Эллиптическая криптография

Эллиптическая криптография

- Безопасность RSA и Elgamal обеспечивается ценой использования больших ключей
- Требуется альтернативный метод, который дает тот же самый уровень безопасности, но с меньшими размерами ключей
- Одним из этих перспективных вариантов является криптография на основе эллиптических кривых (*Elliptic Curve Cryptography — ECC*)

Эллиптические кривые в вещественных числах

- Эллиптические кривые обычно применяются для вычисления длины кривой в окружности эллипса:

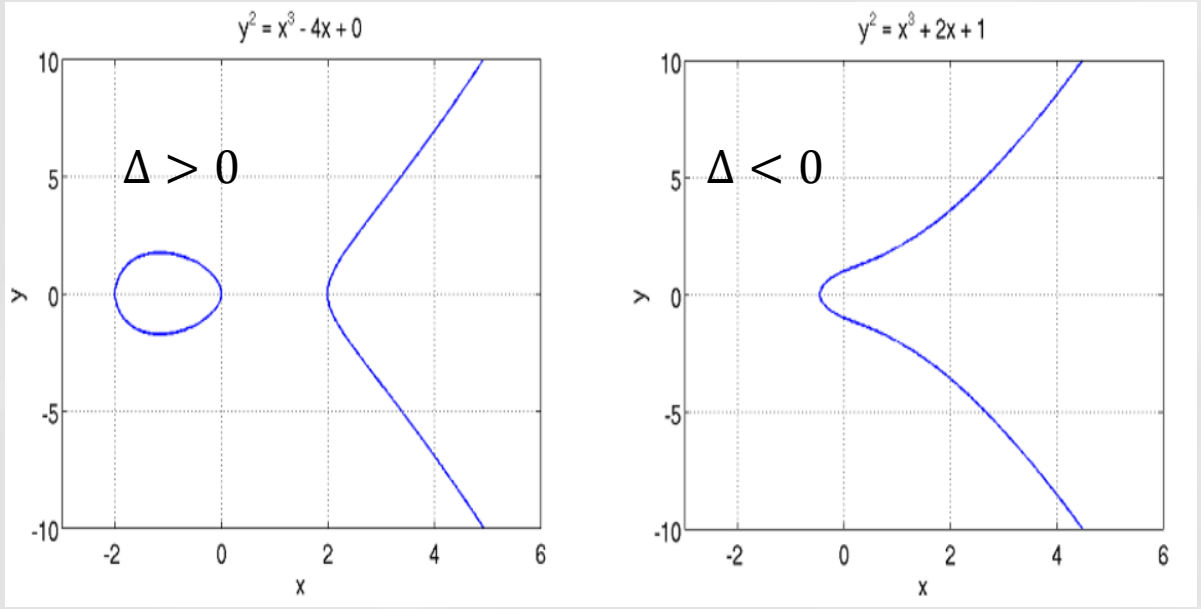
$$y^2 + \text{axy} + by = x^3 + cx^2 + \text{dx} + e$$

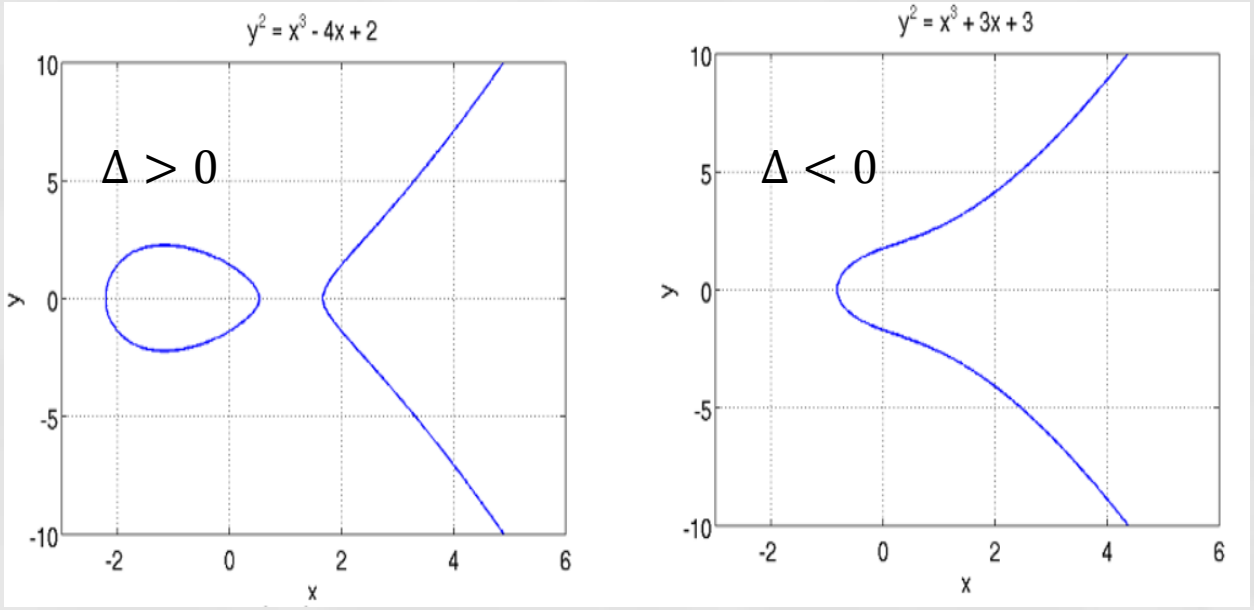
- В криптографии распространение получил частный вид эллиптических кривых (обычная формулировка Вейерштрасса):

$$y^2 = x^3 + \text{ax} + b$$

- Если дискриминат $\Delta = -16(4a^3 + 27b^2) \neq 0$, уравнение представляет несингулярную (гладкую) эллиптическую кривую, иначе сингулярную (с особыми точками)

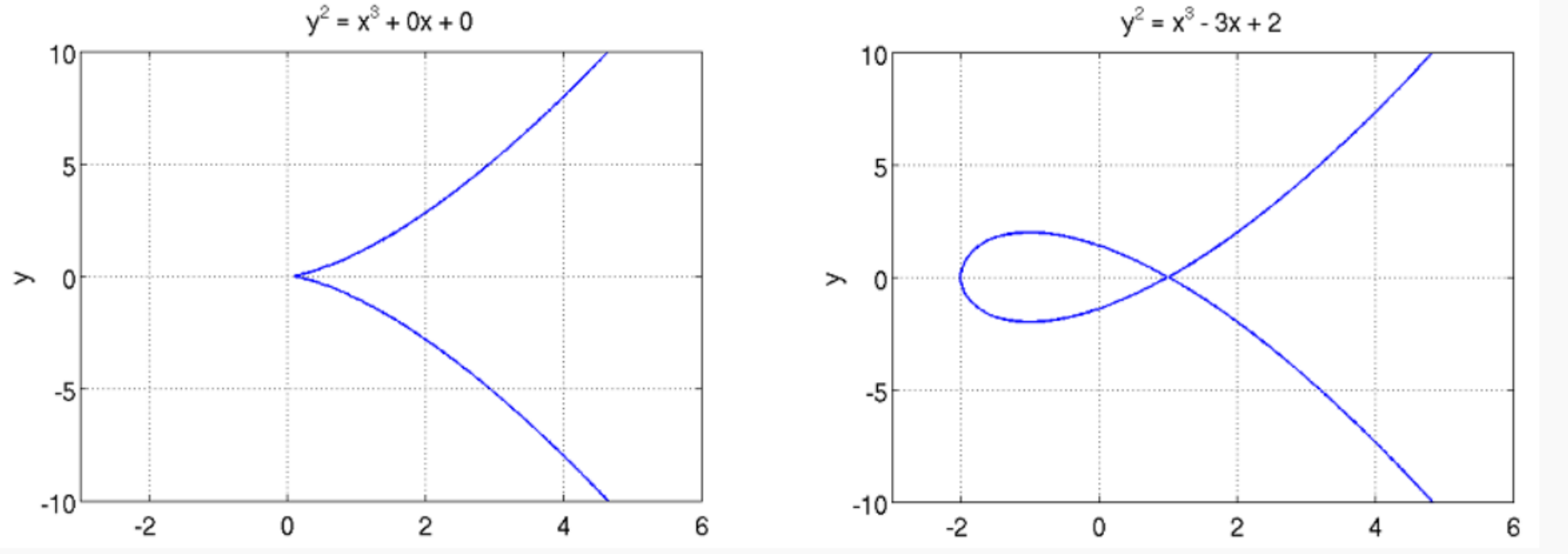
Примеры несингулярных эллиптических кривых





- График не имеет особых точек (возврата и самопересечений)
- График имеет две части, если дискриминат Δ положителен и одну часть, если значение дискриминанта Δ отрицательно
- *Замечательным свойством несингулярных кривых является то, что любая прямая, проходящая через две различные точки кривой ещё раз пересекает кривую и эта третья точка пересечения является единственной !*

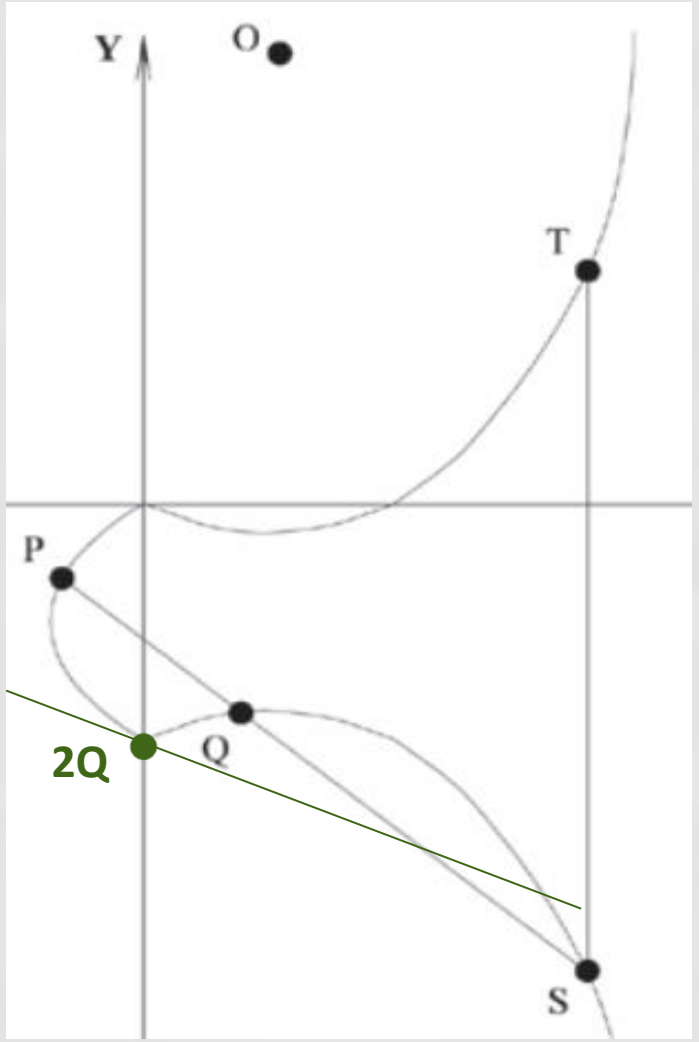
Примеры сингулярных эллиптических кривых



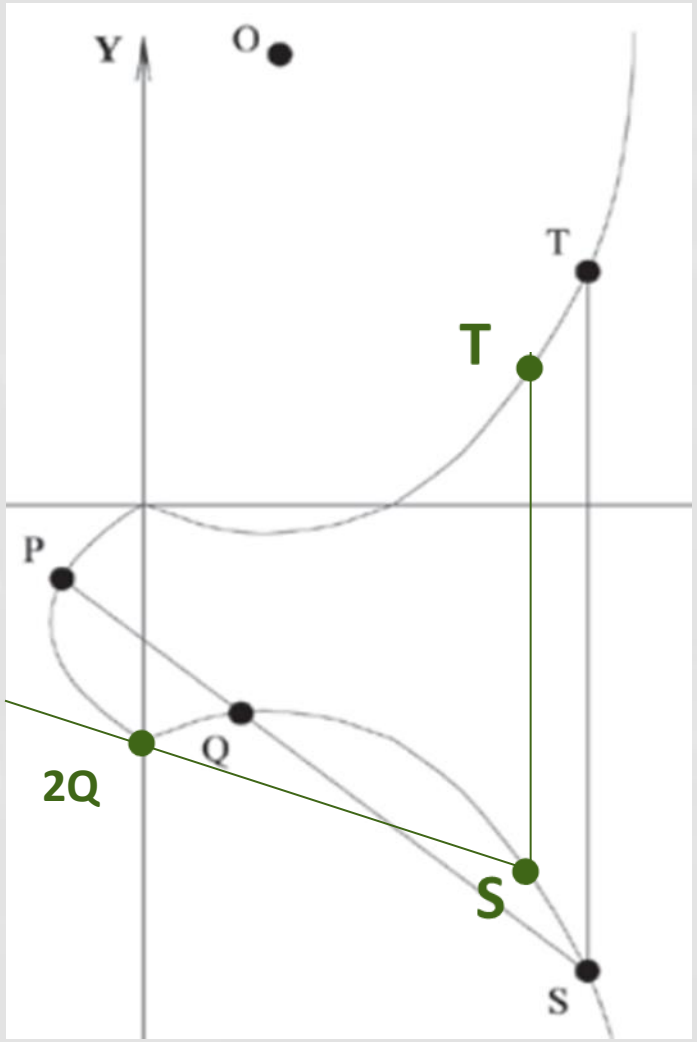
- При использовании сингулярных кривых стойкость эллиптической криптосистемы значительно снижается

Свойства точек эллиптической кривой

- Будем считать, что:
  - На плоскости существует бесконечно удаленная точка **O**, принадлежащая кривой, в которой сходятся все вертикальные прямые линии
  - Если три точки эллиптической кривой лежат на прямой линии, то их сумма есть **O**
  - Касательная к кривой пересекает точку касания два раза



Сложение точек эллиптической кривой



- Точка **O** выступает в роли нулевого элемента: **O**=-**O** и для любой точки P на кривой справедливо P + **0** = P
- Вертикальная линия пересекает кривую в двух точках с одной и той же абсциссой (координатой x), например, S = (x, y), T = (x, -y), и в бесконечно удаленной точке: S + T + **O** = **O** и T = -S
- Чтобы сложить две точки P и Q с разными координатами x, следует провести через эти точки прямую и найти точку пересечения ее с эллиптической кривой: P + Q + S = **O**
- Чтобы удвоить точку Q, следует провести касательную в точке Q и найти другую точку пересечения S с эллиптической кривой. Тогда Q + Q +S= 2 x Q +S=**O**
- Умножение точки P эллиптической кривой на положительное число k определяется как сумма k точек P

Эллиптические кривые в криптографии

- Эллиптические кривые над вещественными числами приводит нас к проблеме округления (открытые и закрытые тексты должны представляться целыми числами !) и служат геометрическими моделями операций над точками
- В криптографии используются только кривые над конечными полями, т.е. координаты точек кривой принадлежат конечному полю

Эллиптические кривые в криптографии

- Элементами эллиптической кривой являются пары неотрицательных целых чисел, которые меньше p $(p>3)$ и удовлетворяют частному виду эллиптической кривой

$$y^2 = (x^3 + ax + b) mod\ p$$

- Такую кривую будем обозначать $E_p(a, b)$. При этом числа a и b должны быть меньше p и должны удовлетворять условию $(4a^3 + 27b^2) mod\ p \neq 0$
- Любая точка на $E_p(a, b)$ вычисляется следующим образом:
  - Для значения x, $0 <= x <= p$, вычисляется $(x^3 + ax + b)\ mod\ p$
  - Для каждого из полученных на предыдущем шаге значений выясняется имеет ли это значение квадратом целого числа. Если является, то определяется y

Пример-задание

- Задана кривая $E_{13}(1,1)$: $y^2 = (x^3 + x + 1) mod\ 13$
- Заданы точки *P(4, 2), R(3,5)* и *Q(7,0)*
- Проверить принадлежность заданных точек кривой $E_{13}(1,1)$

Ответ на задание

- Для кривой $E_{13}(1,1)$ результаты проверки принадлежности точек *P(4, 2), R(3,5)* и *Q(7,0)* следующие:
  - Вычисляем $(4^3 +4+1)\ mod\ 13 = (12 + 4 + 1)\ mod\ 13=4=2^2$ (на кривой)
  - Вычисляем $(3^3 +3+1)\ mod\ 13 = (27 + 3 + 1)\ mod\ 13=5$ (вне кривой)
  - Вычисляем $(7^3 +7+1)\ mod\ 13 = (5 + 7 + 1)\ mod\ 13=0=0^2$ (на кривой)

Операции над точеками $E_p(a,b)$

- *P + **0** = P; P+Q=Q+P (коммут.); (P+Q)+R=P+(Q+R) (ассоциат.)*
- Если *P = (x,y),* то *P + (x,-y) = 0*. Точка *(x,-y)* является отрицательным значением точки *P* и обозначается -P. Точка -P лежит на эллиптической кривой, т.е. принадлежит $E_p\ (a,b)$.
- Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ определяется по следующим формулам:
- $x_3 = (\lambda^2 - x_1 - x_2)\ mod\ p \quad y_3 = (\lambda(x_1 - x_3) - y_1) mod\ p$

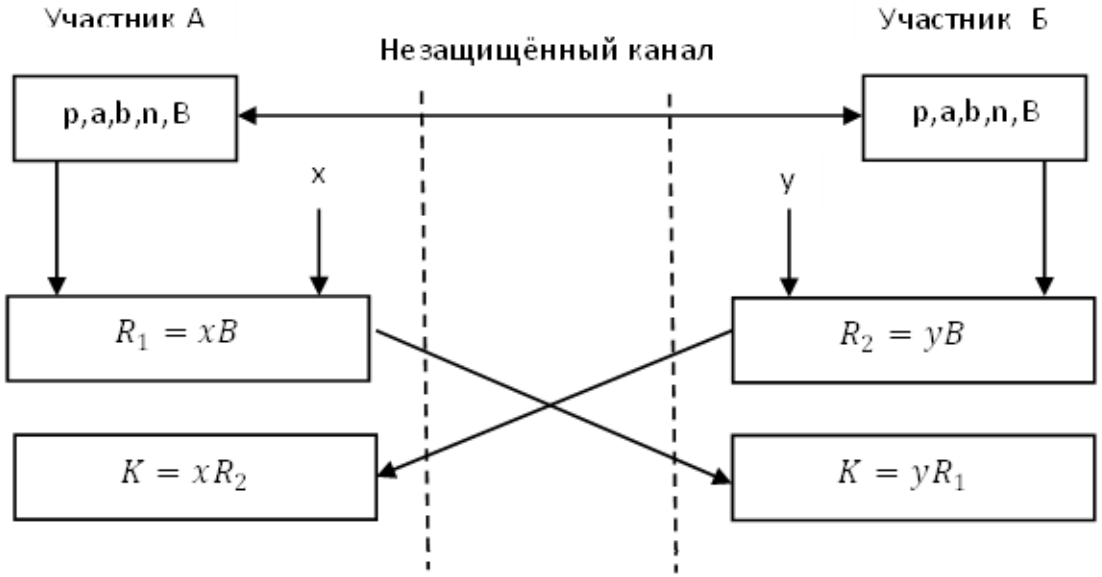
$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) mod p, & P \neq Q \\ ((3x_1^2 + a))/2y_1\ mod p, & P = Q \end{cases}$$

- λ- угловой коэффициент секущей, проведенный через точки *P* и *Q*

Свойства эллиптической кривой над конечным полем

- Точки эллиптической кривой образуют группу порядка m (количество точек кривой)
- Множество точек, кратных точки Q образуют циклическую подгруппу порядка n: $n \times Q=0$ с базовой точкой Q
- Задача поиска $k < n$, связывающего две точки циклической подгруппы зависимостью $P = k \times Q$ является вычислительно сложной
- Детали в *https://habr.com/ru/post/335906/*

Протокол Диффи-Хеллмана для эллиптических кривых (ECDH)

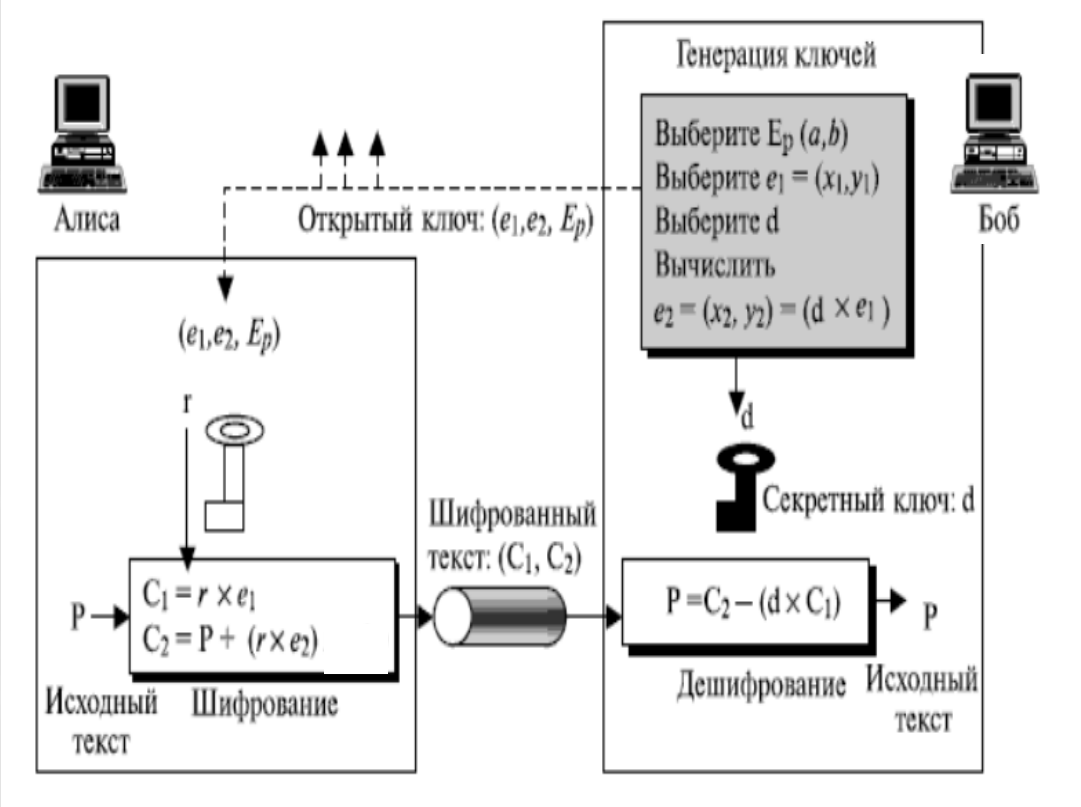


- Группа точек эллиптической кривой $E_p(a, b)$
- *B* – базовая точка (порождающий элемент) циклической подгруппы точек {kB, k=1,n} порядка n: *nB=0*
- *x, y* - большие случайные числа такие, что *0 < x < n , 0 < y < n*
- Поскольку:

$$xR_2 = x(yB) = xyB$$
$$yR_1 = y(xB) = xyB$$

- Стороны фактически создают материал для генерации симметричного ключа (координаты точки xyB)

Шифр Эль-Гамаля на эллиптических кривых



- Получатель выбирает кривую $E_p(a, b)$, точку e_1 на кривой, выбирает секретной число d и вычисляет еще одну точку $e_2 = d \times e_1$
- Открытый ключ $E_p(a, b), e_1, e_2$
- Отправитель сопоставляет открытому тексту точку P на кривой и создает шифровку C_1, C_2, выбрав случайное r

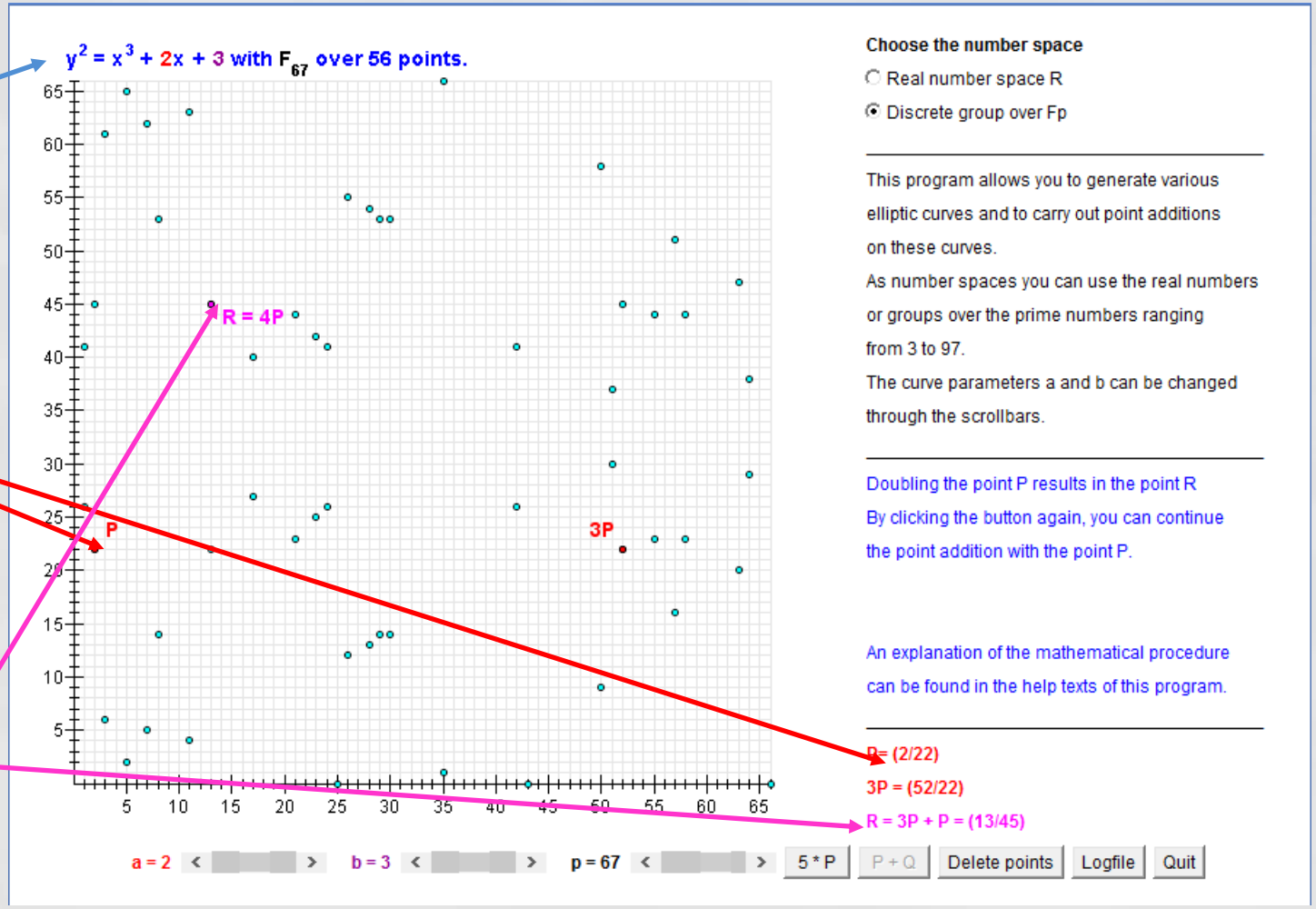
$$C_1 = r \times e_1 \quad C_2 = P + r \times e_2$$

- Получатель выполняет расшифровку:

$$C_2 - (d \times C_1) = P + r \times d \times e_1 - d \times r \times e_1 = P$$

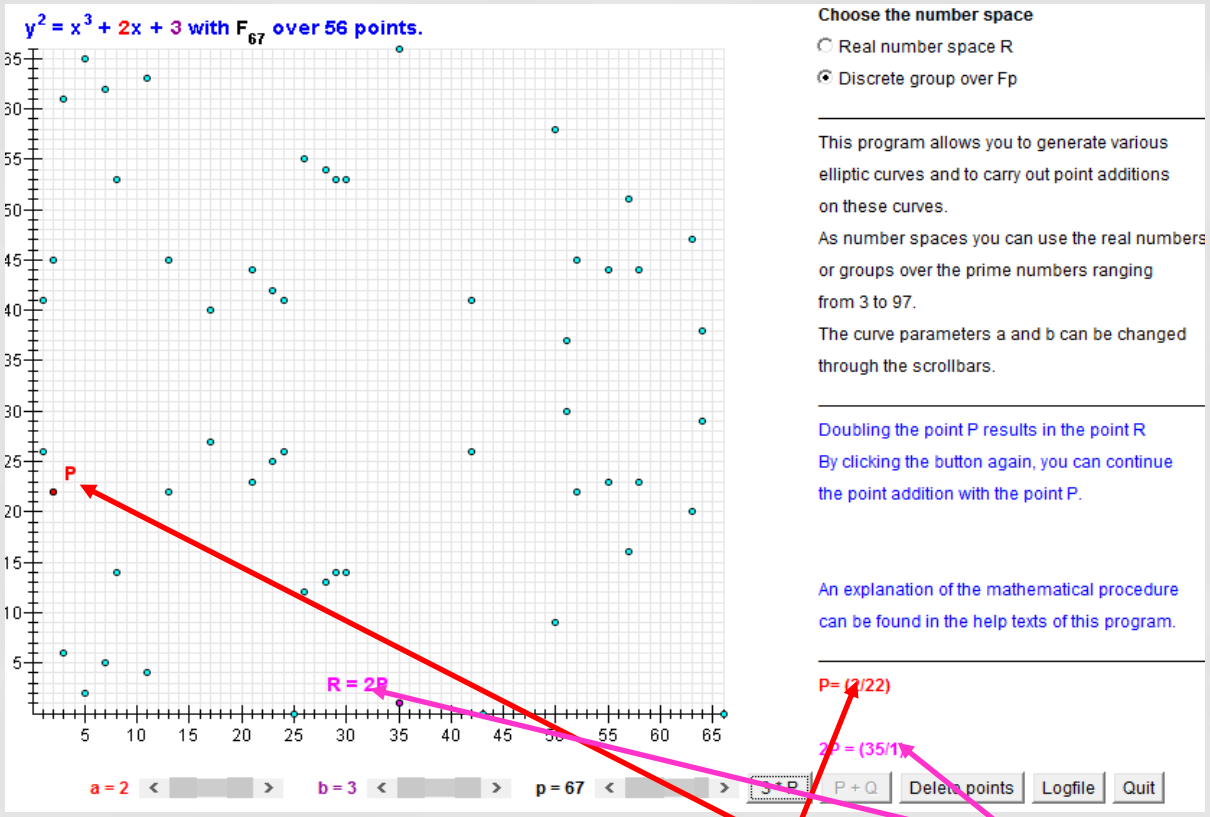
Пример генерации ключа

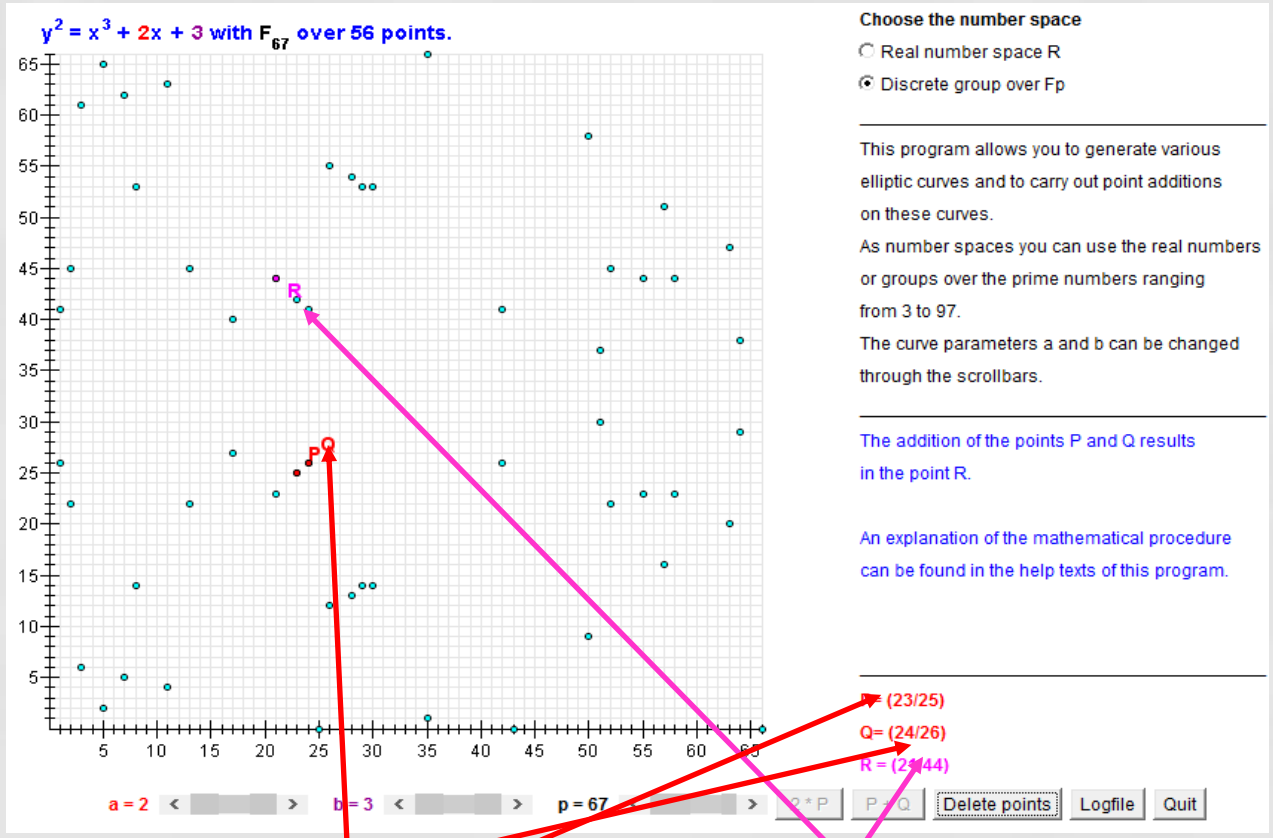
- Выбираем кривую $E_{67}(2,3)$
- Выбираем точку $e_1=(2,22)$
- Выбираем закрытый ключ d=4
- Вычисляем $e_2 = d \times e_1=4 \times (2,22)=(13,45)$



Пример зашифрования

- Текст представляется точкой P=(24,26) и выбираем случайное r=2

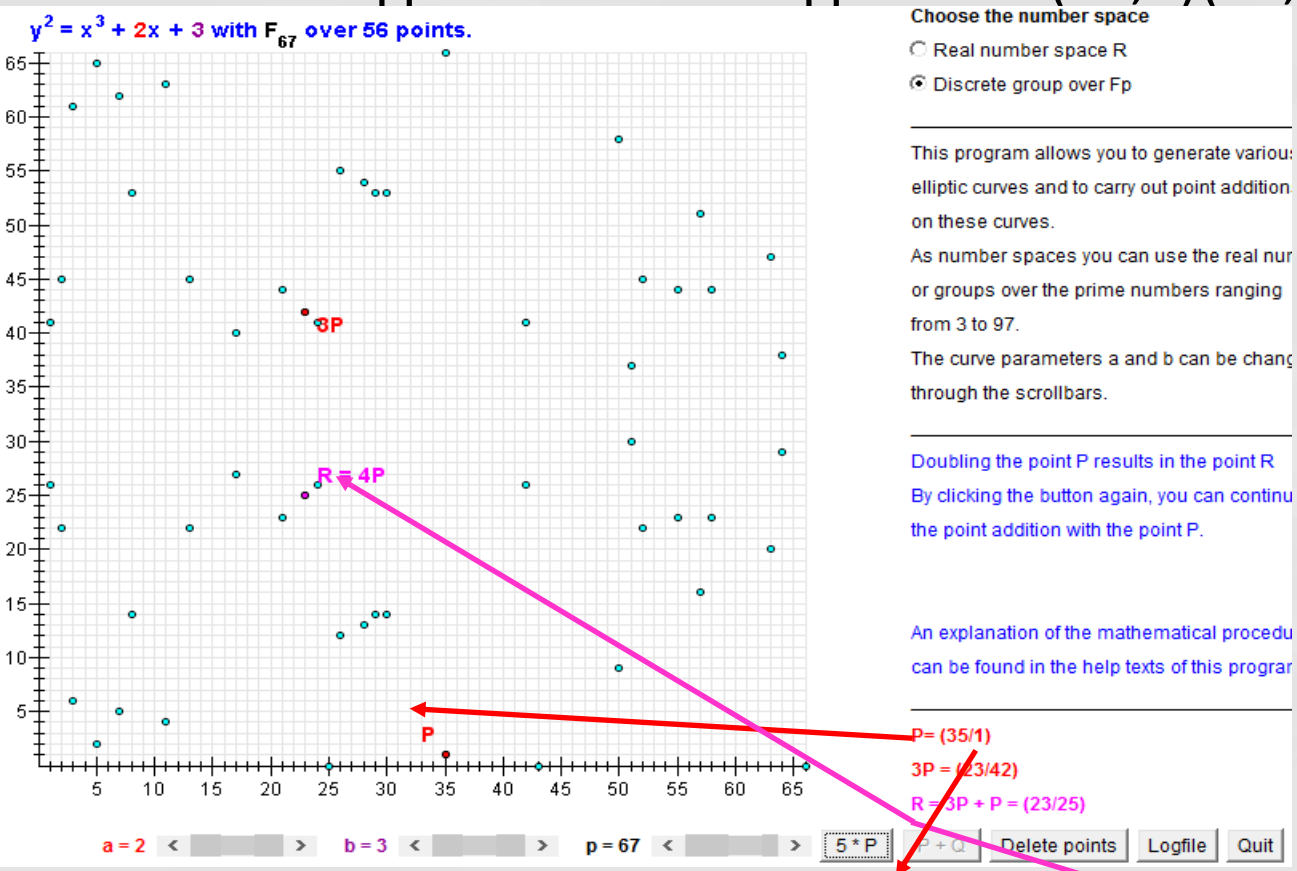


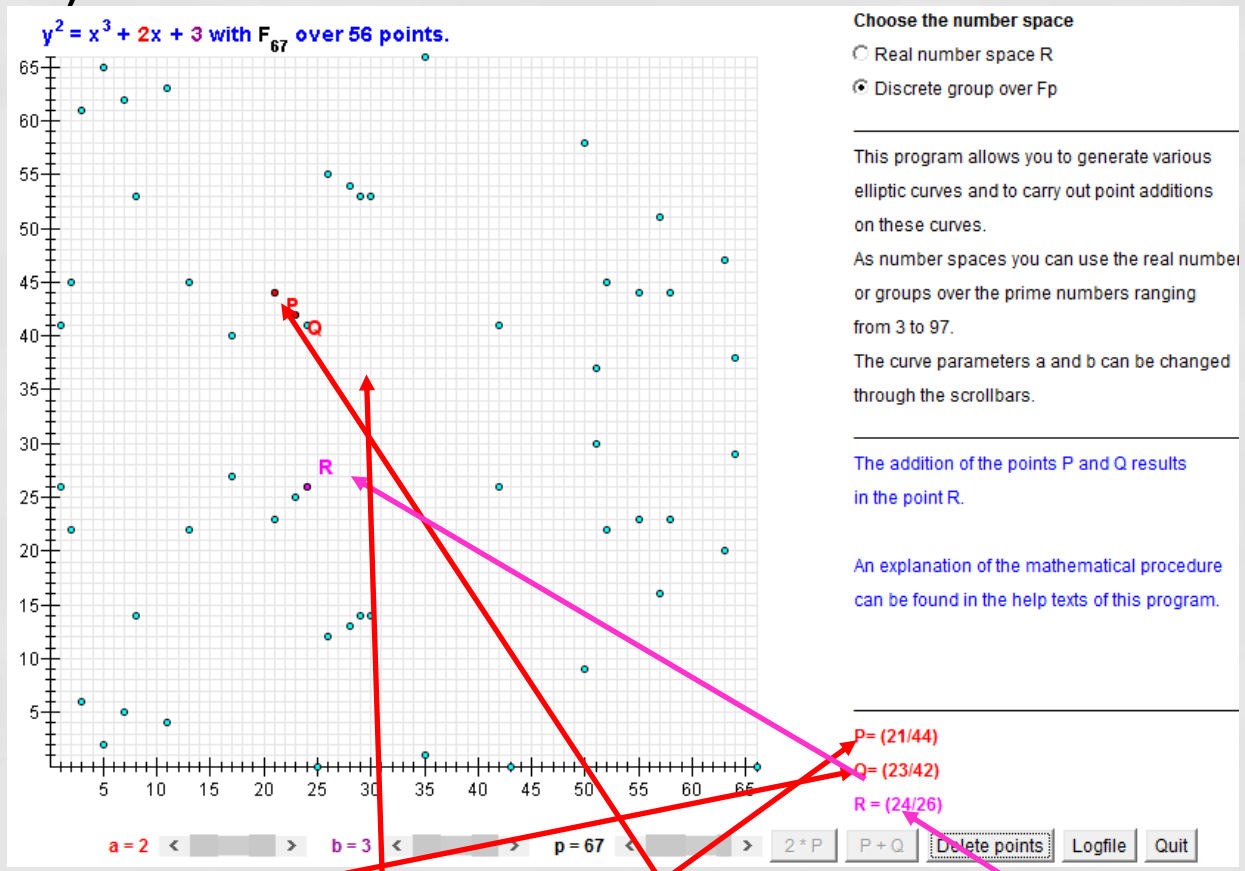


- Находим $C_1 = r \times e_1$=2 × (2,22) =(35,1) и C_2=P+r × e_2 =(24,26)+2× (13,45) = (21,44)

Пример расшифрования

- Расшифровываем шифротекст (35,1)(21,44)





- Вычисляем $\mathrm{d} \times C_1 = 4 \times (31,1) = (23,25)$, $-(23,25) = (23,42)$, $P = C_2 - \mathrm{d} \times C_1 = (24,26)$

Эллиптическая кривая Curve25519

- Предложена специалистом по компьютерной безопасности, американцем Daniel Bernstein (разработчик хэш-функции CubeHash, поточного шифра Sasla20)
- Используется кривая $y^2 = x^3 + 486662x^2 + x$ над полем вычетов по модулю простого числа $2^{255} - 19$ (что и дало название схеме выработки асимметричных ключей)
- Эллиптическая кривая и набор параметров к ней подобранных таким образом, чтобы обеспечить более высокое быстродействие (в среднем, 20-25%)
- Устойчивость к атакам по побочным каналам (timing attacks)
- Curve25519 используется как обмен ключами по умолчанию в OpenSSH и в IOS

Свойства метода с использованием эллиптической кривой

- Возведение в степень в алгоритме Эль-Гамаля заменено умножением точки на константу в модели
- Умножение в алгоритме Эль-Гамаля заменено сложением точек в модели
- Инверсия в алгоритме Эль-Гамаля — мультипликативная инверсия заменяется аддитивной инверсией точки на кривой
- Вычислительные затраты, поэтому, меньше в модели
- Для того же самого уровня безопасности (вычислительные затраты на атаки) модуль p, будет меньшим в эллиптической системе (ECC), чем в RSA (см. следующий слайд)

Таблица сравнения размеров ключей RSA и ECC (от NIST) для получения одинакового уровня защиты

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

Спасибо за внимание