УДК 004.056.55

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И МЕТОДЫ ИХ ГЕНЕРАЦИИ

Разумов П. В. , Бачило А. О.,
Черкесова Л. В. , Сафарьян О. А.
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
therazumov@gmail.com
a-bachilo@mail.ru
chia2002@inbox.ru
safari_2006@mail.ru

Проведено комплексное исследование эллиптических кривых, представлены их описание и характеристика. Выявлены характеристики, обеспечивающие свойства, при которых эллиптическая кривая является наиболее стойкой в криптосистемах. Проведено достаточное количество экспериментов, не имеющих аналогов в мировой практике, позволивших сделать вывод, что метод комплексного умножения будет более быстрым алгоритмом на практике, это даст возможность разработчикам криптоалгоритмов с открытым ключом использовать данный алгоритм в реальных условиях.

Ключевые слова: эллиптическая кривая, криптосистема, комплексное умножение, аддитивная группа, эндоморфизм кольца, дискретный логарифм, скрученные эллиптические кривые.

UDC 004.056.55

ELIPTIC CURVES AND METHODS OF THEIR GENERATION

Razumov P. V., Bachilo A. O.,
Cherkesova L. V., Safaryan O. A.
Don State Technical University, Rostov-on-Don, Russian Federation
therazumov@gmail.com
a-bachilo@mail.ru
chia2002@inbox.ru
safari_2006@mail.ru

The article is devoted to a complex study of elliptic curves, their description and characteristics. The characteristics providing the properties under which the elliptic curve is the most stable in cryptosystems are revealed. A sufficient number of experiments have been carried out, as a result of which it follows that the method of complex multiplication will be a faster algorithm in practice, which would allow developers of public-key cryptalgorithms to use this algorithm in real conditions.

Key words: elliptic curve, cryptosystem, complex multiplication, additive group, endomorphism of a ring, discrete logarithm, twisted elliptic curves.

Введение. В связи с повсеместным распространением информационных систем в наши дни остро встает вопрос защищённости хранимых и передаваемых данных. С одной стороны, наблюдается потребность субъектов информационных систем в надёжном механизме аутентичности передаваемых данных. С другой — современные криптографические протоколы, обладая высоким уровнем криптографической стойкости, позволяют субъектам систем передачи данных обладать абсолютной уверенностью в надёжности коммуникационных систем [1].

Вследствие этого за последние годы широкое применение получили различные информационные системы, использующие средства асимметричной криптографии, работа которых основана на использовании открытого ключа шифрования. Согласно научным исследованиям учёных, среди криптосистем, использующих открытый ключ, наиболее стойкими к атакам различного рода являются криптосистемы, основанные на эллиптических кривых (ЭК).

Результаты данной работы основываются на исследованиях таких учёных, как Нил Коблиц, Рене Чуф, Джозеф Сильверман, Артур Аткин, Скотт Ванстоун, Альфред Менезес, Тацуаки Окамото

[2]. Некоторые положения применительно к методикам генерации криптографически стойких эллиптических кривых получили развитие в ходе написания данной работы.

Использование эллиптических кривых в криптосистемах предложили американские ученые Нил Коблиц и Виктор Миллер в 1985 г. [3–5].

Необходимостью разработки методов генерации криптографически стойкой эллиптически кривой, применяемой в реальных криптосистемах, является проблема выбора криптографически стойкой эллиптической кривой для асимметричной криптосистемы, которая, в первую очередь, обусловлена трудоемкостью вычислений и сложной реализацией существующих алгоритмов.

Постановка задачи. В ходе исследования выявлены два наиболее перспективных подхода к реализации методов генерации криптографически стойкой эллиптической кривой. Обсуждаемыми в работе алгоритмами являются методика «случайного выбора» эллиптической кривой и подход, основывающийся на применении метода комплексного умножения. Использование данных алгоритмов генерации способствует повышению криптостойкости системы в целом.

В данной работе приведено описание эллиптических кривых, дана их общая характеристика, а также рассмотрены алгоритмы генерации криптографически стойких эллиптических кривых. Приведено их подробное описание.

Целью данной работы является исследование алгоритмов генерации криптографически стойких эллиптических кривых для определения оптимального метода их применения в условиях отражения атаки злоумышленника на секретные зашифрованные данные, передаваемые по каналу связи. В процессе достижения поставленной цели авторами были сформулированы и успешно решены следующие задачи: исследование эллиптических кривых с точки зрения обеспечения безопасности и эффективности, выявление методов генерации криптографически стойких эллиптических кривых; анализ существующих подходов к генерации эллиптической кривой, основанный на случайном переборе ЭК как математических объектов, использующих метод комплексного умножения.

Основная часть. Основоположниками криптографии на основе эллиптических кривых стали американские ученые Нил Коблиц и Виктор Миллер, которые в 1985 году независимо друг от друга предложили системы криптографической защиты на основе открытого ключа, которые используют свойства аддитивной группы точек на эллиптической кривой для реализации шифрования. Впоследствии работы этих исследователей легли в основу криптографии на эллиптических кривых [3].

Изучением вопроса генерации криптостойких эллиптических кривых занимались немецкий ученый Геральд Байер и швейцарский исследователь Йоханнес Баучман. В своей совместной работе «Методы генерации эллиптических кривых», опубликованной в 27 августа 2002 года в качестве доклада агентству по развитию информационных технологий Японии. В этой работе они описали подходы к созданию эллиптических кривых над полем p (где p — простое число) и над полем 2^n, а также привели сравнение исследуемых методов [6].

В России данной проблемой занимались В. В. Пылин в диссертации «Алгоритмы и методы генерации эллиптической кривой для асимметричной криптосистемы» (2008 г.) и Н. В. Расторгуева в диссертации «Подбор параметров эллиптических кривых и анализ их криптостойкости для использования в асимметричных криптосистемах» (2014 г.) [7, 8].

Применение эллиптических кривых в криптографии. Безопасность криптосистем на эллиптических кривых определяется количеством точек $E(F_p)$. Таким образом, чтобы решить, подходит ли группа рациональных точек для использования в криптографии, необходимо знать порядок ее группы.

Первый подход, называемый случайным подходом, выбирает случайную кривую E. Порядок группы $E(F_p)$ определяется с использованием алгоритмов подсчета точек. На основании подсчета количества точек можем определить, является ли данная группа подходящей для использования в криптографии. Если окажется, что найденная эллиптическая кривая не удовлетворяет безопасности криптосистемы, выбирается другая эллиптическая кривая [2].

Второй метод использует теорию комплексного умножения (CM-метод — complex multiplication method). Рассматриваемый метод имеет достаточно большое отличие от предыдущего. В данном методе в первую очередь выполняется поиск подходящих точек группы. Это может быть осуществлено без знания соответствующих эллиптических кривых по заданным входным данным. После того как множество точек найдено, эллиптическая кривая определяется с помощью формул комплексного умножения [2].

Исследование криптографически стойких ЭК над полем F_p. Пусть $q = p$ является простым числом, где $p \geq 5$. Эллиптической кривой над полем F_p является пара $E = (a,b) \in F_p^2$, где $4a^3 + 27b^2 \neq 0$. Точка на кривой E является решением $(x, y) \in F_p^2$ таким, что $y^2 = x^3 + ax + b$ или точка на бесконечности O, которая действует как единичный элемент. Множество точек E над полем F_p обозначается $E(F_p)$. Приведенная структура называется группой рациональных точек E над полем F_p [1].

Эллиптическая кривая является криптографически стойкой, если она удовлетворяет условиям безопасности и эффективности.

Сначала рассмотрим стойкость кривой с точки зрения безопасности. Безопасность криптосистемы на эллиптических кривых основана на сложности решения проблемы дискретного логарифма в $E(F_p)$. На данный момент известно несколько алгоритмов решения дискретных логарифмов. Для того чтобы сделать их разрешение невозможным, требуется, чтобы эллиптическая кривая E удовлетворяла следующим условиям.

1) $|E(F_p^m)| = k \times r, r \geq 2^{160}$ - простое, $k > 0$ — целое;

2) простые числа r и p различны;

3) порядок p в мультипликативной группе F_p^* из F_r не менее B, где $B \geq 20$.

Первое условие исключает применение общих алгоритмов дискретного логарифма. Второе условие делает невозможной аномальную атаку. И, наконец, последнее условие исключает атаки на закрытые ключи, такие как известные атаки Менезеса, Окамото, Ванстоуна, а также атаки Фрея и Рюка [6].

Далее рассмотрим криптографическую стойкость криптосистем на эллиптических кривых с точки зрения эффективности. Предположим, что эллиптическая кривая E, заданная над конечным полем F_p, удовлетворяет условиям безопасности. Если эта кривая используется в криптографической системе, тогда эффективность этой системы зависит от эффективности арифметических операций в конечном поле F_p. Поэтому p должно быть малым, насколько это возможно. Это следует из теоремы Хассе:

$$(\sqrt{|E(F_p)|} - 1)^2 \leq p \leq (\sqrt{|E(F_p)|} + 1)^2 \quad (1)$$

Следовательно, $|E(F_p)|$ также необходимо быть небольшим.

Рассмотрим первое условие безопасности:

$$|E(F_p^m)| = k \times r \quad (2)$$

где $r \geq 2^{160}$ – простое, $k > 0$ – целое (кофактор).

Безопасность криптосистемы, в которой используется $E(F_p)$, основана на сложности решения проблемы дискретного логарифма в подгруппе порядка r в группе точек эллиптической кривой $E(F_p)$. Таким образом, k должно быть малым. Далее мы улучшаем первое условие.

$|E(F_p^m)| = k \times r$, где $r \geq 2^{160}$ – простое, $k > 0$ – целое.

Третье условие подразумевает, что эндоморфизм кольца $End(E(F_p))$ ЭК над алгебраическим замыканием F_p является мнимым квадратичным порядком.

Подводя итоги, нужно сказать, что эллиптическая кривая $E(F_p)$ является криптографически стойкой, если она удовлетворяет следующим условиям:

1) $|E(F_p^m)| = k \times r, где \geq$, где $r \geq 2^{160}$ – простое, $k \leq 4$ – целое;

2) $p \neq r$.

3) $p^s \equiv 1 \bmod r, 1 \leq s \leq 20$.

Методы генерации криптографически стойких эллиптических кривых. Продолжая исследование, рассмотрим два метода нахождения криптографически стойкой эллиптической кривой. Для этого должна быть решена следующая задача: пусть r_0 и k_0 – положительные целые числа, где $r \geq 2^{160}$, $k \leq 4$. Необходимо найти эллиптические кривые, чьи коэффициенты $k \times r$ такие, что $r \geq r_0$, $k \geq k_0$. Следовательно, целые числа r_0 и k_0 служат границами для r и k для определения эффективности и безопасности [2].

Перед рассмотрением алгоритмов мы опишем алгоритм проверки простого p, называемый $isstrongP(r_0, k_0, p, N)$. На вход алгоритма поступают положительные целые числа r_0 и k_0, где $r \geq 2^{160}$, $k \leq 4$, простое p и целочисленное N.

Данный алгоритм возвращает простое r, если $N = k \times r$ является порядком криптографически стойкой эллиптической кривой E над полем F_p, где $r \geq r_0$, $k \geq k_0$; иначе – выведет 0. Рассмотрим более подробно данный алгоритм.

Алгоритм проверки простого p:

1) //проверяется, принадлежит ли N интервалу Хассе:

2) if $|N - (p+1)| > 2\sqrt{p}$ then

3) return (0);

4) $r \leftarrow 0$; $k \leftarrow 0$; //инициализируем r и k, равными 0;

5) //проверка условия 1:

6) for $i \leftarrow 1$; $i \leq k_0$; $i \leftarrow i+1$ do;

7) if $i \mid N$ and $is\,\mathrm{Pr}ime(N/i, 50) = true$ and $N/i \geq r_0$ then

8) $r \leftarrow N/i$; $k \leftarrow i$; break;

9) if $r = 0$ then

10) return (0);

11) //проверка условия 2:

12) If $p = r$ then

13) return (0);

14) //проверка условия 3:

15) $pr \leftarrow 1 \bmod r$;

16) for $i \leftarrow 1;\ i \le 19;\ i \leftarrow i+1$ do

17) $pr \leftarrow p \times pr \bmod r$;

18) if $pr = 1$ then

19) return (0);

20) return (r).

Алгоритм, основанный на случайном выборе ЭК. Первая задача состоит в том, чтобы найти простое число p. На сегодняшний день не известны атаки на криптосистемы эллиптической кривой, которые используют свойства некоторого поля F_p. Таким образом, выбор простого числа p не является критическим. Однако мы должны рассмотреть граничные условия $r \ge r_0$ и $k \ge k_0$. Переменная b является длиной бита $k_0 \times r_0$. Мы предлагаем выбрать такое p, что $k_0 \times r_0 \le p \le 2b$. Метод $get\,\mathrm{Pr}\,ime(k_0, r_0)$ возвращает такое простое число. Пользователь может выбрать свою собственную реализацию $get\,\mathrm{Pr}\,ime$, например, использовать простые числа в интервале $[k_0 \times r_0, 2b]$ [9].

После того как p известно, далее выполняется следующее: выберем параметры a и b, для которых $4a^3 + 27b^2 \ne 0 \bmod p$, определим порядок группы рациональных точек кривой (a,b) над F_p и, наконец, проверим, криптографически сильная ли эта группа.

В первую очередь выясним, как выбрать a и b. Обычно выбор параметров происходит случайным образом. Основная идея состоит в том, чтобы использовать одностороннее свойство криптографической хеш-функции. Через h обозначим такую хеш-функцию, а L — длину в битах на выходе h. Предполагаем, $L \ge 160$. Чтобы генерировать кривую случайным образом, сначала выбирается битовая строка длиной не менее L. Мы пишем $SEED$ для этой строки (строит из битовой строки новую последовательность). Как только $SEED$ известно, значение $h(SEED)$ используется для вычисления a и b общеизвестным детерминированным алгоритмом. Таким образом, если мы предоставим $SEED$, хеш-функцию h и детерминированный алгоритм вычисления (a,b) из $h(SEED)$, любой субъект может проверить, что a и b фактически вычисляются с использованием $SEED$. Одностороннее свойство h гарантирует, что параметры фактически выбраны случайным образом. В этой работе мы будем писать $getParamaters(p, SEED)$ для любого алгоритма, который возвращает эллиптические кривые E, определенные над F_p в случайном порядке.

Если кривая $E = (a,b)$ выбрана, мы должны определить порядок группы кривой $E(F_p)$. В настоящее время наиболее известным алгоритмом для решения данной задачи является алгоритм SEA. SEA-алгоритм был разработан американскими учеными Чуфом, Элкисом и Аткином. Обозначим $SEA(p,E)$. Обозначим результат $SEA(p,E)$ через N. Если $isStrongP(r_0, k_0, p, N) \ne 0$, то наша задача решена. В противном случае нам нужно вызвать $getParameters(p, SEED)$, $SEA(p,E)$ и $isStrongP(r_0, k_0, p, N)$, пока мы не добьемся успеха.

Алгоритм случайного выбора ЭК

1) $p \leftarrow get\,\mathrm{Pr}\,ime(r_0, k_0)$;

2) while true do

3) $E \leftarrow getParameters(p, SEED)$;

4) $N \leftarrow SEA(p,E)$;

5) $r \leftarrow isStrongP(r_0, k_0, p, N)$;

6) if $r \neq 0$ then

7) return $(p, E, r, N / r)$.

Метод комплексного умножения. Центральным термином в рамках метода комплексного умножения является мнимый квадратичный дискриминант [1]. Обозначим такой дискриминант через Δ. Это отрицательное целое число: $\Delta = 0,1 \bmod 4$.

Через O_Δ мы обозначаем мнимый квадратичный порядок дискриминанта Δ:

$$O_\Delta = Z(\frac{\Delta + \sqrt{\Delta}}{2}) \quad (3)$$

Кроме того, запишем $h(A)$ для O_Δ. Если p — простое число, то оно называется нормой в O_Δ; если существуют целые числа t, y, то:

$$t^2 - \Delta y^2 = 4p \quad (4)$$

Если p является нормой в O_Δ, то эллиптические кривые $E_{1,p}$ и $E_{2,p}$ над полем F_p с кольцом эндоморфизмов O_Δ строятся по следующей схеме, используя комплексное умножение.

$$|E_{1,p}(F_p)| = p + 1 - t, |E_{2,p}(F_p)| = p + 1 + t \quad (5)$$

Пусть $H \in Z[X]$ — минимальный многочлен $j[\frac{\Delta + \sqrt{\Delta}}{2}]$, где j — эллиптическая модулярная функция. Степень H равна $h(\Delta)$. По модулю p многочлен H разбивается на линейные множители. Пусть $H(j_p) \equiv 0 \bmod p$. Предположим, что $\Delta < -4$. Тогда имеем: $j_p \in \{0;1728\}$.

Пусть S_p — квадратичный нестационарный $\bmod p$. Вместе с уравнением:

$$(a_p, b_p) = (3k_p, 2k_p), \quad (6)$$

где $k_p = \frac{j_p}{1728 - j}$.

Мы имеем

$$\{E_{1,p}, E_{2,p}\} = \{(a_p, b_p), (a_p s_p^2, b_p s_p^3)\} \quad (7)$$

Эллиптические кривые $E_{1,p}$ и $E_{2,p}$ называются скрученными эллиптическими кривыми над полем F_p [10]. Для данной конструкции не известно, какая из эллиптических кривых $E_{1,p}$ и $E_{2,p}$ является криптографически стойкой. Однако, выбирая точки на каждой кривой и проверяя, является ли их порядок делителем $p + 1 + t$ или $p + 1 - t$, можно идентифицировать кривые $E_{1,p}$ и $E_{2,p}$. Нам нужно знать представление простого числа p, как в формуле (4). Тогда мы знаем групповые порядки $E_{1,p}(F_p)$ и $E_{2,p}(F_p)$ из формулы (5). Используя эти порядки и алгоритм *isstrongP*, мы можем проверить условия безопасности. Обычно большая часть времени тратится на вычисление полинома H. Причина в том, что коэффициенты H становятся довольно большими даже для дискриминанта с небольшим значением.

Однако в зависимости от значения $\Delta \bmod 24$ можно использовать альтернативные многочлены, коэффициенты которых очень малы по сравнению с H. Работа с этими полиномами значительно ускоряет метод «комплексного умножения» на практике. Битовая сложность метода «комплексного умножения» инвариантна.

Сравнительный анализ методов. В этом разделе сравниваются случайный подход и метод «комплексного умножения», чтобы найти криптографически сильную группу эллиптических кривых над F_p. Будем сравнивать влияние на безопасность и эффективность.

Для начала разберемся с безопасностью. Основным преимуществом случайного подхода является то, что каждая криптографически сильная группа эллиптических кривых над F_p вычисляется с примерно одинаковой вероятностью. Метод комплексного умножения применим только в том случае, если используются небольшие дискриминанты, например, дискриминанты со значениями не более 1000. Тогда сгенерированные кривые являются особыми в случае, если их кольцо эндоморфизмов имеет значение не более чем 1000. Таким образом, не каждая криптографически сильная группа эллиптических кривых может выводиться методом комплексного умножения.

Теперь обсудим эффективность. Разберем случай при $k_0 = 1$, то есть мы ищем группу эллиптических кривых простого порядка. Запишем b для длины бит r_0. Ранее было заявлено, что битовая сложность случайного подхода зависит только от b. Однако битовая сложность комплексного умножения зависит от значения используемого мнимого квадратичного дискриминанта. Далее будет рассмотрено, для какого значения оба подхода имеют одно и то же время выполнения на практике для некоторого заданного фиксированного b. Это число названо значением пересечения, и обозначается оно $h_c(b)$.

Для определения $h_c(b)$ сначала было измерено время выполнения случайного подхода $P(r_0, k_0)$. Отмечено, что здесь реализована стратегия раннего прерывания и использование скрученной кривой, которая описана выше.

Все тесты были выполнены на различных видах компьютеров и средств вычислительной техники с использованием программного обеспечения свободного доступа. Результаты исследований приведены в табл. 1.

Таблица 1

Среднее время выполнения случайного подхода для получения криптографически сильной эллиптической группы $E(F_p)$ простого порядка

B	160	170	180	190	200	210
Время выполнения (мин.)	3,63	4.87	7.97	10.3	13.1	16.7
$h_c(b)$	50	820	960	1040	1090	1200

В табл. b означает длину бита p. Было проведено 100 вычислительных экспериментов, на основании которых были определены среднестатистические значения.

На основании проведённых экспериментов было выявлено, что метод комплексного умножения будет более быстрым алгоритмом на практике, если $h(\Delta) < h_c(b)$ при дискриминанте Δ, используемой в методе комплексного умножения. По данным табл. 1 можно сделать вывод, что значение пересечения довольно велико. Таким образом, даже если учесть дополнительное требование GISA (немецкое агентство информационной безопасности) о том, что значение фундаментального дискриминанта, соответствующего Δ, составляет не менее 200, метод комплексного умножения предпочтительнее метода случайного выбора ЭК по длине бит ключей, использующихся в криптосистемах.

Заключение. Применение эллиптических кривых является одной из основных и наиболее надежных технологий построения открытых ключей в асимметричной криптографии. Основным критерием стойкости таких криптографических систем является проблема сложности решения дискретного логарифма.

Для противостояния имеющимся алгоритмам решения данной задачи характеристики эллиптической кривой должны удовлетворять некоторым определенным условиям. Соответственно, эллиптические кривые, удовлетворяющие таким условиям, являются криптографически сильными.

Важной задачей эллиптической криптографии является генерация криптографически сильных эллиптических кривых над конечным полем простого порядка. Существует несколько способов генерации, среди которых наиболее распространенными и надежными являются случайный подход к генерации эллиптической кривой и подход, использующий метод комплексного умножения. После генерации методами расчета числа точек находится порядок кривой и проверяется выполнение известных условий. К сожалению, алгоритмы расчета числа точек эллиптической кривой над большими полями слишком медленны.

Если кольцо эндоморфизмов эллиптической кривой имеет малое число классов, то метод комплексного умножения предпочтительнее метода случайной генерации. Но при больших значениях дискриминанта ($D > 200$) существующие методы комплексного умножения становятся непрактичными из-за низкой скорости. Поэтому наиболее актуальной является разработка быстрых алгоритмов генерации эллиптических кривых методом комплексного умножения.

Библиографический список

1. H. Baier. Efficient Algorithms for Generating Elliptic Curves over Finite Fields Suitable for Use in Cryptography. PhD thesis, Darmstadt University of Technology,2002.

2. Harald Baier and Johannes Buchmann. Generation Methods of Elliptic Curves. An evaluation report for theInformation-technology Promotion Agency, Japan, 2002.

3. Koblitz N. Elliptic curve cryptosistems // Mathematics of Computation. 48 (1987). P. 203–204

4. Miller V. Uses of elliptic curves in cryptography // Advances in Cryptology: Proceedings of Crypto’85. Lecture Notes in Computer Science. 218 (1986). Springer-Verlag. P. 417–426.

5. NIST Recommended Elliptic Curves for Federal Government Use. National Instituteof Standards and Technology, 1999.

6. H. Baier. How to find Elliptic Curve Groups of Prime Order. Technical Report,Darmstadt University of Technology, 2002. Technical Report TI-6/02.

7. Ишмухаметов, Ш. Т. Математические основы защиты информации: электронное учебное пособие для студентов института вычислительной математики и информационных технологий / Ш. Т. Ишмухаметов, Р. Г. Рубцова. — Казань : Казанский федеральный университет, 2012. — 138 с.

8. Пылин, В. В. Алгоритмы и методы генерации эллиптической кривой для асимметричной криптосистемы : автореф. дис. … канд. техн. наук. — Санкт-Петербург, 2008. — 147 с.

9. Schoof R. Ellitic curves over finite fields and computation of square roots. Vol. 44. No. 170. P. 283–494. Apr. 1985.

10. Schoof R. Ellitic curves over finite fields and computation of square roots. Vol. 44. No. 170. P. 283–494. Apr. 1985.