Эллиптические кривые

Лекция №7

Сравнение ECC и RSA

Зачем нужны эллиптические кривые, если системы RSA, Эль-Гамаля и алгоритм Диффи-Хеллмана и так работают хорошо?

Простой ответ дал NIST, представив таблицу сравнения размеров ключей RSA и ECC, необходимых для получения одинакового уровня защиты.

Размер ключа RSA (биты)	Размер ключа ECC (биты)
1024	160
2048	224
3072	256
7680	384
15360	521

Авторы ECC

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

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

Эллиптическая кривая (ЭК)

- **Эллиптическая кривая (ЭК)** — это просто множество точек, описываемое уравнением *Вейерштрасса:*

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

где коэффициенты **a** и **b** удовлетворяют неравенству

$$4a^3 + 27b^2 \neq 0$$

(это необходимо, чтобы исключить особые кривые)

- http://mathworld.wolfram.com/EllipticCurve.html - более детальное описание эллиптических кривых

Условие несингулярности ЭК

- **Эллиптическая кривая** над полем действительных чисел задается уравнением:

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

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

- Тогда график этой кривой будет **симметричен** относительно оси абсцисс и точки его пересечения с этой осью – это корни кубического уравнения:

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

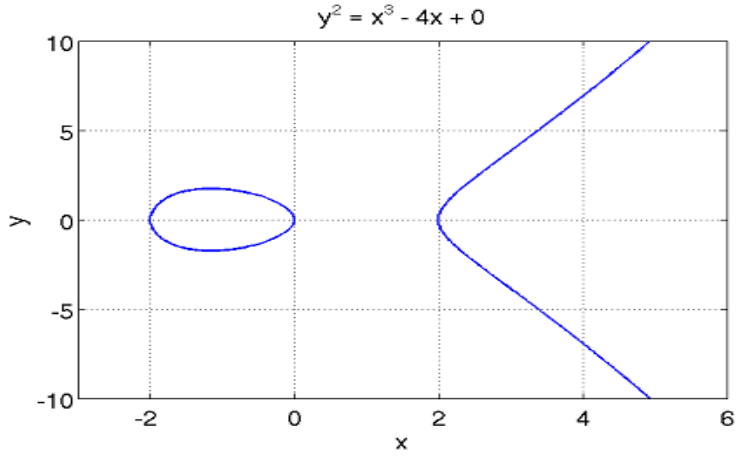
- **Дискриминант** этого уравнения:

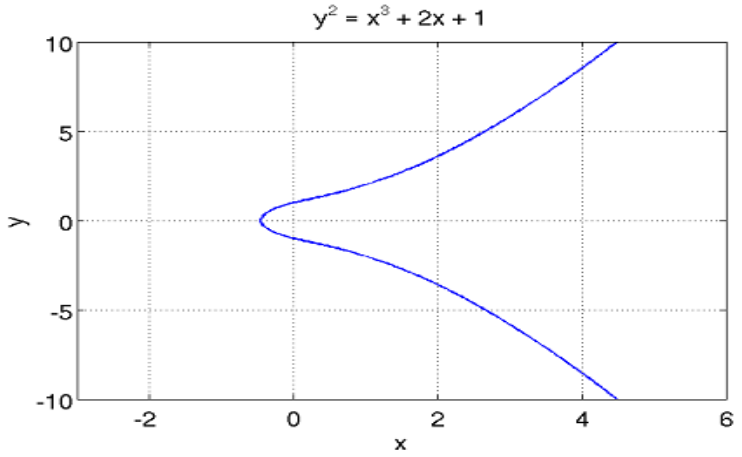
$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$$

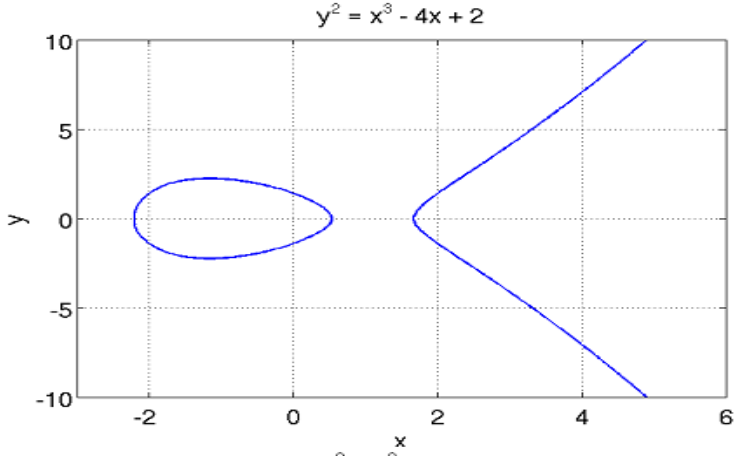
Условие несингулярности ЭК

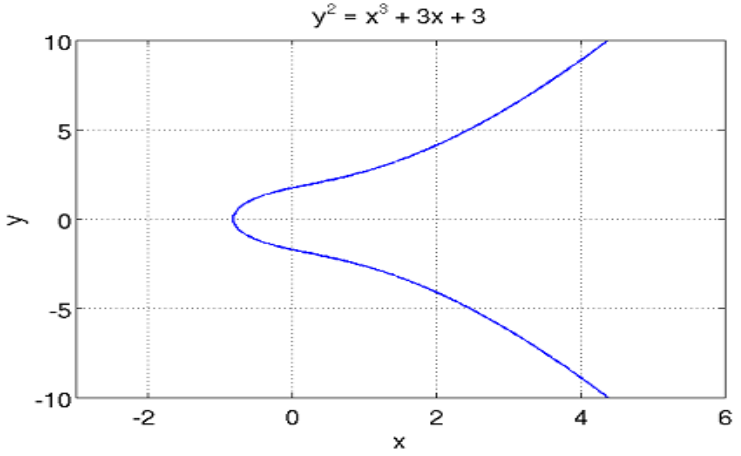
- если **D < 0**, то уравнение имеет три разных действительных корня (кривая №1)
- если **D = 0**, то уравнение имеет три действительных корня, два из которых являются одинаковыми (кривая №2)
- если **D > 0**, то уравнение имеет один действительный корень (кривая №3)

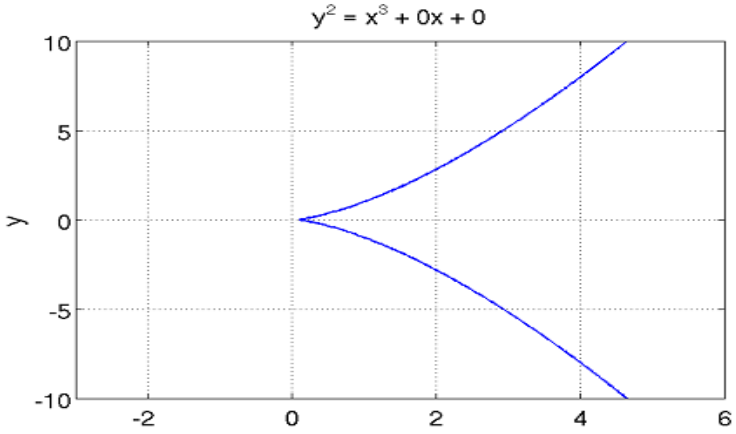
- То есть кривая $y^2 = x^3 + ax + b$ будет **несингулярной**, при условии, что ее дискриминант $D \neq 0$, а это выполняется при условии когда $4a^3 + 27b^2 \neq 0$

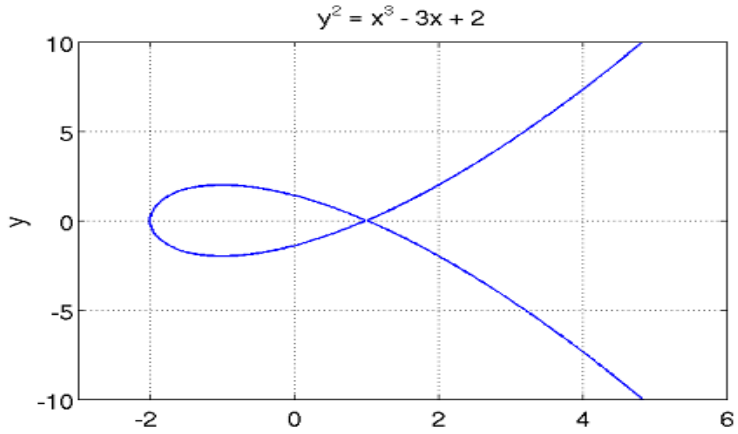

$y^2 = x^3 - 4x + 0$
10
5
0
-5
-10
-2
0
2
4
6
x
y


$y^2 = x^3 + 2x + 1$
10
5
0
-5
-10
-2
0
2
4
6
x
y


$y^2 = x^3 - 4x + 2$
10
5
0
-5
-10
-2
0
2
4
6
x
y

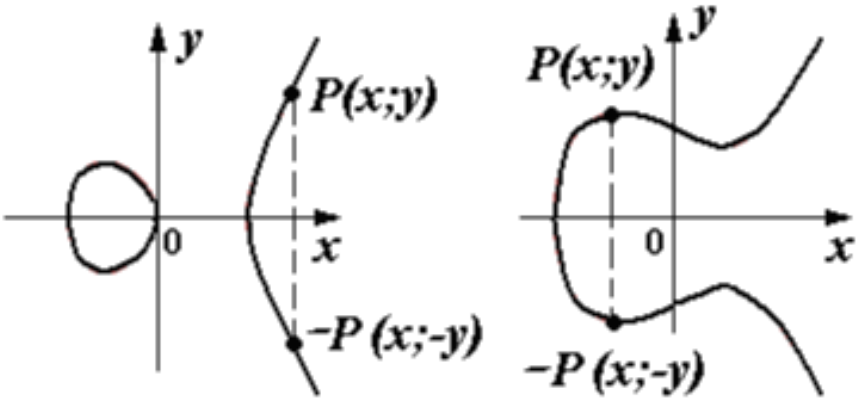

$y^2 = x^3 + 3x + 3$
10
5
0
-5
-10
-2
0
2
4
6
x
y


$y^2 = x^3 + 0x + 0$
10
5
0
-5
-10
-2
0
2
4
6
y


$y^2 = x^3 - 3x + 2$
10
5
0
-5
-10
-2
0
2
4
6
y

Определение обратной точки ЭК

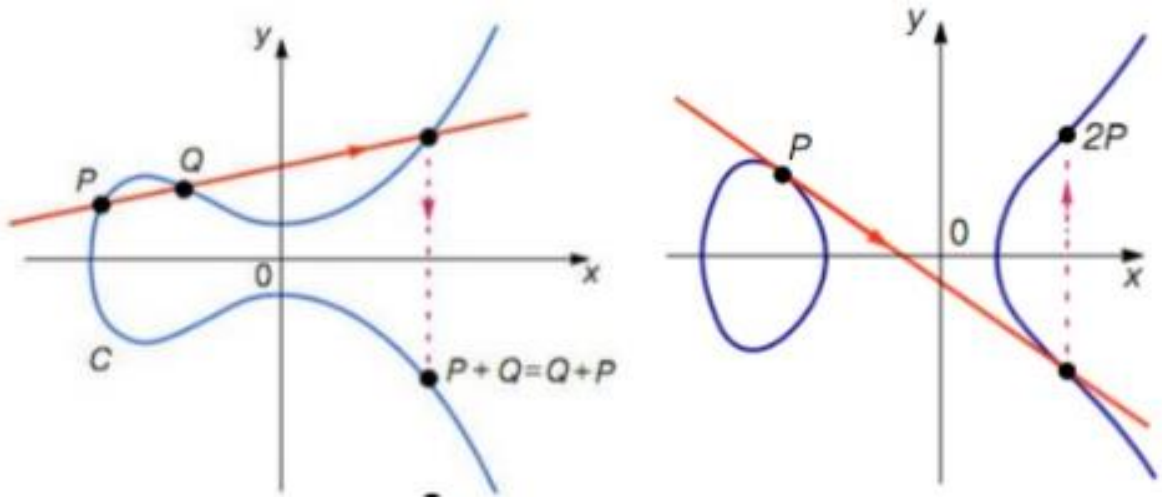
- Симметрия кривой относительно оси абсцисс дает наглядное определением **обратной точки**
- **Обратной точкой** для точки $P(x; y)$ на эллиптической кривой называют точку $-P(x; -y)$



Свойства несингулярных кривых

Несингулярные кривые обладают двумя очень важными свойствами:

- **Свойство №1**: Любая прямая, проходящая через **две различные точки** кривой всегда пересекает эту кривую еще в **одной единственной** точке
- **Свойство №2**: Касательная к эллиптической кривой в **любой точке** пересекает эту кривую еще в **одной единственной** точке



Бесконечно удаленная точка

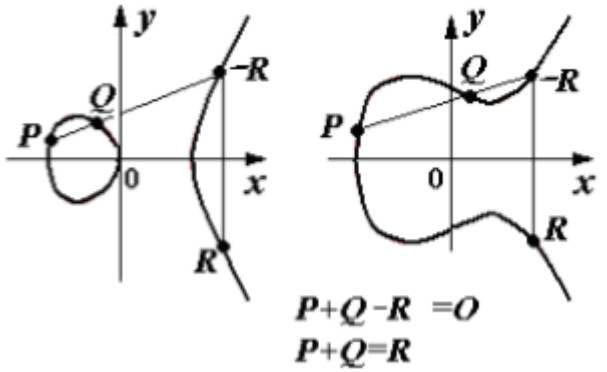
- Исключением является случай, когда точка проходит через прямые P и $-P$ – она будет перпендикулярна оси абсцисс, поэтому нам понадобится, чтобы частью кривой являлась **бесконечно удалённая точка** (также известная как идеальная точка). С этого момента мы будем обозначать бесконечно удалённую точку символом **0** (ноль)

$$\left\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0\right\} \cup \{0\}$$

- **Бесконечно удалённая точка** — математический объект, в разных математических теориях представляющий геометрическую актуальную бесконечность

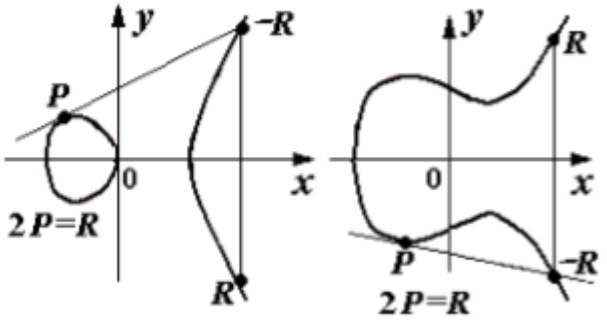
Свойства несингулярных кривых

- **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**



- Если суммируемые точки **P** и **Q** совпадают то **P + Q = P + P = R**, что равносильно **удвоению точки**

2P = R



Сложение и удвоение точек

- 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 нам нужно рассмотреть два случая:
- Когда $P \neq Q$ - мы получим формулу для **скалярного сложения** двух точек ЭК
- Когда $P = Q$ - мы получим формулу для **скалярного умножения** (точнее пока удвоения) двух точек ЭК
- Получившиеся формулы будем использовать для того чтобы выполнять операции сложения и умножения точек эллиптических кривых
- Подробное решение можно найти здесь: https://habr.com/ru/post/335906/

Сложение и удвоение точек

Сложение:

$$P=(x_1,y_1), Q=(x_2,y_2)$$

$$P+Q=(x_3,y_3)$$

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2$$

$$y_3=-y_1+\frac{y_2-y_1}{x_2-x_1}(x_1-x_3)$$

Удвоение

$$P=(x_1,y_1)$$

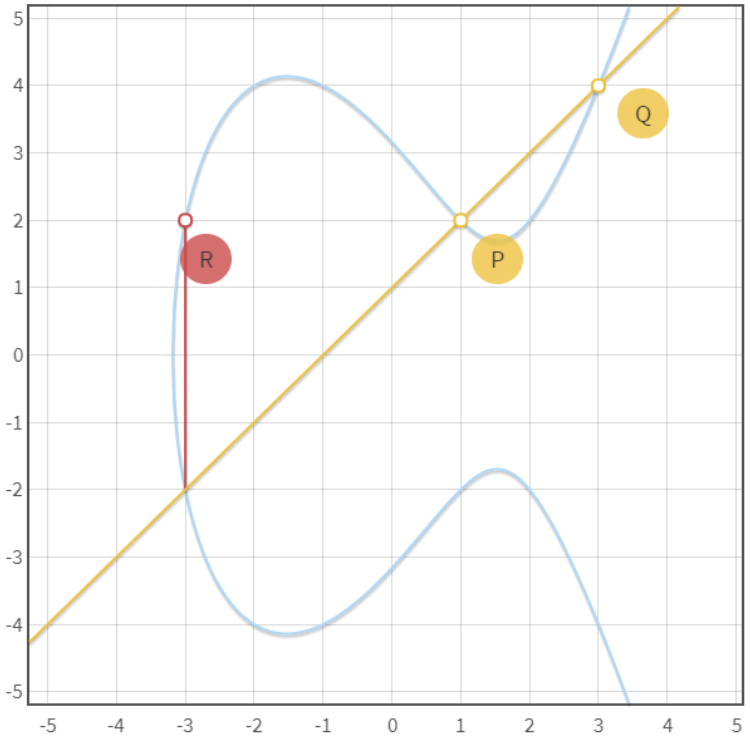
$$2P=(x_2,y_2)$$

$$x_2=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1$$

$$y_2=-y_1+\frac{3x_1^2+a}{2y_1}(x_1-x_2)$$

- Формулы сложения и удвоения точек эллиптической кривой справедливы для всех полей, в том числе и конечных

Пример сложения P=(1,2), Q=(3,4)



Curve:	a	-7	b	10
P:	x	1	y	2
Q:	x	3	y	4
$R = P + Q$:	x	-3	y	2

Point addition over the elliptic curve $y^2 = x^3 - 7x + 10$ in $\mathbb{R}$.

https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html

Определение группы

В математике **группа** — это множество, для которого мы определили двоичную операцию, называемую «сложением» и обозначаемую символом **+**. Чтобы множество **G** было группой, сложение нужно определить таким образом, чтобы оно соответствовало четырём следующим свойствам:

1. **Замыкание**: если ***a*** и ***b*** входят в **G**, то ***a + b*** входит в **G**
2. **Ассоциативность**: $(a + b) + c = a + (b + c)$
3. Существует **единичный элемент** 0, такой, что:

$$a + 0 = 0 + a = a$$

4. У каждого элемента есть **обратная величина**, то есть:

для каждого ***a*** существует такое ***b***, что $a + b = 0$

Если мы добавим пятое требование:

5. **Коммутативность**: если $a + b = b + a$, то группа называется **абелевой группой**

ЭК над полем F_P

Множество точек, которые ранее имели следующий вид

$$\{(x,y) \in \mathbb{R}^2 \quad | \quad y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0\} \cup \{0\}$$

Теперь превращаются

$$\{(x,y) \in (\mathbb{F}_p)^2 \quad | \quad y^2 \equiv x^3 + ax + b \pmod{p}, \quad 4a^3 + 27b^2 \not\equiv 0 \pmod{p}\} \cup \{0\}$$

ЭК над полем F_P

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 $R(x_3; y_3) = 2P(x_1; y_1)$	$\lambda = \frac{3x_1^2 + a}{2y_1} (\mathrm{mod}\, p);$ $x_3 = \lambda^2 - 2x_1 (\mathrm{mod}\, p);$ $y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p)$
$O + O = O;$ $P(x; y) + O = P(x; y);$ $P(x; y) + P(x; -y) = O$	

Поиск всех точек ЭК над GF(p)

Так можно найти точки только при малом p

1. Для каждого целого значения x, где $0 \leq x \leq p$, вычислить y^2 по формуле $y^2 = x^3 + ax + b \ (mod\ p)$
2. Для всех значений y^2 выяснить будут ли они квадратичными вычетами по модулю p, то есть можно ли из них извлечь квадратный корень. Это можно сделать вычислив значение $\left(\frac{y^2}{p}\right)$ - в математике это называется символом Лежандра
   - Если $\left(\frac{y^2}{p}\right) = 1$, то является вычетом
   - Если $\left(\frac{y^2}{p}\right) = -1$, то не является вычетом

   Если выполнено первое условие и корень существует, то необходимо найти два значения корня y_1 и y_2

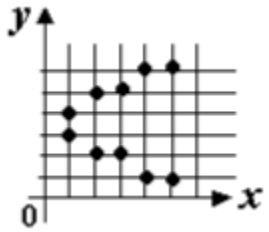
Поиск всех точек ЭК над GF(p)

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

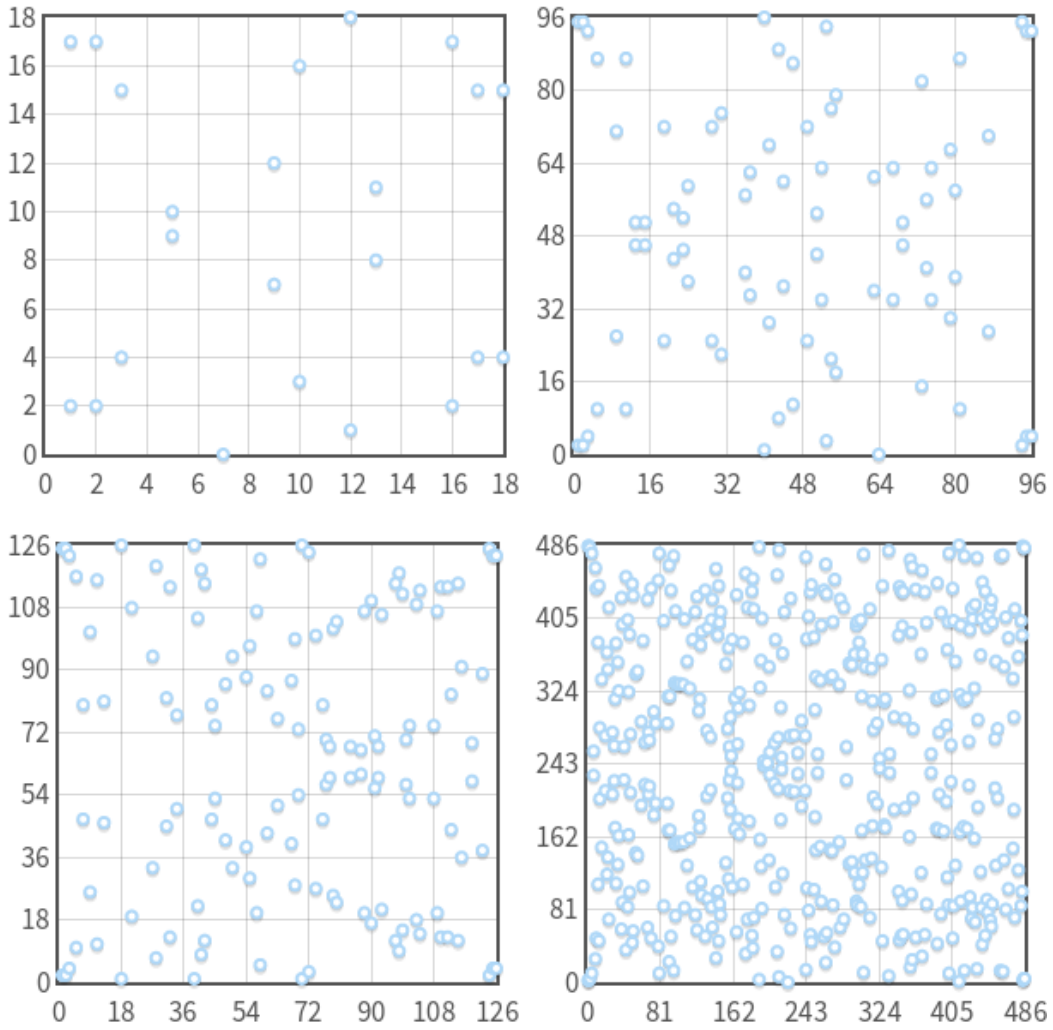
Решение:
$E_7(2,6)$ - это кривая $y^2 = x^3 + 2x + 6\ (mod\ 7)$
Посчитаем все значения $x^3 + 2x + 6\ (mod\ 7)$ и $y^2\ (mod\ 7)$ для всех $x, y = 1,2,3, \dots, 6$

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 для которых $x^3 + 2x + 6\ (mod\ 7) = y^2\ (mod\ 7)$. Это точки (1,3), (1,4), (2,2), (2,5), (3,2), (3,5), (4,1), (4,6), (5,1), (5,6) и 0



Примеры точек для ЭК над полем F_P



$$y^2 \equiv x^3 - 7x + 10 \pmod{p}$$

$$p = 19, 97, 127, 487$$

Порядок группы ЭК

- Эллиптическая кривая, определённая над конечным полем, имеет конечное количество точек
- Количество точек в группе называется **порядком группы**
- Проверка всех возможных значений для *x* в интервале от 0 до $P-1$ будет невыполнимым способом подсчёта точек, потому что потребует $O(p)$ шагов, а эта задача «сложна», если P - большое простое число
- Первый алгоритм для подсчета количества точек ЭК в конечном поле был предложен Рене Шуфом. Позже Эликс и Аткин внесли в него некоторые изменения, после чего он стал известен, как алгоритм SEA
- Верхнюю и нижнюю границы порядка группы определяется теоремой Хассе
- **Теорема Хассе**. Для порядка N_E группы точек ЭК над полем $GF(q)$, где q – число элементов поля справедливо неравенство:

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

Скалярное умножение

- Точку nP, равную n-кратному сложению точки P в аддитивной группе точек ЭК называют **скалярным произведением точки на число** n

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ раз}}$$

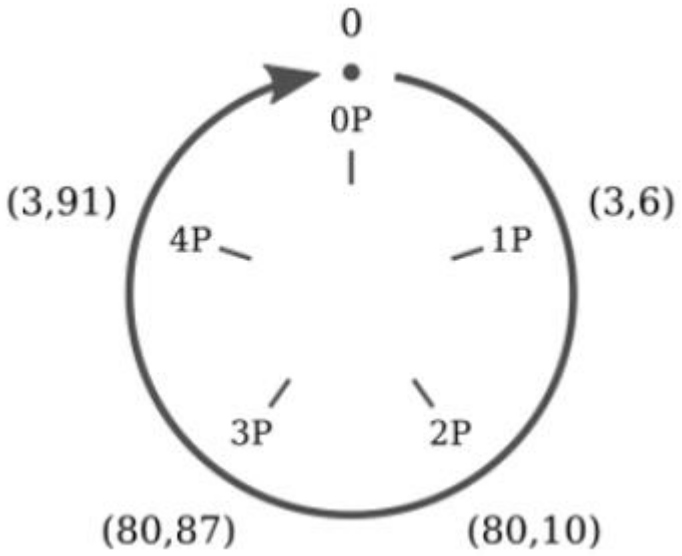
- Арифметика ЭК не содержит прямых формул умножения для вычисления кратного nP для заданной точки $P(x, y)$, поэтому данную операцию выполняют с использованием операции сложения и удвоения точки
- Для этого нужно представить число n в двоичной системе, а затем вычислить сумму точек, для которых установлены единичные биты
- **Пример**: $13_{10} = 1101_2 \rightarrow 13P = 8P + 4P + P$

Примечание:

- Умножение точки на число аналогично возведению в степень в случае RSA и требует небольшого числа сложений. Например, для умножения точки на число длиной 200 бит будет выполнено в среднем 100 операций удвоения и 66 операций сложения
- В RSA для аналогичной операции возведения в степень с показателем длиной 200 бит требуется 300 операций умножения

Скалярное умножение

- Умножение точек ЭК над конечным полем $GF(P)$ обладает интересным свойством - **цикличностью**
- Возьмем кривую $y^2 = x^3 + 2x + 3\ (mod\ 97)$ и точку $P(3,6)$ и вычислим все величины, кратные P



Циклические подгруппы

- $0P = 0$
- $1P = (3, 6)$
- $2P = (80, 10)$
- $3P = (80, 87)$
- $4P = (3, 91)$
- $5P = 0$
- $6P = (3, 6)$
- $7P = (80, 10)$
- $8P = (80, 87)$
- $9P = (3, 91)$
- ...

- $5kP = 0$
- $(5k + 1)P = P$
- $(5k + 2)P = 2P$
- $(5k + 3)P = 3P$
- $(5k + 4)P = 4P$

$$kP = (k \bmod 5)P$$

Циклические подгруппы

- То же относится и к остальным точкам, не только к $P = (3,6)$

$$nP + mP = \underbrace{P + \cdots + P}_{n \text{ раз}} + \underbrace{P + \cdots + P}_{m \text{ раз}} = (n+m)P$$

- Это означает, что если мы складываем два значения, кратных P, то получаем значение кратное P.
- Этого достаточно для того, чтобы доказать, что множество кратных P значений — это **циклическая подгруппа** группы, образованной эллиптической кривой
- «**Подгруппа**» — это группа, являющаяся подмножеством другой группы. «**Циклическая подгруппа**» — это подгруппа, элементы которой циклически повторяются, как мы показали в предыдущем примере. Точка P называется генератором или базовой точкой циклической подгруппы.

Порядок точки P

- **Порядок точки P** – это наименьшее натуральное число n, при котором выполняется условие $nP = 0$
- Например, вычислим порядок точки $P(9,4)$ для группы $E_{11}(6,3)$:
  - $2(9,4) = (7,6)$
  - $3(9,4) = (7,5)$
  - $4(9,4) = (9,7)$
  - $\mathbf{5}(9,4) = 0$

  Следовательно на кривой $E_{11}(6,3)$ порядок точки $P(9,4)$ равен 5

- Для того чтобы найти порядок n точки P эллиптической кривой нужно решить уравнение $nP = 0$

Дискретное логарифмирование

- Операция скалярного умножения – аналог операции возведения в степень в конечном поле
- 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 $mP = Q$
- Задача дискретного логарифмирования на ЭК 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 $O\sqrt{n}$)
- 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

Использование ECC

- 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 $\{1, 2, \ldots, p-1\}$	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	$g \in Z_p^*$; $h \equiv g^a \pmod p$; найти a	$P \in E(GF(p))$; $Q = mP$; найти m

Алгоритм Диффи-Хеллмана на ECC

1. Два пользователя **Алиса** и **Боб** выбирают общие параметры:
   - Эллиптическую кривую над конечным полем
   - Точку P на этой кривой, имеющую большой порядок n
2. Общие параметры передаются открытым каналом связи
3. **Алиса** случайно выбирает число c – свой секретный ключ
4. **Боб** выбирает число d – свой секретный ключ
5. **Алиса** находит свою точку $Q = cP$
6. **Боб** находит свою точку $R = dP$
7. **Алиса** и **Боб** обмениваются точками Q и R по открытому каналу
8. **Алиса**, получив точку R, вычисляет точку $S = cR$
9. **Боб**, получив точку Q, вычисляет точку $S = dQ$

Так как $cR = c(dP) = d(cP) = dQ$, то значение S – и есть общий ключ **Алисы** и **Боба**

Примечание: данный алгоритм получил название **ECDH**

Алгоритм Диффи-Хеллмана на ECC

Пример: Сгенерировать общий ключ для двух пользователей по схеме Диффи-Хеллмана, если выбрана ЭК $E_{211}(0,-4)$ и $P(2,2)$

Решение:

Кривая $E_{211}(0,-4)$ это уравнение $y^2 = x^3 - 4\ (mod\ 211)$. Порядок точки P равен 241, так как $241P = 0$

1. **Алиса** случайно выбирает число $c = 121$
2. **Боб** выбирает число $d = 203$
3. **Алиса** находит свою точку $Q = cP = 121(2,2) = (115,48)$
4. **Боб** находит свою точку $R = dP = 203(2,2) = (130,203)$
5. **Алиса** и **Боб** обмениваются точками Q и R по открытому каналу
6. **Алиса**, вычисляет точку $S = cR = 121(130,203) = (161,69)$
7. **Боб**, вычисляет точку $S = dQ = 203(115,48) = (161,69)$

В результате у **Алисы** и **Боба** получается одно и тоже число S

Система Эль-Гамаля на ECC

Генерация ключей:

1. Два пользователя **Алиса** и **Боб** выбирают общие параметры:
   - Эллиптическую кривую над конечным полем
   - Точку P на этой кривой, имеющую большой порядок n
2. Общие параметры передаются открытым каналом связи
3. **Алиса** выбирает секретный ключ a_A и находит точку $Q_A = a_A P$
4. **Боб** выбирает секретный ключ a_B и находит точку $Q_B = a_B P$

Точка Q_A – открытый ключ **Алисы**, число a_A – закрытый ключ **Алисы**

Точка Q_B – открытый ключ **Боба**, число a_B – закрытый ключ **Боба**

Система Эль-Гамаля на ECC

Шифрование:

1. **Алиса** выбирает случайное целое число k и определяет точки kP и kQ_B
2. **Алиса** вычисляет сумму $R = M + kQ_B$

Криптограмма, соответствующая шифрованию сообщения M, состоит из пары точек (kP, R). Точка kP называется **точкой-подсказкой**

3. Криптограмма (kP, R) посылается **Бобу**

Дешифрование:

1. **Боб** вычисляет $a_B \cdot kP$
2. **Боб** находит разность $R - a_B \cdot kP = M$ (вычитание заменяется сложением с обратной точкой $-a_B \cdot kP$

Поскольку $R - a_B \cdot kP = M + kQ_B - ka_BP = M$

Система Эль-Гамаля на ECC

Пример: Зашифровать и расшифровать сообщение соответствующее точке $M(12,6)$, используя ЭК $E_{23}(9,17)$ и базовую точку $P(4,5)$

Решение

Генерация ключей

1. Выберем закрытый ключ получателя $a_B = 3$
2. Найдем точку $Q_B = 3 \cdot P = 3 \cdot (4,5) = (13,13)$ - это ОК получателя

Шифрование

1. Выберем случайное число k = 5
2. Зная открытый ключ получателя найдем точку $kP = 5P = (1,21)$
3. Определим точку $kQ_B = 5(13,13) = (8,7)$
4. Вычисляем $R = M + kQ_B = (12,6) + (8,7) = (16,18)$
5. Пара точек $\{kP, R\} = \{(1,21), (16,18)\}$ является криптограммой

Дешифрование

1. Вычисляем $a_B \cdot kP = 3(1,21) = (8,7)$
2. $M = R - a_B \cdot kP = (16,18) - (8,7) = (16,18) + (8,-7) = (12,6)$

Система Эль-Гамаля на ECC

Генерация ключей

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

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

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

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

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

Система Эль-Гамаля на ECC

Шифрование

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

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

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

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

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

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: $((1,21);\ (16,18))$.

Как кодировать сообщение M?

- Для кодирования сообщения M 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 $r\mathrm{P}$ (естественно, далее точки $r\mathrm{P}$ шифруются)
- **Второй вариант** основан на следующем свойстве эллиптической кривой: для любого числа $x \leq \left[\frac{n}{2}\right]$ 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 прообразом для кода. Тогда, зная координаты (x', y') любой из точек P_1 или P_2 можно восстановить x, вычисляя целую часть $\left[\frac{x'}{2}\right]$

Поиск ЭК и базовой точки

- Для использования эллиптической криптографии участники протокола должны согласовать все параметры, определяющие эллиптическую кривую
- Генерация эллиптической кривой состоит из следующих шагов:
    1. Генерация характеристики поля Галуа (число p)
    2. Генерация коэффициентов кривой (a, b)
    3. Вычисление порядка N_E группы точек кривой
    4. Генерация базовой точки P
    5. Определение порядка базовой точки кривой h

- Для определения порядка базовой точки кривой, желательно чтобы так называемый **кофактор** $h = \frac{N_E}{n}$ был небольшим (n – это порядок точки)

Поиск ЭК и базовой точки

Алгоритм **случайного выбора:**

1. Выбираем какое-нибудь большое конечное поле $GF(q)$ с характеристикой $p > 3$, в котором кривую можно будет задать уравнением $y^2 = x^3 + ax + b$
2. Генерируем случайные числа $x, y, a \in GF(q)$
3. Вычисляем $b = y^2 - (x^3 + ax)$
4. Проверяем условие $4a^3 + 27b^2 \neq 0 \ (mod\ p)$
5. Если условие выполнено, то кривая подобрана, если нет, то выбираем другую случайную тройку $x, y, a \in GF(q)$ и возвращаемся к шагу 3
6. Когда кривая подобрана, то точка $P(x, y)$ лежит на кривой

Поиск ЭК и базовой точки

- Алгоритм **редукция глобальной пары Кривая – Точка** чаще всего используется для определения параметров ЭК
- Существует **15** эллиптических кривых, рекомендованных NIST(США)
- Федеральные стандарты обработки информации (FIPS) рекомендуют **10** конечных полей. Некоторые из них:
  - поля $GF(p)$, где p – простое и 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
- Пример одной из кривых:

$$y^2 = x^3 + 3176890812513255034763174764138276932727469559 27x + \\ + 7905289660787875871812057202571853543210065 1934.$$

Безопасность ЭК

- На сегодняшний день существуют следующие методы с помощью которых можно решить задачу **дискретного логарифмирования**:
  - Метод полного перебора
  - Алгоритм Полига – Силвера – Хеллманна
  - Алгоритм «Шаг младенца – Шаг великана»
  - P-метод Полларда
  - Параллельные вычисления по методу Полларда на r процессоров

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

Безопасность ЭК

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 $N_E = q$
- Аномальные эллиптические кривые над полем $GF(p)$, когда общее число точек на кривой $N_E = p$, где p – простое число

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