Эллиптическая криптография

Анализ алгоритмов скалярного произведения точек эллиптической кривой

Бычик Ю.Г.
ПОИТ, ФКСиС
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
e-mail: bychyk@gmail.com

***Аннотация* — В данном докладе приведены основные определения и понятия эллиптической криптографии, рассмотрены алгоритмы нахождения скалярного произведения точек эллиптической кривой, проведен теоретический анализ, отражены результаты работы программного средства по оценке эффективности алгоритмов.**

Ключевые слова: эллиптическая криптография; скалярное произведение точек; алгоритмы; эффективность; сравнительный анализ

I. Введение

В связи с быстрыми темпами развития научно-технического прогресса в последние 10 лет многие стандарты и подходы, использовавшиеся в сфере электронно - цифровой коммерции и электронного документооборота, стали неактульными. Большинство методов, основанных на проблеме факторизации, с ростом вычислительной мощности компьютеров стали более уязвимыми к криптографическим атакам. В связи с этими обстоятельствами возникла необходимость построения систем с более совершенными алгоритмами и протоколами.

Альтернативным подходом является использование эллиптической криптографии. На базе эллиптических кривых спроектированы алгоритмы и методы, позволяющие более эффективно решать проблемы информационной безопасности. Ключ с размером 160 бит в эллиптической криптографии обеспечивает уровень защиты, аналогичный уровню защиты RSA с размером ключа 1024 бит. Эллиптическая криптография основана на проблеме нахождения дискретного логарифма для пары точек эллиптической кривой.

Для эффективного использования эллиптической криптографии необходимо решать ряд проблем, связанных с производительностью. Наиболее затратной является операция скалярного произведения точек эллиптической кривой. Для решения данной проблемы необходимо провести анализ существующих алгоритмов и оценку экспериментальных данных.

II. Элементы эллиптической криптографии

Рассматриваемые эллиптические кривые [1] описываются уравнениями следующего вида (1):

$$y^2 = x^3 + ax + b \ (mod\ n) \tag{1}$$

где n – большое простое число, характеристика конечного поля F_n; x, y, a, b принадлежат F_n; $4a^3 + 27b^2 \neq 0 \ (mod\ n)$;

Основным элементом эллиптической кривой является точка. Точка обозначается $P(x,y)$. Существует точка, инверсная данной, имеющая следующее определение: $T = -P(x,y)$.

Одним из основных свойств эллиптической кривой является свойство секущей. Секущая, проходящая через график эллиптической кривой, пересекает его в трех точках. Пусть P и Q – различные точки эллиптической кривой, при этом инверсная точка для точки P не равна точке Q. Прямая, проходящая через данные точки, пересекает кривую в третьей точке, инверсной точке R.

Возможны следующие случаи для секущей и графика эллиптической кривой [2]: $P+Q = R$; $P+Q = P + P = R$ $(Q = P)$; $P+Q = P + P = 0$ $(Q=P, R = 0)$; $P + Q = 0$ $(R = 0)$;

Имея набор правил для вычисления значений точки, можно определить операцию умножения числа на точку(2):

$$kP = \underbrace{P + P + P + \ldots + P + P}_{k} \tag{2}$$

где k – целое положительное число; P – точка эллиптической кривой.

Для нахождения скалярного произведения (2) используются последовательные операции дублирования и сложения точек эллиптической кривой [2,3,4].

Для нахождения координат точки $R(x_R,y_R)$, равной сумме [4] двух точек $P(x_P,y_P)$ и $Q(x_Q,y_Q)$ используют следующие выражения (3,4,5):

$$\lambda = \frac{(y_P - y_Q)}{(x_P - x_Q)}, \tag{3}$$

$$x_R = \lambda^2 - x_P - x_Q, \tag{4}$$

$$y_R = -y_P + \lambda(x_P - x_R). \tag{5}$$

Для удвоения точки [4] $P(x_P,y_P)$ используют следующие выражения (6,7,8):

$$\lambda = \frac{(3x^2{}_P + a)}{2y_P}, \tag{6}$$

$$x_R = \lambda^2 - 2x_P, \tag{7}$$

$$y_R = -y_P + \lambda(x_P - x_R). \tag{8}$$

Для эллиптической группы (1) справедливы все правила, описанные для эллиптических кривых для действительных чисел. Выражения (3, 4, 5, 6, 7, 8) выполняются по модулю n.

Для оптимизации вычислений существует множество подходов, направленных как на модификацию параметра k в kP, так и на модификацию выражений (3, 4, 5, 6, 7, 8).

III. Обзор алгоритмов скалярного произведения

A. *Алгоритм удвоения- сложения*

Классический алгоритм [5] для нахождения скалярного произведения, использует двоичное представление k. Описывается следующим псевдокодом:

Библиотека БГУИР

Входные значения: Битовое представление *k,* точка *P*.

Выходное значение: Точка $Q = kP$

Q = O
For i = n – 1 to 0 do
Q = 2Q (Doubling)
If (k_i= 1) then
Q = Q + P (Addition)
Return Q

В среднем количество операций дублирования равно (n-1), количество операций сложения равно n/2..

B. *Алгоритм удвоения-сложения-вычитания*

Использует представление числа в троичной форме (NAF – non-adjacent form). Для -1 в разряде используется операция инвертирования точки эллиптической кривой.

При использовании метода удвоения – сложения - вычитания [5] в среднем используется (n-1) операций дублирования и (n-1)/3 операций сложения. Недостатком данного метода является использование дополнительной памяти для хранения *NAF(k)*.

C. *Алгоритм удвоения-сложения-вычитания с использованием окон*

Классический алгоритм [6] с использованием окон разбивает двоичное представление числа *k* на группы бит одинаковой длины. Если количество бит невозможно поделить на *w*, к двоичному представлению добавляются старшие нулевые биты. Затем для каждого $d \in \{0,1,2...2^{w-1}\}$ выполняются вычисления *dP*, где *P* – точка эллиптической кривой, для которой необходимо найти $Q = kP$. Так для $w = 2$ необходимой найти *P, 2P, 3P* на стадии предварительных вычислений

Алгоритм скалярного умножения с использованием окон позволяет выполнять меньшее количество операций сложения точек эллиптической кривой. Количество операций дублирования точки $n+1$, количество операций сложения равно $2^w - 2 + nw^{-1}$, где *n* – размер двоичного представления числа *k*, *w* – величина окна.

Алгоритм удвоения-сложения-вычитания с использованием окон [7] является модификацией алгоритма с использованием окон и двоичной формы числа *k.* Применяя *NAF* форму числа с окнами размера *w* возможно сократить вес Хемминга числа. Количество операций дублирования остается аналогичным, количество операций сложения точек уменьшается.

D. *Алгоритм Монтгомери*

Вводит избыточность в вычисления. При использовании данного алгоритма время выполнения зависит только от количества бит, а не от количества единичных разрядов. Данный подход исключает криптоанализ с использованием временных задержек [8].

E. *Алгоритм с модификацией 2P + Q*

Для нахождения *2P + Q* в прямом порядке необходимо выполнить *2I + 4M + 3S* (3,4,5,6,7,8).

Наиболее затратной операцией при расчетах является операция инвертирования. Следовательно, необходимо выполнить ряд преобразований для замены операции инвертирования на операции умножения и возведения в квадрат. Так операция инвертирования в конечном поле занимает в 80 раз больше, чем операция умножения. При использовании модифицированного подхода количество операций для *2P + Q* равно *I + 2S + 9M* [9].

IV. Экспериментальные результаты

Для проведения тестов использовалось разработанное программное средство и компьютер со следующими техническими характеристиками:

- процессор Intel Core 2 Duo T7250 2 GHz.
- оперативная память 2.00 GB, 333 MHz.

Результаты представлены в таблице 1:

Табл. 1. Экспериментальные результаты

Алгоритмы	Время выполнения алгоритма для различных кривых (мс)				
	112 бит	160 бит	224 бит	384 бит	521 бит
Монтгомери	53	112	262	1015	2213
Удвоения - сложения	40	95	190	784	1727
Модификация 2P + Q	39	78	187	750	1641
Алгоритм удвоения-сложения - вычитания	45	84	179	688	1521
Удвоения-сложения-вычитания с окном (w = 6)	34	73	160	614	1358

[1] Коблиц, Н. Введение в эллиптические кривые и модулярные формы / Н.Коблиц.- М.: Мир, 1988 – 320с.
[2] Hitchin, N Advances in elliptic curve cryptography / N. Hitchin - Cambridge University Press – Cambridge, 2005
[3] Jurisic, A. Elliptic curves and cryptography /A. Jurisic, A. Menezes // Dr. Dobb's Journal, Apr, 1977, P 26-37
[4] SEC 1: Elliptic curve cryptography / Certicom Research. – Sep, 20, 2000
[5] Balasubramaniam, P. Elliptic curve scalar multiplication algorithm using complementary recording, Applied Mathematics and Computation, vol. 190, issue 1, 2007, P. 51-56
[6] Harsandeep, B. Perfomance analysis of point multiplication methods for elliptic cryptography/ Computer Engineering and Technology conference, Punjab, India, Mar. 19, 2010, doc. 172
[7] Md. Rafiqul, I. A new point multiplication method for elliptic curve cryptography using modified base representation / Internation Journal of The Computer, the Internet and Management, vol. 16, issue 2, May, 2008, P. 9 -16
[8] Ciet, M. Trading inversions for multiplications in elliptic curve cryptography./ M. Joye, K. Lauter, P. Montgomery // Design, Codes and Cryptography, vol. 39, issue 2, 2006, P. 189-206
[9] Iqbal H., Jebril An impoved to compute 2P + Q on elliptic curve over finite field of characteristic $\neq 2,3$ / Special Issue of the International Journal of the Computer, the Internet and Management, vol. 17, issue SP1, Mar, 2009

Библиотека БГУИР