Часть III. Электронная цифровая подпись. Процессы формирования и проверки электронной цифровой подписи

Электронная цифровая подпись (далее кратко: цифровая подпись, или ЭЦП) к сообщению позволяет решить три задачи:

- осуществить аутентификацию источника сообщения;
- установить целостность сообщения;
- обеспечить невозможность отказа от авторства (т.е. факта подписи конкретного сообщения).

Цифровая подпись реализуется на основе двухключевых криптографических преобразований, в которых используются два ключа – *открытый* и *секретный*. С помощью секретного ключа формируется сама подпись, а с помощью открытого ключа осуществляется проверка подписи (без задания секретного ключа). Общедоступный открытый ключ формируется либо на основе секретного ключа, либо оба вырабатываются одновременно по специальным процедурам, причем предполагается, что вычисление секретного ключа по открытому ключу является вычислительно сложной математической задачей. Надежность схемы цифровой подписи определяется сложностью решения следующих задач:

- *подделки подписи*, т.е. формирования подписи под документом лицом, не являющимся владельцем секретного ключа;
- *создания подписанного сообщения*, т.е. нахождения хотя бы одного сообщения с правильной подписью;
- *подмены сообщения*, т.е. нахождения двух сообщений с одинаковой подписью.

В качестве подписываемого документа (сообщения) может быть использован любой файл. Подписанный файл создается из исходного (неподписанного) файла путем добавления к нему цифровой подписи. Каждая подпись содержит следующую информацию:

- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписывающем документ;
- идентификатор подписавшего (открытый ключ);
- собственно цифровую подпись.

Для реализации цифровой подписи необходимы два алгоритма:

- алгоритм вычисления цифровой подписи;
- алгоритм проверки цифровой подписи.

Отметим, что подписывается обычно не само сообщение M, длина которого может быть произвольной, а его сжатый образ $h = H(M)$ фиксированной длины, полученный путем хеширования сообщения.

III.1. Схемы цифровой подписи с использованием дискретных логарифмов в простом конечном поле

Алгоритмы цифровой подписи, формируемой на основе дискретных логарифмов, используют следующие параметры:

p – большое простое число;

q – большое простое число, являющееся делителем числа $p - 1$;

$g = \gamma^{\frac{p-1}{q}} mod\ p,$

где γ – любое число, для которого $1 < \gamma < p - 1$,

$y = g^x mod\ p,$

где $x \in [2, q - 1]$ – случайное число.

Первые три параметра p, q и g открыты и могут быть общими для группы абонентов криптосети. Секретным ключом абонента, подписывающего сообщение m, является x, а

открытым – y. В алгоритме используется однонаправленная хеш-функция H, с помощью которой вычисляется хеш-значение $h = \mathrm{H}(m)$ подписываемого сообщения m.

Подписью для сообщения m служит пара чисел (r, s), вычисляемая следующим образом:

1) абонент, подписывающий сообщение m, выбирает случайное число $k \in [1, q-1]$ (число k является секретным и одноразовым, после формирования подписи уничтожается и больше не используется);

2) вычисляется хеш-значение $h = H(m)$ для сообщения m;

3) вычисляется первая часть подписи:

$$r = g^k mod\ p;$$

4) вторая часть подписи – число s – извлекается из обобщенного уравнения подписи

$$ak = b + cx\ mod\ q.$$

Параметры a, b, c могут принимать различные значения. Некоторые варианты представлены в табл. 2.

При проверке подписи получатель должен убедиться в том, что выполняется следующее соотношение, называемое уравнением проверки:

$$r^a = g^b y^c\ mod\ q.$$

В другой схеме, более приближенной к существующим стандартам цифровой подписи (например, в России и США), число r определяется как

$$r = (g^k\ mod\ p)\ mod\ q.$$

При данном уравнении подписи, уравнение проверки имеет следующий вид:

$$r = (g^{u_1} \cdot y^{u_2} mod\ p)\ mod\ q,$$

где $u_1 = a^{-1}b\ mod\ q$, $u_2 = a^{-1}c\ mod\ q$.

Таблица 2

Некоторые схемы цифровой подписи с использованием дискретных логарифмов ($\rho = r\ mod\ q$)

Номер схемы	a, b, c	Уравнение подписи	Значение s $(mod\ q)$	Уравнение проверки $(mod\ p)$
1.	ρ, s, h	$\rho k = s + hx$	$s = \rho k - hx$	$r^\rho = g^s y^h$
2.	ρ, h, s	$\rho k = h + sx$	$s = (\rho k - h)x^{-1}$	$r^\rho = g^h y^s$
3.	s, ρ, h	$sk = \rho + hx$	$s = (\rho + hx)\ k^{-1}$	$r^s = g^\rho y^h$
4.	s, h, ρ	$sk = h + \rho x$	$s = (h + \rho x)\ k^{-1}$	$r^s = g^h y^\rho$
5.	h, ρ, s	$hk = \rho + sx$	$s = (hk - \rho)x^{-1}$	$r^h = g^\rho y^s$
6.	h, s, ρ	$hk = s + \rho x$	$s = hk - \rho x$	$r^h = g^s y^\rho$
7.	$\rho h, s, 1$	$\rho hk = s + x$	$s = \rho hk - x$	$r^{\rho h} = g^s y$
8.	$\rho h, 1, s$	$\rho hk = 1 + sx$	$s = (\rho hk - 1)x^{-1}$	$r^{\rho h} = g y^s$
9.	$s, \rho h, 1$	$sk = \rho h + x$	$s = (\rho h + x)k^{-1}$	$r^s = g^{\rho h} y$
10.	$s, 1, \rho h$	$sk = 1 + \rho hx$	$s = (1 + \rho hx)k^{-1}$	$r^s = g y^{\rho h}$
11.	$1, \rho h, s$	$k = \rho h + sx$	$s = (k - \rho h)x^{-1}$	$r = g^{\rho h} y^s$
12.	$1, s, \rho h$	$k = s + \rho hx$	$s = k - \rho hx$	$r = g^s y^{\rho h}$
13.	$\rho h, sh, 1$	$\rho hk = sh + x$	$s = \rho k - h^{-1}x$	$r^{\rho h} = g^{sh} y$
14.	$\rho h, 1, sh$	$\rho hk = 1 + shx$	$s = kx^{-1} - (hx)^{-1}$	$r^{\rho h} = g y^{sh}$
15.	$sh, \rho h, 1$	$shk = \rho h + x$	$s = (\rho + xh^{-1})k^{-1}$	$r^{sh} = g^{\rho h} y$
16.	$sh, 1, \rho h$	$shk = 1 + \rho hx$	$s = (1 + \rho hx)(hk)^{-1}$	$r^{sh} = g y^{\rho h}$
17.	$1, \rho h, sh$	$k = \rho h + shx$	$s = (k - \rho h)(hx)^{-1}$	$r = g^{\rho h} y^{sh}$
18.	$1, sh, \rho h$	$k = sh + \rho hx$	$s = kh^{-1} - x$	$r = g^{sh} y^{\rho h}$
19.	$\rho h, \rho s, 1$	$\rho hk = \rho s + x$	$s = hk - x\rho^{-1}$	$r^{\rho h} = g^{\rho s} y$

20.	$\rho h, 1, \rho s$	$\rho hk = 1 + \rho sx$	$s = x^{-1}(hk - \rho^{-1})$	$r^{\rho h} = gy^{\rho s}$
21.	$\rho s, \rho h, 1$	$\rho sk = \rho h + x$	$s = k^{-1}(h + x\rho^{-1})$	$r^{\rho s} = g^{\rho h}y$
22.	$\rho s, 1, \rho h$	$\rho sk = 1 + \rho hx$	$s = (\rho^{-1} + hx)k^{-1}$	$r^{\rho s} = gy^{\rho h}$
23.	$1, \rho h, \rho s$	$k = \rho h + \rho sx$	$s = (k\rho^{-1} - h)x^{-1}$	$r = g^{\rho h}y^{\rho s}$
24.	$1, \rho s, \rho h$	$k = \rho s + \rho hx$	$s = k\rho^{-1} - hx$	$r = g^{\rho s}y^{\rho h}$
25.	$sh, \rho s, 1$	$shk = \rho s + x$	$s = x(hk - \rho)^{-1}$	$r^{sh} = g^{\rho s}y$
26.	$\rho s, sh, 1$	$\rho sk = sh + x$	$s = x(\rho k - h)^{-1}$	$r^{\rho s} = g^{sh}y$
26.	$sh, 1, \rho h$	$shk = 1 + \rho hx$	$s = (h^{-1} + \rho x)k^{-1}$	$r^{sh} = gy^{\rho h}$

III.2. Некоторые стандарты цифровой подписи

2.1. Федеральный стандарт США

В 1994 году Национальный институт стандартов США предложил для использования окончательный вариант стандарта цифровой подписи DSS (Digital Signature Standard) и соответствующий ему алгоритм DSA ($Digital\ Signature\ Algorithm$):

Открытые параметры системы для группы абонентов:

p – простое число от 512 до 1024 битов;

q – 160-битовый простой делитель $p - 1$;

$g = \gamma^{(p-1)/q} mod\ p$, где γ – любое число меньше $p - 1$, для которого $g > 1$.

Секретный ключ подписывающего сообщения:

x – 160-битовое число, $x \in [1, q - 1]$.

Открытый ключ подписывающего сообщения:

$y = g^x\ mod\ p$ – p-битовое число.

q – 160-битовый простой делитель $p - 1$;

$g = \gamma^{(p-1)/q} mod\ p$, где γ – любое число меньше $p - 1$, для которого $g > 1$.

Секретный ключ подписывающего сообщения:

x – 160-битовое число, $x \in [1, q - 1]$.

Открытый ключ подписывающего сообщения:

$y = g^x\ mod\ p$ – p-битовое число.

Вычисление подписи (r, s) *для сообщения* m:

$k \in [1, q-1]$ выбирается случайно;

$r := (g^k\ mod\ p)\ mod\ q$;

$s := (k^{-1}\ h + xr)\ mod\ q$,

где $h = H(m)$ – хеш-значение сообщения m, вычисленное согласно алгоритму SHA.

Проверка подписи:

$w := s^{-1}\ mod\ q$;

$u_1 := (hw)\ mod\ q$;

$u_2 := (rw)\ mod\ q$;

$v := ((g^{u_1} \cdot g^{u_2})\ mod\ p)\ mod\ q$.

Если $v = r$, то подпись правильна.

В стандарте рекомендуется конкретный метод генерации параметров системы – простых чисел p и q, позволяющий избежать слабых значений p и q и проверить, что эти числа генерировались случайным образом.

2.2. ГОСТ Р34.10-94

Алгоритм похож на DSA, но использует другое уравнение подписи, приводящее к другому уравнению проверки подписи. Алгоритм также использует однонаправленную хеш-функцию H из стандарта ГОСТ Р34.11-94, возвращающую 256-битовое хеш-значение $h = H(m)$:

Открытые параметры системы для группы абонентов:

p – простое число, длина которого находится в диапазоне либо от 509 до 512 битов, либо от 1020 до 1024 битов;

q – простой делитель $p - 1$ длиной от 254 до 256 битов;

a – любое число, меньшее $p - 1$, для которого $a^q mod\ p = 1$.

Секретный ключ подписывающего сообщение:

x – число, меньшее q.

Открытый ключ подписывающего сообщение:

$y\ = a^x mod\ p$.

Вычисление подписи (r, s) *для сообщения* m:

$k \in [1, q - 1]$ выбирается случайно;

$r := (a^k mod\ p)\ mod\ q$;

$s := (xr + kh)\ mod\ q$.

Если $h\ mod\ q = 0$, то $h := 1$; если $r = 0$ или $s = 0$, то генерируется другое k и вычисления выполняются заново. Подписью служат два 256-битовых числа: $r\ mod\ 2^{256}$, $s\ mod\ 2^{256}$.

Проверка подписи:

Проверяются условия $0 < s < q$ и $0 < r < q$; если хотя бы одно из них не выполнено, то подпись считается недействительной; вычисляется хеш-значение $h' = H(m')$ полученного сообщения m'; если $h' = 0$, то $h' := 1$; вычисляются

$v := (h')^{q-2} mod\ q$;

$z_1 := s \cdot v\ mod\ q$;

$z_2 := ((q - r) \cdot v)\ mod\ q$;

$u := ((a^{z_1} \cdot y^{z_2})\ mod\ p) mod\ q$;

Если $u = v$, то подпись считается правильной; в противном случае подпись считается недействительной.

Стандарт предписывает процедуру выработки параметров системы p, q и a.

2.3. ГОСТ Р 34.10-2001

Настоящий стандарт содержит описание процессов формирования и проверки электронной цифровой подписи (ЭЦП), реализуемой с использованием операций группы точек эллиптической кривой над простым конечным полем.
Стандарт разработан взамен ГОСТ Р 34.10-94.

2.3.1. Обозначения

V_{256} – множество всех двоичных векторов длиной 256 бит;

V_∞ – множество всех двоичных векторов произвольной конечной длины;

$\mathbb{Z}$ – множество всех целых чисел;

p – простое число, $p > 3$;

$\mathbb{F}_p$ – конечное простое поле, представляемое как множество из p целых чисел $\{0, 1, \ldots, p - 1\}$;

$b\ (mod\ p)$ – минимальное не отрицательное число, сравнимое с b по модулю p;

M – сообщение пользователя, $M \in V_\infty$;

$(\overline{h}_1 \| \overline{h}_2)$ – конкатенация (объединение) двух двоичных векторов;

a, b – коэффициенты эллиптической кривой;

m – порядок группы точек эллиптической кривой;
q – порядок подгруппы группы точек эллиптической кривой;
O – нулевая точка эллиптической кривой;
P – точка эллиптической кривой порядка q;
d – целое число – ключ подписи;
Q – точка эллиптической кривой – ключ проверки;
ζ – цифровая подпись под сообщением M.

2.3.2. Общие положения

Общепризнанная схема цифровой подписи охватывает три процесса:
– генерация ключей (подписи и проверки);
– формирование подписи;
– проверка подписи.

В данном стандарте процесс генерации ключей (подписи и проверки) не рассмотрен. Механизм цифровой подписи определяется посредством реализации двух основных процессов
– формирование подписи;
– проверка подписи.

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:
– осуществить контроль целостности передаваемого подписанного сообщения,
– доказательно подтвердить авторство лица, подписавшего сообщение,
– защитить сообщение от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 1.

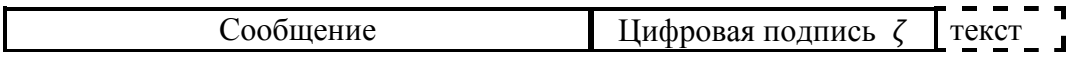

Рис 1. *Схема подписанного сообщения*

Поле "текст", показанное на рис. 1 и дополняющее поле "цифровая подпись", может содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в стандарте схема цифровой подписи реализована с использованием операций группы точек эллиптической кривой, определенной над простым конечным полем, а также хэш-функции.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Цифровая подпись, представленная в виде двоичного вектора длиной 512 бит, вычисляется с помощью определенного ниже набора правил.

2.3.3. Математические определения

Пусть задано простое число $p > 3$. Тогда *эллиптической кривой E*, определенной над простым конечным полем $\mathbb{F}_p$, называется множество пар чисел (x, y), $x, y \in F_p$, удовлетворяющих тождеству

$$y^2 = x^3 + ax + b \ (mod\ p), \qquad (1)$$

где $a, b \in \mathbb{F}_p$ и $4a^3 + 27b^2 \not\equiv 0 \ (mod\ p)$.

Инвариантом эллиптической кривой называется величина $J(E)$, удовлетворяющая тождеству

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2}(mod\ p). \qquad (2)$$

Коэффициенты a, b эллиптической кривой E, по известному инварианту $J(E)$, определяются следующим образом

$$\begin{cases} a \equiv 3k(mod\ p), \\ b \equiv 2k(mod\ p), \end{cases} \tag{3}$$

где $k = \dfrac{J(E)}{1728 - J(E)}\ (mod\ p), \qquad J(E) \neq 0$ или 1728 .

Пары (x, y), удовлетворяющие тождеству (1), называются *точками эллиптической кривой* E; x и y − соответственно x- и y-координатами точки.

Точки эллиптической кривой обозначаются через $Q(x, \mathrm{y})$ или просто Q. Две точки эллиптической кривой равны, если равны их соответствующие x- и y-координаты.

На множестве всех точек эллиптической кривой E введена операция сложения, которая обозначается знаком " + ". Операция сложения точек $Q_1(x_1, \mathrm{y}_1)$ и $Q_2(x_2, y_2)$, результатом которой будет точка $Q_3(x_3, y_3)$, определяется следующим образом.

Если $x_2 \neq x_1$, то

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \quad (mod\ p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1\ (mod\ p), \end{cases} \tag{4}$$

где $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}(mod\ p)$.

Если $x_2 = x_1$ и $y_2 = y_1 \neq 0$, то

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 \quad (mod\ p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1\ (mod\ p), \end{cases} \tag{5}$$

где $\lambda = \dfrac{3x_1^2 + a}{2y_1}(mod\ p)$.

Наконец, если $x_2 = x_1$ и $y_1 = -y_2\ (\mathrm{mod}\ p)$, то сумму точек Q_1 и Q_2 будем называть *нулевой точкой* $\mathcal{O}$, не определяя ее x- и y-координаты (при $b \neq 0$ можно обозначить $\mathcal{O} = (0,0)$). В этом случае точка Q_2 называется *отрицанием* точки Q_1. Для нулевой точки $\mathcal{O}$ выполнены равенства

$$Q + \mathcal{O} = \mathcal{O} + Q = Q \tag{6}$$

где Q − произвольная точка эллиптической кривой E .

Относительно введенной операции сложения множество всех точек эллиптической кривой E, вместе с нулевой точкой, образуют конечную абелеву (т.е. коммутативную) группу порядка m , для которого выполнено неравенство

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 - 2\sqrt{p}. \tag{7}$$

Точка Q называется точкой кратности k, или просто кратной точкой эллиптической кривой E, если для некоторой точки P выполнено равенство

$$Q = P + \cdots + P = kP. \tag{8}$$

2. 3.4. Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

− простое число $p > 2^{255}$ − модуль эллиптической кривой. Верхняя граница данного числа должна определяться при конкретной реализации схемы цифровой подписи;

− эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$;

− 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:

$$m = nq, \ \ n \in Z, \ \ n \geq 1; \qquad 2^{255} < q < 2^{256}, \tag{9}$$

− точка $P \neq 0$ эллиптической кривой E , с координатами $(x_p. y_p)$, удовлетворяющая равенству $qP = 0$;

− хэш-функция $h(\cdot)$: $V_\infty \longrightarrow V_{256}$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные вектора длины 256 бит. Хэш-функция определена в ГОСТ Р 34.11.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

− ключом подписи − целым числом d, удовлетворяющим неравенству $0 < d < q$;

− ключом проверки − точкой эллиптической кривой Q с координатами (x_q, y_q) , удовлетворяющей равенству $dP = Q$.

На приведенные выше параметры схемы цифровой подписи накладываются следующие требования:

− должно быть выполнено условие $p^t \neq 1(mod\ p)$ для всех целых $t =, 2, \ldots B$, где B удовлетворяет неравенству $B \geq 31$;

− должно быть выполнено неравенство $m \neq p$;

− инвариант кривой должен удовлетворять условию $J(E) \neq 0$ или 1728.

2. 3.5. Двоичные векторы

Для определения процессов формирования и проверки цифровой подписи необходимо установить соответствие между целыми числами и двоичными векторами длины 256 бит.

Рассмотрим следующий двоичный вектор длиной 256 бит, в котором младшие биты расположены справа, а старшие − слева

$$\overline{h} = (\alpha_{255}, \ldots, \alpha_0),\ \ \overline{h} \in V_{256} \tag{10}$$

где α_i, $i = 0, \ldots, 255$, равно либо 1, либо 0. Будем считать, что число $\alpha \in Z$ *соответствует* двоичному вектору $\overline{h}$, если выполнено равенство

$$\alpha = \sum_{i=0}^{255} \alpha_i\, 2^i. \tag{11}$$

Для двух двоичных векторов $\overline{h}_1$ и $\overline{h}_2$, соответствующих целым числам α и β, определим операцию конкатенации (объединения) следующим образом. Пусть

$$\overline{h}_1 = (\alpha_{255}, \ldots, \alpha_0), \quad \overline{h}_2 = (\beta_{255}, \ldots, \beta_0), \tag{12}$$

тогда их объединение имеет вид

$$\overline{h}_1 \| \overline{h}_2 = (\alpha_{255}, \ldots, \alpha_0, \beta_{255}, \ldots, \beta_0) \tag{13}$$

и представляет собой двоичный вектор длиной 512 бит, составленный из коэффициентов векторов $\overline{h}_1$ и $\overline{h}_2$

С другой стороны, приведенные формулы определяют способ разбиения двоичного вектора h длиной 512 бит на два двоичных вектора длиной 256 бит, конкатенацией которых он является.

2. 3.6. Формирование цифровой подписи

Каждый пользователь должен иметь ключ подписи d и ключ проверки подписи $Q(x_q, y_q)$.

Для получения цифровой подписи под сообщением $M \in V_\infty$ необходимо выполнить следующие действия (шаги):

Шаг 1 − вычислить хэш-код $\overline{h} = h(M)$ сообщения M.

Шаг 2 − вычислить целое число a, двоичным представлением которого является вектор $\overline{h}$, и определить $e = a(mod\ q)$. Если $e = 0$, то положить $e = 1$.

Шаг 3 − сгенерировать случайное (псевдослучайное) целое число $k \in [1, q - 1]$,

Шаг 4 − вычислить точку кривой $C = kP$ и определить $r = x_c\ (mod\ q)$, где x_c − - координата точки C . Если $r = 0$, то вернуться к шагу 3.

Шаг 5 − вычислить значение $s \equiv (rd + ke)(mod\ q)$. Если $s = 0$, то вернуться к шагу 3.

Шаг 6 − вычислить двоичные векторы $\overline{r}$ и $\overline{s}$, соответствующие r и s, и определить цифровую подпись $\zeta = (\overline{r} \parallel \overline{s})$ как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи d и подписываемое сообщение M, а выходным результатом − цифровая подпись ζ.

2. 3.7. Проверка цифровой подписи

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***.

Шаг 2 − вычислить хэш-код $\overline{h} = h(M)$ полученного сообщения M.

Шаг 3 − вычислить целое число a, двоичным представлением которого является вектор $\overline{h}$, и определить $e = a\ (mod\ q)$ Если $e = 0$, то положить $e = 1$.

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

Шаг 5 − вычислить значения

$$z_1 = sv\ (mod\ q),\ z_2 = -rv\ (mod\ q)$$

Шаг 6 − вычислить точку кривой $C = z_1P + z_2Q$ и определить $R = x_c(mod\ q)$ где x_c − -координата точки C.

Шаг 7 − если выполнено равенство $R = r$, то подпись ***принимается***, в противном случае, подпись ***неверна***.

Исходными данными этого процесса являются подписанное сообщение M, цифровая подпись ζ, и ключ проверки Q, а выходным результатом − свидетельство о достоверности или ошибочности данной подписи.

2. 3.8. Приложение. Контрольный пример

Все числовые значения приведены в десятичной и шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления. Символ "||" обозначает перенос числа на новую строку. Например, запись

$$12345\|67890_{10}$$
$$499602D2_{16}$$

представляет целое число 1234567890, соответственно, в десятичной и шестнадцатеричной системах счисления.

Модуль эллиптической кривой. В данном примере параметру p присвоено следующее значение:

$p =$ 57896044618658097711785492504343953926‖
$6349923328202820197287920039565648210 41_{10}$
$p_{(256)} =$ 8000000000000000000000000000000000‖
$00000000000000000000000000000431_{16}$

Коэффициенты эллиптической кривой. В данном примере параметры a и b принимают следующие значения:

$a = 7_{10}$
$a = 7_{16}$
$b =$ 43308876546767276905765904595650931995‖
$94211179445103958325296884203384958041 4_{10}$
b = 5FBFF498AA938CE739B8E022FBAFEF40563‖
$F6E6A3472FC2A514COCE9DAE23B7E_{16}$

Порядок группы точек эллиптической кривой. В данном примере параметр m принимает следующее значение:

$m =$ 57896044618658097711785492504343953 92‖
$708293458372545062238097359213763106961 9_{10}$
$m =$ 8000000000000000000000000000000001‖
$50FE8A1892976154C59CFC193ACCF5B3_{16}$

Порядок циклической подгруппы группы точек эллиптической кривой. В данном примере параметр q принимает следующее значение:

$q =$ 57896044618658097711785492504343953 92‖
$708293458372545062238097359213763106961 9_{10}$
$q =$ 8000000000000000000000000000000001‖

$$50FE8A1892976154C59CFC193ACCF5B3_{16}$$

Коэффициенты точки эллиптической кривой. В данном примере координаты точки P принимают следующие значения:

$$x_P = 2_{10}$$
$$x_P = 2_{16}$$
$$y_P = 40189740565390375033354494229370597\|$$
$$75635739389905545080690979365213431566280_{10}$$
$$y_P = 8E2A8A0E65147D4BD6316030E16D19\|$$
$$C85C97FOA9CA267122B96ABBCEA7E8FC8_{16}.$$

Ключ подписи. В данном примере считается, что пользователь обладает следующим ключом подписи d:

$$d = 55441196065363246126355624130324183 1\|$$
$$96576709222340016572108097750006097525544_{10}$$
$$d = 7A929ADE789BB9BE10ED359DD39A72C\|$$
$$11B60961F49397EEE1D19CE9891EC3B28_{16}$$

Ключ проверки. В данном примере считается, что пользователь обладает ключом проверки Q, координаты которого имеют следующие значения:

$$x_q = 57520216126176808443631405023338071\|$$
$$1766301049063136321828967413422066048594 03_{10}$$
$$x_q = 7F2B49E270DB6D90D8595BEC458B5\|$$
$$0C58585BAlD4E9B788F6689DBD8E56FD80B_{16}$$
$$y_q = 176149444192137815438093919496540 80\|$$
$$03194266204536363926070984785943828676399 4_{10}$$
$$y_q = 26F1B489D6701DD185C8413A977B3\|$$
$$CBBAF64D1C593D26627DFFB101A87FF77DA_{16}$$

Процесс формирования цифровой подписи. Пусть после выполнения шагов $1-3$ получены следующие числовые значения:

$$e = 20798893674476452017134061561508270 13\|$$
$$06371425153796532899526172526614688724 21_{10}$$
$$e = 2DFBC1B372D89A1188C09C52E0EE\|$$
$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$$
$$k = 53854137677348463731403841147996619 2\|$$
$$41504003434302020712960838528893196233395_{10}$$
$$k = 77105C9B20BCD3122823C8CF6FCC\|$$
$$7B956DE33814E95B7FE64FED924594DCEAB3_{16}$$

При этом кратная точка $C = kP$ имеет координаты:

$$x_c = 29700980915817952874371204983938256 9\|$$
$$90422752107994319651632687982059210933395_{10}$$
$$x_c = 41AA28D2F1AB148280CD9ED56FED\|$$
$$A41974053554A42767B83AD043FD39DC049316_{16}$$
$$y_c = 32842535278684663477094665322517084 5\|$$
$$06804721032454543268132854556539274060910_{10}$$
$$y_c = 489C375A9941A3049E33B34361DD\|$$
$$204172AD98C3E5916DE27695D22A61FAE46E_{16}$$

Параметр $r = x(mod\ q)$ принимает значение:

$$r = 29700980915817952874371204983938256 9\|$$
$$90422752107994319651632687982059210933395_{10}$$
$$r = 41AA28D2F1AB148280CD9ED56FED\|$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$

Параметр $s = (rd + ke)\ (mod\ q)$ принимает значение:

$$s = 57497340027008465417892531001914703\|$$
$$84552270426490985639337189991755158395 52_{10}$$
$$s = 1456C64BA4642A1653C235A98A60249BC\|$$
$$D6D3F746B631DF928014F6C5BF9C40_{16}$$

Процесс проверки цифровой подписи. Пусть после выполнения шагов $1-3$ получено следующее числовое значение:

$$e = 20798893674476452017134061561508270 13\|$$
$$06371425153796532899526172526614688724 21_{10}$$
$$e = 2DFBC1B372D89A1188C09C52EOEE\|$$
$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$$

При этом параметр $v = e^{-1}(\mathrm{mod}\ q)$ принимает значение:

$v = 176866836059344686773017138249002685\|$
$62746883080675496715288036572431145718978_{10}$
$v = 271A4EE429F84EBC423E388964555BB\|$
$29D3BA53C7BF945E5FAC8F381706354C2_{16}$

Параметры $z_1 = sv(mod\ q)$ и $z_2 = -rv(\mathrm{mod}\ q)$ принимают значения:

$z_1 = 37699167500901938556841057293512656 1\|$
$08841345190491942619304532412743720999759_{10}$
$z_1 = 5358F8FFB38F7C09ABC782A2DF2A\|$
$3927DA4077D07205F763682F3A76C9019B4F_{16}$
$z_2 = 14171998427343472112515917969500765 7\|$
$69246655838972862114499932653333671092 21_{10}$
$z_2 = 3221B4FBBF6D101074EC14AFAC2D4F7\|$
$EFAC4CF9FEC1ED11BAE336D27D527665_{16}$

Точка $C = z_1P + z_2Q$ имеет координаты:

$x_c = 297009809158179528743712049839382569 9\|$
$04227521079943196516326879820592109333 95_{10}$
$x_c = 41AA28D2F1AB148280CD9ED56FED\|$
$A41974053554A42767B83AD043FD39DC0493_{16}$
$y_c = 328425352786846634770946653225170845 0\|$
$68047210324545432681328545565392740609 10_{10}$
$y_c = 489C375A9941A3049E33B34361DD\|$
$204172AD98C3E5916DE27695D22A61FAE46E_{16}$

Тогда параметр $r = x_c(\mathrm{mod}\ q)$ принимает значение: $r = x_c(mod\ q)$

$R = 297009809158179528743712049839382569 9\|$
$04227521079943196516326879820592109333 95_{10}$
$R = 41AA28D2F1AB148280CD9ED56FED\|$
$A41974053554A42767B83AD043FD39DC0493_{16}$

Поскольку выполнено равенство $R = r$, то цифровая подпись ***принимается***.