УДК 621.327

ПРЕДСТАВЛЕНИЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ НАД ДВОИЧНЫМИ ПОЛЯМИ

В.Ю. Ковтун, А.А. Смирнов, Я.Ю. Стасева
(представил д.т.н., проф. Ю.В. Стасев)

Рассмотрен один из возможных подходов в представлении точек эллиптической кривой над двоичными полями, направленному для уменьшения времени выполнения операций над ними. Предложены некоторые оригинальные подходы к уже существующим методам представления.

В последние годы интенсивно развивается направление криптографии, основанное на преобразованиях в группе точек эллиптических кривых. Интерес к нему обусловлен, с одной стороны, тем, что эти преобразования являются богатым источником конечных абелевых групп, обладающих полезными структурными свойствами, так и тем, что на их основе строятся криптосистемы с характеристиками, которыми обладают криптосистемы, выполняющие преобразования над $GF(p)$ и $GF(2^m)$, но при существенно меньшем размере ключа.

Запишем наиболее общее выражение Вейерштрасса для простых и двоичных конечных полей [1]:

– для простых конечных полей $GF(p)$ с $p>3$:

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

где a и b элементы $GF(p)$, для которых $4a^3 + 27b^2 \neq 0 \pmod p$;

– для двоичных расширенных полей $GF(2^m)$:

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

где $a \in \{0, 1\}$ и $b \in GF(2^m)$ при $b \neq 0$.

Роль основной криптографической функции выполняет операция умножения точек кривой на скаляр на основе операции сложения точек кривой. Таким образом, скорость выполнения этой операции зависит непосредственно от скорости выполнения операции сложения точек. Изменив представление точки кривой можно уменьшить количество критичных ко времени операций над точками. Кривую на плоскости можно задать с помощью аффинных и проективных координат. Рассмотрим аффинные координаты. Пусть k – поле. Аффинная плоскость над k есть

$$A^2(k) = k^2. \tag{3}$$

Неконстантный полином $f \in k\,[X, Y]$ не должен иметь повторяющихся

множителей в $k^{al}[X, Y]$. Зададим плоскую аффинную кривую C_f над k, точки которой с координатами, принадлежащими любому полю $K \supset k$, обращают в ноль f в K^2 [1]:

$$C_f(K) = \{(x, y) \in K^2 \mid F(x, y) = 0\}. \quad (4)$$

Пусть E – эллиптическая кривая над $GF(2^m)$, заданная выражением (2), а $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ – точки на кривой, причем $P_1(x_1, y_1) \neq -P_2(x_2, y_2)$.

Рассмотрим операцию сложения в аффинных координатах точек

$$P_3(x_3, y_3) = P_1 + P_2,$$

которая может быть вычислена как:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a; \quad (5) \qquad y_3 = (x_1 + x_3)\lambda + x_3 + y_1, \quad (6)$$

где $\lambda = \dfrac{y_1 + y_2}{x_1 + x_2}$, если $P_1 \neq P_2$; (7) $\lambda = \dfrac{y_1}{x_1 + x_2}$, если $P_1 = P_2$. (8)

Таким образом, для выполнения сложения двух различных точек, необходимо выполнить: одно возведение в квадрат, одно умножение, одно деление, 8 сложений. Для выполнения операции удвоения необходимо выполнить: одно возведение в квадрат, одно умножение, одно деление, 8 сложений. Наиболее трудоемкой операцией, среди перечисленных выше, является деление [2]. При большом количестве выполнения операций сложения, становится заметно влияние этой операции на работу криптосистемы. Одним из возможных способов уменьшить влияние операции деления на интенсивное сложение точек, есть переход к проективным координатам.

Проективная плоскость над полем F:

$$P^2(F) = \{(x, y, z) \in F^3 \mid (x, y, z) \neq (0, 0, 0)\}, \quad (9)$$

где $(x, y, z) \sim (x', y', z')$, только если существует $c \neq 0$, такое, что $(x', y', z') = (cx, cy, cz)$. Мы запишем $(x:y:z)$ для классов эквивалентности (x, y, z). Пусть точка $P \in P^2(F)$, тогда тройка $(x, y, z) \in L(P)$ представляет точку P в F^3, а $P \to L(P)$ является биекцией из $P^2(F)$ во множество таких линий [1].

На сегодняшний день существует несколько видов проективных координат. Начнем со стандартных проективных координат.

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

$$(X/Z; Y/Z). \quad (10)$$

Пусть E – эллиптическая кривая над $GF(2^m)$, заданная выражением (2). Подставляя соответствующие координаты (10) в (2), получаем проективную запись эллиптической кривой

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3. \quad (11)$$

Пусть заданы две точки на кривой в проективных координатах: $P_1(X_1:Y_1:Z_1)$ и $P_2(X_2:Y_2:Z_2)$, причем $P_1(X_1:Y_1:Z_1) \neq -P_2(X_2:Y_2:Z_2)$. Рассмот-

рим операцию сложения в стандартных проективных координатах точек

$$P_3(X_3:Y_3:Z_3) = P_1+P_2,$$

выражение для вычисления которых может быть получено путем подстановки координат точек P_1 и P_2 в виде (10) в выражения (5), (6), (7), (8).

После несложных математических преобразований имеем: если $P_1 \neq P_2$, то для выполнения сложения двух различных точек, необходимо выполнить 3 возведения в квадрат, 13 умножений, 8 сложений, а если $P_1 = P_2$, то для выполнения удвоения точки, необходимо выполнить 2 возведения в квадрат, 6 умножений, 3 сложения. Если одна из точек представлена в аффинных, а другая в проективных координатах ($P_1(X_1,Y_1,Z_1)$, $P_2(X_2,Y_2,1)$), то для выполнения удвоения точки необходимо выполнить 2 возведения в квадрат, 10 умножений, 7 сложений.

Перейдем к проективным координатам Якоби. Проективной точке $(X:Y:Z)$, $Z \neq 0$, ставится в соответствие точка с аффинными координатами

$$\left(X/Z^2; Y/Z^3\right). \tag{12}$$

Пусть E – эллиптическая кривая над $GF(2^m)$, заданная выражением (2). Подставляя соответствующие координаты (12) в (2), получаем проективную запись эллиптической кривой

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6. \tag{13}$$

Пусть заданы две точки на кривой в проективных координатах: $P_1(X_1:Y_1:Z_1)$; $P_2(X_2:Y_2:Z_2)$. Рассмотрим операцию сложения точек в проективных координатах Якоби

$$P_3(X_3:Y_3:Z_3) = P_1+P_2,$$

выражение для вычисления которых может быть получено путем подстановки координат точек P_1 и P_2 в виде (12) в выражения (5), (6), (7), (8).

Если $P_1 \neq P_2$, то для выполнения сложения двух различных точек необходимо выполнить 5 возведений в квадрат, 14 умножений, 7 сложений.

Произведем преобразования способом, отличным от [3]:

$$Y_3' = (Y_1 \cdot Z_2^3 + Y_2 \cdot Z_1^3 + Z_3) \cdot X_3 + ((Y_1 \cdot Z_2^3 + Y_2 \cdot Z_1^3) \cdot X_2 Z_1^2 + Y_2 Z_1^3 \cdot (X_1 \cdot Z_2^2 + X_2 \cdot Z_1^2)) \cdot (X_1 \cdot Z_2^2 + X_2 \cdot Z_1^2)^2; \tag{14}$$

произведем замену:

$$A = Y_1 \cdot Z_2^3 + Y_2 \cdot Z_1^3;\ B = X_1 \cdot Z_2^2 + X_2 \cdot Z_1^2;\ C = Z_1 \cdot Z_2$$

и запишем в виде:

$$X_3 = A \cdot (A + Z_3) + B^2 \cdot B + aZ_3^2; \tag{15}$$

$$Y_3' = (A + Z_3) \cdot X_3 + (A \cdot X_2 Z_1^2 + Y_2 Z_1^3 \cdot B) \cdot B^2; \tag{16}$$

$$Z_3 = C \cdot B. \tag{17}$$

Таким образом, для выполнения сложения двух различных точек, необходимо выполнить 4 возведения в квадрат, 14 умножений, 7 сложений.

Если $P_1 = P_2$, то для выполнения сложения двух одинаковых точек необходимо выполнить 5 возведений в квадрат, 5 умножений, 4 сложения.

В случае, когда одна из точек представлена в проективных, а другая в аффинных координатах ($P_1(X_1, Y_1, Z_1)$, $P_2(X_2, Y_2, 1)$), для выполнения сложения двух одинаковых точек необходимо выполнить 4 возведения в квадрат, 10 умножений, 8 сложений.

Рассмотрим проективные координаты Лопеса-Дахаба. Проективной точке ($X:Y:Z$), $Z \neq 0$, ставится в соответствие точка с аффинными координатами

$$\left(X/Z; Y/Z^2\right). \tag{18}$$

Пусть E – эллиптическая кривая над $GF(2^m)$, заданная выражением (2). Подставляя соответствующие координаты (18) в (2), получаем проективную запись эллиптической кривой [2]:

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6. \tag{19}$$

Пусть заданы две точки на кривой в проективных координатах: $P_1(X_1:Y_1:Z_1)$, $P_2(X_2:Y_2:Z_2)$. Рассмотрим операцию сложения в оптимизированных проективных координатах точек

$$P_3(X_3:Y_3:Z_3) = P_1 + P_2,$$

выражение для вычисления которых может быть получено путем подстановки координат точек P_1 и P_2 в виде (18) в выражения (5), (6), (7), (8).

Если $P_1 \neq P_2$, то для выполнения сложения двух разных точек, необходимо выполнить 5 возведений в квадрат, 13 умножений, 8 сложений, иначе [2] для удвоения точки необходимо выполнить 5 возведений в квадрат, 4 умножения, 4 сложения. В случае, когда одна из точек представлена в проективных, а другая в аффинных координатах ($P_1(X_1, Y_1, Z_1)$, $P_2(X_2, Y_2, 1)$) [2], для выполнения удвоения точки необходимо выполнить 4 возведения в квадрат, 9 умножений, 8 сложений. К аналогичным результатам, но с тремя возведениями в квадрат, можно прийти, если изменить порядок вычислений.

Результаты, полученные в [2], и описанные выше, приведены в табл. 1, 2 соответственно.

Таблица 1

Количество арифметических операций над элементами $GF(2^m)$ при выполнении операций над точками эллиптической кривой [2]

Система координат	Общее сложение		Общее сложение (смешанные координаты)		Удвоение	
	*	/	*	/	*	/
Аффинная, (x, y)	2	1	-	-	2	1
Стандартная проективная*, ($X/Z, Y/Z$)	13	-	12	-	7	-
Проективная Якоби*, ($X/Z^2, Y/Z^3$)	14	-	10	-	5	-
Проективная Лопеса-Дахаба, ($X/Z, Y/Z^2$)	14	-	9	-	4	-

Таблица 2

Количество арифметических операций над элементами $GF(2^m)$ при выполнении операций над точками эллиптической кривой (авторская реализация)

Система координат	Общее сложение				Общее сложение (смешанные координаты)				Удвоение			
	/	^2	*	+	/	^2	*	+	/	^2	*	+
Аффинная, (x, y)	1	1	1	9	-	-	-	-	1	1	1	8
Стандартная проективная, $(X/Z, Y/Z)$	-	3	13	8	-	2	10	7	-	2	6	3
Проективная Якоби, согласно [3], $(X/Z^2, Y/Z^3)$	-	5	14	7	-	4	10	8	-	5	5	4
Проективная Якоби*, $(X/Z^2, Y/Z^3)$	-	4	14	7	-	4	10	8	-	5	5	4
Проективная Лопеса-Дахаба*, $(X/Z, Y/Z^2)$	-	5	13	8	-	3	9	8	-	5	4	4

* – изменен порядок выполнения операций в вычислении координат, направленный на уменьшения количества критичных ко времени операций

Таким образом, по приведенным в табл. 2 данным, видно однозначное преимущество по количеству критичных ко времени операций при использовании проективных координат над аффинными. При этом количество операций в поле $GF(2^m)$ можно уменьшить за счет упорядочения последовательности их выполнения. Предлагается авторская реализация некоторых аналитических выражений, которые содержат меньшее количество операций, по сравнению с существующими.

ЛИТЕРАТУРА

1. *Milne J.S. Elliptic curves. – 1996.*
2. *Hankrson D., Hernandez J.L., Menezes A. Software implementation of elliptic curve cryptography over binary fields // Advances in Cryptology Crypto '99.*
3. *IEEE P1363 / D9 (Draft Version 9). Standard Specifications for Public Key Cryptography, 1999.*

Поступила 28.10.2002

КОВТУН Владислав Юрьевич, *адъюнкт ХВУ. В 2000 году окончил ХВУ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*

СМИРНОВ Алексей Анатольевич*, адъюнкт ХВУ. В 1999 году окончил ХВУ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*

СТАСЕВА Яна Юрьевна, *сотрудник лаборатории ХВУ. В 2002 году окончила ХНУРЭ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*