Лекция 4 (2 семестр) БСит

ВСТУПЛЕНИЕ

Асимметричными криптосистемами, основанными на эллиптических кривых над конечными полями, занимается раздел криптографии, называемый ***эллиптической криптографией.*** В англоязычной литературе этому термину соответствует ***Elliptic Curve Criptography*** *(аббревиатура* ***ECC****).*

Большинство продуктов и стандартов криптографии с открытым ключом основано на алгоритме RSA. Однако в связи с развитием методов криптоанализа и вычислительной техники длина ключа, обеспечивающая надежную защиту RSA, в последние годы резко увеличилась, что обусловило дополнительную нагрузку на системы в приложениях, использующих RSA. Это породило множество проблем, особенно для узлов связи, специализирующихся на электронной коммерции, где требуется защита больших транзакций. В связи с этим и появился конкурент RSA — эллиптическая криптография. Привлекательность подхода на основе эллиптических кривых по сравнению с RSA заключается в том, что с использованием эллиптических кривых обеспечивается эквивалентная защита при меньшей длине ключа.

Хотя эллиптические кривые исследовались уже более сотни лет, интерес к ним проявляли исключительно узкие специалисты в области теории чисел. Так было примерно до 1985 г., пока одновременно и независимо Нил Коблиц (N. Coblitz) и Виктор Миллер (V. Miller) не предложили использовать эллиптические кривые для построения криптосистем с открытым ключом.

После этого интерес к эллиптическим кривым стал расти в геометрической прогрессии. Кроме того, интересный пример уже не из криптографии: на основе этих кривых английский математик Эндрю Уайлс построил свое доказательство Великой теоремы Ферма *(по этой теореме утверждается, что не существует натуральных решений уравнения* $x^n + y^n = z^n$ *для* $n > 2$*)*.

Среди литературы на русском языке по эллиптическим кривым отметим, книгу Н. Коблица «Курс теории чисел и криптографии» и две книги А. Болотова, С. Гашкова, А. Фролова и А. Часовских под названием «Элементарное введение в эллиптическую криптографию».

§18. ГРУППЫ И ПОЛЯ (ПОВТОРЕНИЕ ИЗ ТЕОРИИ ЧИСЕЛ)

Группа – это множество G элементов любой природы, для которых определена бинарная алгебраическая операция o, называемая ***групповой***, удовлетворяющая условиям:

1^0 для любой пары элементов $a,b\in G$ в группе существует элемент $c=a\circ b$ (замкнутость операции);

2^0 если $a,b,c\in G$, то $(a\circ b)\circ c=a\circ(b\circ c)$ (ассоциативность);

3^0 существует ***нейтральный элемент*** e, для которого $a\circ e=e\circ a=a$, где $a\in G$;

4^0 для $\forall a\in G$ существует ***обратный элемент*** a', для которого $a\circ a'=a'\circ a=e$.

Если $a\circ b=b\circ a$, то группа называется ***коммутативной*** или ***абелевой***.

Группа, в которой групповой операцией есть умножение, называется ***мультипликативной*** (в этом случае обратный элемент a^{-1}, нейтральный элемент 1). Если же групповая операция – сложение, то группу относят к ***аддитивным*** (обратный элемент $-a$, нейтральный элемент 0).

Если группа имеет конечное число элементов, то ее называют ***конечной***, а число ее элементов называют ***порядком группы*** и обозначают $|G|$ или $\#G$.

Примеры конечных групп:

- кольцо вычетов по модулю $Z_n=\{0,1,2,...n-1\}$ с групповой операцией $c\equiv a+b(\mathrm{mod}\,n)$ – аддитивная группа;
- если $p-$простое, то множество $Z_p{}^*=Z_p/\{0\}=\{1,2,...,p-1\}$ с групповой операцией $c\equiv ab(\mathrm{mod}\,p)$ будет мультипликативной группой $Z_p{}^*$ кольца вычетов Z_p (только при простом p для всех ненулевых элементов существует обратный).

Группа G называется ***циклической***, если в группе существует такой элемент $g\in G$, что для любого элемента a найдется число $i\geq 0$, при котором $a=g^i$. Сам элемент g называют ***порождающим элементом группы*** (генератором) и говорят, что группа порождена элементом g. Это записывают $G=\langle g\rangle$. Так, примерами циклических групп будут аддитивная группа $Z_n=\{0,1,2,...,n-1\}=\langle 1\rangle$, мультипликативная группа $Z_p{}^*=\langle p-1\rangle$.

Поле – это множество F элементов любой природы, для которых определены две бинарные операции сложения и умножения, удовлетворяющие условиям:

1^0 если $a,b,c\in F$, то $(a+b)+c=a+(b+c)$;

2^0 существует элемент 0, для которого $a+0=0+a=a, a\in F$;

3^0 существует элемент $-a$, т. е. $a+(-a)=0,\quad a\in F$;

4^0 $a+b=b+a$;

5^0 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$;

6^0 существует элемент 1, для которого $1\cdot a=a\cdot 1=a$, $a\in F$;

7^0 существует обратный элемент a^{-1} для $\forall a\in F$, т.е. $a^{-1}\cdot a=a\cdot a^{-1}=1$;

8^0 $a\cdot b=b\cdot a$;

9^0 $a\cdot(b+c)=a\cdot b+a\cdot c$.

Ранее в математических курсах встречались бесконечные поля рациональных чисел Q, действительных чисел R и комплексных чисел C. Если же поле имеет конечное число элементов, то его называют ***конечным***, а число его элементов – ***порядком поля***. Например, запишем кольцо вычетов $\mathrm{mod}18$: $Z_{18}=\{0,1,2,3,...,17\}$. Так как обратный элемент существует только для тех ненулевых элементов, которые являются взаимно простыми с модулем (т.е. для $1,5,7,11,13,17$), то мультипликативная группа $Z_{18}^{\ *}=\{1,5,7,11,13,17\}$ элементов кольца образует поле. Если же модуль p простой, то любой ненулевой элемент $1,2,3,...,p-1$ имеет обратный и поэтому мультипликативная группа $Z_p^{\ *}=\{1,2,...,p-1\}$ есть поле. Например, $Z_5=\{0,1,2,3,4\}$ – простейший пример конечного поля из 5 элементов.

Конечные поля еще называют ***полями Галуа*** по имени французского математика Галуа. Поэтому для конечных полей из q элементов существует два обозначения: F_q и $GF(q)$, где GF читается «поле Галуа». В этих обозначениях $F_5=\{0,1,2,3,4\}$.

В 1893 г. американский математик Мур доказал, что для каждого простого числа p и положительного целого n существует конечное поле из $q=p^n$ элементов, единственное с точностью до изоморфизма.

Характеристикой поля F_q называется наименьшее положительное число p, при котором в поле выполнено равенство $p\cdot 1=0$. Это записывают $char\ F=p$. Например, поле $Z_5=\{0,1,2,3,4\}$ имеет характеристику $p=5$, так как равенство $p\cdot 1\equiv 0$ выполняется только при $p=5$.

§19. ГРУППА ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Основные определения. ***Эллиптической кривой*** E над полем F называется множество точек $(x;y)$, координаты которых принадлежат полю и удовлетворяют кубическому уравнению

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in F. \qquad (1)$$

Вместо (1) используется и функция двух переменных

$$f(x;y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0. \qquad (2)$$

Эллиптическую кривую E называют ***сингулярной*** , если на кривой существует хотя бы одна ***особая*** точка $(x;y)$, в которой одновременно

$$\frac{\partial f}{\partial x} = 0 \quad \text{и} \quad \frac{\partial f}{\partial y} = 0. \qquad (3)$$

В противном случае кривая называется ***несингулярной***. Такие кривые являются гладкими, т.е. не имеют точек возврата и самопересечений, в любой их точке можно провести касательную. Именно эти кривые и представляют интерес для криптографии.

В зависимости от характеристики поля с помощью замены координат уравнение (1) приводится к разным каноническим формам:

- если характеристика поля $p \neq 2$ и $p \neq 3$, то

$$y^2 = x^3 + ax + b \qquad (4)$$

(эта форма называется ***формой Вейерштрасса***);

- если характеристика поля $p = 3$, то

$$y^2 = x^3 + a_2x^2 + a_4x + a_6; \qquad (5)$$

- если же характеристика поля $p = 2$, то каноническое уравнение переводится в одну из форм:

$y^2 + y = x^3 + ax + b$ – суперсингулярные кривые (6)

или

$y^2 + xy = x^3 + ax + b$ – несуперсингулярные кривые. (7)

Условие несингулярности эллиптической кривой. Над полем действительных чисел эллиптическая кривая задается уравнением

$$y^2 = x^3 + ax + b.$$

Так как

$$y = \pm\sqrt{x^3 + ax + b},$$

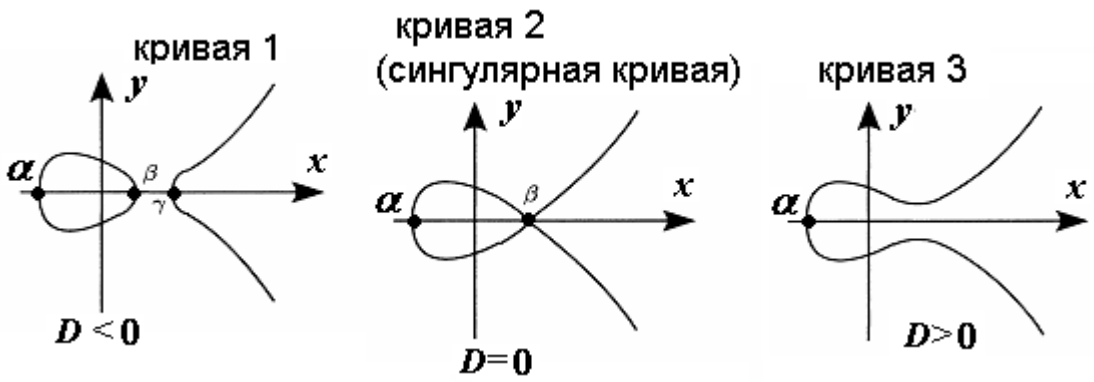
то график кривой симметричен относительно оси абсцисс. Точки его пересечения с этой осью – корни кубического уравнения

$$x^3 + ax + b = 0.$$

Дискриминант этого уравнения $D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$. При этом:

- если $D < 0$, то уравнение имеет три разных действительных корня α, β и γ. Типичный график – кривая 1 из двух частей;

- если $D=0$, то уравнение имеет действительные корни α, β, β, два из которых одинаковы. Типичный график – кривая 2. В этом случае точка $(\beta;0)$ – особая, а кривая сингулярная;
- если $D>0$, то уравнение имеет один действительный корень α и два комплексных. Типичный график – кривая 3.

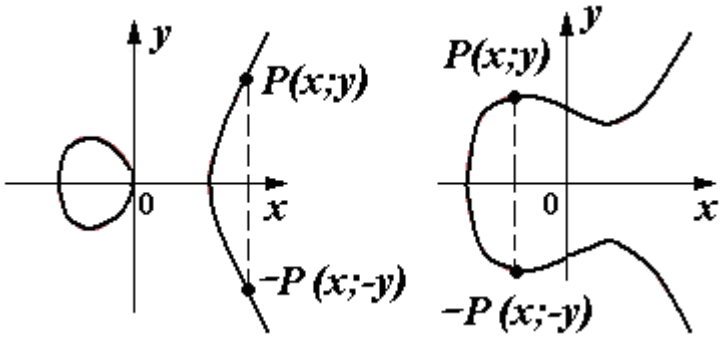


Аналогичные результаты будут и для конечных полей.

Таким образом, если характеристика поля $p\neq 2$ и $p\neq 3$, то кривая $y^2=x^3+ax+b(\mathrm{mod}\ p)$ будет несингулярной при условии, что ее дискриминант $D\neq 0$, а это, в свою очередь, эквивалентно условию $4a^3+27b^2\neq 0(\mathrm{mod}\ p)$.

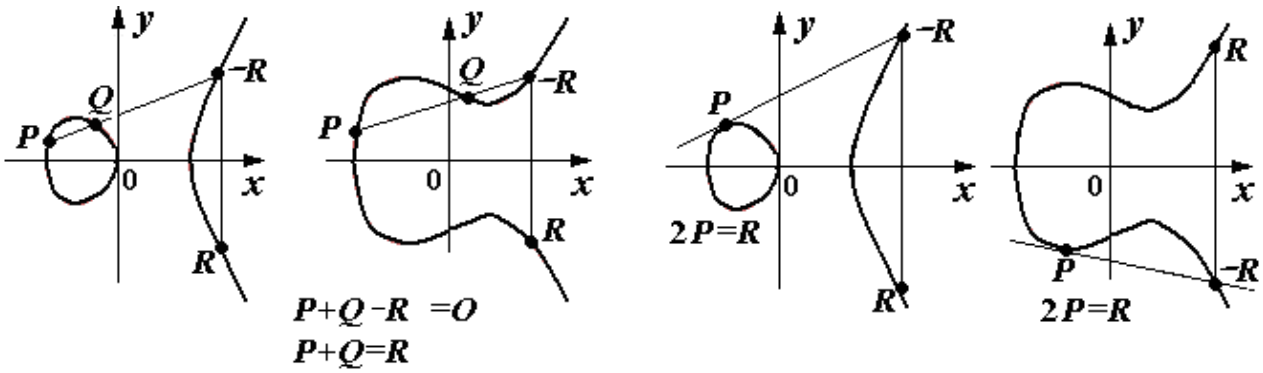
Законы сложения точек кривой и построение группы точек кривой. Симметрия кривой относительно оси Ox дает наглядное определение обратной точки. А именно: ***обратной точкой*** для точки $P(x;y)$ на эллиптической кривой называют точку $-P(x;-y)$.

Замечательным свойством несингулярных кривых является то, что любая прямая, проходящая через две различные точки кривой пересекает кривую в единственной точке. Кроме того, касательная к эллиптической кривой в любой точке (кроме точек перегиба) пересекает ее еще в одной точке.



Такие особенности позволяют задать групповую операцию, называемую ***сложением точек эллиптической кривой***.

Суммой двух точек P и Q называется точка $R=P+Q$, обратная третьей точке пересечения эллиптической кривой и прямой, проходящей через точки P и Q.



Суммирование точек Удвоение точки

Если суммируемые точки P и Q совпадают, то $P+Q=P+P=R$, что равносильно ***удвоению точки*** $2P=R$. При $P=Q$ секущая PQ превращается в касательную к кривой и геометрически удвоенная точка $2P$ – это точка, обратная к точке пересечения этой касательной и эллиптической кривой.

Найдем координаты точки $R=P+Q=(x_3;y_3)$, выразив их через координаты точек $P(x_1;y_1)$ и $Q(x_2;y_2)$. При этом точки P и Q могут быть различными или совпадающими. В соответствии с этим имеем два случая:

1). $P\neq\pm Q$. Запишем уравнение прямой PQ. Угловой коэффициент прямой PQ равен:

$$\lambda=\frac{y_2-y_1}{x_2-x_1}.$$

Уравнение PQ: $y=y_1+\lambda(x-x_1)$. Ищем третью точку пересечения кривой и прямой PQ:

$$\begin{cases} y^2=x^3+ax+b, \\ y=y_1+\lambda(x-x_1) \end{cases} \Rightarrow \quad (y_1+\lambda(x-x_1))^2=x^3+ax+b$$

Возводя в квадрат и группируя подобные члены, получим кубическое уравнение $x^3-\lambda^2x^2+\ldots=0$. По теореме Виета для кубических уравнений сумма корней кубического уравнения равна коэффициенту при x^2, взятому с противоположным знаком, т.е.

$$x_1+x_2+x_3=\lambda^2\ .$$

$$x_3=\lambda^2-x_1-x_2\,.$$

Подставив x_3 в уравнение прямой PQ, находим ординату точки $-R$:

$$y_3'=y_1-\lambda(x_3-x_1)\,.$$

Точка $R(x_3; y_3)$ – симметрична точке $-R$ относительно оси Ox, поэтому

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

2). При $P = Q$, $R = 2P$. Дифференцируем обе части равенства $y^2 = x^3 + ax + b$:

$$2ydy = 3x^2 + a.$$

В точке $P(x_1; y_1)$ производная равна угловому коэффициенту касательной к кривой:

$$\lambda = \left.\frac{dy}{dx}\right|_{(x_1; y_1)} = \frac{3{x_1}^2 + a}{2y_1}.$$

Координаты удвоенной точки $R(x_3; y_3) = 2P$:

$$x_3 = \lambda^2 - 2x_1;$$
$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Формулы сложения и удвоения точек эллиптической кривой справедливы для всех полей, в том числе и конечных, кроме полей характеристик 2 и 3. В последнем случае приведение по модулю 2 или 3 приведет в этих формулах к 0^{-1} Но аналогично можно вывести похожие формулы для операций и в полях характеристики 2 или 3.

Чтобы построить группу E точек эллиптической кривой, выберем в качестве нейтрального элемента группы точку $O(x\ ;\infty)$, для которой положим:

$$P + (-P) = O, \qquad \forall P \in E.$$

Прямая, проходящая через точки P и $-P$, перпендикулярна к оси абсцисс и поэтому можно принять, что третья точка пересечения перпендикуляра и кривой уходит в бесконечность вдоль оси ординат. Поэтому точку O называют ***точкой на бесконечности*** (***бесконечно удаленной точкой***) кривой.

Согласно теореме Анри Пуанкаре множество точек эллиптической кривой вместе с введенной точкой на бесконечности образует коммутативную группу относительно операции сложения точек: для этого есть все необходимые свойства – замкнутость, коммутативность, ассоциативность, наличие обратного элемента и нейтральный элемент.

Приходим к такому определению.

Группой точек эллиптической кривой над конечным полем $GF(p)$ называется множество точек $(x; y)$, координаты которых принадлежат полю и удовлетворяют уравнению: $y^2 = x^3 + ax + b(\mathrm{mod}\ p)$, если характеристика поля $p \neq 2; 3$ и

$a,b \in GF(p)$, $4a^3 + 27b^2 \not\equiv 0 (\mathrm{mod}\ p)$. К группе точек эллиптической кривой также относится точка $O(x;\infty)$. Принятое обозначение группы $E_p(a,b)$.

Сведем формулы для операций с точками $E_p(a,b)$ в таблицу:

Операция	Поле характеристики p, где $p \neq 2$ и $p \neq 3$
Сложение точек $P \neq \pm Q$ $P(x_1;y_1) + Q(x_2;y_2) = R(x_3;y_3)$	$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\ p)$; $x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p)$; $y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p)$
Удвоение точки $R(x_3;y_3) = 2P(x_1;y_1)$	$\lambda = \frac{3{x_1}^2 + a}{2y_1} (\mathrm{mod}\ p)$; $x_3 = \lambda^2 - 2x_1 (\mathrm{mod}\ p)$; $y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p)$
$O + O = O$; $P(x;y) + O = P(x;y)$; $P(x;y) + P(x;-y) = O$	

Поиск всех точек эллиптической кривой над конечным полем $GF(p)$ *(* так можно найти точки только при малом p **):**

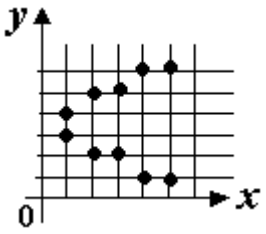
1) Для каждого целого значения x, где $0 \le x \le p$, вычислить y^2 по формуле $y^2 = x^3 + ax + b (\mathrm{mod}\ p)$.
2) Для всех значений y^2 выяснить, будут ли они квадратичными вычетами по модулю p, т. е. можно ли их них извлечь корень квадратный. Это можно, например, выяснить, вычислив символ Лежандра $\left(\frac{y^2}{p}\right)$. Значение y^2 будет квадратичным вычетом при условии, что $\left(\frac{y^2}{p}\right) = 1$, и невычетом, – если $\left(\frac{y^2}{p}\right) = -1$. В этом случае на кривой $E_p(a,b)$ точек с таким значением x нет. Если же корень существует, то найти два значения корня y_1 и y_2

(исключение только $y=0$). Точки $(x;y_1)$ и $(x;y_2)$ будут принадлежать кривой $E_p(a,b)$.

Пример 1. Найти все точки эллиптической кривой $E_7(2,6)$.

Р е ш е н и е. $E_7(2,6)$ – это кривая $y^2=x^3+2x+6(\mathrm{mod}\,7)$. Считаем значения $x^3+2x+6(\mathrm{mod}\,7)$ и $y^2(\mathrm{mod}\,7)$ для $x,y,=1,2,...,6$.

x	1	2	3	4	5	6
$x^3+2x+6(\mathrm{mod}\,7)$	2	4	4	1	1	3
y	1	2	3	4	5	6
$y^2(\mathrm{mod}\,7)$	1	4	2	2	4	1



Группа $E_7(2,6)$ состоит из точек $(x;y)$, при которых $y^2(\mathrm{mod}\,7)=x^3+2x+6(\mathrm{mod}\,7)$. Это точки $(1,3)$, $(1,4)$, $(2,2)$, $(2,5)$, $(3,2)$, $(3,5)$, $(4,1)$, $(4,6)$, $(5,1)$, $(5,6)$ и O. На графике есть симметрия относительно прямой $y=p/2=3,5$.

Пример 2. Вычислить: а) $(8,3)+(3,6)$; б) $2(1,8)$ в группе $E_{11}(1,6)$.

Р е ш е н и е. Кривая $E_{11}(1,6)$ – это $y^2=x^3+x+6(\mathrm{mod}11)$.

а) $(x_1,y_1)=(8,3)$; $(x_2,y_2)=(3,6)$.

$$\lambda=\frac{y_2-y_1}{x_2-x_1}=\frac{6-3}{3-8}=\frac{3}{-5}\equiv -3\cdot 5^{-1}\equiv -3\cdot 9\equiv 6(\mathrm{mod}11);$$

$$x_3=\lambda^2-x_1-x_2\equiv 36-8-3\equiv 3(\mathrm{mod}11);$$

$$y_3=\lambda(x_1-x_3)-y_1=6(8-3)-3\equiv 5\ \Rightarrow\ (8,3)+(3,6)=(3,5).$$

б) $(x_1,y_1)=(1,8)$; $\quad\lambda=\dfrac{3x_1{}^2+a}{2y_1}=\dfrac{3\cdot 1+1}{2\cdot 8}=\dfrac{4}{16}=4^{-1}\equiv 3(\mathrm{mod}11);$

$$x_3=\lambda^2-2x_1=9-2\cdot 1\equiv 7(\mathrm{mod}11);$$

$$y_3=\lambda(x_1-x_3)-y_1=3(1-7)-8\equiv 7(\mathrm{mod}11);\quad\Rightarrow\ 2(1,8)=(7,7).$$

Число элементов группы точек эллиптической кривой $E_p(a,b)$ называют ***порядком этой группы***. Верхняя и нижняя границы для порядка группы определяются теоремой Хассе.

Теорема Хассе. Для порядка N_E группы точек эллиптической кривой над полем $GF(q)$ (q – число элементов поля) справедливо неравенство

$$q+1-2\sqrt{q}\le N_E\le q+1+2\sqrt{q}.$$

Из неравенства Хассе вытекает, что число точек на эллиптической кривой отличается от общего числа элементов поля самое большее, на величину, меньшего порядка, чем $O(\sqrt{q})$.

В общем случае найти точное число точек эллиптической кривой довольно сложно. Первый алгоритм для подсчёта количества точек эллиптической кривой над конечным полем с полиномиальной сложностью, был предложен Рене Шуфом. В первое время считалось, что алгоритм Шуфа мало пригоден для применения на практике, но Элкис и Аткин внесли в него несколько важных добавлений, после чего он стал известен как алгоритм SEA (по первым буквам фамилий авторов).

§20. ПОРЯДОК ТОЧКИ В ГРУППЕ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Из предыдущих операций сложений точек и удвоения точки на число вытекает операция ***скалярного умножения точки на число*** в группе точек эллиптической кривой. Точку mP, равную m-кратному сложению точки P в аддитивной группе точек эллиптической кривой, называют ***скалярным произведением точки на число*** m, а сами точки mP – ***скалярными кратными точки***. Таким образом,

$$mP = \underbrace{P + P + \ldots + P}_{m};$$

При этом $0 \cdot P = O$; $-mP(x,y) = mP(x,-y)$.

Арифметика эллиптических кривых не содержит прямых формул для вычисления кратного mP для заданной точки $P(x,y)$, то эту операцию выполняют с использованием операций сложения, вычитания и удвоения точки. Для этого надо представить число m в двоичной системе $m = b_t b_{t-1} \ldots b_0$, где $b_i \in \{0;1\}$, потом вычислить все точки $2P$, $4P$, …, $2^t P$ и подсчитать сумму тех точек $2^i P$, для которых $b_i = 1$.

Пример. $13_{10} = 1101_2 \Rightarrow 13P = 8P + 4P + P$.

Умножение точки на число аналогично возведению в степень в случае RSA и требует небольшого числа сложений. Например, для умножения точки на число длины 200 бит будет выполнено в среднем 100 операций удвоения точки и 66 операций сложения точек. Для сравнения: при возведении числа в степень с показателем длины 200 бит в среднем выполняется 300 операций умножения.

Порядок точки P – это наименьшее натуральное число n, при котором $nP = O$. Например, в группе $E_{11}(6,3)$ имеем $2(9,4) = (7,6)$;

$3(9,4)=(7,5);\ 4(9,4)=(9,7);\ 5(9,4)=O \Rightarrow$ на кривой $E_{11}(6,3)$ порядок точки $(9,4)$ равен 5.

Если точка P имеет порядок n, то

- множество $\{O, P, 2P, ..., (n-1)P\}$ образует циклическую подгруппу в $E_p(a,b)$;
- порядок любой точки является делителем общего числа точек эллиптической кривой, т.е. порядка группы точек эллиптической кривой;
- при $n=|E|$, точка является образующим элементом (генератором) группы. При соответствующем выборе параметров a и b число точек на кривой может равняться простому числу и тогда любая точка кривой, кроме O, будет порождать всю группу.

Чтобы найти порядок n точки P эллиптической кривой $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$ над полем $GF(p)$, надо решить уравнение $nP = O$. Это можно сделать, например, с помощью такого алгоритма.

Алгоритм вычисления порядка точки эллиптической кривой

1^0. Вычислить $m=\lceil \sqrt{N_1} \rceil$ – округление с избытком, где $N_1 = p+1+2\sqrt{p}-$ максимальная оценка порядка группы точек эллиптической кривой, полученная из теоремы Хассе.

2^0. Построить таблицу пар $(j,\ jP)$ для $j=1,2,...,m$.

3^0. Вычислить $\alpha = -mP$.

4^0. Положить $\gamma = O$ – бесконечно удаленная точка.

5^0. Для $i=1,2,...,m-1$ выполнить следующие действия:

4.1 проверить, будет ли точка γ содержаться в таблице, построенной на шаге 1;

4.2 если $\gamma = jP$, то считать $n = mi + j$;

4.3 положить $\gamma = \gamma + \alpha$.

Пример. Найти порядок точки $P(0,1)$ эллиптической кривой $y^2 = x^3 + x + 1$ над простым полем $GF(5)$.

Р е ш е н и е. $N_1 = p+1+2\sqrt{p} = 5+1+2\sqrt{5} \approx 10 \Rightarrow$ $m=\lceil \sqrt{N_1} \rceil = \lceil \sqrt{10} \rceil = 4$.

Строим таблицу

j	1	2	3	4
jP	$(0,1)$	$(4,2)$	$(2,1)$	$(3,4)$

Находим $\alpha = -mP = -4(0,1) = -(3,4) = (3,-4)(\mathrm{mod}\,5) \equiv (3,1)$.

Положим $\gamma = O$. Эта точка в таблице не содержится. Далее находим $i = 1 \Rightarrow \gamma = \gamma + \alpha = O + (3,1) = (3,1)$ – нет в таблице;

$i = 2 \Rightarrow \gamma = \gamma + \alpha = (3,1) + (3,1) = (0,1)$ – есть в таблице при $j = 1$;

$\Rightarrow n = mi + j = 4 \cdot 2 + 1 = 9$. Порядок точки $P(0,1)$ равен 9

§21. ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Операция скалярного умножения – аналог операции возведения в степень в конечном поле. Поэтому в эллиптической криптографии в роли прямой задачи выступает ***скалярное умножение точки*** кривой, т.е. вычисление $Q = mP$ при известных m и P. Обратная задача по традиции называется ***дискретным логарифмированием на эллиптической кривой*** и формулируется так: зная точки P и Q, найти такое число m, для которого $mP = Q$.

Стойкость шифров на эллиптических кривых определяется сложностью решения задачи дискретного логарифмирования в группе точек кривой т.е. сложностью решения уравнения $mP = Q$ относительно m, где точки P и Q принадлежат одной циклической подгруппе. Предполагают, что задача дискретного логарифмирования на эллиптической кривой даже более трудная, чем такая же задача в конечных полях и для ее решения существуют только экспоненциальные алгоритмы. Самые быстрые из них – это алгоритм Шенкса и ρ-метод Полларда (у обоих временная сложность $O(\sqrt{n})$). А вот построить субэкспоненциальные алгоритмы для дискретного логарифмирования на тех принципах, использование которых привело к успеху в случае конечных полей, невозможно, поскольку на эллиптических кривых нет аналогов простых чисел или неприводимых многочленов.

Исключение составляют некоторые суперсингулярные эллиптические кривые, для которых проблема дискретного логарифма решается эффективно. Для суперсингулярных кривых в 1993 году ***Менезес***, ***Окатамо*** и ***Ванстоун*** разработали алгоритм (***MOV–атака***), основанный на преобразовании Вейля – Тейта и сводящий задачу дискретного логарифмирования на эллиптической кривой над полем $GF(q)$ к аналогичной задаче в некотором конечном расширении исходного поля $GF(q^k)$, где логарифмировать можно намного эффективнее. Однако, данное сведение полезно только, если степень k мала. Это условие выполняется, в основном, для суперсингулярных эллиптических кривых. В остальных случаях подобное сведение практически никогда не приводит к субэкспоненциальным алгоритмам.

Поэтому суперсингулярные кривые перестали использоваться для шифрования и электронной цифровой подписи. Но в 2000 г. А. Джоукс нашел замечательные применения преобразованию Вейля – Тейта в криптографии, разработав трехсторонний однораундовый протокол ключевого соглашения Диффи – Хеллмана. Отсюда родилось построение открытого ключа пользователя на основе его общеизвестных идентификационных данных (имя, адрес и др.) и на сегодняшний день эта тематика одна из самых популярных.

Если порядок N_E группы точек кривой есть произведение малых простых чисел, то дискретное логарифмирование можно эффективно провести с помощью алгоритма Полига – Хеллманна.

Ниже мы сформулируем конкретные условия, которые помогут исключить использование в криптографии таких кривых (см. далее).

§22. СХЕМА ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДИФФИ-ХЕЛЛМАНА НАД ГРУППОЙ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Криптоалгоритмы на эллиптических кривых строятся аналогично алгоритмам в простых конечных полях. Фактически возведение в степень по большому модулю, определяющее стойкость шифра, заменяется на скалярное произведение точки эллиптической кривой. Словарь перевода обычного криптоалгоритма в эллиптический такой:

Термины и понятия	Криптосистема над простым конечным полем	Криптосистема на эл. кривой над конечным полем
Группа	Z_p*	$E(GF(p))$
Элементы группы	целые $\{1,2,...,p-1\}$	точки $P(x;y)$ на кривой и точка O
Групповая операция	умножение по модулю p	сложение точек
Обозначения	элементы g и h	точки P и Q
	обратный элемент g^{-1}	обратная точка $-P$
	деление $g \cdot h^{-1}$	вычитание точек $P-Q$
	возведение в степень g^a	скалярное умножение mP
Проблема дискретного логарифмирования	$g \in Z_p*$; $h \equiv g^a (\mathrm{mod}\ p)$; найти a	$P \in E(GF(p))$; $Q = mP$; найти m

Суть перехода к эллиптическим кривым заключается в замене относительно медленной операции возведения в степень по большому модулю в алгоритме RSA на более быструю операцию скалярного умножения на эллиптической кривой, при этом сохраняются операции над целыми числами по небольшому модулю.

В качестве первого примера приведем ***эллиптический аналог открытого распределения ключей Диффи-Хеллмана (ECDH)***.

Два пользователя **A** и **B** выбирают общие параметры:

- эллиптическую кривую над конечным полем;
- точку P на этой кривой, имеющую большой порядок n (она не обязательно должна быть порождающим элементом группы точек кривой, но порожденная ею подгруппа должна быть большой, предпочтительно того же порядка, что и сама группа). Точка P называется ***базовой***.

Общие параметры передаются открытым каналом связи.

1. Пользователь **A** случайно выбирает число c – свой секретный ключ, а пользователь **B** случайно выбирает для своего секретного ключа число d (числа близки по порядку к общему числу N_E точек кривой). Далее пользователи находят свои точки $Q = cP$ и $R = dP$ соответственно.

2. Пользователи обмениваются точками Q и R по открытому каналу.

3. Пользователь **A**, получив точку R, вычисляет точку $S = cR$.

4. Пользователь **B**, получив точку Q, вычисляет точку $S = dQ$.

Так как $cR = c(dP) = d(cP) = dQ$, то значение S – общий ключ пользователей.

Пример. Сгенерировать общий ключ для двух пользователей по схеме Диффи – Хеллмана, если выбрана эллиптическая кривая $E_{211}(0,-4)$ и точка $P(2,2)$.

Р е ш е н и е. Кривая $y^2 = x^3 - 4 (\mathrm{mod}\, 211)$. Порядок точки P равен 241, так как $241P = O$. Пусть секретный ключ пользователя **A** будет $c = 121$, а пользователя **B** – число $d = 203$. Пользователь **A** вычисляет $121P = 121(2,2) = (115,48)$, а пользователь **B** находит $203P = 203(2,2) = (130,203)$. Пользователь **A** передает пользователю **B** открытый ключ – точку $(115,48)$, пользователь **B** передает пользователю **A** свой ключ – точку $(130,203)$. Далее идут такие вычисления:

пользователь **A**: $121(130,203) = (161,169)$;

пользователь **B**: $203(115,48) = (161,169)$.

Общий секретный ключ $(161,169)$– пара чисел. Если его использовать как секретный ключ для симметричного шифра, то для этой цели можно выбрать просто абсциссу точки x=161 или некоторую функцию от x $\Rightarrow$ общий секретный ключ 161= 10100001.

Чтобы взломать эту схему, противник должен вычислить числа c и d из соотношений $Q = cP$ и $R = dP$, т.е. провести дискретное логарифмирование, для которого не существует эффективного логарифма. Но протокол Диффи – Хеллманна, однако, не защищен от противника, который имеет доступ к каналу связи и может подменить пересылаемые точки Q и R.

§23. КРИПТОСИСТЕМА МЕССИ – ОМУРЫ НАД ГРУППОЙ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Перед началом шифрования пользователи должны по открытому каналу обменяться такими параметрами криптосистемы:

- конечное поле $GF(q)$, q – большое число;
- уравнение эллиптической кривой E над полем $GF(q)$;
- порядок кривой N_E (общее число точек кривой).

Пусть пользователь **A** хочет послать зашифровать сообщение M, пользователю **B**. Пусть этому сообщению соответствует точка P. Тогда:

1). Пользователи **A** и **B** должны независимо и тайно выбрать себе из интервала $(1; N_E)$ по целому случайному числу e, для которого НОД$(e, N_E) = 1$ и далее вычислить обратный к нему элемент $d = e^{-1} (\mathrm{mod}\, N_E)$. Далее нижние индексы A и B указывают на владельца числа. Эти числа пользователи сберегают в секрете.

2). Пользователь **A** должен вычислить точку $e_A P$ и отослать ее пользователю **B**.

3) Пользователь **B** должен вычислить точку $e_B e_A P$ и отослать ее пользователю **A**.

4) Пользователь **A** должен вычислить точку $d_A e_B e_A P$. Так как $d_A e_A \equiv 1 (\mathrm{mod}\, N_E)$, то $d_A e_B e_A P = e_B P$. Эту точку пользователь **A** отсылает **B**.

5) Пользователь **B** должен: вычислить точку $d_B e_B P$. Так как $d_B e_B \equiv 1 (\mathrm{mod}\, N_E)$, то $d_B e_B P = P \Rightarrow$ **B** прочитает сообщение.

§24. КРИПТОСИСТЕМА ЭЛЬ-ГАМАЛЯ НАД ГРУППОЙ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Перед началом шифрования по открытому каналу пользователи должны согласовать следующие параметры криптосистемы:

- конечное поле $GF(q)$;
- уравнение эллиптической кривой E над полем $GF(q)$
- ***базовая точка*** P (знать общее число точек кривой необязательно).

Пусть пользователь **A** хочет послать пользователю **B** сообщение M, которому поставлена в соответствие точка $M(x;y)$ эллиптической кривой.

Пользователь **A** должен: выбрать себе ***секретный ключ*** a_A –и найти точку $Q_A = a_A P$. Точка Q_A– ***открытый ключ*** пользователя **A**.

Пользователь **B** должен: выбрать себе ***секретный ключ*** a_B – целое случайное число и найти точку $Q_B = a_B P$. Точка Q_B– ***открытый ключ*** пользователя **B**.

Открытые ключи (точки Q_A и Q_B) несекретны и становятся общедоступными.

Пользователь **A** для шифрования должен:

1) выбрать случайное целое число k, определить точки kP и kQ_B;
2) вычислить сумму $R = M + kQ_B$. Криптограмма, соответствующая шифрованию точки M, состоит из пары точек: $(kP; R)$. Точка kP называется ***точкой-подсказкой***.
3) криптограмма пересылается пользователю **B**.

Пользователь **B** для дешифрования должен:

1) вычислить $a_B \cdot kP$.
2) найти разность $R - a_B kP = M$ (здесь вычитание – это сложение с обратной точкой $-a_B kP$).

Поскольку $R - a_B kP = M + kQ_B - ka_B P = M$,

$\uparrow \; a_B P = Q_B$

то такое дешифрование даст именно точку, отвечающую открытому тексту M.

Пример. Выбрав эллиптическую кривую $E_{23}(9,17)$ над полем $GF(23)$, зашифровать сообщение, отвечающее точке $M(12,6)$ и дешифровать полученную криптограмму.

Р е ш е н и е.

Генерация ключей получателем шифрованного текста

Пусть базовая точка $P(4,5)$. Выберем закрытый ключ получателя $a_B = 3$. Найдем точку $Q_B = 3P$. Очевидно $3P = 2P + P$.

Удвоение точки $P(4,5)$:

$$\lambda = \frac{3x_1^{\,2} + a}{2y_1} (\mathrm{mod}\ p) = \frac{3 \cdot 4^2 + 9}{2 \cdot 5} (\mathrm{mod}\, 23) = \frac{57}{10} = 57 \cdot 10^{-1} \equiv$$

$$\equiv 57 \cdot 7 \equiv 8 (\mathrm{mod}\, 23);$$

$$x_3 = \lambda^2 - 2x_1 (\mathrm{mod}\ p) = 64 - 2 \cdot 4 = 56 \equiv 10 (\mathrm{mod}\, 23);$$

$$y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p) = 8(4 - 10) - 5 = -53 \equiv 16 (\mathrm{mod}\, 23);$$

$$\Rightarrow \ 2P = (10,16).$$

Вычислим $3P = 2P + P = (10,16) + (4,5)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5 - 16}{4 - 10} = \frac{11}{6} = 11 \cdot 6^{-1} (\mathrm{mod}\, 23) = 11 \cdot 4 \equiv 21 (\mathrm{mod}\, 23);$$

$$x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p) = 21^2 - 10 - 4 (\mathrm{mod}\, 23) = 427 \equiv 13;$$

$$y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p) = 21(10 - 13) - 16 (\mathrm{mod}\, 23) \equiv 13.$$

$$\Rightarrow \quad Q_B = 3P = (13,13).$$

Секретный ключ получателя – число $a_B = 3$, открытый ключ – точка $Q_B(13,13)$.

Шифрование

Выберем случайное целое число $k = 5$. Зная открытый ключ получателя, найдем точку $5P$.

$$5P = 2P + 3P = (10,16) + (13,13);$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{13 - 16}{13 - 10} = -1 (\mathrm{mod}\, 23) \equiv 22 (\mathrm{mod}\, 23);$$

$$x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p) = 22^2 - 10 - 13 (\mathrm{mod}\, 23) \equiv 1;$$

$$y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p) = 22(10 - 1) - 16 (\mathrm{mod}\, 23) \equiv 21.$$

$$\Rightarrow \quad kP = 5P = (1,21).$$

Определим точку $kQ_B = 5Q_B$. Подобно предыдущему найдем

$$3Q_B = 2Q_B + Q_B = (15,13); \qquad 5Q_B = 2Q_B + 3Q_B = (8,7).$$

Вычислим сумму

$$R = M + kQ_B = (12,6) + 5Q_B = (12,6) + (8,7) = (16,18).$$

Криптограмма: $((1,21);\ (16,18))$.

Дешифрование

Зная свой закрытый ключ $a_B = 3$, получатель вычисляет $a_B(1,21) = 3(1,21)$.

$3(1,21) = 2(1,21) + (1,21)$;

$2(1,21) = (7,20)$; $3(1,21) = (7,20) + (1,21) = (8,7)$;

$M = R - a_B kP = (16,18) - (8,7) = (16,18) + (8,-7) = (12,6)$.

Замечание. Как кодировать текстовое сообщение точками кривой? Необходимо буквы сообщения заменить числовым кодом (можно использовать стандартную кодировку ASCII) и каждому коду (т.е. числам от 0 до 255) сопоставить какую-то точку кривой. По **первому варианту** это можно сделать, составив таблицу, в которой букве с кодом r соответствует абсцисса x точки rP (естественно, далее точки rP шифруются). **Второй вариант** основан на следующем свойстве эллиптической кривой: для любого числа $x \le \lfloor n/2 \rfloor$ на эллиптической кривой **с** высокой вероятностью найдется точка с координатами $P_1(2x;\ y_1)$ или $P_2(2x+1;\ y_2)$, которая может служить образом для кода. Тогда, зная координаты $(x';\ y')$ любой из точек P_1 или P_2 можно восстановить x, вычисляя целую часть $\lfloor x'/2 \rfloor$.

§25. ВЫБОР ЭЛЛИПТИЧЕСКОЙ КРИВОЙ И БАЗОВОЙ ТОЧКИ

В настоящее время для целей криптографии обычно используются эллиптические кривые над простым полем и над полем характеристики 2.

Для использования эллиптической криптографии участники протокола должны согласовать все параметры, определяющие эллиптическую кривую.

Генерация эллиптической кривой состоит из следующих шагов:

- генерация характеристики поля Галуа;
- генерация коэффициентов кривой;
- вычисление порядка N_E группы точек кривой;
- генерация базовой точки;
- определение порядка базовой точки кривой. Желательно, чтобы так называемый кофактор $h = N_E / n$ был небольшим (n – порядок точки, $h \le 4$ и даже лучше, если $h = 1$).

В системах Диффи – Хеллмана и Эль-Гамаля существует два подхода к выбору эллиптической кривой и базовой точки на ней.

1. ***Случайный выбор***. Выбираем какое-либо большое конечное поле $GF(q)$ с характеристикой $p > 3$, в котором кривую можно будет задать уравнением $y^2 = x^3 + ax + b$. Произвольно задав тройку чисел

$x, y, a \in GF(q)$, вычисляем $b = y^2 - (x^3 + ax)$ и проверяем условие $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, p)$. Если оно выполнено, то кривая подобрана, а если нет, то выбираем другую случайную тройку x, y, a и повторяем процесс. Когда кривая подобрана, то точка $P(x;y)$ лежит на кривой. Если условие $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, p)$ не выполнено, то выбираем другую тройку x, y, a и т.д.

2. ***Редукция глобальной пары кривая – точка по*** $\mathrm{mod}\, p$ (*редукция данных – это сведение данных со сложной структурой к более простой форме*). Пусть E – эллиптическая кривая над полем рациональных чисел (назовем ее «глобальной») и $P(x;y)$ – точка бесконечного порядка на кривой. Например, точка $P(0;0)$ является точкой бесконечного порядка на кривой $y^2 + y = x^3 - x^2$ и порождает всю группу рациональных точек на кривой. Далее выбираем большое простое число p и выполняем редукцию: для всех больших p коэффициенты в уравнении кривой E будут иметь обратные элементы по $\mathrm{mod}\, p$ и могу рассматриваться как коэффициенты в уравнении кривой по $\mathrm{mod}\, p$. Можно с помощью специальной замены переменных свести уравнение кривой к виду $y^2 = x^3 + ax + b$, где кубический многочлен не будет иметь кратных корней и дает поэтому эллиптическую кривую над полем $GF(p)$. Если координаты точки $P(x;y)$ также привести по модулю, то это даст искомую точку на эллиптической кривой. При использовании второго способа мы раз и навсегда фиксируем кривую E и точку $P(x;y)$, а меняя значения p, получаем много разных кривых над полем $GF(p)$.

Одна из гарантий, того что выбранная базовая точка $P(x;y)$ будет генератором группы, – это выбор таких кривой и поля, для которых количество точек кривой N_E – простое число (тогда любая точка будет генератором).

Таким образом, параметры необходимые для криптографического протокола в случае несингулярной кривой над полем с характеристикой $p \neq 2,3$ – это набор p, a, b, G, n, h. Для поля $GF(2^m)$ набор параметров несколько иной – (m,f,a,b,G,n,h). Существует 15 эллиптических кривых, рекомендованных NIST(США). Федеральные стандарты обработки информации (FIPS) рекомендуют 10 конечных полей. Некоторые из них: поля $GF(p)$, где простое p имеет длину 192, 224, 256, 384 или 521 бит, поля $GF(2^m)$, где m=163, 233,283, 409, 571. Для каждого конечного поля рекомендуется одна кривая. Эти конечные

поля и эллиптические кривые выбраны из-за высокого уровня безопасности и эффективности программной реализации.

Например, одна из этих кривых:

$$y^2 = x^3 + 3176890812513255034763174764138276932727469559 27x +$$
$$+ 7905289660787875871812057202571853543210065193 4.$$

§26. БЕЗОПАСНОСТЬ КРИПТОГРАФИИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Безопасность, обеспечиваемая эллиптической криптографией, зависит от трудности решения задачи дискретного логарифмирования. Как отмечалось, это можно сделать с помощью:

- метода полного перебора;
- алгоритма Полига – Силвера – Хеллманна;
- алгоритма «шаг младенца – шаг великана» (число шагов $\sqrt{n}$);
- ρ-метод Полларда (число шагов $\pi\sqrt{n}/2$);
- параллельные вычисления в ρ-метод Полларда (число шагов $\pi\sqrt{n}/2r$, r – число процессоров).

Эллиптическая криптография		RSA	
Длина ключа (бит)	Время взлома (MIPS-годы)	Длина ключа (бит)	Время взлома (MIPS-годы)
150	$3{,}8\cdot10^{10}$	512	$3\cdot10^{4}$
205	$7{,}1\cdot10^{18}$	768	$2\cdot10^{8}$
234	$3{,}8\cdot10^{28}$	1024	$3\cdot10^{11}$
		1280	$1\cdot10^{14}$
		1536	$3\cdot10^{16}$
		2048	$3\cdot10^{20}$
ρ-метод Полларда для проведения дискретного логарифмирования		метод факторизации чисел с помощью решета числового поля общего вида.	

В таблице сравнивается эффективность ρ-метода Полларда и метода факторизации больших чисел с помощью решета числового поля общего вида. Видно, что тот же уровень защиты достигается в случае эллиптической криптографии при значительно меньших длинах ключа.

Кроме того, из рекомендаций NIST США по выбору длины ключа симметричного шифра AES следует, что отношение

длина ключа ECC / длина ключа RSA

является нелинейным.

Эквивалентные длины ключей			
Длина ключа ECC (биты)	Длина ключа RSA (биты)	Отношение длин ключей ECC/ RSA	Длина ключа AES (биты)
163	1 024	1: 6	
256	3 072	1 : 12	128
384	7 680	1 : 20	192
512	15 360	1 : 30	256

Implication 1. *For elliptic curve cryptography we select an elliptic curve such that*

$$\#E(K) = N = h \cdot l$$

where l is a large prime and h is very small. Usually one chooses $h = 1, 2$ or 4.

The security criteria for elliptic curves, so that the discrete logarithm problem is difficult, is that one should choose curves E over finite fields $K = \mathbf{F}_q$ such that if

$$\#E(K) = h \cdot l$$

where l is prime, then

- $l > 2^{160}$.
- l should not divide $q^k - 1$ for $k \leq 30$.
- $l \neq q$.
- q should be equal to a large prime, or a prime power of two.

Существует несколько классов криптографически «слабых» кривых, которых следует избегать:

- кривые над $GF(2^m)$, где m – непростое число. Шифрование на этих кривых подвержено атакам Вейля;
- кривые над полем $GF(q)$ с общим числом точек $N_E = q$ уязвимы для атаки, которая отображает точки данной кривой в аддитивную группу поля;
- ***аномальные эллиптические кривые*** над полем $GF(p)$, когда общее число точек на кривой $N_E = p$, p – простое;

Самые сложные схемы на эллиптических кривых, публично взломанные к настоящему времени, содержали 112-битный ключ для конечного простого поля и 109-битный ключ для конечного поля характеристики 2. В июле 2009г. кластер из более чем 200 Sony PlayStation 3 за 3.5 месяца нашел 109-битный ключ. Ключ над полем характеристики 2 был найден в 2004г. с использованием 2600 компьютеров за 17 месяцев.

Коблиц Нил (англ. Koblitz Neal I., родился в 1948 г.) – известный американский математик, профессор математики в Вашингтонском университете, адъюнкт-профессор в Центре прикладных криптографических исследований при университете Ватерлоо. Учился в Гарвардском университете, в 1974г. защитил в Принстоне докторскую диссертацию по математике. Шифрование на эллиптических кривых фактически ведет свою историю с доклада Коблица в университете Вашингтона, в котором он независимо от Миллера заложил основы эллиптической криптографии. Вместе со своей женой Энн Коблиц основал в 1985 г. премию им. Софьи Ковалевской в честь женщин математиков, которая финансируется из фондов семьи Коблиц.

Миллер Саул Виктор (англ. Victor Saul Miller, родился в 1947 г. в США) – известный американский математик, с 1993 г. сотрудник Центра исследований в области связи института оборонного анализа в Принстоне (США). Получил степень бакалавра по математике в Колумбийском университете и степень доктора по математике в Гарварде.

Его основная сфера интересов – вычислительная теория чисел, комбинаторика, сжатие данных и шифрование. Является одним из соавторов изобретения эллиптической криптографии (независимо от Коблица), принимал участие в разработке расширения алгоритма сжатия LZW данных, используемого в международном стандарте V.42bis и других прикладных программах. За эти разработки получил медаль тысячелетия IEEE (крупнейшего профессионального объединения в мире, имеющего целью продвижение инноваций и передового опыта на благо человечества). В 1986 г. предложил алгоритм, ставший базовым для вычисления спариваний Вейтля в эллиптической криптографии.

"Стойкость криптосистем, основанных на эллиптических кривых, недостаточно изучена, во многом из-за переусложненного взгляда на природу самих эллиптических кривых. Очень немногие криптографы понимают, что такое эллиптические кривые, поэтому, в отличие от RSA, нет широкого понимания и консенсуса относительно стойкости, обеспечиваемой их использованием при шифровании. Со временем ситуация может измениться, но сейчас получить оценку стойкости криптосистемы, основанной на эллиптических кривых, - все равно что получить оценку недавно обнаруженной древневавилонской поэзии"

Рональд Ривест, создатель RSA

ПРИЛОЖЕНИЕ

Канонические уравнения эллиптических кривых и арифметические операции с точками

Тип поля и вариант кривой	Каноническое уравнение кривой	Формула сложения $(x_1;y_1)+(x_2;y_2)=(x;y)$ $(x_1;y_1)\neq(x_2;y_2)$	Формула удвоения $(x;y)=2(x_1;y_1)$
Поле характеристики p, где $p\neq 2,3$	$y^2=x^3+ax+b$	$x=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2$ $y=\frac{y_2-y_1}{x_2-x_1}(x_1-x)-y_1$	$x=\left(\frac{3x_1{}^2+a}{2y_1}\right)^2-2x_1$ $y=\frac{3x_1{}^2+a}{2y_1}(x_1-x)-y_1$
Поле характеристики $p=3$	$y^2=x^3+ax^2+bx+c$	$x=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2-a$ $y=\frac{y_2-y_1}{x_2-x_1}(x_1-x)-y_1$	$x=\left(\frac{ax_1-b}{y_1}\right)^2-a+x_1$ $y=\frac{ax_1-b}{y_1}(x_1-x)-y_1$
Поле характеристики $p=2$ Суперсингулярная кривая	$y^2+ay=x^3+ax+b$	$x=\left(\frac{y_2+y_1}{x_2+x_1}\right)^2+x_1+x_2$ $y=\frac{y_2+y_1}{x_2+x_1}(x_1+x)+y_1+a$	$x=\frac{x_1{}^4+b^2}{a^2}$ $y=\frac{x_1^2+b}{a}(x_1+x)+y_1+a$
Поле характеристики $p=2$ Несуперсингулярная кривая	$y^2+axy=x^3+bx^2+c$	$x=\left(\frac{y_2+y_1}{x_2+x_1}\right)^2+\frac{y_2+y_1}{x_2+x_1}+x_1+x_2+b$ $y=\frac{y_2+y_1}{x_2+x_1}(x_1+x)+y_1+x$	$x=x_1^2+\frac{y_1^2}{x_1^2}+x_1+\frac{y_1}{x_1}+b$ $y=x_1^2+\frac{x_1^2+y_1}{x_1}x+x$

2. We have mentioned two classes of elliptic curves over $\mathbb{F}_p$ for which the ECDLP is considered to be easier than in the general case. Name and describe one of these classes.

The two classes we mentioned were **supersingular** and **anomalous**.

For our purposes, we said an elliptic curve E over $\mathbb{F}_p$ was *supersingular* if $|E(\mathbb{F}_p)| = p + 1$. E was called *anomalous* if $|E(\mathbb{F}_p)| = p$.

You did not have to specify why these curves made the ECDLP easier, but in the supersingular case, one can reduce the ECDLP to the DLP in $\mathbb{F}_{p^k}^*$ for $k \in \{1, 2\}$ (which can be solved in subexponential time using index calculus). In the anomalous case, one can reduce the ECDLP to a computation which runs in time $O(\log p)$.

Задача дискретного логарифмирования в группе точек эллиптической кривой

Стойкость основного криптографического преобразования, используемого при вычислении цифровой подписи на эллиптической кривой, определяется сложностью решения задачи дискретного логарифмирования в циклической подгруппе $\langle P \rangle$ большого простого порядка *n* группы точек эллиптической кривой, т.е. сложностью решения уравнения

$$Q = kP, Q \in \langle P \rangle,$$

относительно *k*, *k* – целое число, 1<*k*<*n*.

Напомним, что сложность решения задачи, задаваемой входной последовательностью длиной *t* битов, определяется как число битовых операций $L(t)$, которые необходимо выполнить для получения решения. Если функция $L(t)$ представляет собой многочлен, то такая задача имеет полиномиальную сложность и считается простой. В качестве примеров таких задач можно привести задачу возведения целого числа в степень по модулю целого числа, задачу вычисления наибольшего общего делителя двух целых чисел или задачу доказательства простоты целого числа. Если функция $L(t)$ имеет вид $L(t) = e^{\lambda t}$, где λ-постоянная, то говорят, что задача имеет экспоненциальную сложность. Такие задачи считаются очень сложными и представляют наибольший интерес для криптографии, использующей несимметричные алгоритмы. В теории сложности рассматриваются функции $L(t)$, имеющие промежуточную скорость роста. Эти функции зависят от трех параметров и имеют вид $L(t, v, \lambda) = \exp\left(\lambda t^v (\log t)^{1-v}\right)$, где $0 \le v \le 1, \quad \lambda > 0$. При v=0 $L(t,0,\lambda) = t^\lambda$ получаем полиномиальную сложность, при v=1 $L(t,1,\lambda) = e^{\lambda t}$ имеем экспоненциальную сложность. Если же 0<v<1, то эта промежуточная сложность называется субэкспоненциальной. В нашем случае длина входной последовательности для задач дискретного логарифмирования – это длина двоичного представления числа *n*, т.е. $t = \lceil \log n \rceil$. Поэтому применительно к задаче дискретного логарифмирования экспоненциальная сложность имеет порядок роста n^λ, а субэкспоненциальная сложность для задачи дискретного логарифмирования имеет порядок $\exp\left(\lambda (\log n)^v (\log\log n)^{1-v}\right)$. Очевидно, что чем меньше *v*, тем проще в вычислительном значении задаче и, значит, практически она может быть решена для больших значений *n*.

В произвольной конечной циклической группе (и, следовательно, группе $\langle P \rangle$) задачу дискретного логарифмирования можно решить за $\sqrt{n}$ операций, например, с помощью метода Шэнкса. Это метод заключается в составлении двух списков размером $t = \sqrt{n}$ каждый. Первый список состоит из пар $\{(i, itP),\ i = 0, \text{K}, t-1\}$ и отсортирован по второй компоненте. Второй список состоит из пар вида $\{(j, Q + jP),\ j = 0, \text{K}, t-1\}$ и тоже отсортирован по второй компоненте. Такая

упорядоченность списков позволяет легко найти две пары с равными вторыми компонентами, т.е. (i, itP) и $(j, Q + jP)$ с $itP = Q + jP$. Тогда $k = it - j$ по модулю *n*. Для реализации этого метода требуется достаточно много памяти для хранения таблиц. Дж.Поллард [10] предложил два метода поиска аналогичного совпадения с помощью случайных блужданий, для реализации которых память не нужна.

В этих методах сначала определяется случайное блуждание в группе $\langle P \rangle$. Для этого выбирается небольшой набор точек группы вида $M_i = a_i P + b_i Q, i = 1, \text{K}, s$, s – параметр, зависящий от реализации (обычно, 20-30), a_i, b_i - случайные целые числа, и определяется отображение *f* группы $\langle P \rangle$ в множество целых чисел $\{1, 2, \text{K}, s\}$. Если теперь взять произвольную начальную точку G_0 группы $\langle P \rangle$, то отображение $G_{i-1} \to G_i = G_{i-1} + M_{f(G_{i-1})}, i \geq 1$, определяет случайное блуждание в группе $\langle P \rangle$. Поскольку группа $\langle P \rangle$ – конечная, рано или поздно две точки этого случайного блуждания совпадут, т.е. для некоторых индексов *i* и *l* $x_i P + \overline{x}_i Q = x_l P + \overline{x}_l Q$. Отсюда сразу следует, что $(x_i - x_l)P = (\overline{x}_l - \overline{x}_i)Q$, т.е. $k = (x_i - x_l)(\overline{x}_l - \overline{x}_i)^{-1} \bmod n$, если только НОД$(\overline{x}_l - \overline{x}_i, n) = 1$. Давно известен эффективный алгоритм Флойда поиска циклов в случайных блужданиях [11], а из теории случайных блужданий известно, что среднее время до такого совпадения имеет порядок $\sqrt{n}$ (см., например, [12]). Этот метод называется ρ -методом Полларда.

Второй метод Полларда называется λ-методом . В этом методе параллельно строится два случайных блуждания G_i и H_i с разными начальными состояниями. Снова ищется совпадение точек , только на этот раз точки относятся к разным блужданиям. Когда совпадение найдено, решение задачи дискретного логарифмирования находится тем же способом, что и в ρ-методе. Сложность λ-метода тоже равна $\sqrt{n}$. При очень большом сходстве λ-метод обладает серьезными преимуществами. Во-первых, он хорошо распараллеливается [13] в больших распределенных вычислительных системах типа Интернета, поскольку в отличие от ρ -метода не требует постоянного контакта с сервером. Во-вторых, на самом деле сложность λ-метода равна квадратному корню из длины интервала, который содержит решение задачи дискретного логарифмирования. Это означает, что если известно, что решение этой задачи не распределено равномерно во всем интервале от 1 до *n*-1, то его можно найти существенно быстрее. Именно этот метод был использован в апреле 2000г. для решения задачи дискретного логарифмирования в группе точек эллиптической кривой

$$y^2 + xy = x^3 + x^2 + 1$$

над полем $GF(2^{109})$, порядок которой равен 324518553658426701487448656461467 (108 бит), в рамках организованного группой французских специалистов международного проекта. Задача была решена за 4 месяца с помощью 9500 компьютеров с использованием ресурсов Интернета. Заметим, что выполненного объема вычислений хватило бы для решения 50 задач факторизации 512-битовых чисел. Для решения аналогичной задачи в поле $GF(2^{163})$ с использованием той же вычислительной техники и точно такого же алгоритма потребовалось бы примерно 40 000 000 лет. Этот пример отлично иллюстрирует разницу между алгоритмами экспоненциальной и субэкспоненциальной сложности.

Хорошо известно, что для многих конечных циклических групп существуют алгоритмы решения задачи дискретного логарифмирования субэкспоненцальной сложности. На данный момент самым мощным методом решения рассматриваемой задачи в мультипликативной группе простого конечного поля является метод решета в полях алгебраических чисел (NFS), предложенный Дж.Поллардом [14] для задачи факторизации и перенесенный затем на задачу дискретного логарифмирования [15]. Этот метод позволяет довести значение параметра *v* до 1/3. О мощи этого метода говорит выполненное в августе 1999г. разложение на простые множители целого числа размером в 512 бит. Алгоритм дискретного логарифмирования в поле характеристики 2 с таким же значением параметра *v* был создан Д.Копперсмитом еще раньше [16]. Субэкспоненциальные алгоритмы со значением параметра *v*=1/2 созданы также для якобианов гиперэллиптических кривых большого рода [17] и малого рода (*g*<16) [18].

Все попытки создания субэкспоненцальных алгоритмов для эллиптических кривых закончились неудачей и тому есть серьезные причины. Дело в том, что при создании алгоритмов субэкспоннциальной сложности исходная группа вкладывается в кольцо, в котором существует много малых простых элементов. Например, в субэкспоненциальном алгоритме вычисления дискретного

логарифма в мультипликативной группе простого поля существенно используется тот факт, что случайное целое число с достаточно большой вероятностью можно разложить на простые множители небольшого размера. Аналогичным свойством обладают и целые алгебраические числа, где существует богатый набор целых простых алгебраических чисел, имеющих небольшую норму, а также кольцо многочленов над конечным полем, где достаточно много неприводимых многочленов небольшой степени. На эллиптических кривых точек с такими свойствами нет. Этот факт Н.Коблиц назвал золотым щитом, оберегающим эллиптическую криптографию.

Хотя в самой группе точек эллиптической кривой нет субэкспоненциальных алгоритмов дискретного логарифмирования и маловероятно их появление в будущем, всегда есть возможность сведения исходной задачи дискретного логарифмирования к аналогичной задаче в других группах, где субэкспоненциальные алгоритмы существуют. При определенных условиях это дает возможность получить субэкспоненциальный алгоритм для исходной задачи.

Первое такое сведение построено в 1963 г. А.Менезес, Т.Окамото и С.Вэнстон [4] построили с помощью спаривания Вейля сведение исходной задачи над полем $GF\left(2^m\right)$ к задаче дискретного логарифмирования в мультипликативной группе некоторого расширения $GF\left(2^{km}\right)$ исходного поля. Если степень расширения *k* мала, то для исходной задачи дискретного логарифмирования существует субэкспоненциальный алгоритм. Например, в случае крайне привлекательных с вычислительной точки зрения суперсингулярных кривых $k \le 6$, поэтому пришлось отказаться от применения таких кривых в криптографии. Известно легко проверяемое условие (условие Менезеса-Окамото-Вэнстона), с помощью которого можно выбрать кривую с любым заданным значением *k*. В интересующем нас диапазоне полей достаточно, чтобы *k*>30. Это условие можно назвать локальным в том смысле, что над любым полем существует много кривых, на которых задача дискретного логарифмирования не сводится к субэкспоненциальному случаю и проверка несводимости проводится индивидуально для каждой конкретной кривой. Аналогичное сведение выполняется и с помощью спаривания Тейта [21]. Условие несводимости остается прежним.

Недавно было показано [18], что задача дискретного логарифмирования в группе точек эллиптической кривой сводится к задаче дискретного логарифмирования в якобиане некоторой гиперэллиптической кривой рода $g = 2^{k-1}$, *k* – некоторое число. Если *k*=1, то род *g*=1 и гиперэллиптическая кривая на самом является эллиптической, т.е. в этом случае субэкспоненциального алгоритма не существует. Этому условию удовлетворяют аномальные эллиптические кривые. Если же k>1, то при малом $g = 2^{k-1}$ применим субэкспоненциальный алгоритм [18], при больших $g = 2^{k-1}$ применим субэкспоненциальный по *g* алгоритм [17]. Понятно, что для больших *g* субэкспоненциальность по *g* означает экспоненциальность по *k*, поэтому если *k*=*m*, то субэкспоненциальное сведение становится невозможным. Это условие оказывается глобальным в том смысле, что для каждого конкретного поля почти все кривые над этим полем сводятся или не сводятся к субэкспоненциальному случаю. Таким образом, это условие отбраковывает целиком поля. В результате оказалось, что все поля, степень которых – составное число, не пригодны для криптографических применений. Что же касается полей, степень которых – простое число, то в практически интересном диапазоне *k*=*m* и кривые над этими полями можно использовать в криптографических целях.

Из проведенного анализа следует, что эллиптические кривые, предназначенные для построения криптографических алгоритмов, в частности, алгоритмов вычисления и проверки цифровой подписи, должны удовлетворять следующим требованиям.

- Порядок *n* циклической группы эллиптической кривой должен быть простым числом для исключения применения метода Полига-Хеллмана [31].
- Порядок *n* циклической группы эллиптической кривой должен быть достаточно большим для исключения применения методов экспоненциальной сложности с учетом возможности их распараллеливания. Принимая во внимание перспективы развития вычислительной техники на ближайшие 5-10 лет порядок *n* должен быть не менее 2^{160}.
- Порядок *n* циклической группы эллиптической кривой должен удовлетворять условию Менезеса-Окамото-Вэнстона для исключения сведения задачи дискретного логарифмирования в этой циклической группе к задаче дискретного логарифмирования в мультипликативной группе расширения исходного поля степени менее 30.
- Поле определения эллиптической кривой должно иметь простую степень для исключения сведения задачи дискретного логарифмирования в циклической группе этой кривой к задаче дискретного логарифмирования в якобиане гиперэллиптической кривой рода менее 2^{20}.

Способы представления элементов поля определения и точек эллиптических кривых и методы выполнения операций никак не влияют на криптографическую стойкость цифровой подписи, в

частности, построение эллиптических кривых и методы вычисления их порядка могут быть любыми, лишь бы выполнялись сформулированные выше требования.