НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Практическая работа 2

Построение криптографических операций на эллиптических кривых

Евсютин О.О.

Москва 2024

1 ЦЕЛЬ РАБОТЫ

Целью данной работы является приобретение навыков программной реализации операций над точками эллиптических кривых для построения криптографических преобразований.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

2.1 Эллиптические кривые

Эллиптической кривой над конечным полем вычетов по модулю простого числа $p>3$ называется множество точек $(x, y) \in F_p \times F_p$, удовлетворяющих уравнению $y^2 = x^3 + ax + b$, где $a, b \in F_p$ и $-4a^3 - 27b^2 \neq 0 (mod\ p)$, дополненное бесконечно удаленной точкой 0, не имеющей численного выражения. Данное множество точек, обозначаемое $E_{a,b}(F_p)$, представляет собой абелеву группу относительно операции сложения точек.

В общем случае эллиптическая кривая может быть задана над полем Галуа (полем многочленных вычетов) $F_q = F_{p^n}$, однако в данной работе общий случай не рассматривается, поскольку наиболее распространенные криптографические алгоритмы основываются на эллиптических кривых вида $E_{a,b}(F_p)$.

Операция сложения точек эллиптической кривой задается следующим образом. Чтобы сложить точки P и Q, необходимо провести через них прямую, которая в общем случае будет проходить еще через одну точку эллиптической кривой. Эту третью точку необходимо симметрично отразить относительно оси абсцисс, полученный результат и будет представлять собой сумму $P+Q$.

Зная координаты двух исходных точек $P=(x_1, y_1)$ и $Q=(x_2, y_2)$, достаточно легко вывести формулы для нахождения координат третьей точки $C=(x_3, y_3)=P+Q$. При этом необходимо учесть три случая.

Первый случай. Складываются две одинаковые точки $P=(x_1, y_1)$ и $P=(x_1, y_1)$. При выводе координат результирующей точки необходимо воспользоваться уравнением касательной к эллиптической кривой. Формулы для нахождения координат точки $C=(x_3, y_3)=P+P$ имеют вид

$$\begin{cases} x_3 = \left(\dfrac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \\ y_3 = \left(\dfrac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \end{cases} \quad (1)$$

Второй случай. Складываются две разные точки $P=(x_1, y_1)$ и $Q=(x_2, y_2)$, причем $x_1 \neq x_2$. При выводе координат результирующей точки необходимо воспользоваться

уравнением секущей к эллиптической кривой. Формулы для нахождения координат точки $C=(x_3, y_3)=P+Q$ имеют вид

$$\begin{cases} x_3=\left(\dfrac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2, \\ y_3=\left(\dfrac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1. \end{cases} \quad (2)$$

Третий случай. Складываются две разные точки, $P=(x_1, y_1)$ и $Q=(x_2, y_2)$, причем $x_1=x_2$, $y_1=-y_2$. Такие точки являются взаимно обратными элементами группы $E_{a,b}(F_p)$, то есть $Q=-P$, поэтому их сумма дает нейтральный элемент группы – бесконечно удаленную точку 0.

2.2 Подсчет числа точек эллиптической кривой

Для построения криптографического алгоритма на базе эллиптической кривой $E_{a,b}(F_p)$ необходимо знать порядок группы точек данной эллиптической кривой $\left|E_{a,b}(F_p)\right|$. Границы, в которых находится данное значение, определяются теоремой Хассе.

Теорема Хассе. $\left|\left|E_{a,b}(F_p)\right|-(p+1)\right| \le 2\sqrt{p}$.

Однако при больших значениях p множество возможных значений $\left|E_{a,b}(F_p)\right|$ также может быть достаточно велико.

Наивный алгоритм подсчета числа точек эллиптической кривой достаточно очевиден. Чтобы найти все точки эллиптической кривой, можно использовать полный перебор, подставляя все возможные значения элементов из F_p в качестве x в уравнение эллиптической кривой и определяя, можно ли извлечь квадрат из полученного значения. При положительном исходе в группу $E_{a,b}(F_p)$ необходимо добавить две точки вида $\left(x; \pm\sqrt{y^2}(mod\ p)\right)$ или одну точку, если $y^2(mod\ p)=0$. Кроме того, в группу $E_{a,b}(F_p)$ необходимо включить бесконечно удаленную точку 0.

Очевидно также и то, что такой подсчет целесообразно использовать лишь при малых значениях p.

Более эффективным является алгоритм больших и малых шагов, также называемый алгоритмом «шаг младенца, шаг великана». Данный алгоритм позволяет вычислить порядок любой точки $P \in E_{a,b}(F_p)$ и обладает сложностью $4\sqrt[4]{p}$. Если точка P является образующим группы $E_{a,b}(F_p)$, то алгоритм больших и малых шагов вычисляет порядок данной группы. В противном случае он вычисляет порядок некоторой подгруппы группы $E_{a,b}(F_p)$. Поэтому для вычисления порядка группы $E_{a,b}(F_p)$ может понадобиться несколько запусков алгоритма больших и малых шагов для случайных точек эллиптической кривой.

В основе алгоритма больших и малых шагов лежат две теоремы. Пусть $\left|E_{a,b}(F_p)\right|=N$ и $P \in E_{a,b}(F_p)$ – произвольная точка эллиптической кривой. Тогда по теореме Лагранжа $NP=0$. В свою очередь, теорема Хассе указывает, что множество допустимых значений N удовлетворяет неравенству $p+1-2\sqrt{p} \le N \le p+1+2\sqrt{p}$.

Алгоритм больших и малых шагов.

Вход: эллиптическая кривая $E_{a,b}(F_p)$, точка $P \in E_{a,b}(F_p)$.

Выход: $M=O(P)$ или $N=\left|E_{a,b}(F_p)\right|$.

1. Вычисляем $Q \leftarrow (p+1)P$.

2. Выбираем целое $m>\sqrt[4]{p}$. Вычисляем и запоминаем точки jP для $j=\overline{0,m}$.

3. Вычисляем точки $Q+k(2mP)$ для $k=-m,-(m-1),\dots,m$ до тех пор, пока очередное значение $Q+k(2mP)$ не совпадет с некоторой точкой jP (или $-jP$), после чего присваиваем $l \leftarrow -j$ (или $l \leftarrow j$).

4. Полагаем $M \leftarrow p+1+2mk+l$.

5. Выполняем факторизацию M, полагая, что $p_1, p_2, \dots, p_r$ – это различные простые множители числа M.

6. Вычисляем $\left(\frac{M}{p_i}\right)P$ для $i=\overline{1,r}$. Если $\left(\frac{M}{p_i}\right)P=0$ для некоторого значения i, заменяем значение M значением $\frac{M}{p_i}$ и переходим в шагу 5. Если $\left(\frac{M}{p_i}\right)P \neq 0$ для всех $i=\overline{1,r}$, то $O(P)=M$.

7. Для нахождения $\left|E_{a,b}(F_p)\right|$ повторяем шаги 1–6 для случайно выбранных в $E_{a,b}(F_p)$ точек, до тех пор пока наименьшее общее кратное порядков этих точек не будет делить только одно целое N, удовлетворяющее неравенству $p+1-2\sqrt{p} \le N \le p+1+2\sqrt{p}$. Тогда $\left|E_{a,b}(F_p)\right|=N$.

При больших значениях p подсчет числа точек эллиптической кривой может быть произведен с помощью алгоритма Шуфа.

2.3 Теоретико-числовые алгоритмы для реализации криптографических преобразований

2.3.1 Нахождение обратного элемента по модулю простого числа

Формулы (1) и (2) используют операцию деления, под которой в арифметике остатков подразумевается умножение на обратное по модулю значение. Для нахождения обратного значения по модулю натурального числа применяется расширенный алгоритм Евклида.

Вход: целые числа $a \ge b>0$.

Выход: $d = НОД(a, b)$ и целые x, y, такие, что $ax + by = d$.

1. Полагаем $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.

2. Пока $b > 0$, выполнять следующее:

2.1. $q \leftarrow \left[\frac{a}{b}\right]$, $r \leftarrow a - qb$, $x \leftarrow x_2 - q x_1$, $y \leftarrow y_2 - q y_1$;

2.2. $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$.

3. $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$ и возврат (d, x, y).

Чтобы найти $a^{-1} \bmod n$, необходимо подать на вход алгоритма Евклида пару n a, и если $НОД(a, n) = 1$, вернуть в качестве a^{-1} значение y_2.

Альтернативный способ вычисления $a^{-1} \bmod n$ основан на теореме Эйлера, которая может быть сформулирована следующим образом.

Теорема Эйлера. Пусть натуральное число $a \in Z_n$. Если $НОД(a, n) = 1$, то верно следующее сравнение $a^{\varphi(n)} \equiv 1 (mod\ n)$.

Тогда $a^{-1} \equiv a^{\varphi(n)-1} (mod\ n)$.

2.3.2 Возведение в степень по модулю

Криптографические алгоритмы, основывающиеся на математическом аппарате эллиптических кривых, при их использовании на практике оперируют числами большой битовой длины (или просто большими числами), когда речь идет о сотнях и тысячах бит. Для некоторых операцией над такими числами созданы специальные алгоритмы. В первую очередь, необходимо иметь алгоритм, который позволит осуществлять быстрое возведение в степень по модулю. Данный алгоритм представлен ниже.

Алгоритм возведения в степень по модулю.

Вход: $a, k \in Z_n$, $k = \sum_{i=0}^{t} k_i \cdot 2^i$.

Выход: $a^k \bmod n$.

1. $b \leftarrow 1$. Если $k = 0$, то переход к шагу 5.

2. $A \leftarrow a$.

3. Если $k_0 = 1$, то $b \leftarrow a$.

4. Для $i = \overline{1, t}$ выполняем следующее:

4.1. $A \leftarrow A^2 \bmod n$.

4.2. Если $k_i = 1$, то $b \leftarrow (A \cdot b) \bmod n$.

5. Возврат b.

Сложение точек эллиптической кривой осуществляется по аналогичному алгоритму. Если для данной точки $P \in E_{a,b}(F_p)$ необходимо вычислить точку $Q = kP$, то искомая точка

представляется в виде $\frac{k}{2}(2P)$ или $P+\frac{k-1}{2}(2P)$ в зависимости от четности числа k. Далее происходит удвоение точки P по формулам (1), после чего процесс повторяется, пока не будет вычислена искомая точка.

Известны и более быстрые алгоритмы вычисления кратной точки, однако и приведенный алгоритм является достаточно эффективным для его применения на практике.

2.3.3 Тесты целых чисел на простоту

Еще одним важным аспектом эллиптической криптографии является использование простых чисел.

Наиболее развитые вероятностные алгоритмы проверки чисел на простоту основаны на малой теореме Ферма, которая представляет собой следствие из теоремы Эйлера.

Малая теорема Ферма. Пусть p — простое число, $a \neq 0$ и $a \in Z_p$. Тогда верно сравнение $a^{p-1} \equiv 1 (mod\ p)$.

Соотношение, приведенное в теореме, используется в тесте, проверяющем, является ли заданное число составным. Этот тест называют тестом Ферма.

Тест Ферма.

Вход: нечетное число n.

Выход: ответ на вопрос «является ли n простым».

1. Для $i=\overline{1,t}$ выполняем следующее:

    1.1. Выбираем случайное целое число $a \in [2; n-1]$.

    1.2. Вычисляем $r = a^{n-1} mod\ n$ с помощью алгоритма возведения в степень по модулю.

    1.3. Если $r \neq 1$, то возврат «n — составное».

Тест Ферма по основанию a определяет простоту n с вероятностью $\frac{1}{2}$, после t итераций вероятность ошибки составляет $\frac{1}{2^t}$.

3 ЗАДАНИЕ

1) написать программную реализацию инструмента, позволяющего строить и исследовать группы точек эллиптических кривых $E_{a,b}(F_p)$;
2) построить и исследовать группу точек эллиптической кривой $E_{a,b}(F_p)$, $2^{10} \leq \left|E_{a,b}(F_p)\right| \leq 2^{512}$;
3) подготовить отчет о выполнении работы.

Инструмент для построения и исследования групп точек эллиптических кривых должен обладать следующей функциональностью:

1) принимать на вход значения p, a и b, определяющие эллиптическую кривую, и строить и отображать соответствующую группу точек (полностью или частично) с вычислением ее порядка;
2) принимать на вход точку эллиптической кривой $P=(x_P, y_P)$ и осуществлять вычисление точки заданной кратности;
3) находить подгруппы группы $E_{a,b}(F_p)$ простого порядка.

Отчет должен содержать следующие составные части:

1) раздел с заданием;
2) раздел с описанием особенностей программной реализации;
3) раздел с исследованием построенной эллиптической кривой и объяснением полученных результатов;
4) раздел с выводами о проделанной работе.