Эллиптическая криптография.

Длина ключей, обеспечивающих одинаковый уровень криптостойкости

RSA/DSA	ECC	Отношение длин ключей RSA/ECC	AES
512	106	5:1	-
768	132	6:1	-
1024	160	7:1	-
2048	210	10:1	-
3072	256	12:1	**128**
7680	384	20:1	**192**
15360	**512**	**30:1**	**256**

Эллиптическая криптография

Эллиптической кривой E над полем F_p , *m.e* $E(F_p)$ F называется гладкая кривая, задаваемая уравнением вида:

$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$

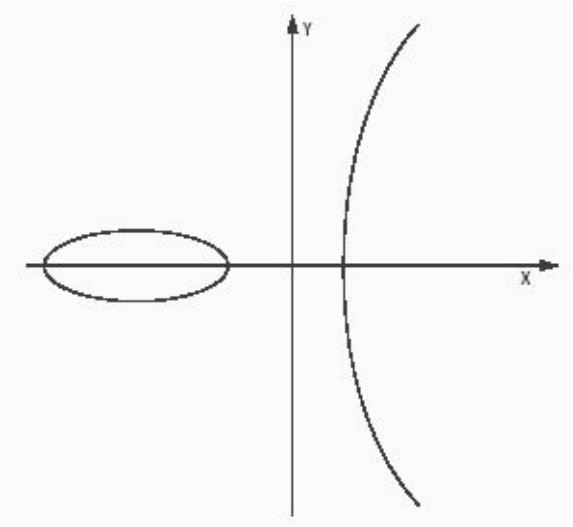
и содержащая также бесконечно удаленную точку, обозначаемую *O*

Для гладкости кривой не должно быть точек, в которых равны нулю обе частные производные, т.е два уравнения

$a_1Y = 3X^2 + 2a_2X + a_4$

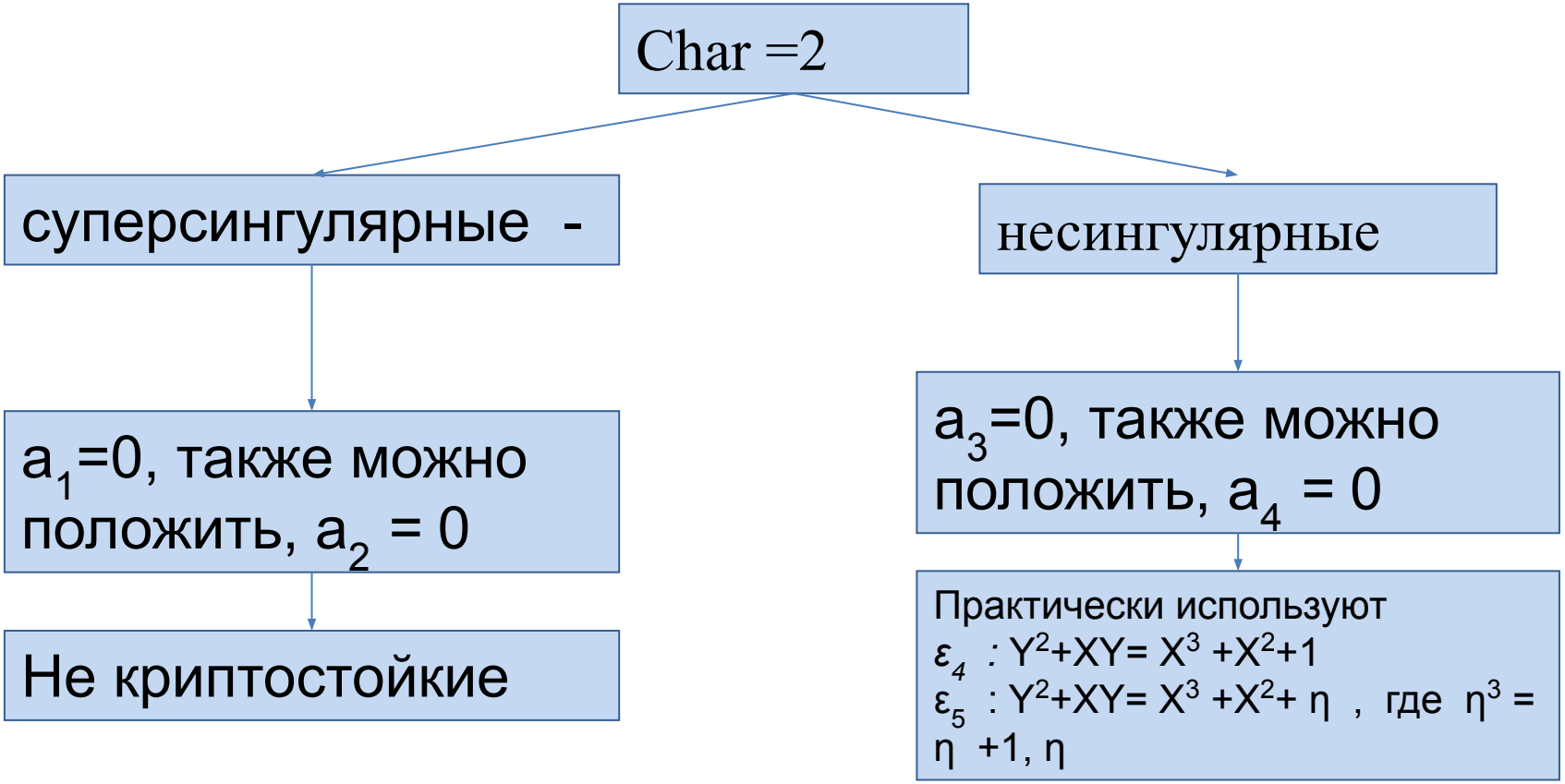
$2Y + a_1X + a_3 = 0$

не должны одновременно удовлетворяться ни в одной точке.



Эллиптическая криптография

Если $p = q^m$, где q - простое и m - положительное целое число, то q называют характеристикой(characteristic) F и обозначают char F, m называют степенью расширения (extension degree).



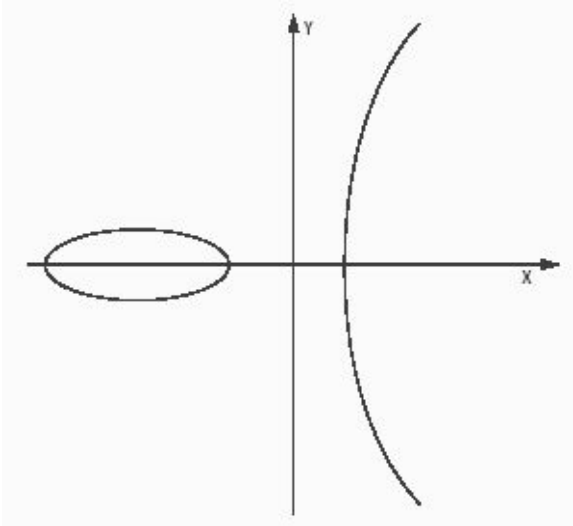
Эллиптическая криптография

Если F_p не является полем характеристики 2, то без потери общности можно полагать, что $a_1=a_3= 0$, а после упрощения левой части, линейной заменой переменной (а именно, $X \rightarrow X - 1/3a_2$) можно также удалить терм X^2. То есть без потери общности можно полагать, что кривая задана уравнением вида $Y^2 = X^3 +aX +b$, $a,b \in F_p$ $char\ F \neq 2, 3$

Понятие эллиптической кривой

В российском ГОСТ используется эллиптическая кривая E над полем Fp $y^2=x^3+ax+b$, задаваемая коэффициентами a и b и содержащая также бесконечно удаленную точку, обозначаемую *O*

p- простое число – модуль эллиптической кривой, $p>2^{255}$



Понятие эллиптической кривой

Множество точек эллиптической кривой вместе с нулевой точкой и с введенной операцией сложения будем называть «группой». Для каждой эллиптической кривой число точек в группе конечно, но достаточно велико.

Число точек эллиптической кривой, включая точку O, называется порядком (order) кривой и обозначается E (F_p). (в ГОСТе m)

Порядок m группы точек эллиптической кривой может быть оценен с помощью неравенства:
$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p}$,
где p — порядок поля, над которым определена кривая

Пример 1. задана эллиптическая кривая E: $Y^2 = X^3 + x + 4$ на поле F_{23}. Точками кривой будут
(0,2) (0,21) (1, 11) (1,12) (4,7)
(4,16) (7,3) (7,20) (8,8) (8,15)
(9,11) (9,12) (10,5) (10,18) (11,9)
(11,14) (13,11) (13,12) (14,5) (14,18)
(15,6) (15,17) (17,9) (17,14) (18,9)
(18,14) (22,5) (22,19) O
Порядок группы $\#E(F_{23}) = 29$.

Понятие эллиптической

Точки эллиптической кривой могут складываться, но не могут умножаться. Однако возможно скалярное умножение, когда соответствующее число раз выполняется прибавление одной и той же точки. В результате получается кратная точка.
$P = Q + Q + Q + \ldots + Q = kQ$

Порядком точки P эллиптической кривой называется наименьшее положительное целое число r , такое что kP=0

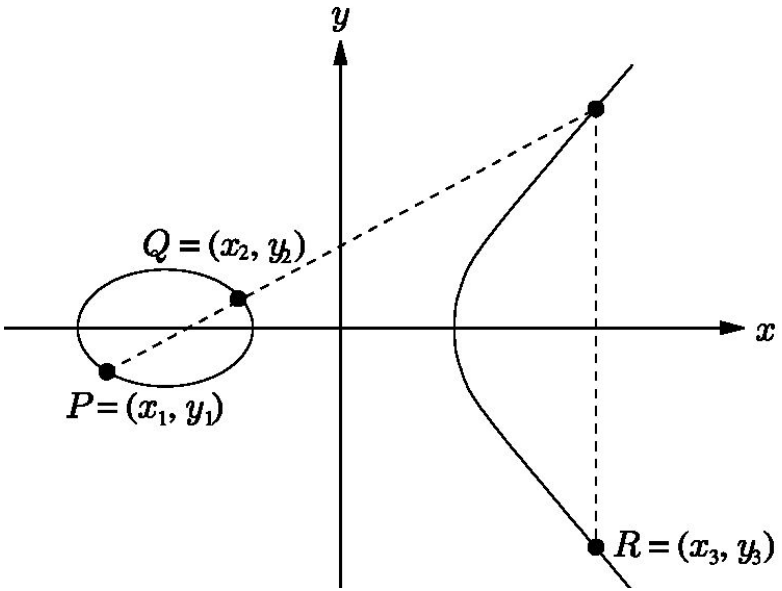
Точка P будет называться **генератором группы**, если кратные ей точки образуют все множество точек эллиптической кривой.

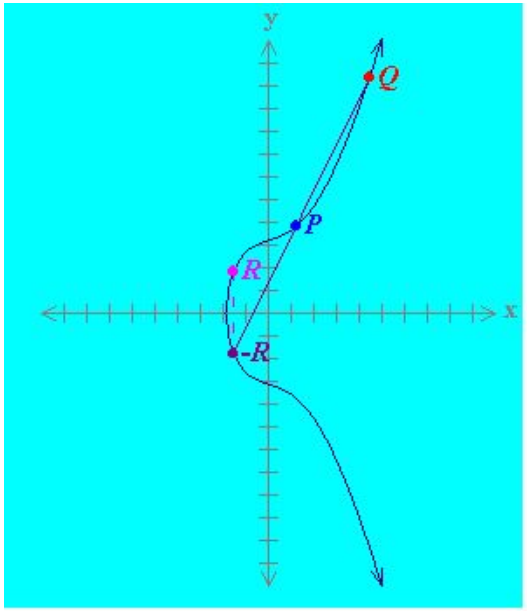
Для кривой, определенной в примере 1, #E (F_{23}) любая точка, кроме O, будет генератором E (F_{23}) . Например, для точки P =(0,2) имеем:

1P = (0, 2)	2P = (13, 12)	3P = (11, 9)
4P = (1, 12)	5P = (7, 20)	6P = (9, 11)
7P = (15, 6)	8P = (14, 5)	9P = (4, 7)
10P = (22, 5)	11P = (10, 5)	12P = (17, 9)
13P = (8, 15)	14P = (18, 9)	15P = (18, 14)
16P = (8, 8)	17P = (17, 14)	18P = (10, 18)
19P = (22, 18)	20P = (4, 16)	21P = (14, 18)
22P = (15, 17)	23P = (9, 12)	24P = (7, 3)
25P = (1, 11)	26P = (11, 14)	27P = (13, 11)
28P = (0, 21)	29P = O.	

Сложение точек на эллиптической кривой

Пусть P = (x_1, y_1) и Q = (x_2, y_2) две различные точки на кривой E. Тогда сумма P и Q, обозначаемая R = (x_3, y_3), определяется следующим образом. Сначала чертим линию через P и Q; эта линия пересекает эллиптическую кривую в третьей точке. Тогда R - отражение этой точки на ось X

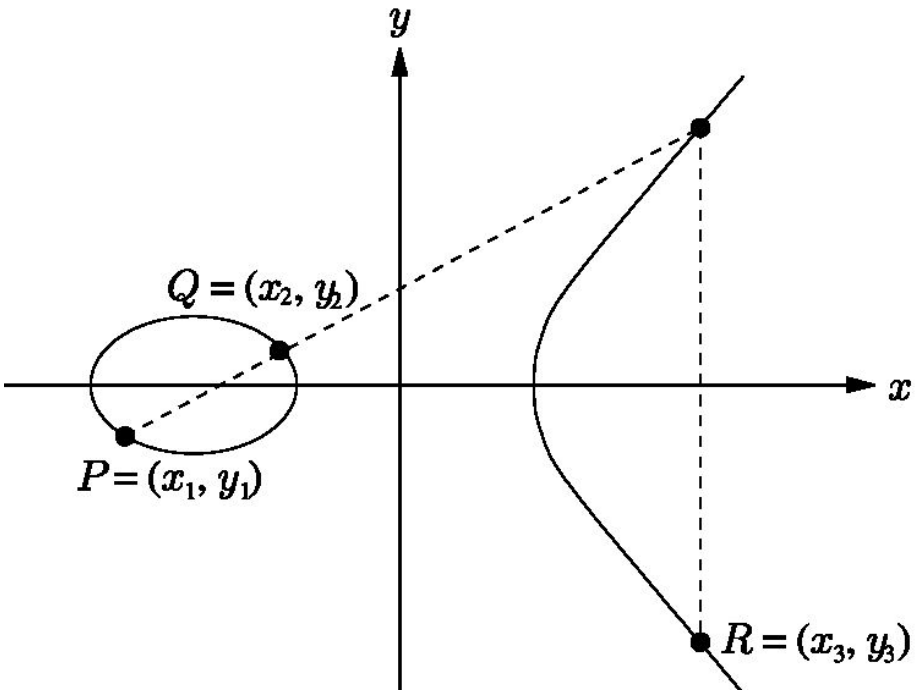




$$P + Q = R$$

Сложение точек на эллиптической кривой

P + Q = R

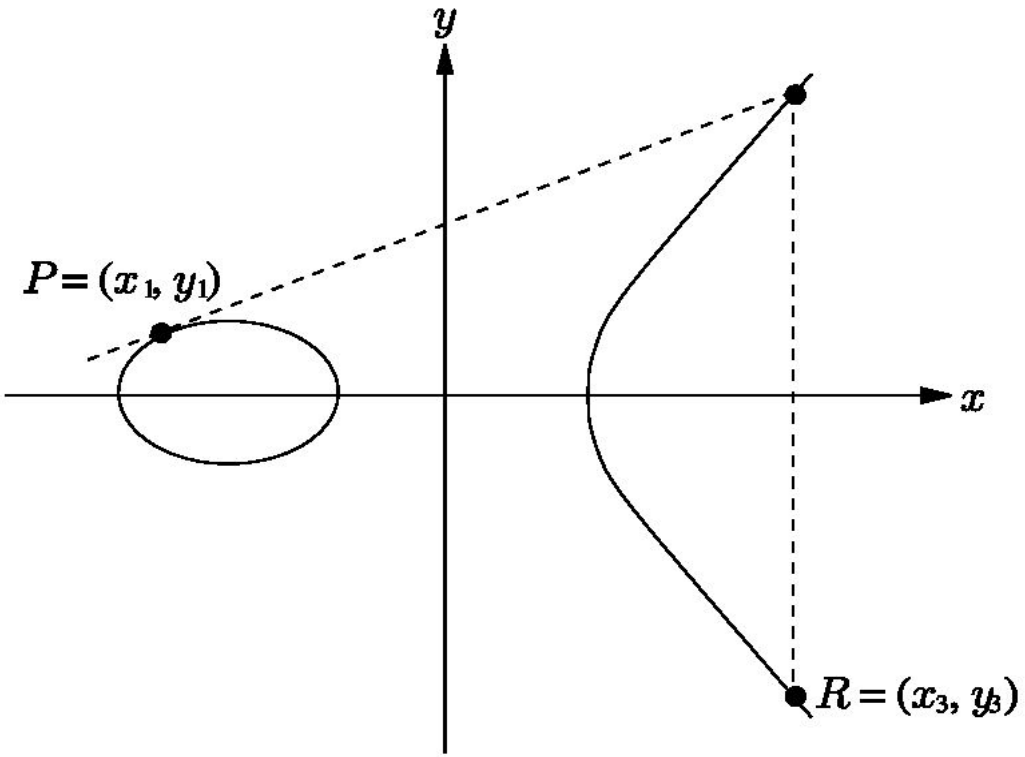


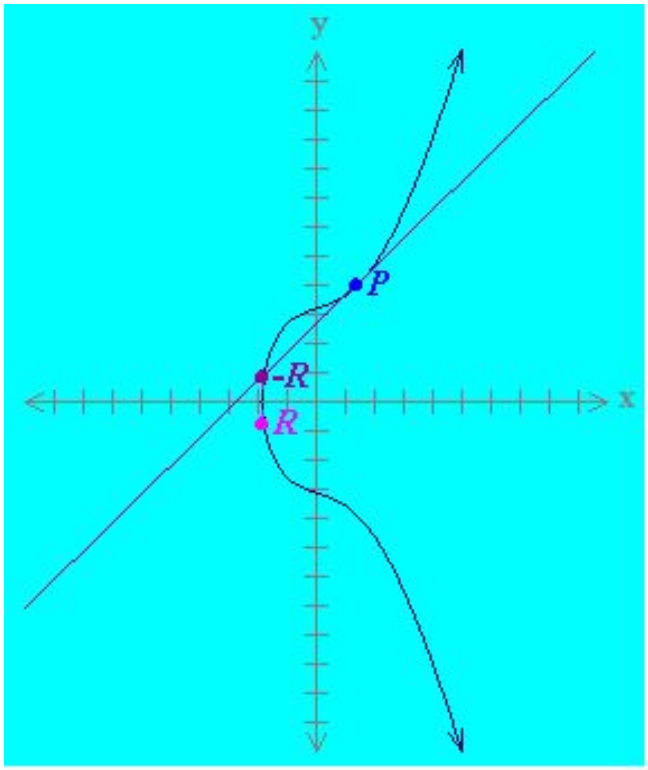
$$x_3 = \lambda^2 - x_1 - x_2 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

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

Удвоение точки

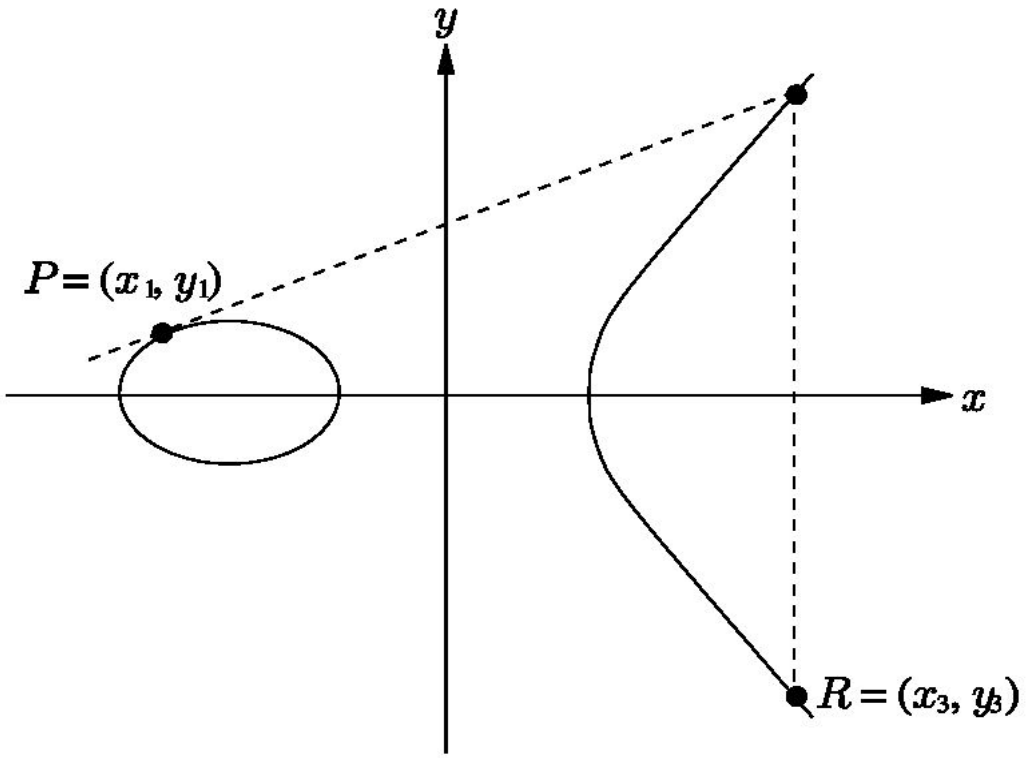
Если P = (x_1, y_1), то для нахождения удвоения P – точки R = (x_3, y_3) строится касательная к эллиптической кривой в точке P. Эта линия пересечёт эллиптическую кривую во второй точке. Тогда R - отражение этой точки на ось X





Удвоение точки

R=P + P = 2 × P



$$x_3 = \lambda^2 - 2x_1 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$$

Открытые и личные ключи

Личный ключ - некоторое случайное число x.

Открытым ключом будем считать координаты точки P = xG на эллиптической кривой P, где G — специальным образом выбранная точка эллиптической кривой («**базовая точка**»)

Координаты точки G вместе с коэффициентами уравнения, задающего кривую, являются параметрами схемы подписи и должны быть известны всем участникам обмена сообщениями. точка G должна иметь порядок q ($2^{254} < q < 2^{256}$).

Отечественный стандарт цифровой подписи ГОСТ 3410-2012

УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст

- содержит описание процессов формирования и проверки электронной цифровой подписи (ЭЦП), реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.

Отечественный стандарт цифровой подписи ГОСТ 3410-2012

1.Стандарт разработан взамен ГОСТ Р 34.10-2001.

2.Необходимость разработки настоящего стандарта вызвана потребностью в реализации ЭЦП разной степени стойкости в связи повышением уровня развития ВТ.

3.Стойкость ЭЦП основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11-2012.

Область применения

Настоящий стандарт определяет

- схему электронной цифровой подписи (ЭЦП)
- процессы формирования и проверки цифровой подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования

Внедрение цифровой подписи на базе настоящего стандарта повышает, по сравнению с РАНЕЕ действовавшей схемой цифровой подписи, уровень защищенности передаваемых сообщений от подделок и искажений.

Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

простое число *p* - модуль эллиптической кривой;

эллиптическая кривая *E* , задаваемая коэффициентами a,b ;

целое число *m* - порядок группы точек эллиптической кривой E;

простое число *q* - порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq,\ n \in Z,\ n \geq 1 \\ 2^{254} < q < 2^{256} \text{ или } 2^{508} < q < 2^{512} \end{cases}; \quad (9)$$

точка P≠*O* эллиптической кривой *E*, с координатами (x_p, y_p) , удовлетворяющая равенству $qP = O$;

хэш-функция отображающая сообщения h (‘):V*→V $_l$ представленные в виде двоичных векторов произвольной конечной длины, в двоичные вектора длины l бит. Хэш-функция определена в ГОСТ Р 34.11-2012

Если $2^{254} < q < 2^{256}$, то $l = 256$. Если $2^{508} < q < 2^{512}$, то $l = 512$.

Основные процессы

Механизм цифровой подписи определяется посредством реализации ***двух основных процессов*** :

- формирование подписи;

- проверка подписи.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, удовлетворяющие требованиям.

Математические объекты. Параметры цифровой подписи

Каждый пользователь схемы цифровой подписи должен обладать :

- **ключом подписи (ЛК)** - целым числом d , удовлетворяющим неравенству $0 < d < q$;
- **ключом проверки(ОК)** - точкой эллиптической кривой $Q = dP$ с координатами (x_q , y_q),.

Формирование цифровой подписи

Для получения цифровой подписи под сообщением $M \in V^*$ необходимо выполнить следующие действия (шаги) по ***алгоритму I:***

Шаг 1 - вычислить хэш-код сообщения

$$M : \bar{h} = h(M)$$

Шаг 2 - вычислить

$$e = h(\mathrm{mod}\, q)$$

Если $e = 0$, то определить $e = 1$.

Шаг 3 - сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству $0 < k < q$.

Шаг 4 - вычислить точку эллиптической кривой $C = kP$ и определить

$$r = x_c (\mathrm{mod}\, q)$$

Где x_c - -координата x точки C. Если $r = 0$, то вернуться к шагу 3

Шаг 5 - вычислить значение

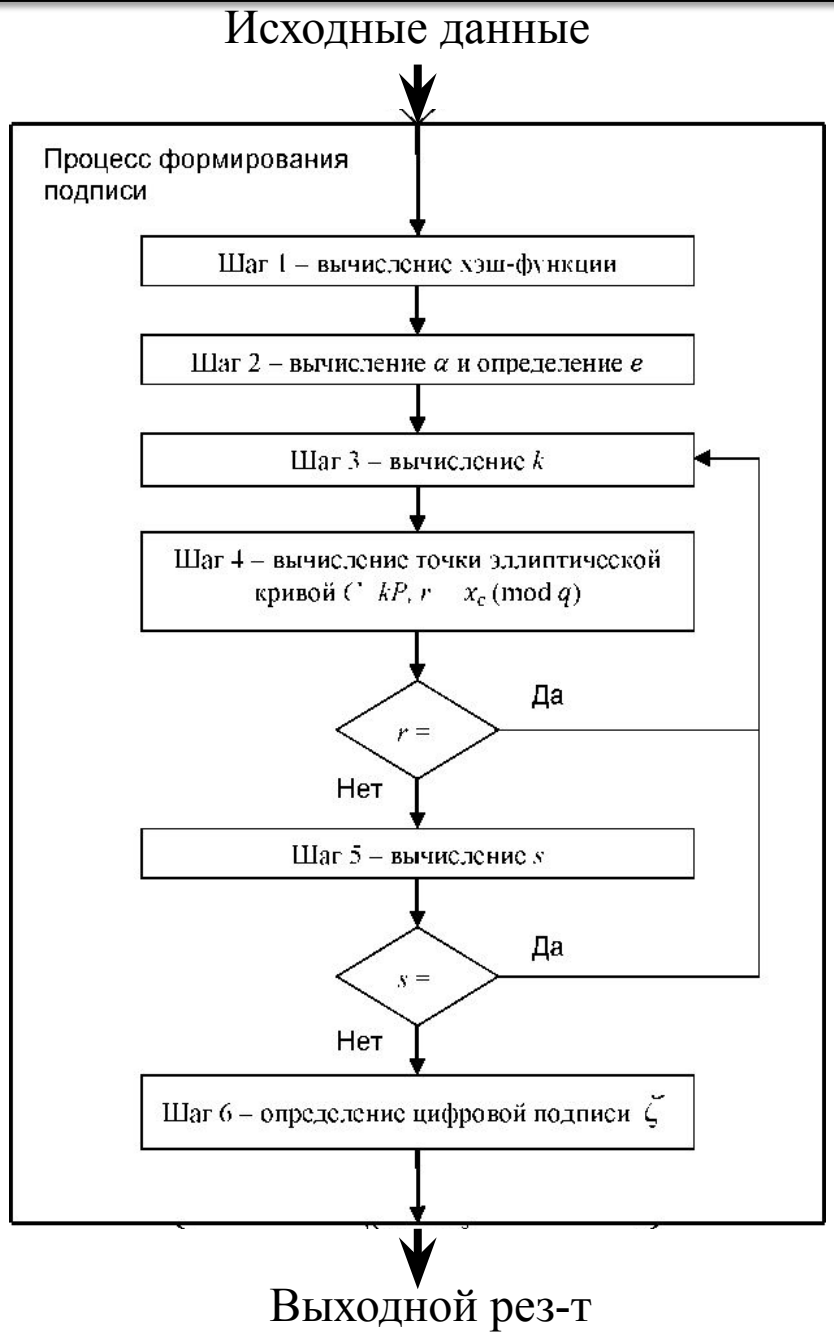
$$s \equiv (rd + ke)(\mathrm{mod}\, q)$$

Если $s = 0$, то вернуться к шагу 3.

Шаг 6 - определить цифровую подпись как конкатенацию двух двоичных векторов.

$$\zeta = (\bar{r} \| \bar{s})$$

Основные процессы. Формирование цифровой подписи

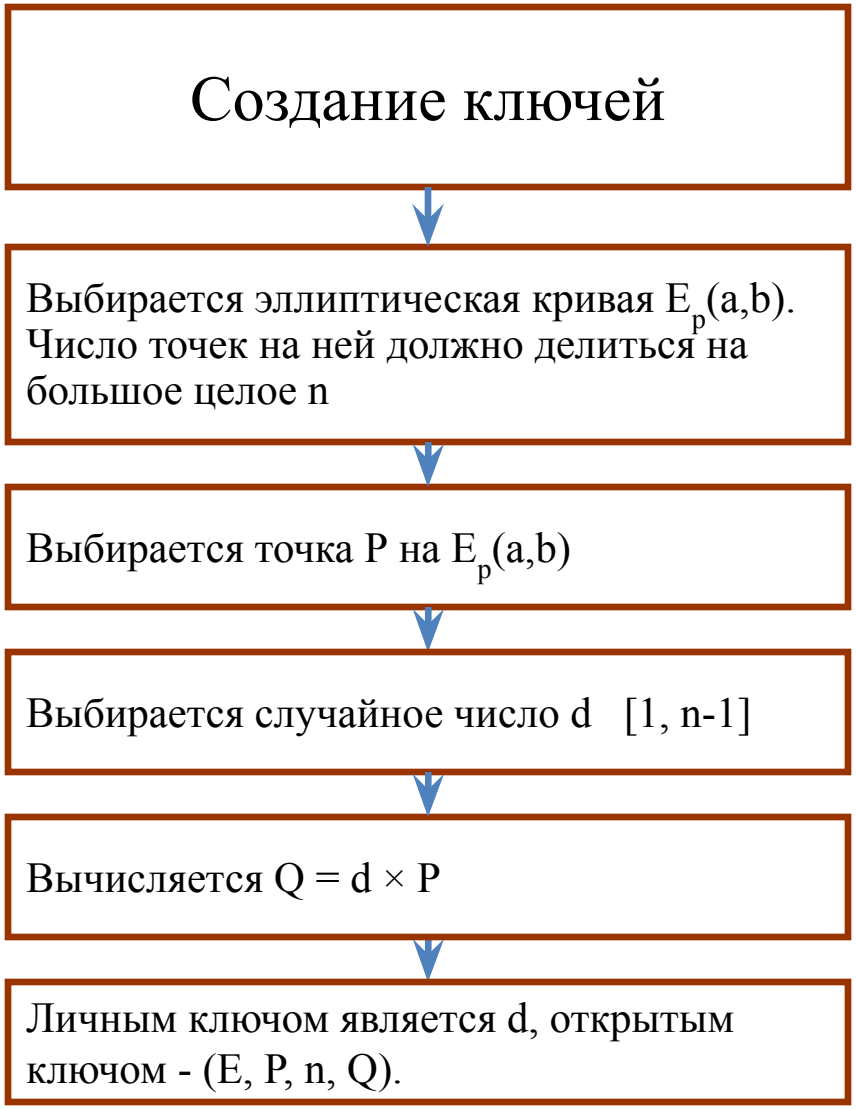


Исходные данные:

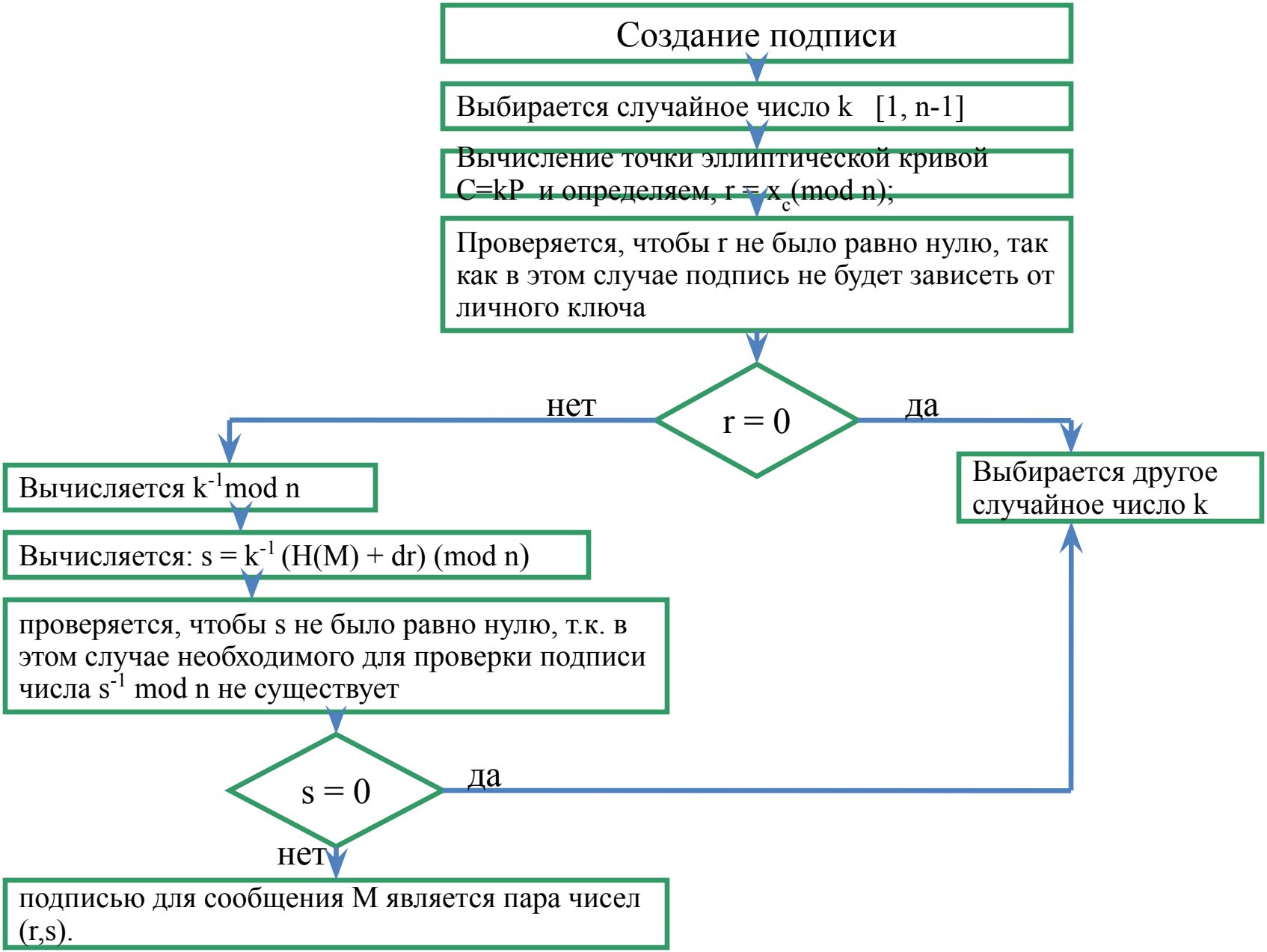
ключ подписи ***d*** и подписываемое сообщение ***M*** .

Выходной результат- цифровая подпись ζ

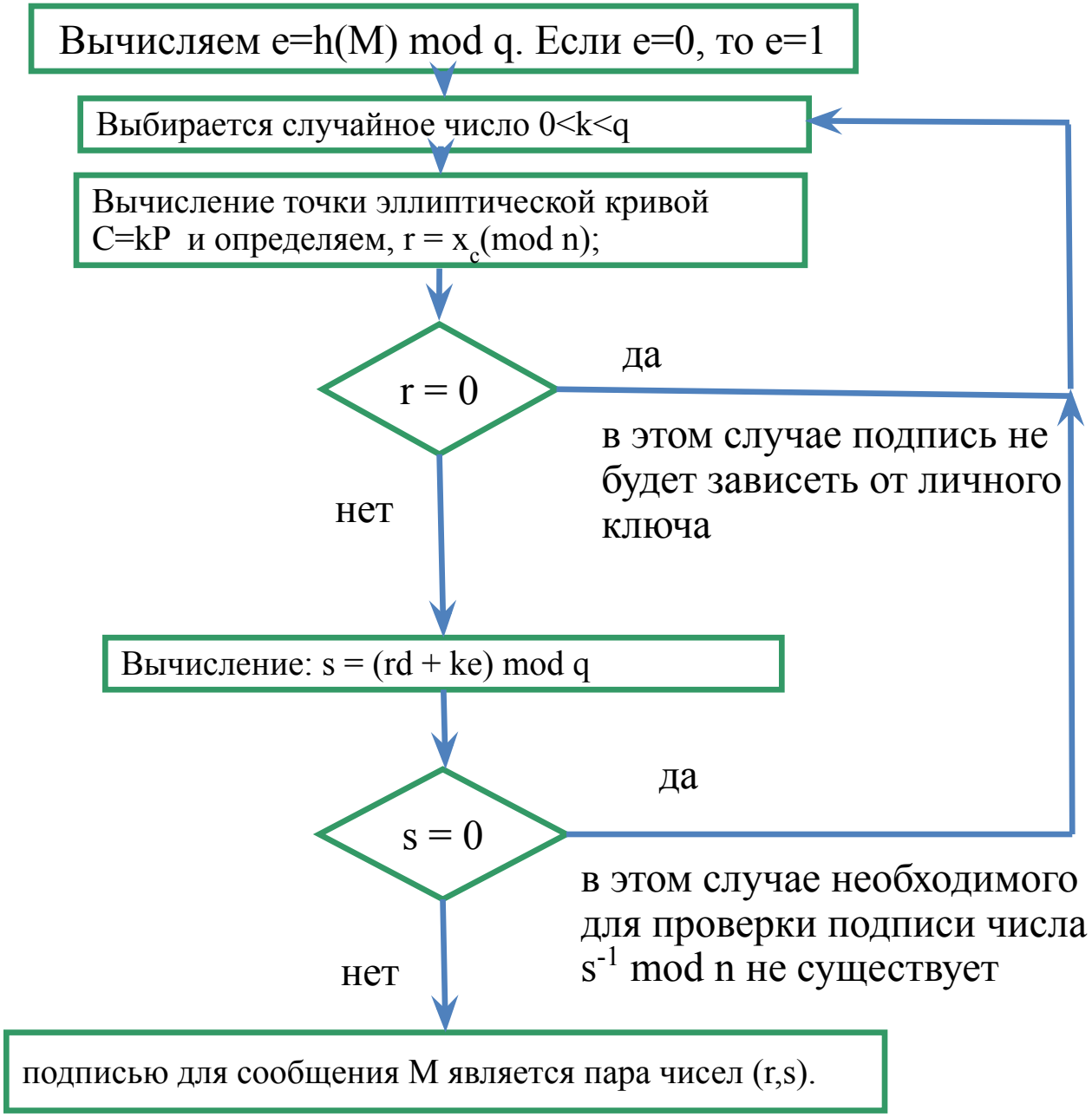
Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.



Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.



Создание электронной подписи на основе эллиптических кривых



Проверка цифровой подписи

Для проверки цифровой подписи ζ , под полученным сообщением M необходимо выполнить следующие действия (шаги) ***по алгоритму II:***

Шаг 1 - по полученной подписи ζ вычислить целые числа r и s . Если выполнены неравенства $0 < r < q$, $0 < s < q$, то перейти к следующему шагу.
В противном случае подпись неверна.

$$\overline{h} = h(M)$$

Шаг 3 - вычислить $e \equiv h(\bmod q)$
Если $e = 0$, то определить $e = 1$.

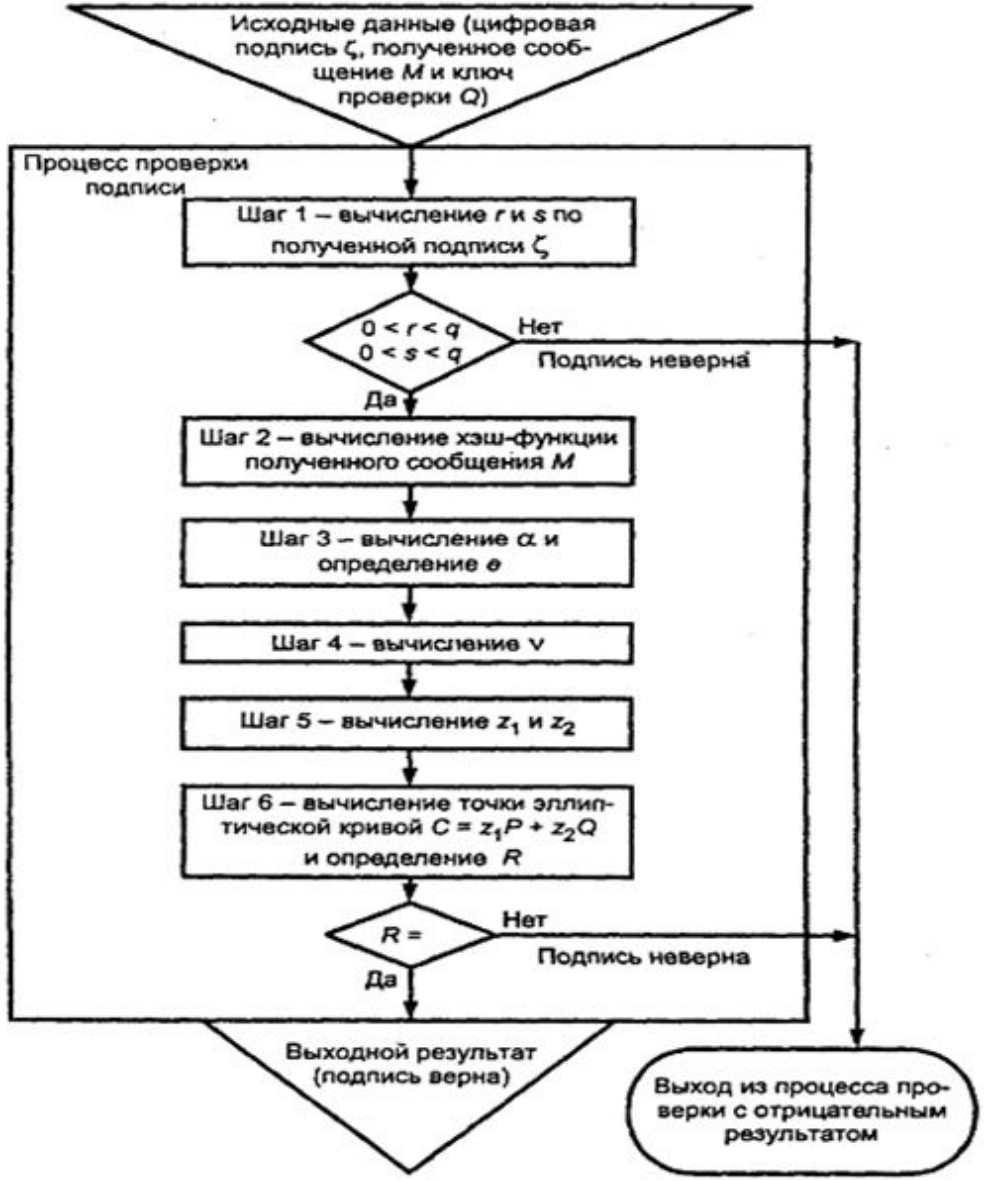
Шаг 4 - вычислить значение $v \equiv e^{-1}(\bmod q)$

Шаг 5 - вычислить значения
$$z_1 \equiv sv(\bmod q), z_2 \equiv -rv(\bmod q)$$

Шаг 6 - вычислить точку эллиптической кривой $C = z_1 P + z_2 Q$ и определить
$R \equiv x_c(\bmod q)$
где x_c - x -координата точки C .

Шаг 7 - если выполнено равенство $R = r$, то подпись принимается.
В противном случае, подпись неверна.

Основные процессы. Проверка цифровой подписи

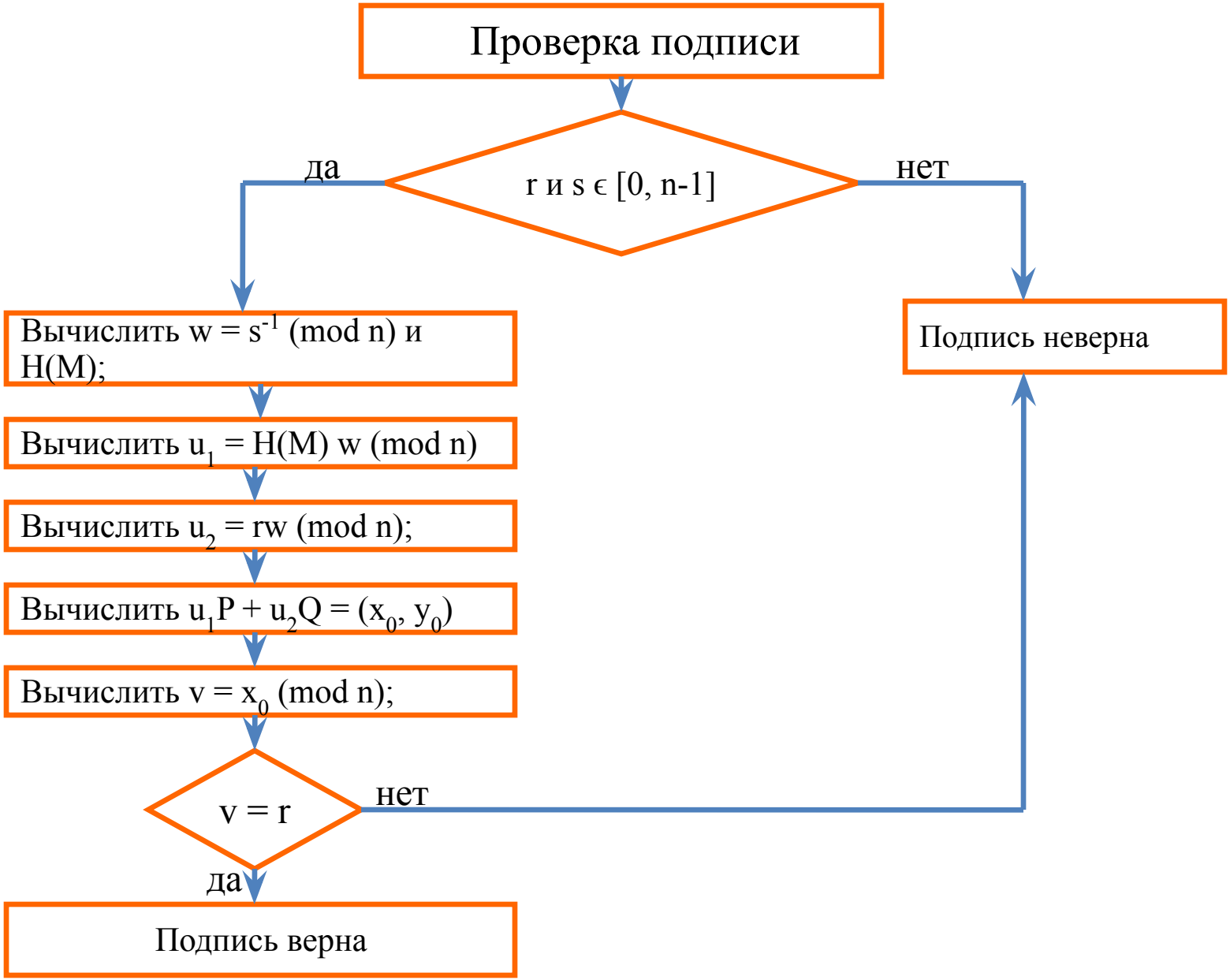


Исходные данные:

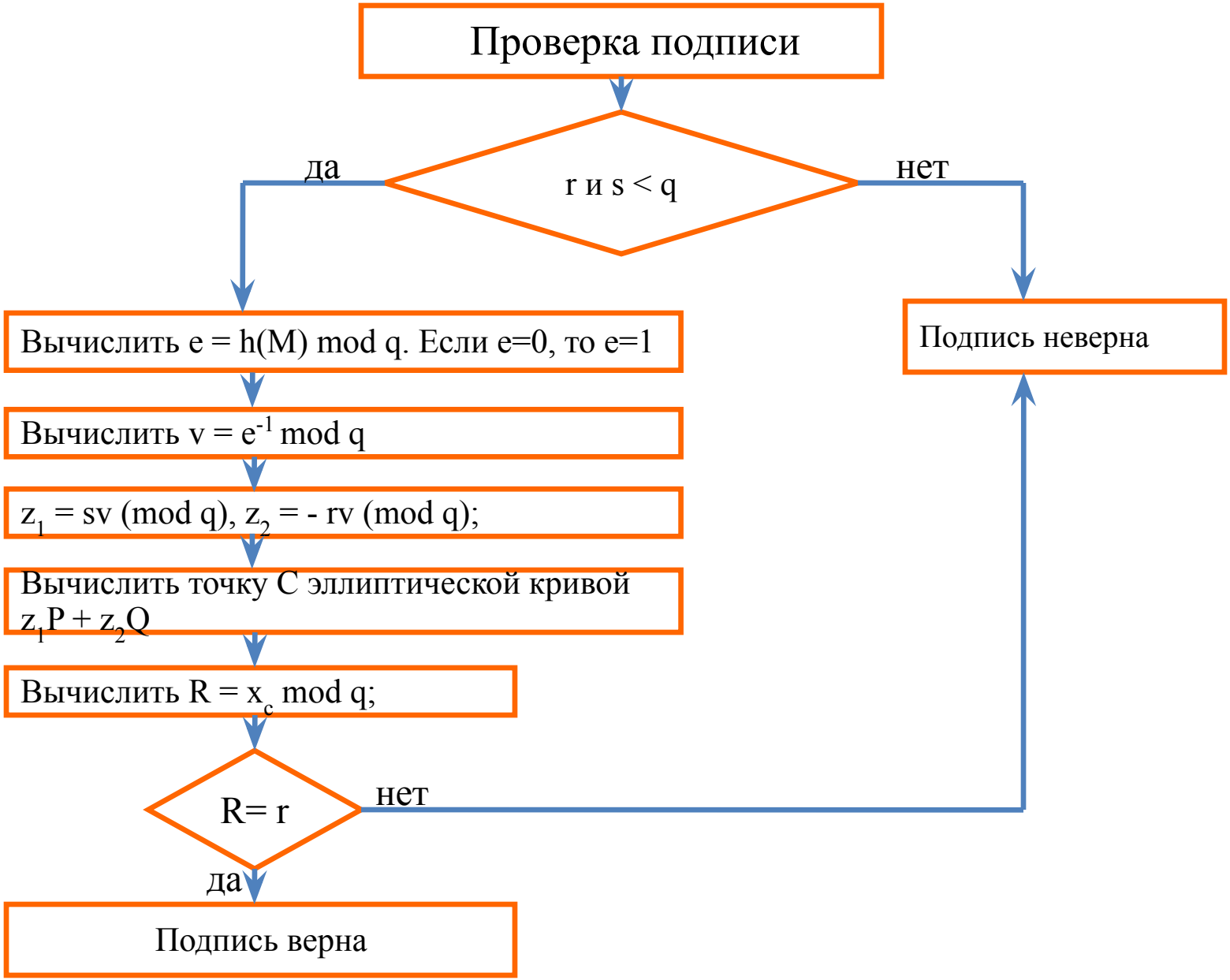
- подписанное сообщение ***M***
- цифровая подпись ζ
- ключ проверки ***Q***

Выходной результат- свидетельство о достоверности или ошибочности данной подписи.

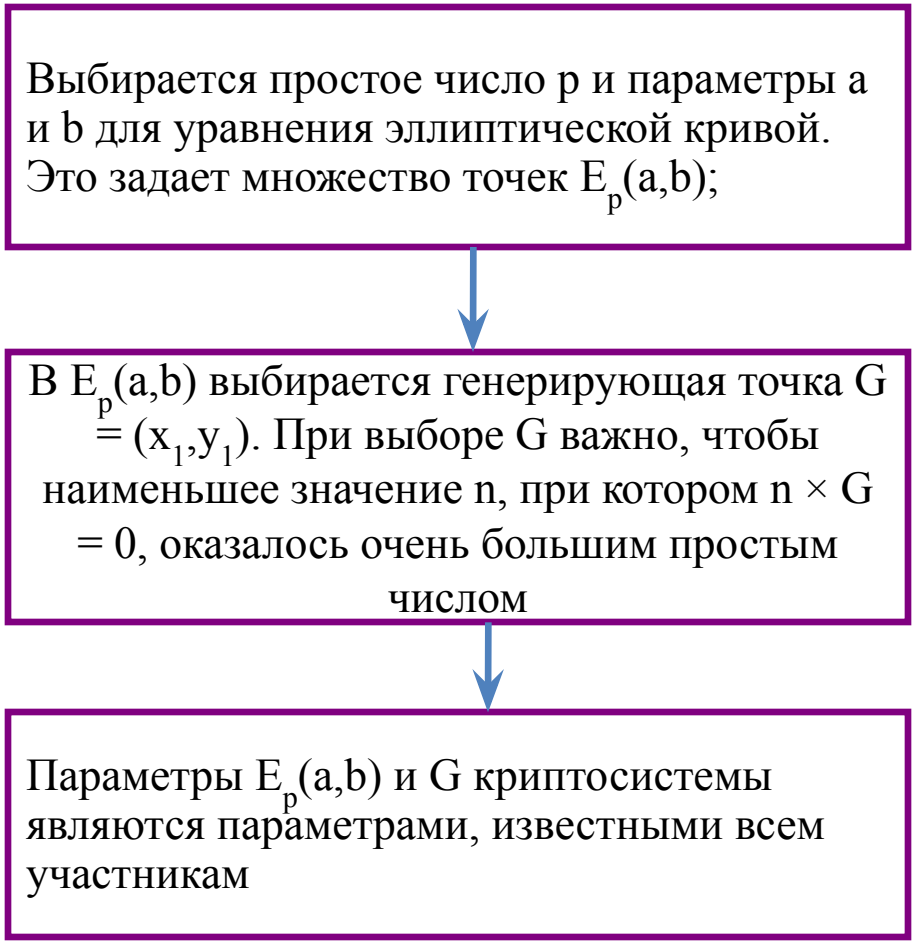
Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.



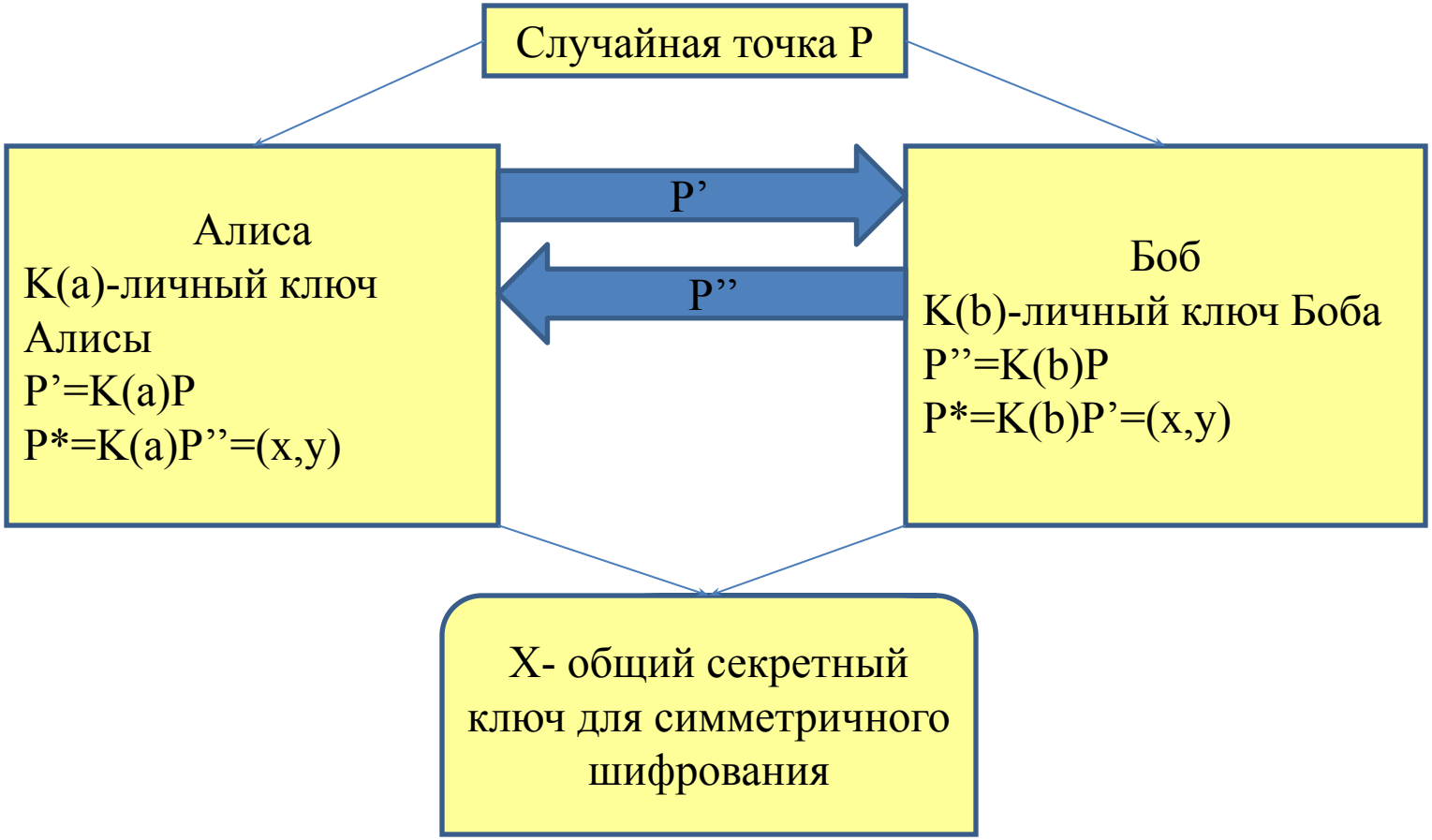
Проверка подписи на основе эллиптических кривых .



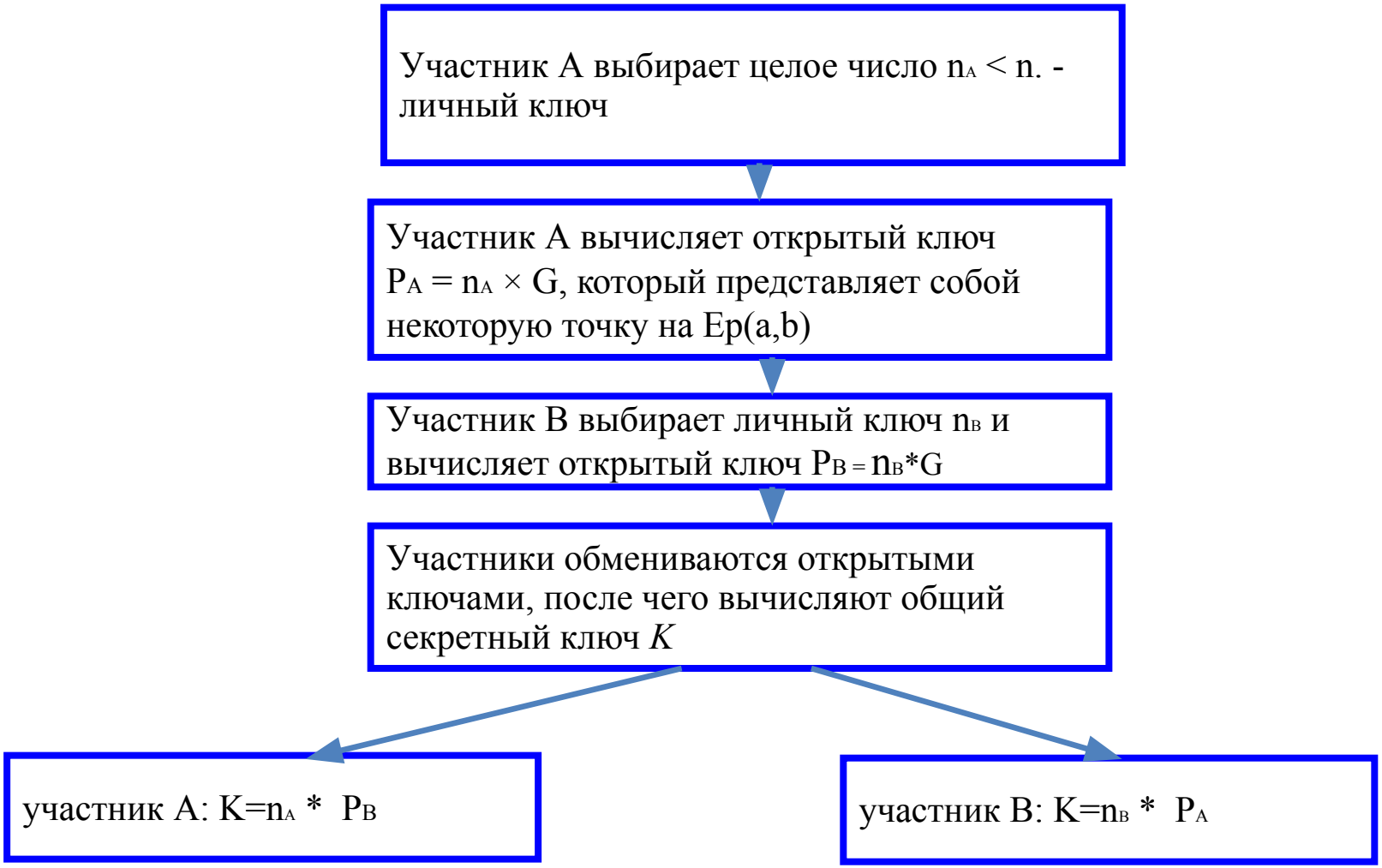
Криптография с использованием эллиптических кривых. Аналог алгоритма Диффи-Хеллмена обмена ключами



Пример алгоритма Диффи-Хеллмена на ЭК



Обмен ключами между пользователями A и B



общий секретный ключ представляет собой пару чисел. Если данный ключ предполагается использовать в качестве сеансового ключа для алгоритма симметричного шифрования, то из этой пары необходимо создать одно значение.

Криптография с использованием эллиптических кривых. Шифрование.

Зашифровать сообщение M, которое может быть представлено в виде точки на эллиптической кривой Pm (x,y);

↓

В качестве параметров рассматривается эллиптическая кривая Ep(a,b) и точка G на ней

↓

участник B выбирает личный ключ nB и вычисляет открытый ключ PB = nB × G

↓

Чтобы зашифровать сообщение Pm используется открытый ключ получателя B PB

↓

Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой:

$$Cm = \{k \times G, Pm + k \times PB\}$$

Криптография с использованием эллиптических кривых. Дешифрование.

Участник B умножает первую координату точки на свой ЛК и вычитает результат из второй координаты:
$Pm + k \times PB - nB \times (k \times G) = Pm + k \times (nB \times G) - nB \times (k \times G) = Pm$

↓

Участник A зашифровал сообщение Pm добавлением к нему kxPB. Противнику для восстановления сообщения придется вычислить k, зная G и $k \times G$

↓

Получатель также не знает k, но ему в качестве подсказки посылается $k \times G$

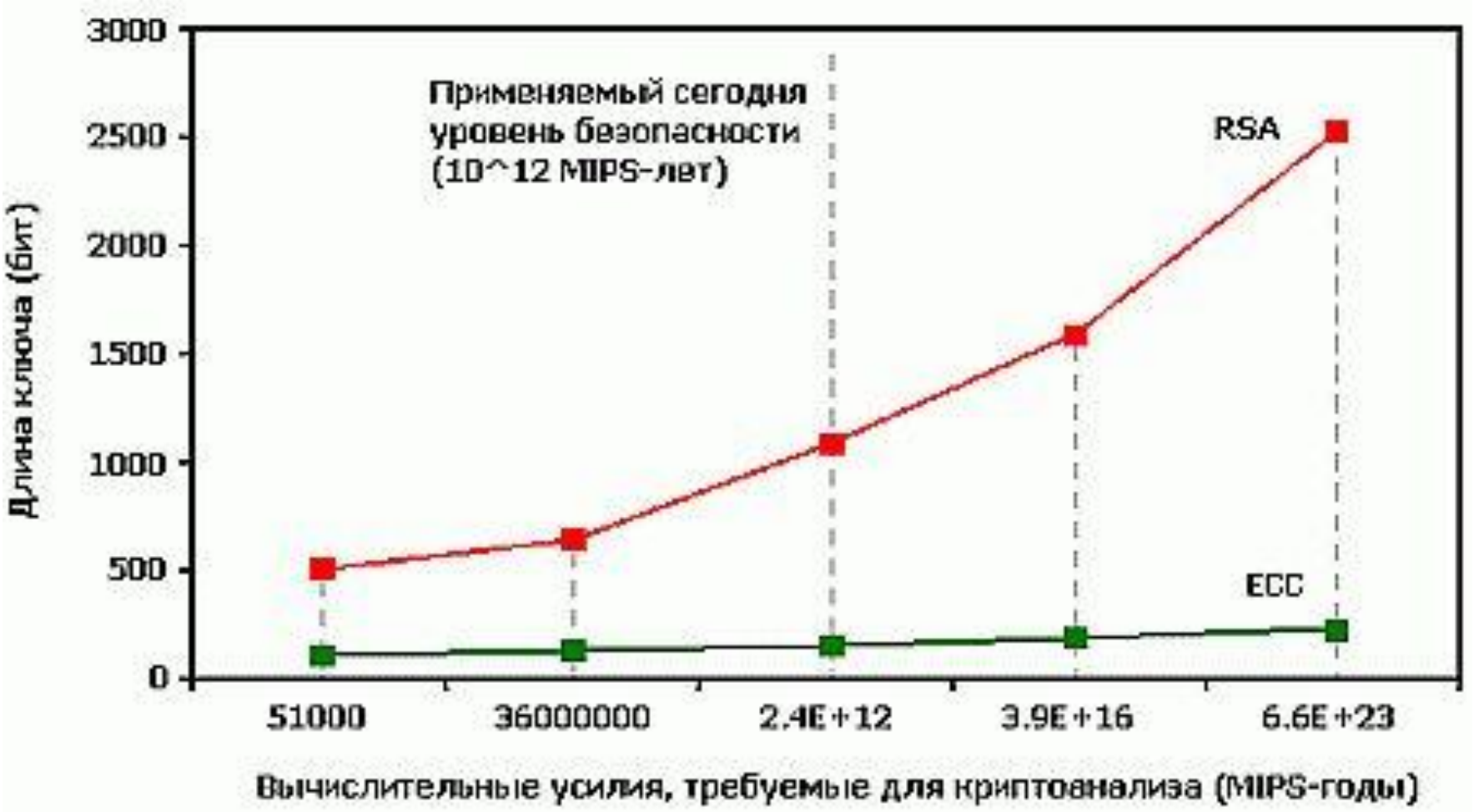
↓

Умножив $\boldsymbol{k \times G}$ на свой личный ключ, получатель получит значение, которое было добавлено отправителем к незашифрованному сообщению

↓

Тем самым получатель, не зная k, но имея свой личный ключ, может восстановить незашифрованное сообщение.

Сравнение криптостойкости с RSA



Сравнительные длины ключей

- При соответствующей криптостойкости

Симметричные алгоритмы	ECC	RSA / DH / DSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360