УДК519.1

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД КОНЕЧНЫМИ ВЕКТОРНЫМИ ПОЛЯМИ

Никулищев Г.И.,Козина Г.Л.
Запорожский национальный технический университет
кафедра защиты информации
E-mail: tymahob@ukr.net

Аннотация

Никулищев Г.И., Козина Г.Л.Эллиптическиекривые над конечнымвекторным полем. *Изучено введение специальной операции над векторами, которая позволяет построить конечное векторное поле.Рассмотрена возможность задания группы точек эллиптической кривой над конечным векторным полем, исследованы характеристики полученной группы. Предлагается использование математического аппарата конечных векторных полей в криптографических алгоритмах.*

Введение

В последние годы, согласно мировым тенденциям, повышается роль электронного документооборота, а, соответственно, и его защиты. Одним из наиболее действенных и надежных средств обеспечения безопасности электронных документов является электронная цифровая подпись (ЭЦП). В Украине действует Закон «Об ЭЦП» и национальный стандарт шифрования ДСТУ 4145-2002 «Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка», также нередко используется национальный стандарт России ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки ЭЦП».

Одним из инструментов обеспечения стойкости криптографических алгоритмов, в частности ЭЦП, является вычислительная сложность математических преобразований. Существует 2 пути повышения вычислительной сложности — увеличение размера задачи, то есть порядка используемых в алгоритме значений, и изменение качества задачи, то есть использование более стойкого математического аппарата.

В современной криптографии часто используется математический аппарат эллиптических кривых (ЭК). ЭК может быть определена над простым или расширенным полем. Алгоритмы шифрования и ЭЦП строятся на основе операций в группе точек ЭК. При этом криптографическая стойкость подобных алгоритмов основывается на сложности задачи дискретного логарифмирования в группе точек эллиптической кривой. В российском стандарте ЭЦП используется простое поле Галуа, в украинском – расширенное.

Оба стандарта для обеспечения достаточной стойкости рекомендуют использовать числа порядка 2^{128}-2^{512} в качестве параметров кривой и степеней полиномов. При увеличении размера задачи увеличивается и ее ресурсоемкость. Снижение требований к вычислительным ресурсам достигается подбором ЭК особого вида или оптимизацией групповой операции на кривой. В данной работе рассматривается подход к оптимизации групповой операции на ЭК, путем определения ее над конечным векторным полем.

Векторные поля

Конечное векторное поле (КВП) – одно из расширений конечного поля Галуа GF(p). Элементами КВП являются вектора конечной длины n, представленные набором коэффициентов (a, b,..,f) при соответствующих базисных векторах e, i,..,z. Количество базисных векторов, составляющих элемент КВП vзависит от величины n. Общий вид элемента КВП представлен выражением (1):

$$v = a \cdot e + b \cdot i + .. + f \cdot z . \quad (1)$$

Коэффициенты при базисных векторах являются элементами поля GF(p). Операция сложения двух векторов определяется сложением координат при соответствующем базисном векторе по модулю p. Операция умножения вектора на число определяется умножением каждого из коэффициентов на это число по модулю p. Операция умножения двух векторов ◦определяется по принципу перемножения многочленов, причем результат произведения двух базисных векторов определяется по таблице, составленной таким образом, чтобы обеспечить ассоциативность операции. Например, может быть использована следующая таблица умножения базисных векторов (табл. 1).

Таблица 1. Умножениебазисныхвекторов.

◦	e	i	j	k	u	…	z
e	e	i	j	k	u	…	z
i	i	τ·j	τ·k	τ·u	τ…	τ·z	τ·μ·e
j	j	τ·k	τ·u	τ…	τ·z	τ·e	μ·i
k	k	τ·u	τ…	τ·z	τ·μ·e	μ·i	μ·j
u	u	τ…	τ·z	τ·μ·e	μ·i	μ·j	μ·k
…	…	τ·z	τ·μ·e	μ·i	μ·j	μ·k	μ·u
z	z	τ·μ·e	τ·i	μ·j	μ·k	μ·u	μ…

Коэффициенты τ и μ также являются элементами поля GF(p). От значения этих коэффициентов зависит порядок мультипликативной группы КВП.Это связано с определением единичного элемента группы – им является вектор с коэффициентом 1 при базисном векторе еи нулевыми коэффициентами при остальных векторах. Если результатом операции умножения между двумя векторами является единичный вектор, то они называются взаимно обратными. Для того, чтобы любой возможный вектор длины nc коэффициентами из поля GF(p) имел обратный и ,соответственно, порядок мультипликативной группы поля равнялся (p^n-1), необходимо, чтобы коэффициенты τ и μ удовлетворяли характеристическому уравнению. Характеристическое уравнение составляется исходя из таблицы умножения базисных векторов и системы линейных уравнений, представляющих коэффициенты единичного вектора через коэффициенты двух взаимно обратных.

В частности, для n=2 и таблицы умножения составленной по табл.1 характеристическое уравнение будет определяться формулой (2)

$$a^2 - \tau \cdot b^2 \neq 0 \bmod p . \quad (2)$$

Соотношение (2) будет выполняться для любыходновременно ненулевых a иb, элементов поля GF(p), только если τ будет квадратичным невычетом в этом поле [1].

Пример 1. При n=2, τ=2, p=5 и операции умножения базисных векторов, заданной по табл.1, порядок мультипликативной группы КВП равен 24, примитивным элементом поля является вектор с координатами (1,3), а элементы (1,4) и (4,4) взаимно обратны. Результатом перемножения векторов (4,1) и (3,3) является элемент (3,0).

Эллиптические кривые над конечными векторными полями

Эллиптической кривой над полем GF(p) называется гладкая кривая, задаваемая уравнением (3):

$$y^2 + a_1 \cdot x \cdot y + a_3 \cdot y = x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_6, \quad (3)$$

где коэффициенты a_i (i=1,2,..,6) являются элементами поляGF(p), а операции производятся по модулю p.

Если характеристика поля, над которым задается кривая, не равна 2 или 3, то ее можно записать в сокращенной форме, определяемой выражением (4):

$$y^2 = x^3 + a \cdot x + b. \quad (4)$$

Если в (4) заменить операции умножения и возведения в степень операцией умножения векторов, то получим выражение (5) для записи ЭК над КВП:

$$y \circ y = x \circ x \circ x + a \circ x + b, \quad (5)$$

где x, y, a, и – элементы КВП.

Множество решений уравнения (5) составляет группу точек ЭК, единичным элементом в которой является, так называемая, бесконечно удаленная точка O. Вектора хи уназываются координатами точек, бесконечно удаленная точка не имеет координат.

Групповая операция сложения для точек ЭК над КВП задается с помощью формул (6) и (7) расчета координат результирующей точки (x_3,y_3) через координаты суммируемых точек (x_1,y_1) и (x_2,y_2):

$$x_3 = \lambda - x_1 - x_2; \quad (6)$$

$$y_3 = \lambda \circ (x_1 - x_3) - y_1. \quad (7)$$

Величина λ определяется по формуле (8), если складываются две разные точки:воздействия

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad (8)$$

и по формуле (9), если точка удваивается:

$$\lambda = \frac{3 \cdot x_1 \circ x_1 + a}{2 \cdot y_1}, \quad (9)$$

где a – коэффициент ЭК.

В формулах (8) и (9) операция деления заменяется умножением на вектор, обратный стоящему в знаменателе.

Определена также операция умножения точки на число, которая вычисляется с помощью необходимого количества последовательных сложений точки самой с собой. Две точки, результатом суммирования которых является бесконечно удаленная точка O, называются взаимно обратными.

Пример 2. Эллиптическая кривая с коэффициентами a=(2,3) и b=(0,4),заданная над полем из примера 1 содержит 17 точек: ((0,4),(2,0)), ((0,4),(3,0)), ((1,0),(1,1)),((1,0),(4,4)),((1,4),(0,2)), ((1,4),(0,3)),((2,0),(0,1)), ((2,0),(0,4)), ((3,0),(1,4)), ((3,0),(4,1)), ((3,2),(2,3)), ((3,2),(3,2)), ((4,1),(2,2)), ((4,1),(3,3)), ((4,3),(1,0)), ((4,3),(4,0)), O. Суммой точек с координатами ((1,4),(0,2)) и ((3,2),(2,3)) является точка ((2,0),(0,4)). Результат

удвоения точки ((1,4),(0,2)) – точка с координатами ((3,0),(1,4)). Точки((1,4),(0,2)) и ((1,4),(0,3)) взаимно обратны.

Порядок эллиптической кривой.

Порядком ЭК называется количество ее точек. В современных криптографических алгоритмах, как правило, используются группы точек ЭК большого простого порядка, поэтому актуальной является задача определения порядка ЭК. Эффективного алгоритма точного определения порядка ЭК на данный момент не существует, применяется метод оценки порядка, то есть определение диапазона значений, которые он может принять.

ДляЭК над простым полем Галуа GF(p) существует теорема Хассе, позволяющая оценить порядок кривой #E(p) [2]. Согласно теореме, значение порядка ЭК над полем GF(p) определяется неравенством (10):

$$p+1-2\cdot\sqrt{p}\le\#E(p)\le p+1+2\cdot\sqrt{p}\,. \qquad (10)$$

Для простого поля величина pпоказывает количество его элементов, то есть, порядок поля. Если коэффициенты таблицы умножения базисных векторов отвечают характеристическому уравнению, то порядком КВП,определенного над полем GF(p) будет величина p^n. Экспериментально проверено, что неравенство (10) остается справедливым и для ЭК над КВП, если вместо pподставить p^n.Таким образом, применение КВП позволяет засчет увеличения количества несложных арифметических операций добиться увеличения порядка группы точек без увеличения порядка используемых чисел [3].

Пример 3. Для поля из примера 1 оценка порядка ЭК по модифицированному неравенству (10) составляет от 16 до 36. ЭК из примера 2 имеет порядок 17, ЭК с коэффициентами a=(4,3) и b=(2,1) имеет порядок 31.

Выводы

Конечное векторное поле является расширением простого поля Галуа GF(p). Над КВП может быть определена эллиптическая кривая большого простого порядка, при этом во время выполнения операций в группе точек ЭКиспользуются элементы поля GF(p). Таким образом, использование ЭК над КВПв существующих криптографических алгоритмах позволит существенно увеличить порядок группы точек ЭК без существенного увеличения вычислительной сложности производимых операций, что приведет к снижению их ресурсоемкости при обеспечении необходимой криптостойкости.

В дальнейшем авторами планируется.анализ КВПи ЭК над ними, выбор оптимальной длины вектора nи значений коэффициентов таблицы умножения базисных векторов для обеспечения максимального выигрыша по скорости и ресурсоемкости при использовании их в криптографических алгоритмах. Планируется адаптация существующих алгоритмов для использования математического аппарата ЭК над КВП.

Литература

7. Nikolay A. Moldovyan. AccelerationoftheEllipticCryptographywithVectorFiniteFields. // I. J. NetworkSecurity. – Trier: UniversitatTrier, 2009. – № 9(2). – С. 180-185

8. Болотов А.А., Гашков С.Б. Алгоритмическиеосновыэллиптическойкриптографии. – М.: МЭИ, 2000. – 100 с.

9. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи: учеб. пособие для вузов по направлению "Прикладные математика и физика"/ Н. А. Молдовян. - СПб.: БХВ-Петербург, 2010. - VII, 289 с.