УДК 512.542

О методах исследования групп точек эллиптических кривых в асимметричной криптографии

Н.В. Савельева
Учреждение образования «Витебский государственный университет им. П.М. Машерова»

В настоящей статье разработан методический подход к изучению актуального и перспективного направления современной асимметричной криптографии – криптографии на основе эллиптических кривых. Исследование носит учебно-методический характер; в нем кратко изложены теоретические аспекты, на которые преподавателю следует сделать акцент при изложении материала, и указаны некоторые виды задач, которые могут быть предложены студентам математических специальностей в рамках лабораторных работ для решения средствами системы вычислительной алгебры GAP. В частности, подробно разобран способ решения типовой учебной задачи в системе GAP. Описанный в данной статье практический способ учебного исследования группы точек эллиптических кривых позволит сформировать у обучаемых знания, умения и навыки, которые позволят им конструировать реальные алгоритмы криптосистем на основе эллиптических кривых и анализировать свойства групп точек в среде GAP.

Ключевые слова: *эллиптическая кривая, проблема выбора эллиптической кривой, группа точек эллиптической кривой, сложение точек эллиптической кривой, проблема дискретного логарифма эллиптической кривой.*

On Investigation Methods of Groups of Points on Elliptic Curves in Asymmetric Cryptography

N.V. Savelyeva
Educational establishment «Vitebsk State University named after P.M. Masherov»

In this paper a methodical approach to the study of current and future trends in modern asymmetric cryptography – cryptography based on elliptic curves – is developed. The article is educational and methodological in nature, it outlines the theoretical aspects which teachers should emphasize when presenting the material. The article identifies some problems that may be offered to students specializing in mathematics while doinge laboratory work for the solution by means of computer algebra system GAP. In particular, the method for solving a standard academic task using GAP is explained in details. The described in this paper practical method of educational research of groups of points on elliptic curves will form knowledge and skills that will enable the trainees to design the actual algorithms for cryptosystems based on elliptic curves and to analyze the properties of groups of points by means of GAP.

Key words: *an elliptic curve, the problem of choosing an elliptic curve, a group of points on an elliptic curve, the addition of points on an elliptic curve, an elliptic curve discrete logarithm problem.*

Стремительный рост вычислительных возможностей отодвигает на задний план известные и широко используемые ранее алгоритмы шифрования, криптостойкость которых в современных условиях перестала удовлетворять необходимым требованиям. Сегодня интерес исследователей привлекает представление блоков информации в криптографических алгоритмах не только в виде чисел (или элементов конечных полей), но и в виде иных алгебраических объектов большей сложности. При этом одним из весьма подходящих типов таких объектов являются точки эллиптических кривых.

Основная причина того, что теория эллиптических кривых над конечными полями нашла применение в криптографии, состоит в том, что эллиптические кривые над конечными полями предоставляют неисчерпаемый источник конечных абелевых групп, которые удобны для вычислений и обладают богатой структурой.

Следует заметить, что криптосистемы на основе эллиптической кривой (Elliptic Curve Cryptography – ECC) получают все большее распространение, особенно при использовании в устройствах с маломощными процессорами и/или маленькой памятью. Типичными областями применения указанных криптосистем являются электронная и мобильная торговля, смарт-карты и интернет-приложения.

Таким образом, научное исследование теории эллиптических кривых в настоящее время актуально и перспективно.

Вместе с тем, с методической точки зрения представляет интерес разработка эффективных подходов к изучению данного направления криптографии студентами математических специальностей в высших учебных заведениях.

Основная цель настоящей работы – показать, на какие теоретические аспекты преподавателю следует сделать акцент в изложении материала, и указать некоторые виды задач, которые могут

быть предложены студентам в рамках лабораторных работ для решения в среде GAP. При этом в качестве основной литературы студентам можно порекомендовать [1–4].

При изложении материала, на наш взгляд, можно придерживаться приведенной ниже последовательности:

1. Проблема дискретного логарифмирования как основа стойкости криптографических систем.
2. Основные понятия теории эллиптических кривых.
3. Сравнение ECC с другими криптографическими алгоритмами.
4. Проблема выбора эллиптической кривой.
5. Задания к лабораторным работам.

Далее кратко приведем содержательное наполнение по каждому из перечисленных пунктов.

1. Проблема дискретного логарифмирования как основа стойкости криптографических систем. В основе любой криптографической системы лежит сложная математическая задача. Все алгоритмы асимметрической криптографии (т.е. криптографии с открытым ключом), будь то алгоритмы для распределения ключей, шифрования или цифровой подписи, базируются на одной из следующих математических проблем: *проблеме факторизации (разложения на множители) больших чисел* и *проблеме дискретного логарифмирования*. Например, защищенность известного алгоритма RSA обусловлена сложностью факторизации 1024-битовых и бóльших чисел, в то время как защищенность большинства других алгоритмов с открытым ключом – Эльгамаля, DSA и др. – основана на проблеме дискретного логарифмирования.

В настоящее время признаны достаточно безопасными и эффективными три типа криптосистем, которые отличаются лежащей в их основе математической задачей:

1) системы разложения целых чисел на множители (например, RSA);

2) дискретные логарифмические системы (например, DSA);

3) дискретные логарифмические системы эллиптических кривых (криптосистемы эллиптических кривых).

2. Основные понятия теории эллиптических кривых. Пусть K – поле характеристики, отличной от 2, 3, и x^3+ax+b (где $a, b \in K$) – кубический многочлен без кратных корней. Эллиптическая кривая над полем K – это множество точек (x, y), $x, y \in K$, удовлетворяющих уравнению $y^2=x^3+ax+b$, вместе с единственным элементом, обозначаемым O и называемым «точка в бесконечности».

Если поле K является полем действительных чисел, то эллиптическая кривая – это обычная плоская кривая (с добавлением еще одной точки O «в бесконечности»).

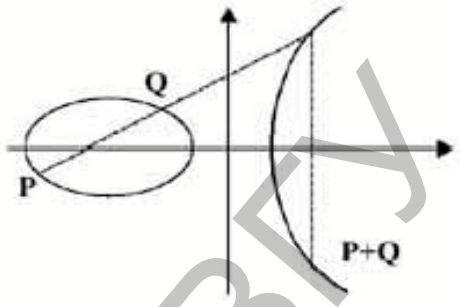

Рис. 1. **Сложение точек на эллиптической кривой.**

Точки эллиптической кривой можно складывать. Сумма двух точек, в свою очередь, тоже лежит на эллиптической кривой (рис. 1).

Математическое свойство, которое делает эллиптические кривые полезными для криптографии, состоит в том, что, если взять две различные точки на кривой, то соединяющая их хорда пересечет кривую в третьей точке (так как мы имеем кубическую кривую). Зеркально отразив эту точку от оси X, мы получим еще одну точку на кривой (так как кривая симметрична относительно оси X). Если мы обозначим две первоначальные точки как P и Q, то получим последнюю – отраженную – точку $P+Q$. Когда третьей точки нет, например, если нужно сложить точку с самой собой, то для этого нужно провести касательную в этой точке. Если касательная направлена вертикально вверх, то считается, что она пересечет кривую в бесконечной точке O, которая расположена в положительном направлении оси Y. Точка O играет роль нуля в этом сложении. Противоположный элемент получится, если отразить точку относительно оси X; если теперь соединить прямой точку и ее противоположную, прямая будет вертикальной, и третьей точкой как раз будет бесконечность: $P+(-P) = O$.

Такое «сложение» удовлетворяет всем известным алгебраическим правилам для целых чисел. Значит, множество всех точек эллиптической кривой является абелевой группой.

Случай, когда эллиптическая кривая рассматривается над конечным полем, представляет для криптографии особый интерес. Заметим, что тогда эллиптической кривой является не линия, а конечное множество отдельных точек,

которые, в свою очередь, образуют конечную абелеву группу.

Проблема дискретного логарифма эллиптической кривой (Elliptic Curve Discrete Logarithm Problem – ECDLP) может быть сформулирована следующим образом:

«Даны "базовая точка" P и расположенная на кривой точка kP (k – целое число); найти значение k».

Отметим, что для эллиптических кривых и базовых точек решение такой задачи весьма затруднительно.

3. Сравнение эллиптических кривых с другими криптографическими алгоритмами. Любая стандартная система, которая базируется на проблеме дискретного логарифма, аналогична системе, основанной на ECDLP. Другими словами, практически любая «современная» криптосистема может быть переформулирована в терминах эллиптических кривых, хотя не для всех схем это дает выигрыш в стойкости. Например, для системы RSA и родственных ей систем, основанных на сложности задачи факторизации, данный переход не позволит усилить схему. В то же время для схем, основанных на сложности задачи логарифмирования в дискретных полях, переход на эллиптические кривые значительно увеличивает их стойкость (табл. 1). Обусловлено это тем, что при надлежащем выборе параметров кривой задача логарифмирования в группе точек кривой существенно сложнее задачи логарифмирования в мультипликативной группе исходного поля.

В табл. 2 и 3 представлены основные соотношения наиболее распространенных криптографических алгоритмов в сравнении с эллиптическими кривыми. Предполагается, что два участника – Алиса и Боб – хотят обмениваться шифрованными сообщениями, используя открытые ключи.

Процесс генерации ключей при использовании эллиптических кривых включает следующие процедуры:

1. Задаются параметры a и b эллиптической кривой.

2. Задаются параметры исходной точки $P(x_p, y_p)$.

3. Выбирается достаточно большое простое число n, например из интервала $2^{150} < n < 2^{160}$, в зависимости от требований к надежности.

4. Генерируется секретный ключ d как число из интервала $[1, 1 – n]$, отвечающее ряду дополнительных требований.

Вычисляется вторая точка эллиптической кривой $Q = (d*P) \ mod \ n$. В качестве открытого ключа берется совокупность $(a, b, x_p, y_p, x_q, y_q)$.

4. Проблема выбора эллиптической кривой. При использовании эллиптических кривых в асимметрической криптографии большое значение имеют выбор самой кривой и вычисление порядка группы, образуемой ее точками.

Таблица 1

Сравнение стойкости криптографических систем

Время на взлом, MIPS-лет	Размер ключа RSA/DSA	Размер ключа ECC	Отношение длин ключей RSA/ECC
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1 024	160	7:1
10^{20}	2 048	210	10:1

Таблица 2

Основные соотношения алгоритмов криптосистемы RSA

№ п/п	Шаг алгоритма	Исходный алгоритм	Случай эллиптических кривых
1.	Определение рабочего модуля n	Алиса заранее выбирает два больших простых числа p и q и вычисляет произведение $n=pq$	
2.	Выработка открытого ключа. Алиса выбирает случайным образом открытый ключ e ($1 < e < n$) и отправляет Бобу пару чисел (n, e)	Число e должно быть взаимно просто с p–1 и q–1	Число e должно быть взаимно просто с p+1 и q+1
3.	Выработка секретного ключа. Алиса вычисляет секретный ключ d	$d = e^{-1} \ mod \ (p–1)(q–1)$	$d = e^{-1} \ mod \ (p+1)(q+1)$

Окончание табл. 2

4.	Боб шифрует сообщение M, получает шифр-текст C и отправляет его Алисе	$C = M^e \bmod n$	$C=e(M, y)$, где y – случайное число; (M, y) – точка эллиптической кривой
5.	Алиса восстанавливает исходное сообщение M, расшифровывая шифр-текст C	$M = C^d \bmod n$	$(M, y) = dC$

Таблица 3

Основные соотношения алгоритмов протокола DH

№ п/п	Шаг алгоритма	Исходный алгоритм	Случай эллиптических кривых
1.	Определение рабочей группы $GF(p)$ (рабочей кривой) базового элемента g (базовой точки). Алиса выбирает и отправляет Бобу…	…большое простое число p и случайное число g: $1 < g < p$	…эллиптическую кривую и случайную точку G на ней
2.	Алиса выбирает случайное число a и вычисляет и отправляет Бобу…	…число $g_a = g^a \bmod p$	…точку $G_a = aG$
3.	Боб выбирает случайное число b и вычисляет и отправляет Алисе…	…число $g_b = g^b \bmod p$	…точку $G_b = bG$
4.	Алиса вычисляет…	...секретное число $k = g_b^a \bmod p$	…секретную точку $K = aG_b$
5.	Боб вычисляет…	...секретное число $k = g_a^b \bmod p$	…секретную точку $K = bG_a$
6.	У Алисы и Боба получается один и тот же секретный элемент, потому что…	$g_b^a \bmod p = (g^b)^a \bmod p = g^{ab} \bmod p\ (g^a)^b \bmod p = g_a^b \bmod p$	$aG_b = a(bG) = (ab)G = b(aG) = bG_a$

Трудность генерации подходящих кривых заключается в том, что при определении системы эллиптической кривой требуются сама кривая и базовая точка (P). Следует обратить внимание на то, что эти элементы не являются тайной и могут быть одинаковыми для всех пользователей системы. Для данной кривой и точки несложно сгенерировать открытые и частные ключи для пользователей (частный ключ – просто случайное целое число k, а открытый ключ – точка kP на кривой). Однако чрезвычайно трудно создать подходящую кривую и точку. Необходимо выбрать подходящую базовую точку P, координаты которой должны иметь достаточно большое значение, чтобы гарантировать трудность взлома ECDLP. Но координаты P должны делиться на количество точек на кривой (точки на кривой вместе с бесконечно удаленной точкой образуют конечную группу). И весьма вероятно, что, найдя число точек на кривой, мы не сможем найти базовую точку.

Для каждой эллиптической кривой число точек в группе конечно, но достаточно велико. Оценка числа M – порядка (числа элементов) группы точек эллиптической кривой – с учетом теоремы Хассе [3, с. 197] такова:

$$q + 1 - 2\sqrt{q} \le M \le q + 1 + 2\sqrt{q},$$

где q – порядок поля, над которым определена кривая. Если в схеме Эль-Гамаля рекомендуется использовать число q порядка 2^{512}, то в случае эллиптической кривой достаточно взять $q > 2^{255}$.

Несмотря на то, что теория эллиптических кривых интенсивно исследуется математиками, реальная безопасность таких систем все еще недостаточно осознана на практике. Главная проблема состоит в том, что истинная сложность ECDLP остается малоисследованной.

5. Задания к лабораторным работам. В качестве заданий к лабораторным работам, например, можно использовать теоретические задания на доказательство каких-либо закономерностей для их проверки средствами вычислительных машин.

Разберем для примера задание а) упражнения 7 (см. с. 200 [3]): доказать, что если $q \equiv 3 \pmod 4$, то число $\boldsymbol{F}_q$-точек на эллиптической кривой $y^2 = x^3 - x$ равно $q+1$.

Заметим, что аналитическое решение данной задачи докажет это утверждение для общего случая, а в системе компьютерной алгебры GAP мы сможем убедиться в его справедливости лишь для заданных q.

Как известно студентам из теории, если удалить нулевой (по сложению) элемент поля $\boldsymbol{F}_q$

(состоящего из q элементов), то останется мультипликативная группа $\boldsymbol{F}_q^*$, которая является циклической и, следовательно, может быть порождена некоторым элементом, скажем, g. Тогда $\boldsymbol{F}_q$ можно записать в виде $\boldsymbol{F}_q = 0 \cup \boldsymbol{F}_q^* = 0 \cup \{g^0, g^1, \ldots, g^{q-1}\}$, где g^0 – единица поля $\boldsymbol{F}_q$ по умножению.

В системе GAP образующий элемент поля $\boldsymbol{F}_q$ обозначается Z(q), где q – порядок поля.

Для решения положим $q = 7$ (тогда количество элементов поля должно равняться 8). Составим и запустим в GAP программу (исходный код которой можно дать студентам) (рис. 2).

Последний цикл **for** выведет на экран все элементы поля в следующем виде:

```
0*Z(7)
Z(7)^0
Z(7)
Z(7)^2
Z(7)^3
Z(7)^4
Z(7)^5
```

```
q:=7;
F:=[];;  # массив будет содержать все элементы конечного поля
eccX:=[];; # X-координаты точек эллиптической кривой
eccY:=[];; # Y-координаты точек эллиптической кривой
F[1]:=0*Z(q);  # 1-ый элемент массива – нулевой (по сложению)
               # элемент конечного поля
for i in [1..q-1] do
    F[i+1]:=Z(q)^(i-1);     # заполнение массива элементами поля
od;

for i in [1..Size(F)] do   # вывод на экран всех элементов поля
    Print(F[i],"\n");
od;
```

Рис. 2.

```
ecc:=function(x,y)
    return y^2-x^3+x; # левая часть уравнения эллиптической кривой
end;;

n:=1;     # Бесконечную точку выводим на экран «вручную»
Print("\n",n,". Бесконечная точка\n");

for i in [1..Size(F)] do          # перебираем все точки группы как
                                  # всевозможные комбинации координат
    d:=0;       # для экономии машинного времени
    for j in [1..Size(F)] do
         # проверяем, принадлежит ли точка заданной кривой
         # (заметим, что 0*Z(q) есть нулевой элемент поля)
         if ecc(F[i],F[j])=0*Z(q) then
              Print(n+1,". ",F[i],", ",F[j],"\n");

              # запоминаем координаты точки кривой
              eccX[n]:=F[i];
              eccY[n]:=F[j];

              n:=n+1; # увеличиваем счетчик точек

              d:=d+1;
              if d=2 then    # известно, что число точек
                             # с одинаковой x-координатой не более 2
              break;         # (экономим машинное время)
              fi;
         fi;
    od;
od;
Print("На заданной эллиптической кривой всего ",n," точек\n");
```

Рис. 3.

Как можно видеть, при использовании GAP мы имеем дело со степенным представлением поля (здесь уместно спросить студентов, какое еще бывает представление поля и как можно перейти от одного представления к другому?).

Очевидно, что не всякая пара элементов из конечного поля $\boldsymbol{F}_q$ будет являться точкой эллиптической кривой. Например, для $q = 7$ из 7*7=49 точек только 8 будут принадлежать эллиптической кривой (уравнение которой задано по условию). В этом можно убедиться, составив программу, приведенную на рис. 3.

Далее студентам целесообразно предложить задание написать функции сложения и удвоения эллиптических точек по их координатам, опираясь на пункты 3–5 [3, с. 190] и используя формулы (4) и (5) [3, с. 191].

С помощью функций сложения и удвоения эллиптических точек из равенства $n\boldsymbol{P}_1 = \boldsymbol{P}_2$ можно найти значение n, что решит проблему ECDLP. Заметим, что проблему ECDLP нам удалось решить лишь для малого значения q!.

Не исключено, что при умножении точки $\boldsymbol{P}_1$ саму на себя несколько раз, на некотором (например, m-ом) шаге точка $m\boldsymbol{P}_1$ может обратиться в единичный элемент мультипликативной группы поля, и тогда элемент $\boldsymbol{P}_1$ мультипликативной группы точек эллиптической кривой будет иметь конечный порядок, равный числу m.

Возвращаясь к рассматриваемой задаче (задание а) упражнения 7 [3, с. 200]), значения q в программе можно варьировать, учитывая условие задачи $q \equiv 3 \ (mod\ 4)$ и требования $q = p^n$ ($q \neq 2$, $q \neq 3$), необходимые для применения формул (4) и (5) [3, с. 191]. При таком выборе значений q мы будем всегда убеждаться в том, что число $\boldsymbol{F}_q$-точек на эллиптической кривой $y^2=x^3-x$ равно $q+1$.

Таким образом, преподавателем дается исходный код GAP-программы, формирующей и выводящей на экран все элементы конечного поля, а студентам предоставляются для решения в системе GAP следующие задачи:

- составление функций сложения и удвоения точек по их координатам;
- нахождение порядка точки эллиптической кривой как элемента мультипликативной группы конечного поля;
- нахождение всех точек на эллиптической кривой, имеющих конечный порядок;
- решение проблемы дискретного логарифма в группе точек для малых порядков поля.

Заключение. Безопасность применения на практике криптосистем на основе эллиптических кривых пока недостаточно осознана. По этой причине такие криптосистемы сегодня получают свое распространение, скорее, как альтернатива, нежели замена системам на основе RSA. Распространение криптосистем на основе эллиптических кривых обусловлено, прежде всего, тем, что системы на основе ECDLP имеют некоторые преимущества, особенно при использовании в устройствах с маломощными процессорами и маленькой памятью.

Однако развитие теории эллиптических кривых в рамках нужд криптографии представляет огромный не только научный, но и учебный интерес. Знания, умения и навыки, сформированные у студентов в процессе изучения рассмотренной в данной статье темы, могут быть использованы студентами при конструировании реальных алгоритмов криптосистем на эллиптических кривых, анализе свойств групп точек в среде GAP. Описанный в настоящем исследовании практический подход будет особенно эффективен, поскольку позволит студентам увидеть, как фундаментальные теоретические результаты теории групп находят свое отражение на практике.

ЛИТЕРАТУРА

1. Болотов, А.А. Алгоритмические основы эллиптической криптографии: учеб. пособие / А.А. Болотов [и др.]. – М.: МЭИ, 2004. – 527 с.
2. Болотов, А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А.А. Болотов [и др.]. – М.: КомКнига, 2006. – 328 с.
3. Коблиц, Н.Н. Курс теории чисел и криптографии / Н.Н. Коблиц. – М.: ТВП, 2001. – 269 с.
4. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C / Б. Шнайер. – М.: Триумф, 2002. – 610 с.

Поступила в редакцию 18.11.2010. Принята в печать 26.02.2011
Адрес для корреспонденции: 210032, г. Витебск, пр-т Победы, д. 27, кв. 121, e-mail: natallia.savelyeva@gmail.com – Н.В. Савельева