ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное

БЗ 6—2001/131

ГОССТАНДАРТ РОССИИ
Москва

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации с участием Всероссийского научно-исследовательского института стандартизации (ВНИИстандарт)

ВНЕСЕН Федеральным агентством правительственной связи и информации при Президенте Российской Федерации

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 12 сентября 2001 г. № 380-ст

3 Настоящий стандарт разработан с учетом терминологии и концепций международных стандартов ИСО 2382-2—76 «Обработка данных. Словарь. Часть 2. Арифметические и логические операции», ИСО/МЭК 9796—91 «Информационная технология. Методы защиты. Схема цифровой подписи с восстановлением сообщения», серии ИСО/МЭК 14888 «Информационная технология. Методы защиты. Цифровые подписи с приложением» и серии ИСО/МЭК 10118 «Информационная технология. Методы защиты. Хэш-функции»

4 ВЗАМЕН ГОСТ Р 34.10—94

© ИПК Издательство стандартов, 2001

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Госстандарта России

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Определения и обозначения 1
3.1 Определения 1
3.2 Обозначения 2
4 Общие положения 3
5 Математические соглашения 3
5.1 Математические определения 4
5.2 Параметры цифровой подписи 4
5.3 Двоичные векторы 5
6 Основные процессы 6
6.1 Формирование цифровой подписи 6
6.2 Проверка цифровой подписи 7
Приложение А Дополнительные термины в области ЭЦП 9
Приложение Б Контрольный пример 9
Б.1 Параметры схемы цифровой подписи 9
Б.2 Процесс формирования цифровой подписи (алгоритм I) 10
Б.3 Процесс проверки цифровой подписи (алгоритм II) 11
Приложение В Библиография 12

Введение

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

Стандарт разработан взамен ГОСТ Р 34.10—94. Необходимость разработки настоящего стандарта вызвана потребностью в повышении стойкости ЭЦП к несанкционированным изменениям. 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.

Настоящий стандарт терминологически и концептуально увязан с международными стандартами ИСО 2382-2 [1], ИСО/МЭК 9796 [2], серии ИСО/МЭК 14888 [3] — [5] и серии ИСО/МЭК 10118 [6] — [9].

Примечание — Основная часть стандарта дополнена тремя приложениями:

- А — дополнительные термины в области ЭЦП;
- Б — описание контрольного примера;
- В — перечень публикаций (библиография) в области ЭЦП.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Information technology. Cryptographic data security.
Formation and verification processes of [electronic] digital signature

Дата введения 2002—07—01

1 Область применения

Настоящий стандарт определяет схему электронной цифровой подписи (ЭЦП) (далее по тексту — цифровая подпись), процессы формирования и проверки цифровой подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения.

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

Стандарт рекомендуется использовать в новых системах обработки информации различного назначения, а также при модернизации действующих систем.

2 Нормативные ссылки

В настоящем стандарте использована ссылка на следующий стандарт:

ГОСТ Р 34.11—94 Информационная технология. Криптографическая защита информации. Функции хэширования

3 Определения и обозначения

3.1 Определения

В настоящем стандарте использованы следующие термины:

3.1.1 **дополнение** (appendix): Строка бит, формируемая из цифровой подписи и произвольного текстового поля (ИСО/МЭК 148881-1 [3]).

3.1.2 **ключ подписи** (signature key): Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи (ИСО/МЭК 14888-1 [3]).

3.1.3 **ключ проверки** (verification key): Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи (ИСО/МЭК 14888-1 [3]).

3.1.4 **параметр схемы ЭЦП** (domain parameter): Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам (ИСО/МЭК 14888-1 [3]).

3.1.5 **подписанное сообщение** (signed message): Набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения.

3.1.6 **последовательность псевдослучайных чисел** (pseudo-random number sequence): Последовательность чисел, полученная в результате выполнения некоторого арифметического (вычислительного) процесса, используемая в конкретном случае вместо последовательности случайных чисел (ИСО 2382-2 [1]).

Издание официальное

3.1.7 **последовательность случайных чисел** (random number sequence): Последовательность чисел, каждое из которых не может быть предсказано (вычислено) только на основе знания предшествующих ему чисел данной последовательности (ИСО 2382-2 [1]).

3.1.8 **процесс проверки подписи** (verification process): Процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки и параметры схемы ЭЦП и результатом которого является заключение о правильности или ошибочности цифровой подписи (ИСО/МЭК 14888-1 [3]).

3.1.9 **процесс формирования подписи** (signature process): Процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП, а в результате формируется цифровая подпись (ИСО/МЭК 14888-1 [3]).

3.1.10 **свидетельство** (witness): Элемент данных, представляющий соответствующее доказательство достоверности (недостоверности) подписи проверяющей стороне (ИСО/МЭК 14888-1 [3]).

3.1.11 **случайное число** (random number): Число, выбранное из определенного набора чисел таким образом, что каждое число из данного набора может быть выбрано с одинаковой вероятностью (ИСО 2382-2 [1]).

3.1.12 **сообщение** (message): Строка бит ограниченной длины (ИСО/МЭК 9796 [2]).

3.1.13 **хэш-код** (hash-code): Строка бит, являющаяся выходным результатом хэш-функции (ИСО/МЭК 148881-1 [3]).

3.1.14 **хэш-функция** (hash-function): Функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

1) по данному значению функции сложно вычислить исходные данные, отображенные в это значение;

2) для заданных исходных данных трудно найти другие исходные данные, отображаемые с тем же результатом;

3) трудно найти какую-либо пару исходных данных с одинаковым значением хэш-функции.

Примечание — Применительно к области ЭЦП свойство 1 подразумевает, что по известной ЭЦП невозможно восстановить исходное сообщение; свойство 2 подразумевает, что для заданного подписанного сообщения трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же ЭЦП, свойство 3 подразумевает, что трудно подобрать какую-либо пару сообщений, имеющих одну и ту же подпись.

3.1.15 **[электронная] цифровая подпись** (digital signature): Строка бит, полученная в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

Примечание — В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями, установлено, что термины **«цифровая подпись»** и **«электронная цифровая подпись (ЭЦП)»** являются синонимами.

3.2 Обозначения

В настоящем стандарте использованы следующие обозначения:

V_{256} — множество всех двоичных векторов длиной 256 бит;
V_{∞} — множество всех двоичных векторов произвольной конечной длины;
Z — множество всех целых чисел;
p — простое число, $p > 3$;
F_p — конечное простое поле, представляемое как множество из p целых чисел $\{0, 1, \ldots, p-1\}$;
$b \pmod p$ — 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.

4 Общие положения

Общепризнанная схема (модель) цифровой подписи (см. 6 ИСО/МЭК 14888-1 [3]) охватывает три процесса:

- генерация ключей (подписи и проверки);
- формирование подписи;
- проверка подписи.

В настоящем стандарте процесс генерации ключей (подписи и проверки) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию.

Механизм цифровой подписи определяется посредством реализации двух основных процессов (см. раздел 6):

- формирование подписи (см. 6.1);
- проверка подписи (см. 6.2).

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.

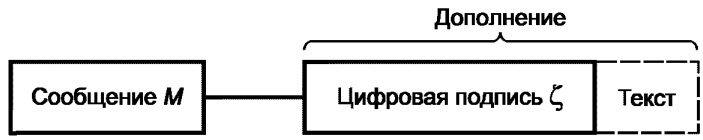


Рисунок 1 — Схема подписанного сообщения

Поле «текст», показанное на данном рисунке и дополняющее поле «цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым 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. Алгоритм вычисления хэш-функции установлен в ГОСТ Р 34.11.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки, определены в 5.2.

Стандарт не определяет процесс генерации параметров схемы цифровой подписи. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы цифровой подписи исходя из требований к аппаратно-программным средствам, реализующим электронный документооборот.

Цифровая подпись, представленная в виде двоичного вектора длиной 512 бит, должна вычисляться с помощью определенного набора правил, изложенных в 6.1.

Набор правил, позволяющих либо принять, либо отвергнуть цифровую подпись под полученным сообщением, установлен в 6.2.

5 Математические соглашения

Для определения схемы цифровой подписи необходимо описать базовые математические объекты, используемые в процессах ее формирования и проверки. В данном разделе установлены основные математические определения и требования, накладываемые на параметры схемы цифровой подписи.

5.1 Математические определения

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

$$y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1}$$

где $a, b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p.

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

$$J(E) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} \pmod{p}. \tag{2}$$

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

$$\begin{cases} a \equiv 3k \pmod{p}, \\ b \equiv 2k \pmod{p}, \text{ где } k = \dfrac{J(E)}{1728 - J(E)} \pmod{p}, \ J(E) \neq 0 \text{ или } 1728. \end{cases} \tag{3}$$

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

Точки эллиптической кривой будем обозначать $Q(x, y)$ или просто Q. Две точки эллиптической кривой равны, если равны их соответствующие x- и y-координаты.

На множестве всех точек эллиптической кривой E введем операцию сложения, которую будем обозначать знаком «+». Для двух произвольных точек $Q_1(x_1, y_1)$ и $Q_2(x_2, y_2)$ эллиптической кривой E рассмотрим несколько вариантов.

Пусть координаты точек Q_1 и Q_2 удовлетворяют условию $x_1 \neq x_2$. В этом случае их суммой будем называть точку $Q_3(x_3, y_3)$, координаты которой определяются сравнениями

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}, \\ y_3 \equiv \lambda (x_1 - x_3) - y_1 \pmod{p}, \end{cases} \quad \text{где } \lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}. \tag{4}$$

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то определим координаты точки Q_3 следующим образом

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 \pmod{p}, \\ y_3 \equiv \lambda (x_1 - x_3) - y_1 \pmod{p}, \end{cases} \quad \text{где } \lambda \equiv \frac{3x_1^2 + a}{2y_1} \pmod{p}. \tag{5}$$

В случае, когда выполнено условие $x_1 = x_2$ и $y_1 \equiv -y_2 \pmod{p}$ сумму точек Q_1 и Q_2 будем называть *нулевой точкой* O, не определяя ее x- и y-координаты. В этом случае точка Q_2 называется *отрицанием* точки Q_1. Для нулевой точки O выполнены равенства

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

где Q — произвольная точка эллиптической кривой E.

Относительно введенной операции сложения множество всех точек эллиптической кривой E, вместе с нулевой точкой, образуют конечную абелеву (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

$$Q = \underbrace{P + \ldots + P}_{k} = kP. \tag{8}$$

5.2 Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

- простое число p — модуль эллиптической кривой, удовлетворяющее неравенству $p > 2^{255}$. 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:

$$\begin{cases} m = nq, \ n \in Z, \ n \geq 1 \\ 2^{254} < q < 2^{256} \end{cases}; \tag{9}$$

- точка $P \neq O$ эллиптической кривой E, с координатами (x_p, y_p), удовлетворяющая равенству $qP = O$;
- хэш-функция $h(\cdot): V_\infty \to V_{256}$, 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 $p^t \neq 1 \pmod q$, для всех целых $t = 1, 2, \ldots B$, 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.

5.3 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

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

$$\overline{h}_2 = (\beta_{255}, \ldots, \beta_0),$$

тогда их объединение имеет вид

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

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 $\overline{h}$ длиной 512 бит на два двоичных вектора длиной 256 бит, конкатенацией которых он является.

6 Основные процессы

В данном разделе определены процессы формирования и проверки цифровой подписи под сообщением пользователя.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, удовлетворяющие требованиям 5.2.

Кроме того, каждый пользователь должен иметь ключ подписи d и ключ проверки подписи $Q(x_q, y_q)$, которые также должны удовлетворять требованиям 5.2.

6.1 Формирование цифровой подписи

Для получения цифровой подписи под сообщением $M \in V_\infty$ необходимо выполнить следующие действия (шаги) по алгоритму I.

Шаг 1 — вычислить хэш-код сообщения $M: \overline{h} = h(M)$. (14)

Шаг 2 — вычислить целое число α, двоичным представлением которого является вектор $\overline{h}$, и определить

$$e \equiv \alpha \pmod{q}. \tag{15}$$

Если $e = 0$, то определить $e = 1$.

Шаг 3 — сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству

$$0 < k < q. \tag{16}$$

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

$$r \equiv x_c \pmod{q}, \tag{17}$$

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

Шаг 5 — вычислить значение

$$s \equiv (rd + ke) \pmod{q}. \tag{18}$$

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 $\zeta = (\overline{r} \| \overline{s})$ как конкатенацию двух двоичных векторов.

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

Схематическое представление процесса формирования цифровой подписи приведено на рисунке 2.

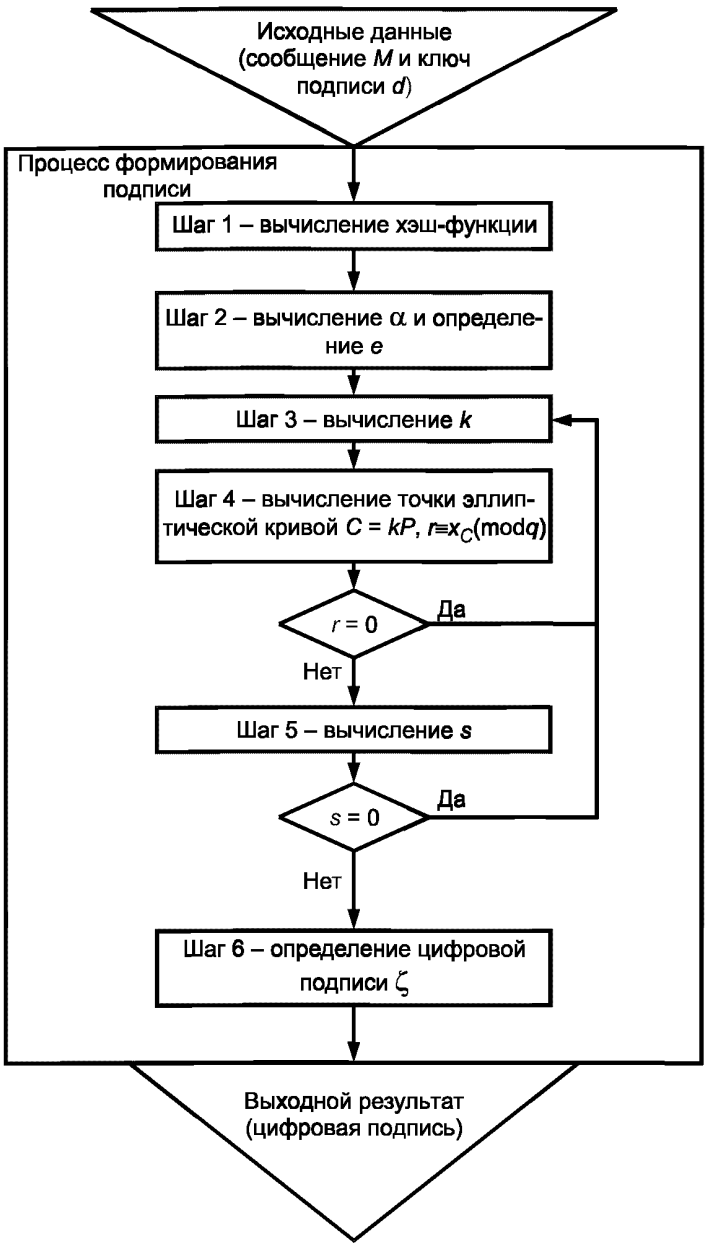


Рисунок 2 — Схема процесса формирования цифровой подписи

6.2 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.

Шаг 2 — вычислить хэш-код полученного сообщения M

$$\overline{h} = h(M). \tag{19}$$

Шаг 3 — вычислить целое число α, двоичным представлением которого является вектор $\overline{h}$, и определить

$$e \equiv \alpha \pmod{q}. \tag{20}$$

Если $e = 0$, то определить $e = 1$.

Шаг 4 — вычислить значение $v \equiv e^{-1} \pmod{q}$. (21)

Шаг 5 — вычислить значения

$$z_1 \equiv sv \pmod{q}, z_2 \equiv -rv \pmod{q}. \quad (22)$$

Шаг 6 — вычислить точку эллиптической кривой $C = z_1 P + z_2 Q$ и определить

$$R \equiv x_c \pmod{q}, \quad (23)$$

где x_c — x-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.

Схематическое представление процесса проверки цифровой подписи приведено на рисунке 3.

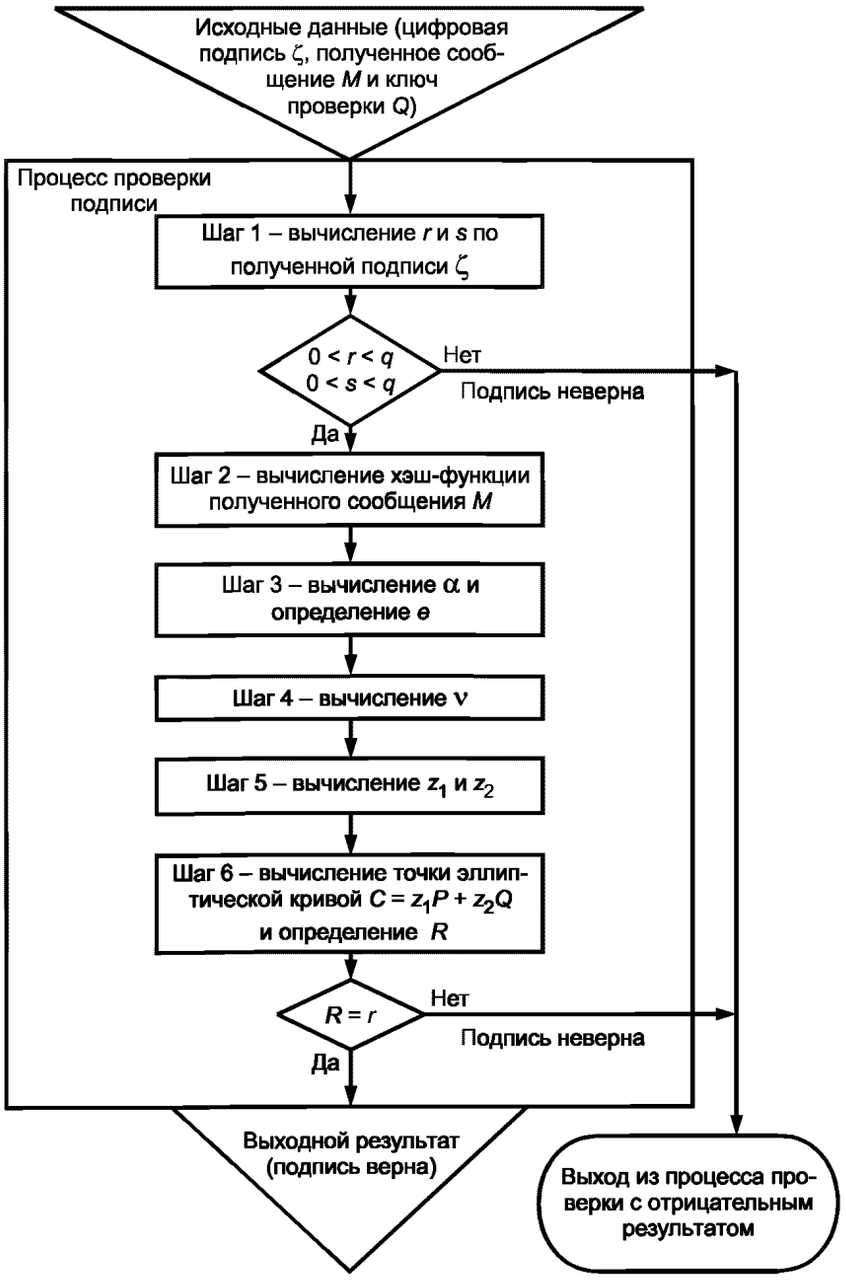


Рисунок 3 — Схема процесса проверки цифровой подписи

ПРИЛОЖЕНИЕ А
(справочное)

Дополнительные термины в области ЭЦП

В настоящем приложении приведены дополнительные международные термины, применяемые в рассматриваемой и смежных областях.

А.1 **заполнение** (padding): Дополнение строки данных лишними битами (ИСО/МЭК 10118-1 [6]).

А.2 **идентификационные данные** (identification data): Последовательность элементов данных, включая отличительный идентификатор объекта, принадлежащая объекту и используемая для его обозначения (ИСО/МЭК 148881-1 [3]).

А.3 **уравнение цифровой подписи** (signature equation): Уравнение, определяемое функцией цифровой подписи (ИСО/МЭК 148881-1 [3]).

А.4 **функция проверки** (verification function): Функция процесса проверки, определяемая ключом проверки, выдающая в качестве результата вычисленное значение свидетельства о достоверности подписи (ИСО/МЭК 148881-1 [3]).

А.5 **функция цифровой подписи** (signature function): Функция в процессе формирования подписи, определяемая ключом подписи и параметрами схемы ЭЦП. Эта функция в качестве исходных данных получает часть исходных данных и, возможно, формирователь последовательности псевдослучайных чисел (рандомизатор), а в результате выдает вторую часть цифровой подписи.

ПРИЛОЖЕНИЕ Б
(справочное)

Контрольный пример

Данное приложение носит справочный характер и не является частью стандарта. Приводимые ниже значения параметров p, a, b, m, q, P, а также значения ключей подписи и проверки d и Q рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящем стандарте.

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

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

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

Б.1 Параметры схемы цифровой подписи

Для формирования и проверки цифровой подписи должны быть использованы следующие параметры (см. 5.2).

Б.1.1 Модуль эллиптической кривой

В данном примере параметру p присвоено следующее значение:

$$p = 57896044618658097711785492504343953926\backslash\backslash$$
$$634992332820282019728792003956564821041_{10}$$
$$p = 8000000000000000000000000000000000000000000000000000000000000431_{16}$$

Б.1.2 Коэффициенты эллиптической кривой

В данном примере параметры a и b принимают следующие значения:

$$a = 7_{10}$$
$$a = 7_{16}$$
$$b = 43308876546767276905765904595650931995\backslash\backslash$$
$$942111794451039583252968842033849580414_{10}$$

b = 5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514C0CE9DAE23B7E$_{16}$

Б.1.3 Порядок группы точек эллиптической кривой

В данном примере параметр m принимает следующее значение:

m = 57896044618658097711785492504343953\\
70829345837254506223809735921376310696 19$_{10}$

m = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$

Б.1.4 Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр q принимает следующее значение:

q = 57896044618658097711785492504343953\\
70829345837254506223809735921376310696 19$_{10}$

q = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$

Б.1.5 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\\
C85C97F0A9CA267122B96ABBCEA7E8FC8$_{16}$

Б.1.6 Ключ подписи

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

d = 55441196065363246126355624130324183 1\\
96576709222340016572108097750006097525544$_{10}$

d = 7A929ADE789BB9BE10ED359DD39A72C\\
11B60961F49397EEE1D19CE9891EC3B28$_{16}$

Б.1.7 Ключ проверки

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

x_q = 57520216126176808443631405023338071\\
17663010490631363218289674134220660485940 3$_{10}$

x_q = 7F2B49E270DB6D90D8595BEC458B5\\
0C58585BA1D4E9B788F6689DBD8E56FD80B$_{16}$

y_q = 17614944419213781543809391949654080\\
03194266204536363926070984785943828676399 4$_{10}$

y_q = 26F1B489D6701DD185C8413A977B3\\
CBBAF64D1C593D26627DFFB101A87FF77DA$_{16}$

Б.2 Процесс формирования цифровой подписи (алгоритм I)

Пусть после выполнения шагов 1 — 3 по алгоритму I (6.1) были 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$_{10}$

$$x_c = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$
$$y_c = 32842535278684663477094665322517084 5\backslash\backslash$$
$$0680472103245454326813285455653927406091 0_{10}$$
$$y_c = 489C375A9941A3049E33B34361DD\backslash\backslash$$
$$204172AD98C3E5916DE27695D22A61FAE46E_{16}$$

Параметр $r = x_c \pmod q$ принимает значение:

$$r = 2970098091581795287437120498393825 69\backslash\backslash$$
$$9042275210799431965163268798205921093339 5_{10}$$
$$r = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$

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

$$s = 5749734002700846541789253100191 4703\backslash\backslash$$
$$8455227042649098563933718999175515839552_{10}$$
$$s = 1456C64BA4642A1653C235A98A60249BCD6D3F746B631DF928014F6C5BF9C40_{16}$$

Б.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1 — 3 по алгоритму II (6.2) было получено следующее числовое значение:

$$e = 2079889367447645201713406156150827013\backslash\backslash$$
$$0637142515379653289952617252661468872421_{10}$$
$$e = 2DFBC1B372D89A1188C09C52E0EE\backslash\backslash$$
$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$$

При этом параметр $v = e^{-1} \pmod q$ принимает значение:

$$v = 1768668360593446867730171382490026 85\backslash\backslash$$
$$6274688308067549671528803657243114571897 8_{10}$$
$$v = 271A4EE429F84EBC423E388964555BB\backslash\backslash$$
$$29D3BA53C7BF945E5FAC8F381706354C2_{16}$$

Параметры $z_1 = sv \pmod q$ и $z_2 = -rv \pmod q$ принимают значения:

$$z_1 = 3769916750090193855684105729351265 61\backslash\backslash$$
$$0884134519049194261930453241274372099975 9_{10}$$
$$z_1 = 5358F8FFB38F7C09ABC782A2DF2A\backslash\backslash$$
$$3927DA4077D07205F763682F3A76C9019B4F_{16}$$
$$z_2 = 1417199842734347211251591796950076 57\backslash\backslash$$
$$6924665583897286211449993265333367109221_{10}$$
$$z_2 = 3221B4FBBF6D101074EC14AFAC2D4F7\backslash\backslash$$
$$EFAC4CF9FEC1ED11BAE336D27D527665_{16}$$

Точка $C = z_1 P + z_2 Q$ имеет координаты:

$$x_c = 2970098091581795287437120498393825 699\backslash\backslash$$
$$0422752107994319651632687982059210933395_{10}$$
$$x_c = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$
$$y_c = 32842535278684663477094665322517084 50\backslash\backslash$$
$$6804721032454543268132854556539274060910_{10}$$
$$y_c = 489C375A9941A3049E33B34361DD\backslash\backslash$$
$$204172AD98C3E5916DE27695D22A61FAE46E_{16}$$

Тогда параметр $R = x_c \pmod q$ принимает значение:

$$R = 2970098091581795287437120498393825 699\backslash\backslash$$
$$0422752107994319651632687982059210933395_{10}$$
$$R = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$

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

ПРИЛОЖЕНИЕ В
(справочное)

Библиография*

[1] ИСО 2382-2—76 Обработка данных. Словарь. Часть 2. Арифметические и логические операции
[2] ИСО/МЭК 9796—91 Информационная технология. Методы защиты. Схема цифровой подписи с восстановлением сообщения
[3] ИСО/МЭК 14888-1—98 Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения
[4] ИСО/МЭК 14888-2—99 Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы на основе подтверждения подлинности
[5] ИСО/МЭК 14888-3—99 Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе сертификата
[6] ИСО/МЭК 10118-1—94 Информационная технология. Методы защиты. Хэш-функции. Часть 1. Общие положения
[7] ИСО/МЭК 10118-2—94 Информационная технология. Методы защиты. Хэш-функции. Часть 2. Хэш-функции с использованием *n*-битного блочного алгоритма шифрации
[8] ИСО/МЭК 10118-3—98 Информационная технология. Методы защиты. Хэш-функции. Часть 3. Десятичные хэш-функции
[9] ИСО/МЭК 10118-4—98 Информационная технология. Методы защиты. Хэш-функции. Часть 4. Хэш-функции, использующие модульную арифметику

* Оригиналы международных стандартов ИСО/МЭК —во ВНИИКИ Госстандарта России.

УДК 681.3.06:006.354 ОКС 35.040 П85 ОКСТУ 5001

Ключевые слова: обработка данных, передача данных, обмен информацией, сообщения, цифровые подписи, защита информации, формирование цифровой подписи, проверка цифровой подписи.

Редактор *В.П. Огурцов*
Технический редактор *О.Н. Власова*
Корректор *Н.Л. Рыбалко*
Компьютерная верстка *А.Н. Золотаревой*

Изд. лиц. № 02354 от 14.07.2000. Сдано в набор 28.09.2001. Подписано в печать 29.10.2001. Усл.печ.л. 1,86. Уч.-изд.л. 1,40. Тираж 549 экз. С 2419. Зак. 1022.

ИПК Издательство стандартов, 107076, Москва, Колодезный пер., 14.
gost.e-ecolog.ru e-mail: gost.e-ecolog.ru
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. "Московский печатник", 103062, Москва, Лялин пер., 6.
Плр № 080102

gost.e-ecolog.ru