Методы асимметричного шифрования

Шифр Голдвассера- Микали

Вероятностное шифрование (шифр GM)

- Проблема классических асимметричных шифров в том, что они слабо скрывают фрагменты текста, о которых может догадываться нарушитель (например, «ДА»/»НЕТ», «Купить»/«Продать»)
- Основная идея – внести случайный фактор в шифрование с отрытым ключом, т.е. поставить в соответствие каждому открытому тексту M множество шифротекстов C_M
- Первая доказуемо безопасная вероятностная схема асимметричного шифрования (GM) была предложена Шафи Голдвассером и Сильвио Микали 1982 г.
- Авторы стали лауреатами Премии Тьюринга за 2012 год в номинации «Новаторская работа, оказавшая существенное влияние на современную криптографию»

GM генерация ключей

- Выбираются простые числа p и q размером в k-бит
- Вычисляется модуль $n = p \times q$
- Выбирается $y \in Z_n$, такое , что:
  - y является квадратичным невычетом по модулю p
    $$\nexists x: x^2 \equiv y \ mod \ p$$
  - y является квадратичным невычетом по модулю q
    $$\nexists x: x^2 \equiv y \ mod \ q$$
- Открытый ключ (n, y), закрытый ключ (p, q)

GM зашифрование

- Представить сообщение M в виде строки битов $m = m_1, m_2,\dots,$ m_T длины T бит
- Для $i = 1, \dots, T$ выполнить:
  - Выбрать случайно $\mathrm{r} \in Z_n^*$
  - Если m_i=1, вычислить c_i=$(yr^2) mod\ n$
  - Если m_i=0, вычислить c_i=$(r^2) mod\ n$
- Сформировать C = $c_1, c_2,\dots, c_T$ длины T целых чисел из Z_n

GM расшифрование

- Для $i = 1, \ldots, T$ выполнить:
  - Вычислить $z_i = c_i^{(p-1)/2} mod\ p$ (критерий Эйлера для квадратичного вычета)
  - Если $z_i = 1$, принять $m_i = 0$ (c_i вычет)
  - Если $z_i = -1$, принять $m_i = 1$ (c_i невычет)
- Сформировать сообщение M в виде строки битов $m = m_1, m_2, \ldots, m_T$ длины T бит

Свойства GM

- Сложность взлома шифра GM(Гольдвассер-Микали) связана с решением задачи о распознавании квадратичных вычетов (QR), которая является общепризнанной трудноразрешимой задачей теории чисел
- Для шифрования сообщения, состоящего из T бит, необходимо выполнить $O(T(log_2 n)^2)$ побитовых операций
- Для расшифровки кортежа (c_1, c_2,…, c_T) требуются $O((log_2 n)^2)$ побитовых операций
- Степень избыточности этого алгоритма равна log_2n: одному биту исходного текста соответствуют log_2n бит зашифрованного текста

Вероятностная версия RSA

- Ключ открытый (n,e), ключ закрытый d
- Зашифрование сообщения в виде строки битов $m = m_1, m_2, \ldots, m_T$
  - если $m_i = 0$, то выбирается случайное четное число $x_i < n$;
  - если $m_i = 1$, то выбирается случайное нечетное число $x_i < n$;
  - Вычисляем $c_i = (x_i^{\,e}) mod\ n$, для всех i=1…T
- Расшифрование строки чисел $c_1, c_2, \ldots, c_T$:
  - $m_i = 0$, если $(c_i^{\,d}) mod\ n$ – четное
  - $m_i = 1$, если $(c_i^{\,d}) mod\ n$ – нечетное
  - Восстанавливаем биты исходного сообщения для всех i=1…T

Пример вычислений:

- Ключ открытый (n=21, e=17), ключ закрытый d=5
- Зашифрование сообщения M =000101:
  - Генерируем четные (4,2,8,2) и нечетные (3,5) числа
  - Вычисляем

$$c1 = c5 = (4\char`^17) \bmod 21 = 16, c2 = (2\char`^17) \bmod 21 = 11, c3 = (8\char`^17) \bmod 21 = 08, c4 = (3\char`^17) \bmod 21 = 12, c6 = (5\char`^17) \bmod 21 = 17.$$

  - Фомируем шифротекст: 16 11 08 12 16 17
- Расшифрование:

$$(16\char`^5) \bmod 21 = 4, (11\char`^5) \bmod 21 = 2, (8\char`^5) \bmod 21 = 8, (12\char`^5) \bmod 21 = 3, (16\char`^5) \bmod 21 = 4, (17\char`^5) \bmod 21 = 5$$

M= 0 0 0 1 0 1

Гомоморфное шифрование

Понятие гомоморфизма

- ***Гомоморфизм*** (от др.-греч. - равный, одинаковый и - вид, форма) — это морфизм в категории алгебраических систем, то есть отображение алгебраической системы А, сохраняющее основные операции и основные отношения
- Отображение $f\colon G_1 \to G_2$называется ***гомоморфизмом групп*** $(G_1,*)(G_2,\times)$, если оно одну групповую операцию переводит в другую:

$$f(a * b) = f(\mathrm{a}) \times f(b).$$

Гомоморфное шифрование

- Введём обозначения:
  - k – ключ;
  - m – открытый текст;
  - $Enc(k, m)$ – шифрующая функция
  - $Dec(k, m)$ – расшифрующая функция
- Функция Enc называется гомоморфной относительно операции сложения или умножения $(*)$ над открытыми текстами m_1, m_2, если существует алгоритм H, который, получив на входе пару $Enc(k, m_1)$ и $Enc(k, m_2)$, выдаст шифровку

$$C = H\big(Enc(k, m_1), Enc(k, m_2)\big),$$

результатом расшифрования которой будет открытый текст $m_1 * m_2$.

Виды гомоморфных криптосистем

- Частично гомоморфная система
  - Криптосистема гомоморфна относительно операции сложения, если $Dec\left(Enc(k,m_1)+Enc(k,m_2)\right)=m_1+m_2$
  - Криптосистема гомоморфна относительно операции умножения, если $Dec\left(Enc(k,m_1)\cdot Enc(k,m_2)\right)=m_1\cdot m_2$.
- Полностью гомоморфная система
  - Криптосистема гомоморфна относительно операции умножения и сложения, если:

$$Dec\left(Enc(k,m_1)\cdot Enc(k,m_2)\right)=m_1\cdot m_2.$$
$$Dec\left(Enc(k,m_1)+Enc(k,m_2)\right)=m_1+m_2.$$

Система RSA гомоморфна по умножению

- Обозначения:
  - (n, e) – открытый ключ
  - m_1, m_2 - открытый текст (шифруемое сообщение)
  - Enc– шифрующая функция
- Доказательство:
  - $\boldsymbol{Enc(m_1)} \cdot \boldsymbol{Enc(m_2)} = m_1^e \bmod n \cdot m_2^e \bmod n = (m_1 \cdot m_2)^e \bmod n = \boldsymbol{Enc(m_1 \cdot m_2)}$

Система EG гомоморфна по умножению

- Обозначения:
  - m_1, m_2 - открытый текст (шифруемое сообщение)
  - $y = g^x mod\ p$ – открытый ключ (y,g,p), закрытый ключ x
  - Случайный эфемерный ключ для m_1 - k_1 для m_2 - k_2
  - Enc– шифрующая функция
- Доказательство:
  - $\boldsymbol{Enc(m_1)} \cdot \boldsymbol{Enc(m_2)}= (g^{k_1} \pmod p), m_1\, y^{k_1} \pmod p)) \cdot (g^{k_2} \pmod p), m_2\, y^{k_2} \pmod p))=$
    $=(y^{k_1 \cdot k_2} \pmod p), (m_1 \cdot m_2) y^{k_1 \cdot k_2} \pmod p))= \boldsymbol{Enc(m_1 \cdot m_2)}$

Шифр Пэйе (1999)

Генерация ключей

- Секретный ключ: (α, μ, p, q)

$$p, q, \alpha = \text{НаименьшееОбщееКратное}(p-1, q-1),$$

$$\mu = \Lambda(g^{\alpha} \, mod \, N^2)^{-1} mod \, N,$$

$$\Lambda(u) = div\frac{u-1}{N} \quad (div - \text{целочисленное деление})$$

- Открытый ключ: (g, N)

$N = p \cdot q$, g – случайное число: $g \in {Z^*}_{N^2}$

${Z^*}_{N^2}$ - множество целых чисел взаимнопростых с N^2. Это множество состоит из $N \cdot \varphi(N)$ чисел.

- Сообщение: не нулевой элемент $m \in Z_N : m < N$

Зашифрование и расшифрование

- Зашифрование:
  - Генерация случайного числа $r \in Z^*_N$
  - $C = g^m \cdot r^N (mod\ N)$

- Расшифрование:
  - $m = (C^\alpha\ mod\ N^2) \cdot \mu\ mod\ N$

Пример: генерация ключей

$p = 7$ и $q = 5$, $N = 7 \cdot 5 = 35$, $N^2 = 1225$ и $\alpha = \text{НОК}(6, 4) = 12$.

Выбираем случайное целое число g, такое что $g \in Z^*_{N^2}$, $g = 3$.

Находим $\mu = \left(\Lambda(g^{\alpha} mod\ N^2)\right)^{-1} mod\ N = 29$.

$(\alpha, \mu, p, q) = (12, 29, 7, 9) -$ закрытый ключ.

Пример: зашифрование и расшифрование

- Зашифрование
  - m=8
  - Выбираем произвольное $r \in \ Z_N^*, \ r = 9,$
  - Вычисляем:

$$C = g^m \cdot r^N \, mod \; N^2 \; = 3^8 \;\; \cdot 9^{35} \, mod \; 1225 = 436 \cdot 949 \, mod \; 1225 = 9393.$$

- Расшифрование
  - $C \; = 939, \; C \in Z_{1225}$
  - Вычисляем $m = \Lambda(C^{\alpha} \, mod \; N^2) \cdot \mu \, mod \; N = L(939^{12} \, mod \; 1225) \cdot 29 \, mod \; 35 = 22 \cdot 29 \, mod \; 35 = 8.$

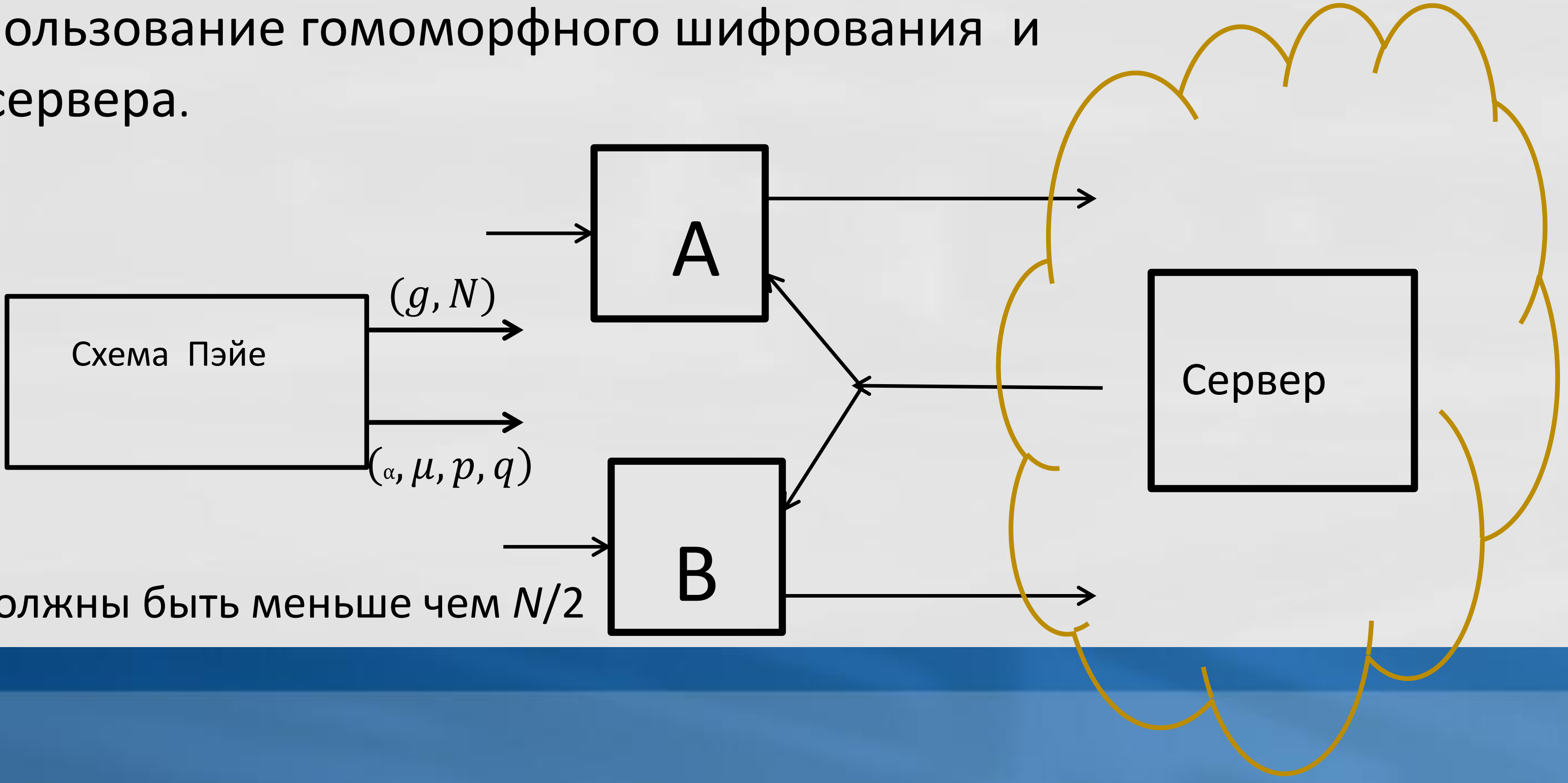
Система Пэйе гомоморфна по сложению

1. При дешифровании произведения двух шифротекстов будет получена сумма соответствующих им открытым текстам:
   - $Dec(Enc(m_1) \cdot Enc(m_2) mod\ N^2) = (m_1 + m_2) mod\ N$
   - Частный случай $Dec(Enc(m_1) \cdot g^{m_2} mod\ N^2) = (m_1 + m_2) mod\ N$;
2. При дешифровании криптограммы, возведенной в степень $d \epsilon Z_n^*$, будет получено произведение открытого текста и показателя степени d:
   - $Dec(Enc(m))^d) mod\ N^2 = d \cdot m\ mod\ N$
   - Частный случай $Dec(Enc(m_1))^{m2}) mod\ N^2 = m_1 \cdot m_2\ mod\ N$.

Применение: анонимные вычисления

Постановка задачи: Алиса и Боб имеют числа x_1 и x_2 и хотят выяснить у кого число больше, не раскрывая самих значений этих чисел.

Идея – использование гомоморфного шифрования и внешнего сервера.



x_1 и x_2 – должны быть меньше чем $N/2$

Протокол анонимных вычислений

1. Пользователь А шифрует число x_1 по схеме Пэйе:

$$C_1 = g^{x_1} \cdot r^N (mod\ N)$$

2. Пользователь Б шифрует число x_2 по схеме Пэйе:

$$C_2 = g^{x_2} \cdot r^N (mod\ N)$$

3. Сервер выполняет преобразование зашифрованных данных

$$C = C_1 \cdot {C_2}^{N-1} \cdot g^l$$

где $l > 0$ - случайное число и отправляет C пользователям.

4. Пользователи А и Б дешифруют C и по свойству гомоморфности получают:

$$Dec(C) = \Lambda\left(C^\alpha\ mod\ N^2\right) \cdot \mu\ mod\ N$$

По свойству гомоморфности: $(x_1 + (N-1) \cdot x_2 + l) mod\ N = (x_1 - x_2 + l) mod\ N$

ЕСЛИ $Dec(C) > \frac{N}{2}$, то $x_1 > x_2$, ИНАЧЕ $x_1 < x_2$

Шифр Джентри

- Первая теоретическая конструкция для полностью гомоморфной криптосистемы, основанная на криптографии на решетках. Была предложена Крейгом Джентри в 2009 году и поддерживает операции сложения и умножения над шифротекстом.
- Самостоятельно разобраться :
  - https://habr.com/ru/articles/255205/ - Гомоморфное шифрование –что это такое ?
  - https://inf.grid.by/jour/article/viewFile/11/13 - Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор)

Применение

1. **Безопасные облачные вычисления:**

Важна производительность, следует применять различные алгоритмы, в зависимости от поставленной задачи.

2. **Электронное голосование:**

Система сможет зашифровать голоса избирателей и провести расчёты над зашифрованными данными, сохраняя анонимность избирателей.

3. Защищённый поиск информации:

Можно предоставить пользователям возможность извлечения информации из поисковых систем с сохранением конфиденциальности: сервисы смогут получать и обрабатывать запросы, а также выдавать результаты обработки, не зная содержание.

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 криптосистема на основе метода эллиптических кривых (*Elliptic Curve Cryptosystem — ECC*)

Эллиптические кривые в вещественных числах

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

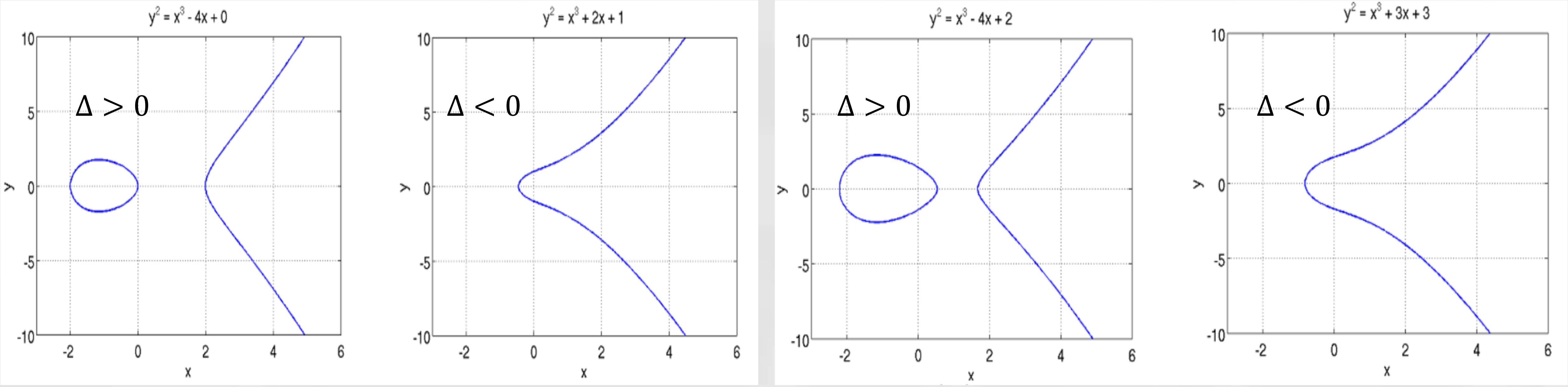
$$y^2 + \mathrm{axy} + by = x^3 + cx^2 + \mathrm{dx} + e$$

- В криптографии распространение получил частный вид эллиптических кривых:

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

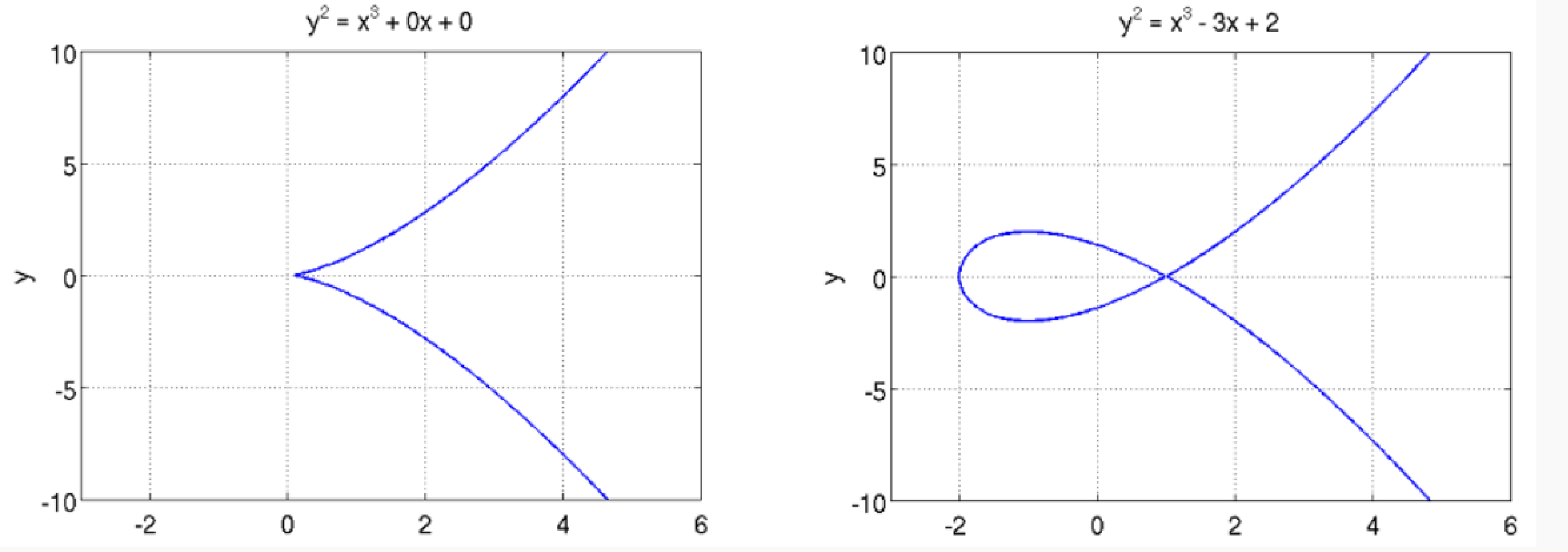
- Если дискриминат $\Delta = -16(4a^3 + 27b^2) \neq 0$, уравнение представляет <u>несингулярную</u> (гладкую) эллиптическую кривую, иначе сингулярную (с особыми точками)

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 !*

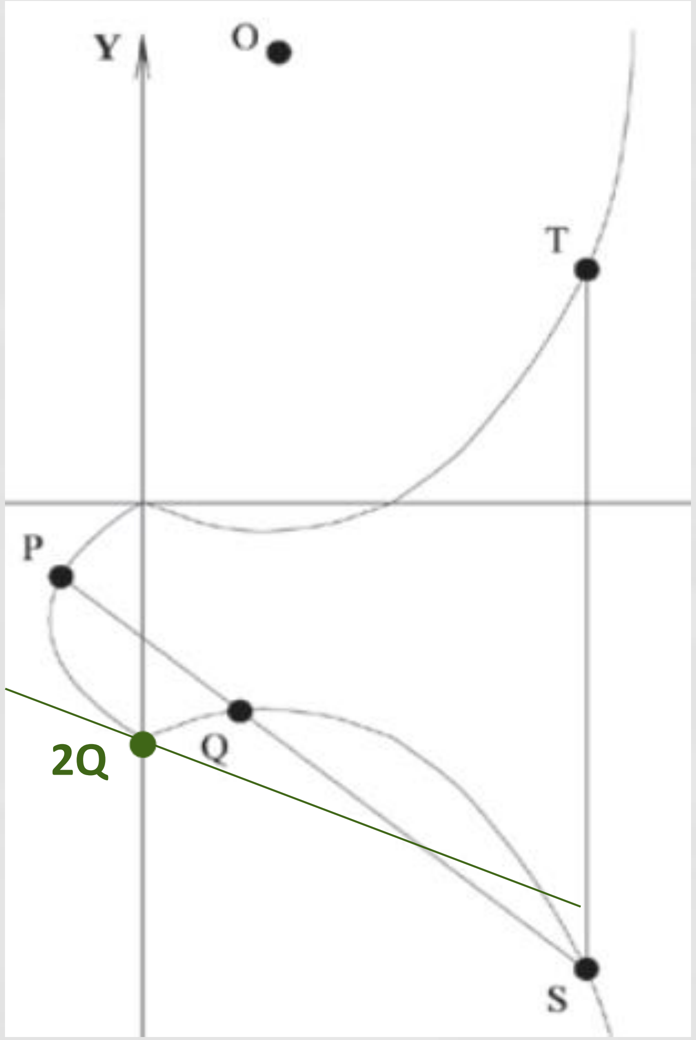
Примеры сингулярных эллиптических кривых



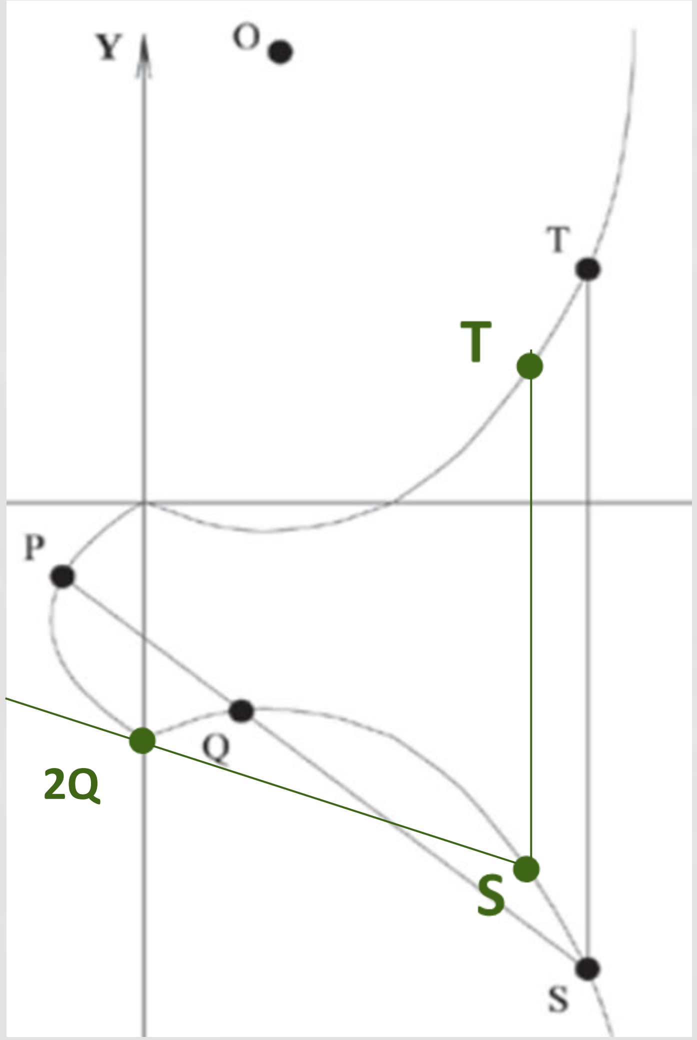
- При использовании сингулярных кривых стойкость эллиптической криптосистемы значительно снижается

Свойства точек эллиптической кривой

- Предполагаем:
  - 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**
- <u>Умножение точки P эллиптической кривой на положительное число k определяется как сумма k точек P</u>

Эллиптические кривые в криптографии

- Эллиптические кривые над вещественными числами приводит нас к проблеме округления (тексты должны представляться целыми числами)
- В криптографии используются только кривые над конечными полями, т.е. координаты точек кривой принадлежат конечному полю

Эллиптические кривые в GF(p)

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

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

- 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 $E_{13}(1,1)$: $y^2 = (x^3 + \mathrm{x} + 1) mod\ 13$
- Выбрать одну из точек *P(4, 2), R(3,5)* и *Q(7,0)*
- Проверить принадлежность выбранной точки кривой $E_{13}(1,1)$

Свойства точек $E_p(a,b)$

- *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:
- $x_3 = (\lambda^2 - x_1 - x_2)\, mod\, p \quad y_3 = (\lambda(x_1 - x_3) - y_1)\, mod\, p$

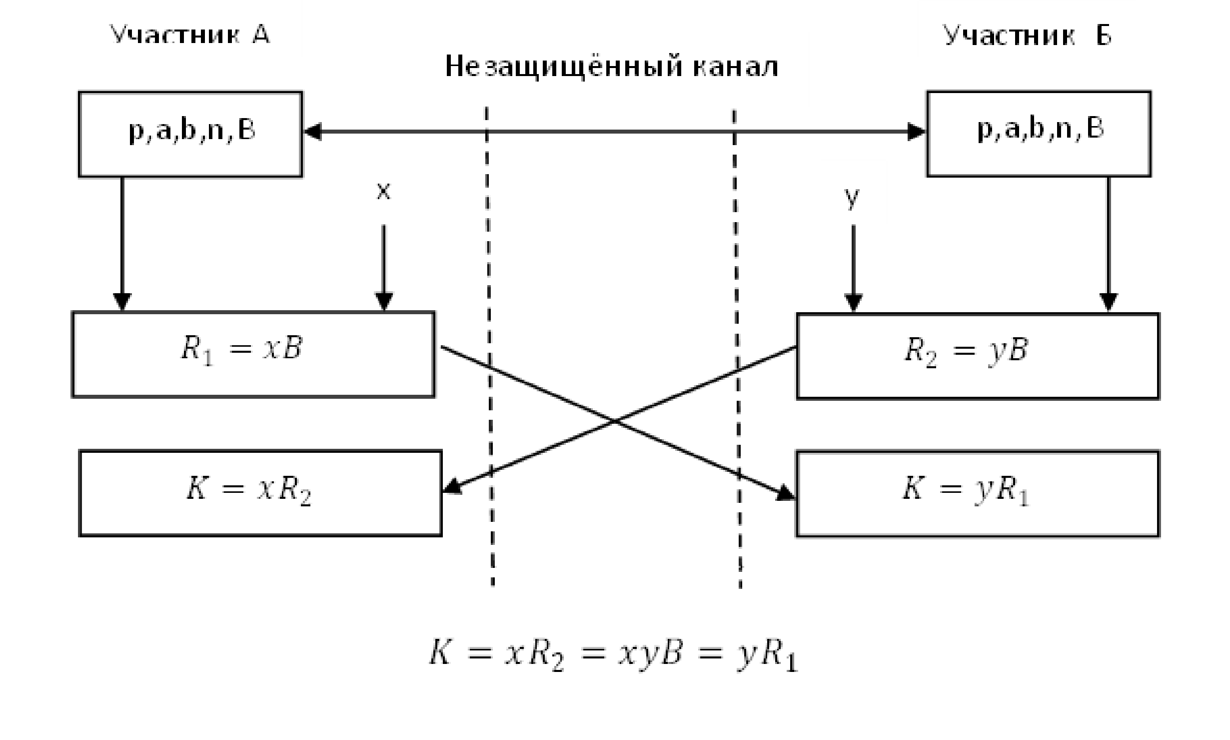
$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) modp, & P \neq Q \\ ((3x_1^2 + a))/2y_1\, modp, & P = Q \end{cases}$$

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

Задача дискретного логарифмирования на эллиптической кривой

- Даны точки P и Q на эллиптической кривой $E_p(a,b)$. Необходимо найти коэффициент $k < p$ такой, что $P = k \times Q$
- Относительно легко вычислить P по данным k и Q, но вычислительно трудно вычислить k, зная P и Q

Протокол Диффи-Хеллмана для эллиптических кривых (ECDH)

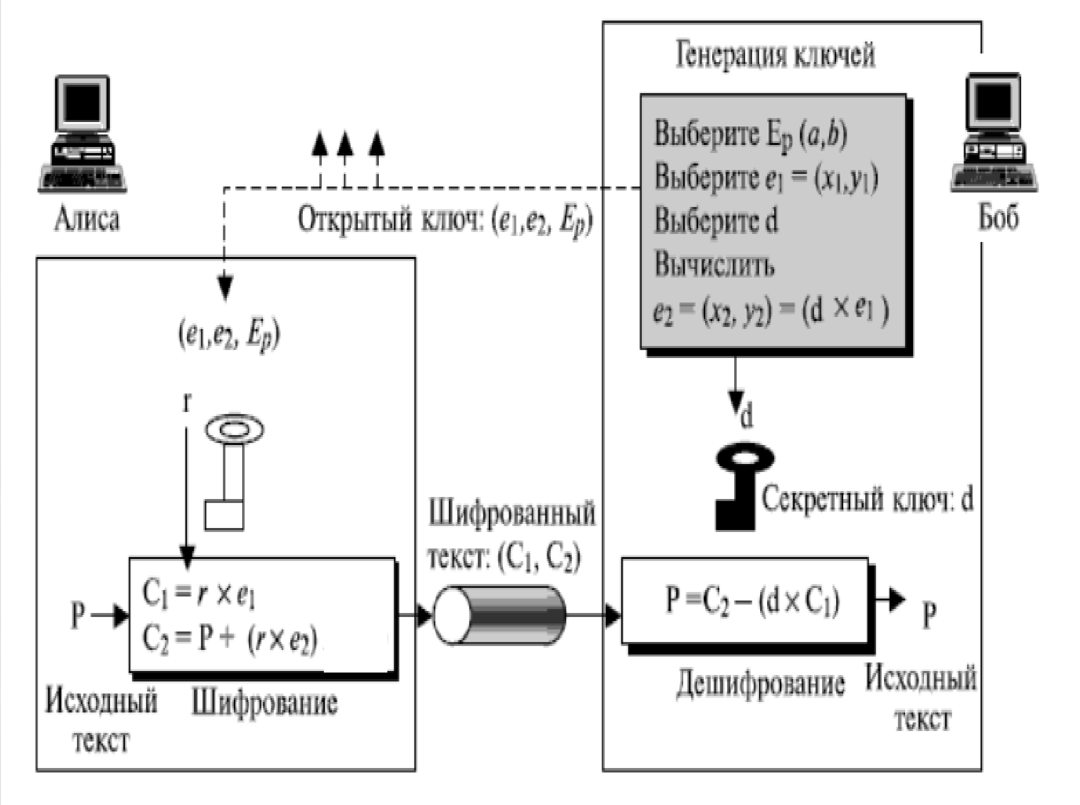


- Группа точек эллиптической кривой $E_p(a, b)$
- *B* – базовая точка (порождающий элемент) циклической подгруппы точек {kB, k=1,n} порядка n: *nB=0*
- *x, y* - большие случайные числа такие, что *0 < x < n , 0 < y < n*
- Поскольку:

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

- Стороны фактически создают материал для генерации симметричного ключа (координаты точки xyB)
- Самостоятельно вспомнить основы: https://habr.com/ru/post/335906/

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:

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

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

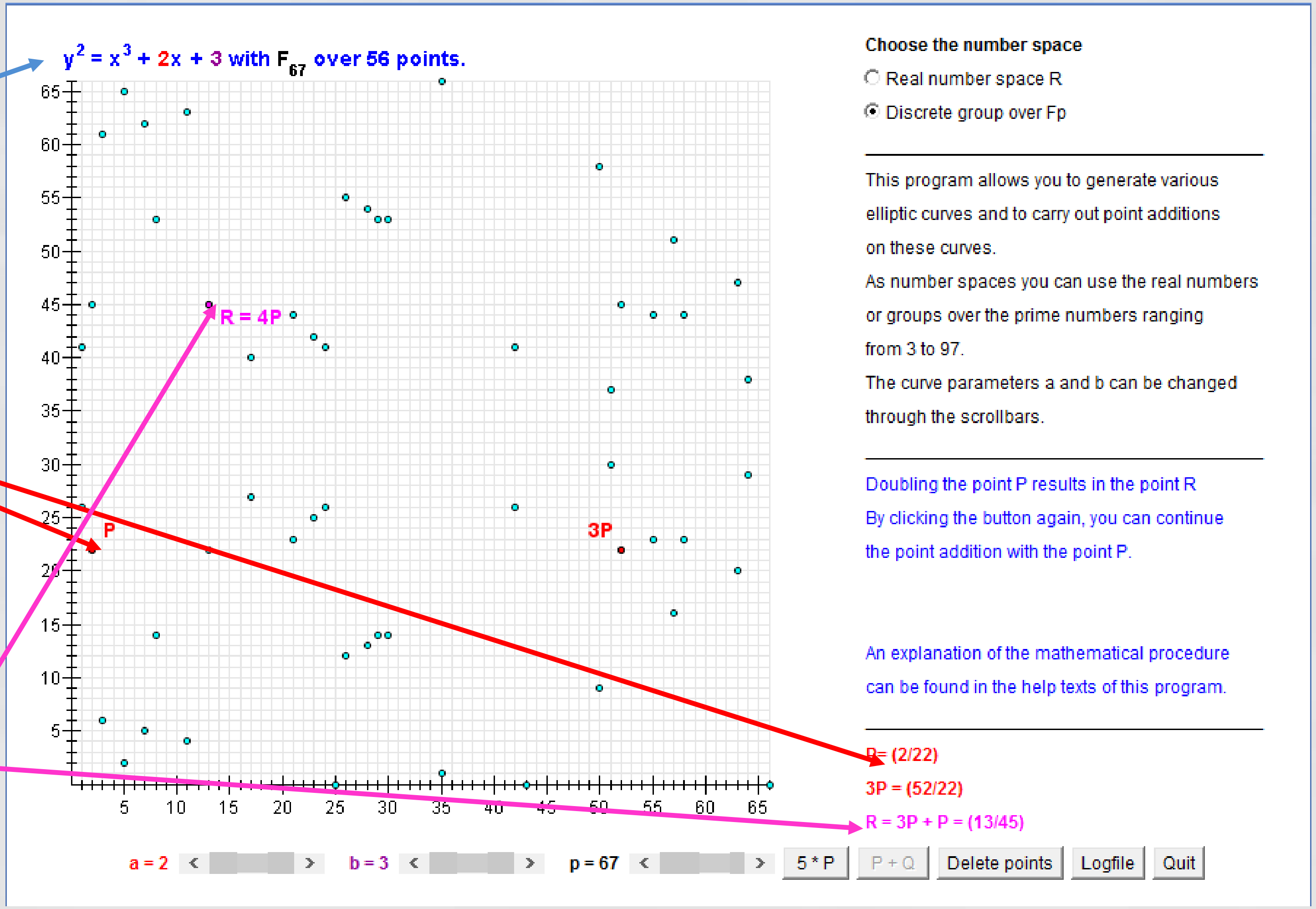
Размер ключа RSA (биты)	*Размер ключа ECC (биты)*
1024	160
2048	224
3072	256
7680	384
15360	521

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, I2p, Tor, Tox и даже в IOS

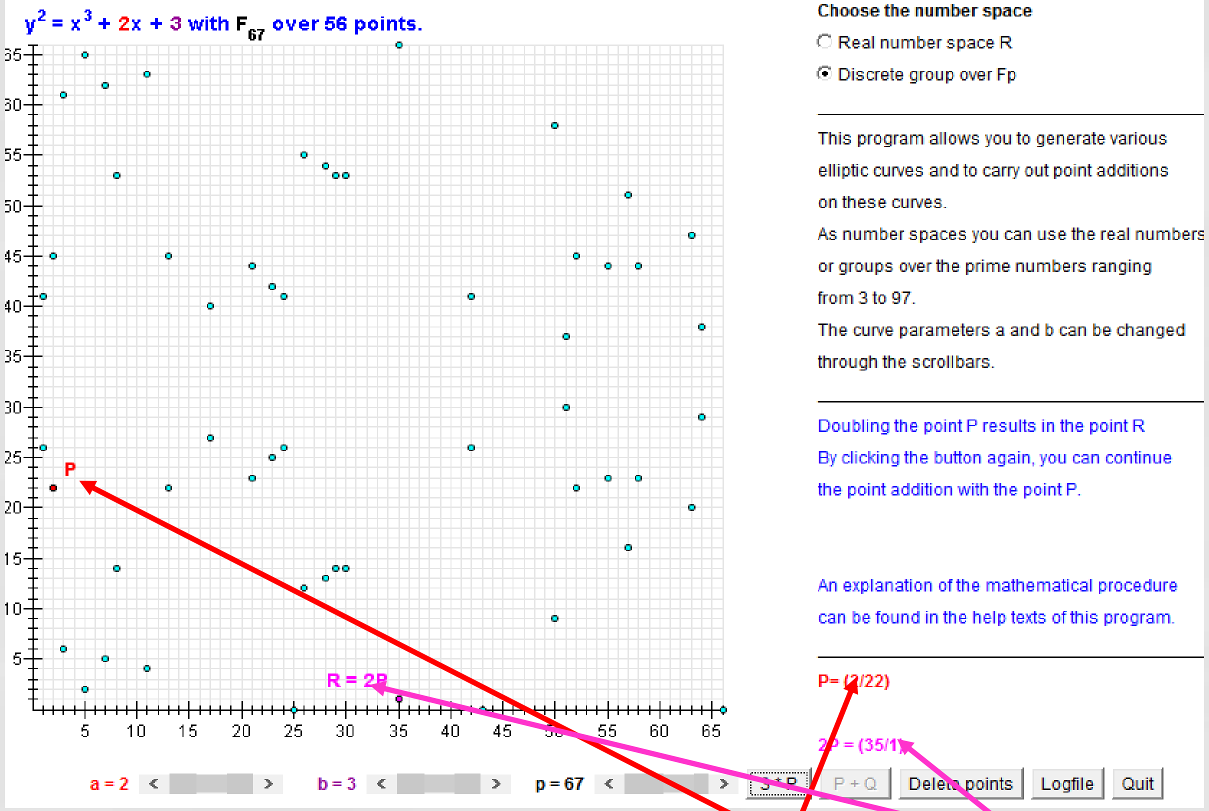
Пример генерации ключа

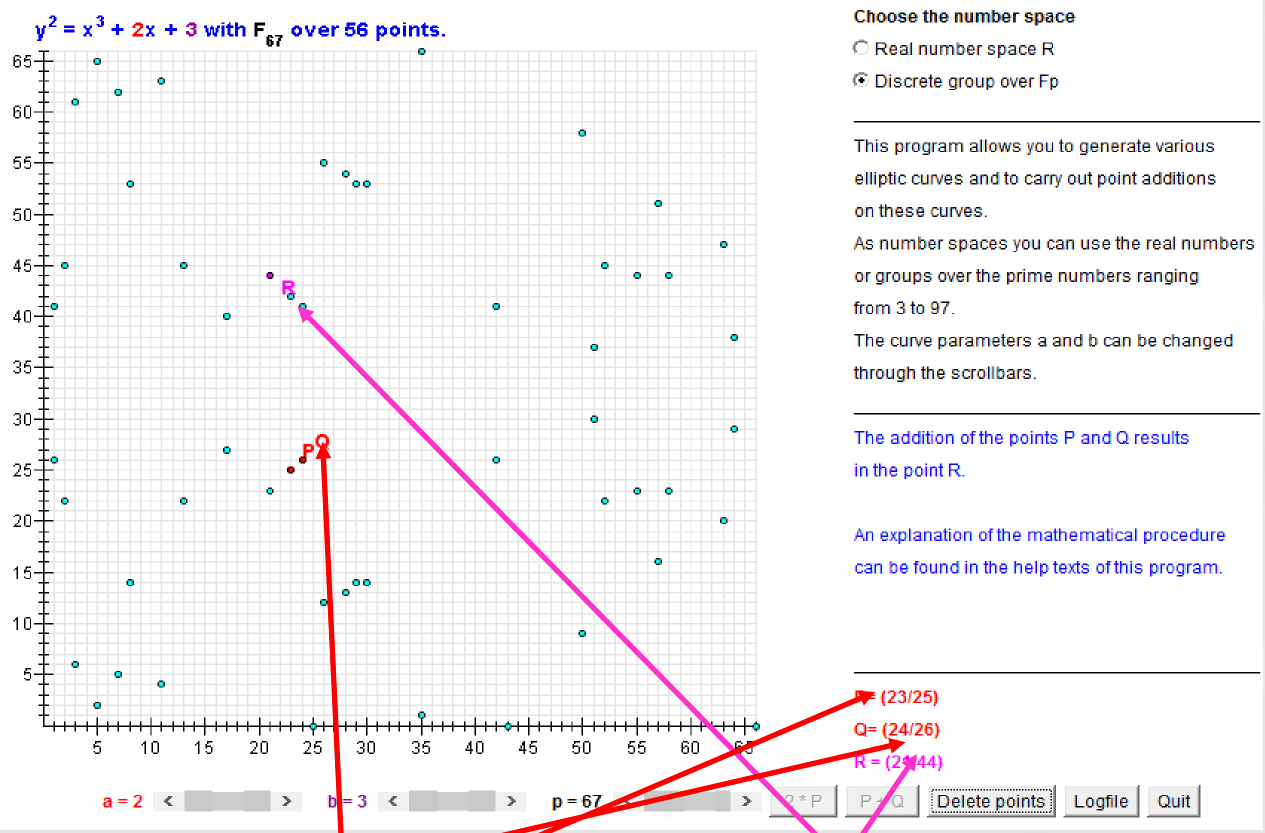
- Выбираем кривую $E_{67}(2,3)$
- Выбираем точку e_1=(2,22)
- Выбираем закрытый ключ d=4
- Вычисляем $e_2 = d \times e_1$=4 × (2,22)=(13,45)



Пример зашифрования

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

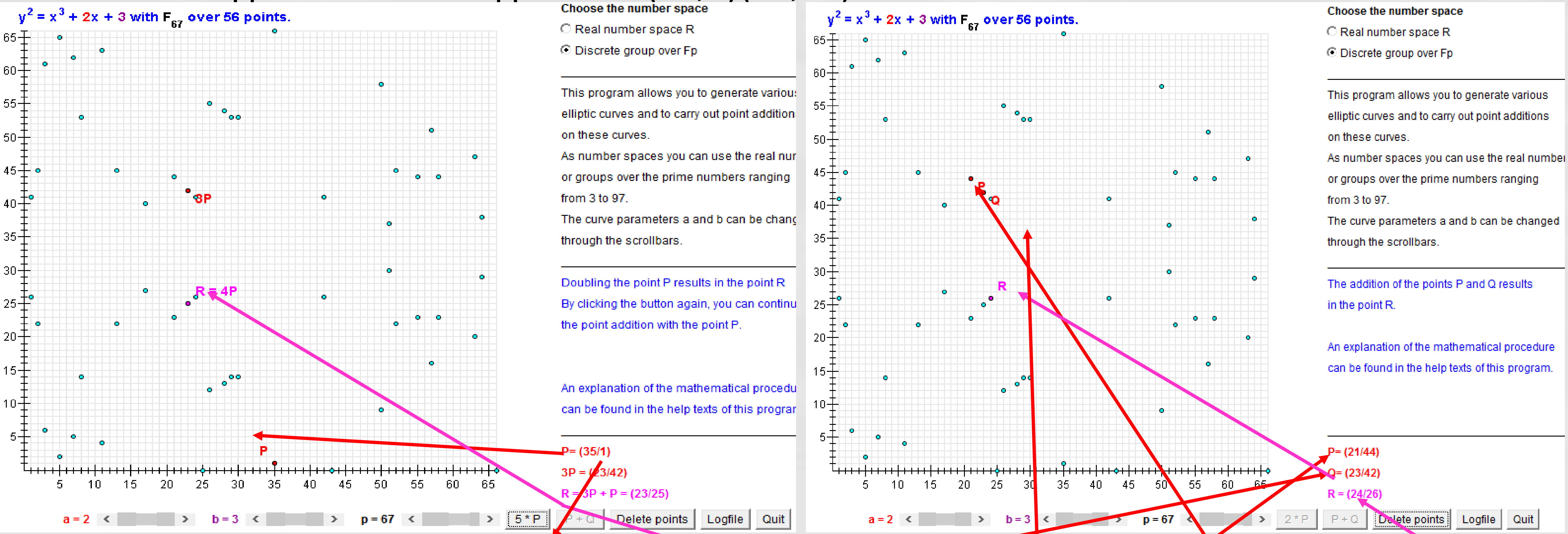




- Находим $C_1 = r \times e_1 = 2 \times (2,22) = (35,1)$ и $C_2 = P + r \times e_2 = (24,26) + 2 \times (13,45) = (21,44)$

Пример расшифрования

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



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

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, может быть меньшим в эллиптической системе (ECC), чем в RSA. Например, ECC с модулем, состоящим из 160 битов, может обеспечить тот же уровень безопасности, как RSA с модулем 1024 битов