829	6,712
t_n	0,010	0,108	0,229

Для проверки сложности выполнения операции умножения (17) выполнены экспериментальные измерения с использованием стандартных библиотек, реализованных в аффинных и проективных координатах. В табл. 1 приведены значения среднего времени выполнения операции (17) в секундах при m = 160, 192 и 256, для аффинных t_a и проективных t_n координат с использованием ЭВМ на процессоре Celeron 600 MHz.

Экспериментальные результаты подтверждают теоретические.

Выводы

Анализ полученных результатов позволяет сделать вывод, что использование проективных координат при умножении является более предпочтительным, учитывая то, что минимальная длина поля, для обеспечения приемлемого уровня стойкости [3], должна быть не менее 160 бит. Меньшая сложность достигается при использовании проективных координат. Величина выигрыша в зависимости от значений d и m может быть определена из рис. 9 и 10.

Список литературы: 1. *X9.62 Public Key Cryptography For The Financial Services Industry*: The Elliptic Curve Digital Signature Algorithm (ECDSA). 1998. 87 с. 2. *X9.63 Public Key Cryptography For The Financial Services Industry*: Key Agreement and Key Transport Using Elliptic Curve Cryptography. 1999. 207 с. 3. *IEEE P1363/D11 (Draft Version 11).* Standard Specifications for Public Key Cryptography. Annex A (Informative). Number-Theoretic Background. 1999. 91 с. 4. *И.Д. Горбенко, С.И. Збитнев* Расширенное поле Галуа $GF(2^m)$. Вычислительная сложность простейших операций над расширенным полем $GF(2^m)$ // Радиотехника. 2000. Вып. 114. 10 с.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 19.03.2001