"ГОСТ Р 34.10-2012. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (утв. и введен в действие Приказом Росстандарта от 07.08.2012 N 215-ст)

Утвержден и введен в действие
Приказом Федерального агентства
по техническому регулированию
и метрологии
от 7 августа 2012 г. N 215-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Information technology. Cryptographic data security. Generation and verification processes of electronic digital signature

ГОСТ Р 34.10-2012

Группа П85

ОКС 35.040

ОКСТУ 5001

Дата введения
1 января 2013 года

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения".

Сведения о стандарте

1. Разработан Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества "Информационные технологии и коммуникационные системы" (ОАО "ИнфоТеКС").

2. Внесен Техническим комитетом по стандартизации ТК 26 "Криптографическая защита информации".

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 215-ст.

4. Взамен ГОСТ Р 34.10-2001.

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет.

Введение

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

Необходимость разработки настоящего стандарта вызвана потребностью в реализации электронной цифровой подписи разной степени стойкости в связи с повышением уровня развития вычислительной техники. Стойкость электронной цифровой подписи основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11-2012.

Настоящий стандарт разработан с учетом терминологии и концепций международных стандартов ИСО 2382-2 [1], ИСО/МЭК 9796 [2] - [3], ИСО/МЭК 14888 [4] - [7] и ИСО/МЭК 10118 [8] - [11].

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт определяет схему электронной цифровой подписи (ЭЦП) (далее - 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 основе настоящего стандарта повышает по сравнению с ранее действовавшей схемой цифровой подписи уровень защищенности передаваемых сообщений от подделок и искажений.

Настоящий стандарт рекомендуется применять при создании, эксплуатации и модернизации систем обработки информации различного назначения.

2. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования

Примечание. При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

3.1. Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1.

Дополнение (appendix): строка бит, формируемая из цифровой подписи и произвольного текстового поля. [ИСО/МЭК 14888-1:2008, [4]]

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 14888-1:2008, [4]]

3.1.3.

Ключ проверки подписи (verification key): элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.

[ИСО/МЭК 14888-1:2008, [4]]

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 14888-1:2008, [4]]

3.1.5.

Подписанное сообщение (signed message): набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения.

[ИСО/МЭК 14888-1:2008, [4]]

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 2382-2:1976, [1]]

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 2382-2:1976, [1]]

3.1.8.

Процесс проверки подписи (verification process): процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки подписи и параметры схемы ЭЦП, результатом которого является заключение о правильности или ошибочности цифровой подписи.

[ИСО/МЭК 14888-1:2008, [4]]

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 14888-1:2008, [4]]

3.1.10. Свидетельство (witness): элемент данных, представляющий соответствующее доказательство достоверности (недостоверности) подписи проверяющей стороне.

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 2382-2:1976, [1]]

3.1.12.

Сообщение (message): строка бит произвольной конечной длины.

[ИСО/МЭК 14888-1:2008, [4]]

3.1.13.

Хэш-код (hash-code): строка бит, являющаяся выходным результатом хэш-функции.

[ИСО/МЭК 14888-1:2008, [4]]

3.1.14.

Хэш-функция (collision-resistant hash-function): функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

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

2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции;

3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

[ИСО/МЭК 14888-1:2008, [4]]

Примечания

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

2. В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями установлено,

что термины "хэш-функция", "криптографическая хэш-функция", "функция хэширования" и "криптографическая функция хэширования" являются синонимами.

3.1.15.

[Электронная цифровая] подпись (signature); ЭЦП: строка бит, полученная в результате процесса формирования подписи. [ИСО/МЭК 14888-1:2008, [4]]

Примечания

1. Строка бит, являющаяся подписью, может иметь внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

2. В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями установлено, что термины "электронная подпись", "цифровая подпись" и "электронная цифровая подпись" являются синонимами.

3.2. Обозначения

В настоящем стандарте применены следующие обозначения:

V_1	- множество всех двоичных векторов длиной l 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, ..., p - 1};
b (mod p)	- минимальное неотрицательное число, сравнимое с b по модулю p;
M	- сообщение пользователя, $M \in V^*$
$(\bar{h}_1 \| \bar{h}_2)$	- 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 подписи;

ζ - цифровая подпись под сообщением M.

4. ОБЩИЕ ПОЛОЖЕНИЯ

Общепризнанная схема (модель) цифровой подписи (см. ИСО/МЭК 14888-1 [4]) охватывает следующие процессы:

- генерация ключей (подписи и проверки подписи);

- формирование подписи;

- проверка подписи.

В настоящем стандарте процесс генерации ключей (подписи и проверки подписи) 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:

- осуществление контроля целостности передаваемого подписанного сообщения;

- доказательное подтверждение авторства лица, подписавшего сообщение;

- защита сообщения от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 1.

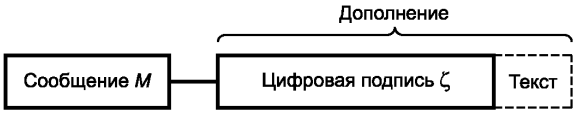

Рисунок 1. Схема подписанного сообщения

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. Алгоритмы вычисления хэш-функции установлены в ГОСТ Р 34.11-2012.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки, определены в 5.2. В настоящем стандарте предусмотрена возможность выбора одного из двух вариантов требований к

параметрам.

Настоящий 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 или 1024 бита, должна вычисляться с помощью определенного набора правил, изложенных в 6.1.

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

5. МАТЕМАТИЧЕСКИЕ ОБЪЕКТЫ

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, предъявляемые к параметрам схемы цифровой подписи.

5.1. Математические определения

Эллиптической кривой E, определенной над конечным простым полем F_p (где p > 3 - простое число), называется множество пар (x, y), $x, y \in F_p$, удовлетворяющих уравнению

$$y^2 = x^3 + ax + b \pmod p. \quad (1)$$

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 уравнению

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

Пары (x, y), где x, y - элементы поля F_p, удовлетворяющие уравнению (1), называются "точками эллиптической кривой E"; x и y - соответственно x- и y-координатами точки.

Точка эллиптической кривой обозначается Q (x, y) или просто Q. Две точки эллиптической кривой равны, если равны их соответствующие x- и y-координаты.

На множестве точек эллиптической кривой E определена операция сложения, обозначаемая знаком "+". Для двух произвольных точек $Q_1(x_1, y_1)$ и $Q_2(x_2, y_2)$ эллиптической кривой E рассматривают несколько случаев.

Для точек Q_1 и Q_2, координаты которых удовлетворяют условию $x_1 \neq x_2$, их суммой называется точка $Q_3(x_3, y_3)$, координаты которой определяются сравнениями

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \pmod p, \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod p, \end{cases} \quad (3)$$

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

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

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

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

Если выполнены условия $x_1 = x_2$ и $y_1 = -y_2 (\mathrm{mod}\, p)$, то сумма точек Q_1 и Q_2 называется нулевой точкой O без определения ее x- и y-координат. В этом случае точка Q_2 называется отрицанием точки Q_1. Для нулевой точки O выполнены равенства

$$Q + O = O + Q = Q, \quad (5)$$

где Q - произвольная точка эллиптической кривой E.

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

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}. \quad (6)$$

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

$$Q = \underbrace{P + \ldots + P}_{k} = kP. \quad (7)$$

5.2. Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

- простое число p - модуль эллиптической кривой;

- эллиптическая кривая E, задаваемая 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:

$$\begin{cases} m = nq,\ n \in Z,\ n \geq 1 \\ 2^{254} < q < 2^{256} \text{ или } 2^{508} < q < 2^{512} \end{cases}; \quad (8)$$

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

- хэш-функция $V^* \to V_l$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные векторы 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.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

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

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

К приведенным выше параметрам схемы цифровой подписи предъявляют следующие требования:

- должно быть выполнено условие $p^t \neq 1 \pmod q$ для всех целых t = 1, 2, ... B, где B = 31, если $2^{254} < q < 2^{256}$, и B = 131, если $2^{508} < q < 2^{512}$;

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

- инвариант кривой должен удовлетворять условиям: $J(E) \neq 0$ и $J(E) \neq 1728$.

5.3. Двоичные векторы

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

Рассмотрим следующий двоичный вектор длиной l бит, в котором младшие биты расположены справа, а старшие - слева:

$$\bar{h} = (\alpha_{l-1}, \ldots, \alpha_0), \quad \bar{h} \in V_l \quad (9)$$

где α_i, i = 0,.., l - 1 равно либо 1, либо 0.

Число $\alpha \in Z$ соответствует двоичному вектору $\bar{h}$, если выполнено равенство

$$\alpha = \sum_{i=0}^{l-1} \alpha_i 2^i. \quad (10)$$

Для двух двоичных векторов

$$\bar{h}_1 = (\alpha_{l-1}, \ldots, \alpha_0),$$
$$\bar{h}_2 = (\beta_{l-1}, \ldots, \beta_0), \quad (11)$$

соответствующих целым числам α и β, операция конкатенации (объединения) определяется следующим образом:

$$\bar{h}_1 \| \bar{h}_2 = (\alpha_{l-1}, \ldots, \alpha_0, \beta_{l-1}, \ldots, \beta_0). \quad (12)$$

Объединение представляет собой двоичный вектор длиной 2l бит, составленный из компонент-векторов $\bar{h}_1$ и $\bar{h}_2$.

Формулы (11) и (12) определяют способ разбиения двоичного вектора $\bar{h}_1 \| \bar{h}_2$ длиной 2l бит на два двоичных вектора длиной l 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, соответствующие требованиям 5.2.

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

6.1. 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:

$$\bar{h} = h(M). \quad (13)$$

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

$$e = \alpha \pmod q. \quad (14)$$

Если e = 0, то определить e = 1.

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

$$0 < k < q. \quad (15)$$

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

$$r = x_c \pmod q. \quad (16)$$

где x_c - x-координата точки C.

Если r = 0, то вернуться к шагу 3.

Шаг 5 - вычислить значение

$$s = (rd + ke)(\mathrm{mod}\ q). \quad (17)$$

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.

Схема процесса формирования цифровой подписи приведена на рисунке 2.

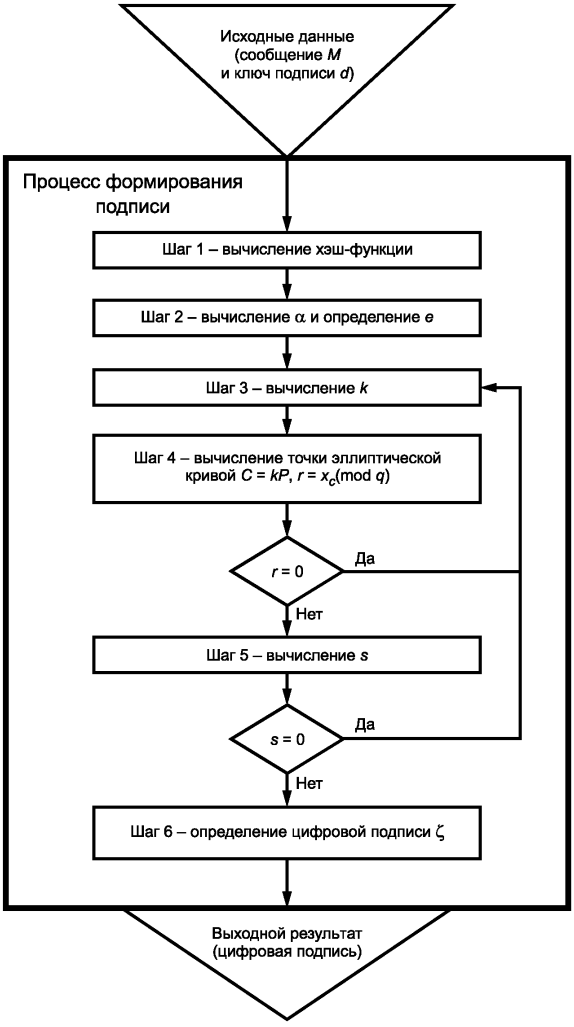

Рисунок 2. Схема процесса формирования цифровой подписи

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:

$$\bar{h} = h(M). \quad (18)$$

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

$$e = \alpha \pmod q. \quad (19)$$

Если e = 0, то определить e = 1.

Шаг 4 - вычислить значение

$$v \equiv e^{-1} \pmod q. \quad (20)$$

Шаг 5 - вычислить значения

$$z_1 \equiv sv \pmod q, \quad z_2 \equiv -rv \pmod q. \quad (21)$$

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

$$R \equiv x_c \pmod q, \quad (22)$$

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 подписи Q, а выходным результатом - свидетельство о достоверности или ошибочности данной подписи.

Схема процесса проверки цифровой подписи приведена на рисунке 3.

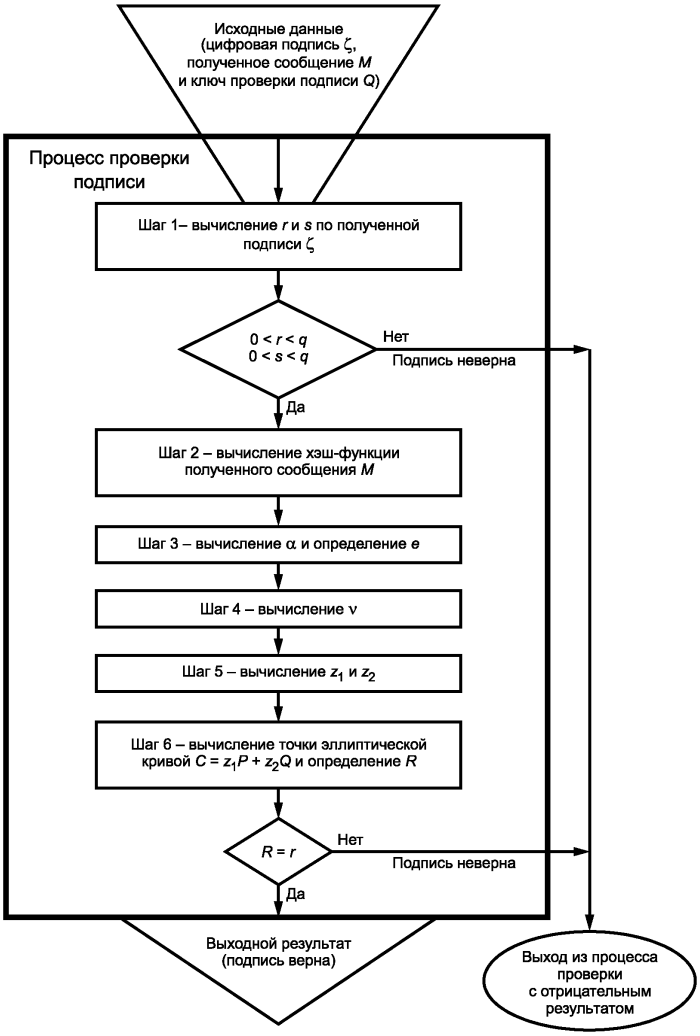

Рисунок 3. Схема процесса проверки цифровой подписи

Приложение А
(справочное)

КОНТРОЛЬНЫЕ ПРИМЕРЫ

Приводимые ниже значения параметров p, a, b, m, q, P, a также значения ключей подписи и проверки подписи 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\\

$$67890_{10}$$

$$499602D2_{16}$$

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

А.1. Пример 1

А.1.1. Параметры схемы цифровой подписи

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

А.1.1.1. Модуль эллиптической кривой

В данном примере параметру p присвоено следующее значение:

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

$$p = 8000000000000000000000000000000$$
$$0000000000000000000000000000000431_{16}.$$

А.1.1.2. Коэффициенты эллиптической кривой

В данном примере параметры a и b принимают следующие значения:

$$a = 7_{10},$$

$$a = 7_{16},$$

$$b = 43308876546767276905765904595650931995\backslash\backslash$$
$$942111794451039583252968842033849580414_{10},$$

$$b = 5FBFF498AA938CE739B8E022FBAFEF40$$
$$563F6E6A3472FC2A514C0CE9DAE23B7E_{16}.$$

А.1.1.3. Порядок группы точек эллиптической кривой

В данном примере параметр m принимает следующее значение:

$$m = 57896044618658097711785492504343953927\backslash\backslash$$
$$708293458372545062238097359213763106961 9_{10},$$

$$m = 8000000000000000000000000000000150$$
$$FE8A1892976154C59CFC193ACCF5B3_{16}.$$

А.1.1.4. Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр q принимает следующее значение:

$$q = 57896044618658097711785492504343953\backslash\backslash$$
$$7082934583725450622380973592137631069619_{10},$$

$$q = 8000000000000000000000000000000150$$
$$FE8A1892976154C59CFC193ACCF5B3_{16}.$$

А.1.1.5. Коэффициенты точки эллиптической кривой

В данном примере координаты точки P принимают следующие значения:

$$x_p = 2_{10},$$

$$x_p = 2_{16},$$

$$y_p = 40189740565390375033354494229370597\backslash\backslash$$
$$7563573938990554508069097936521343156628 0_{10},$$

$$y_p = 8E2A8A0E65147D4BD6316030E16D19\backslash\backslash$$
$$C85C97F0A9CA267122B96ABBCEA7E8FC8_{16}.$$

А.1.1.6. Ключ подписи

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

$$d = 55441196065363246126355624130324183 1\backslash\backslash$$
$$9657670922234001657210809775000609752554 4_{10},$$

$$d = 7A929ADE789BB9BE10ED359DD39A72C\backslash\backslash$$
$$11B60961F49397EEE1D19CE9891EC3B28_{16}.$$

А.1.1.7. Ключ проверки подписи

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

$$x_q = 57520216126176808443631405023338071\backslash\backslash$$
$$1766301049063136321828967413422066048594 03_{10},$$

$$x_q = 7F2B49E270DB6D90D8595BEC458B5\backslash\backslash$$
$$0C58585BA1D4E9B788F6689DBD8E56FD80B_{16},$$

$$y_q = 17614944419213781543809391949654080\backslash\backslash$$
$$0319426620453636392607098478594382867639 94_{10},$$

$$y_q = 26F1B489D6701DD185C8413A977B3\backslash\backslash$$
$$CBBAF64D1C593D26627DFFB101A87FF77DA_{16}.$$

А.1.2. Процесс формирования цифровой подписи (алгоритм I)

Пусть после выполнения шагов 1 - 3 по алгоритму I (см. 6.1) были получены следующие числовые значения:

$$e = 207988936744764520171340615615082701 3\backslash\backslash$$
$$0637142515379653289952617252661468872421_{10},$$

$$e = 2DFBC1B372D89A1188C09C52E0EE\backslash\backslash$$
$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16},$$

$$k = 538541376773484637314038411479966192\backslash\backslash$$
$$4150400343430202071296083852889319623339 5_{10},$$

$$k = 77105C9B20BCD3122823C8CF6FCC\backslash\backslash$$
$$7B956DE33814E95B7FE64FED924594DCEAB3_{16}.$$

При этом кратная точка C = kP имеет координаты:

$$x_c = 297009809158179528743712049839382569\backslash\backslash$$
$$9042275210799431965163268798205921093339 5_{10},$$

$$x_c = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16},$$

$$y_c = 328425352786846634770946653225170845\backslash\backslash$$
$$0680472103245454326813285455653927406091 0_{10},$$

$$y_c = 489C375A9941A3049E33B34361DD\backslash\backslash$$
$$204172AD98C3E5916DE27695D22A61FAE46E_{16}.$$

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

$$r = 297009809158179528743712049839382569\backslash\backslash$$
$$9042275210799431965163268798205921093339 5_{10},$$

$$r = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}.$$

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

$$s = 57497340027008465417892531001914703\backslash\backslash 84552270426490985639337189991755158395 52_{10},$$

$$s = 1456C64BA4642A1653C235A98A60249 BCD6D3F746B631DF928014F6C5BF9C40_{16}.$$

А.1.3. Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1 - 3 по алгоритму II (см. 6.2) были получены следующие числовые значения:

$$e = 20798893674476452017134061561508270 13\backslash\backslash 06371425153796532899526172526614688724 21_{10},$$

$$e = 2DFBC1B372D89A1188C09C52E0EE\backslash\backslash C61FCE52032AB1022E8E67ECE6672B043EE5_{16}.$$

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

$$v = 17686683605934468677301713824900268 5\backslash\backslash 62746883080675496715288036572431145718978_{10},$$

$$v = 271A4EE429F84EBC423E388964555BB\backslash\backslash 29D3BA53C7BF945E5FAC8F381706354C2_{16}.$$

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

$$z_1 = 37699167500901938556841057293512656 1\backslash\backslash 08841345190491942619304532412743720999759_{10},$$

$$z_1 = 5358F8FFB38F7C09ABC782A2DF2A\backslash\backslash 3927DA4077D07205F763682F3A76C9019B4F_{16},$$

$$z_2 = 14171998427343472112515917969500765 7\backslash\backslash 69246655838972862114499932653333671092 21_{10},$$

$$z_2 = 3221B4FBBF6D101074EC14AFAC2D4F7\backslash\backslash EFAC4CF9FEC1ED11BAE336D27D527665_{16}.$$

Точка $C = z_1P + z_2Q$ имеет координаты:

$$x_c = 29700980915817952874371204983938256 99\backslash\backslash 04227521079943196516326879820592109333 95_{10},$$

$$x_c = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash A41974053554A42767B83AD043FD39DC0493_{16},$$

$$y_c = 32842535278684663477094665322517084506804721032454543268132854556539274060910_{10},$$

$$y_c = 489C375A9941A3049E33B34361DD\backslash\backslash 204172AD98C3E5916DE27695D22A61FAE46E_{16}.$$

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

$$R = 29700980915817952874371204983938256990422752107994319651632687982059210933395_{10},$$

$$R = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash A41974053554A42767B83AD043FD39DC0493_{16}.$$

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

А.2. Пример 2

А.2.1. Параметры схемы цифровой подписи

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

А.2.1.1. Модуль эллиптической кривой

В данном примере параметру p присвоено следующее значение:

$$p = 3623986102229003635907788753683874306021320925534678605086546150450856166624002482588482022271496854025090823603058735163734263822371964987228582907372403_{10},$$

$$p = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\backslash\backslash F1D852741AF4704A0458047E80E4546D35B8336FAC224DD81664BBF528BE6373_{16}.$$

А.2.1.2. Коэффициенты эллиптической кривой

В данном примере параметры a и b принимают следующие значения:

$$a = 7_{10},$$

$$a = 7_{16},$$

$$b = 151865506921082853450895003471404315492$$
$$8747527740206436\backslash\backslash 1940188233528099824437937$$
$$3282975691478597467486604160539788367 75\backslash\backslash$$
$$9662632641399013695904743581182639 6_{10},$$

$$b = 1CFF0806A31116DA29D8CFA54E57EB748BC$$
$$5F377E49400FDD788B649ECA1AC4\backslash\backslash 361834013B$$
$$2AD7322480A89CA58E0CF74BC9E540C2ADD689$$
$$7FAD0A3084F302ADC_{16}.$$

А.2.1.3. Порядок группы точек эллиптической кривой

В данном примере параметр m принимает следующее значение:

$$m = 362398610222900363590778875368387430$$
$$6021320925534678605086546 1\backslash\backslash 5045085616$$
$$6623969164898305032863068499961404079 4$$
$$3793658545586519221 2\backslash\backslash 9707348088126181206197 43_{10},$$

$$m = 4531ACD1FE0023C7550D267B6B2FEE$$
$$80922B14B2FFB90F04D4EB7C09B5D2D15D\backslash\backslash$$
$$A82F2D7ECB1DBAC719905C5EECC423F1D$$
$$86E25EDBE23C595D644AAF187E6E6DF_{16}.$$

А.2.1.4. Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр q принимает следующее значение:

$$q = 3623986102229003635907788753683874306021320 9$$
$$2553467860508654 61\backslash\backslash 5045085616662396916489830503$$
$$2863068499961404079437936585455865192212\backslash\backslash$$
$$9707348088126181206197 43_{10},$$

$$q = 4531ACD1FE0023C7550D267B6B2FEE809$$
$$22B14B2FFB90F04D4EB7C09B5D2D15D\backslash\backslash$$
$$A82F2D7ECB1DBAC719905C5EECC423F1D$$
$$86E25EDBE23C595D644AAF187E6E6DF_{16}.$$

А.2.1.5. Коэффициенты точки эллиптической кривой

В данном примере координаты точки P принимают следующие значения:

$$x_p = 1928356944067022849399309401243137$$
$$5989977866354595079743570754913077665\backslash\backslash$$
$$9268583544106555768100318487481965800 4$$
$$9032123328842523358302507295276323 8\backslash\backslash$$
$$3493573274_{10},$$

$$x_p = 24D19CC64572EE30F396BF6EBBFD7A6C5213B3$$
$$B3D7057CC825F91093A68CD762\backslash\backslash FD60611262CD838$$
$$DC6B60AA7EEE804E28BC849977FAC33B4B530F1B$$
$$120248A9A_{16}.$$

$$y_p = 2288728693371972859970012155529478 41$$
$$6353562327329506180 3\backslash\backslash 1449742593110286030$$
$$1572814141997072271708807066593850650334$$
$$1523818\backslash\backslash 5734779888586480760509872401385 4_{10},$$

$$y_p = 2BB312A43BD2CE6E0D020613C857ACDD$$
$$CFBF061E91E5F2C3F32447C259F39B2\backslash\backslash C83AB1$$
$$56D77F1496BF7EB3351E1EE4E43DC1A18B91B2$$
$$4640B6DBB92CB1ADD371E_{16}.$$

A.2.1.6. Ключ подписи

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

$$d = 6100818041363730982195381532398475830 06$$
$$8455190695315629823881 35\backslash\backslash 35489060630178225$$
$$5383608393423372379057665527595116827307 02$$
$$504645883\backslash\backslash 7440766121180466875860_{10},$$

$$d = BA6048AADAE241BA40936D47756D7C93$$
$$091A0E8514669700EE7508E508B102072\backslash\backslash$$
$$E8123B2200A0563322DAD2827E2714A2636B$$
$$7BFD18AADFC62967821FA18DD4_{16}.$$

A.2.1.7. Ключ проверки подписи

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

$$x_q = 909546853002536596556690768669830310006929272546556281596 3\backslash\backslash 729653703124985631823204368928700528428086082628324568582235 80\backslash\backslash 713780290717986855863433431150561_{10},$$

$$x_q = 115DC5BC96760C7B48598D8AB9E740D4C4A85A65BE33C1815B5C320C854621D\backslash\backslash D5A515856D13314AF69BC5B924C8B4DDFF75C45415C1D9DD9DD33612CD530EFE1_{16},$$

$$y_q = 292145720337442562062432449734248415455640700823559488705164895 8\backslash\backslash 3750953913429732739738028774142824608862660932913944189501686375 8\backslash\backslash 98410632660057247682237207 6_{10},$$

$$y_q = 37C7C90CD40B0F5621DC3AC1B751CFA0E2634FA0503B3D52639F5D7FB72AFD6\backslash\backslash 1EA199441D943FFE7F0C70A2759A3CDB84C114E1F9339FDF27F35ECA93677BEEC_{16}.$$

А.2.2. Процесс формирования цифровой подписи (алгоритм I)

Пусть после выполнения шагов 1 - 3 по алгоритму I (см. 6.1) были получены следующие числовые значения:

$$e = 289796388168286857556282727855386504917374519787182519956294 7\backslash\backslash 419041388950970536661109553499954248733088719748844538964641281654 4\backslash\backslash 635132969738277062720459 64_{10},$$

$$e = 3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591\backslash\backslash 7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C_{16}.$$

$$k = 175516356025850499540628279921125280333451031747737791650 2\backslash\backslash 081442431820570750344461029867509625089092272358661268724735168078105417\backslash\backslash 475297103098799586329 45_{10},$$

$$k = 359E7F4B1410FEACC570456C680149694631$$
$$2120B39D019D455986E364F3\\65886748ED7A44$$
$$B3E794434006011842286212273A6D14CF70EA3$$
$$AF71BB1AE679F1_{16}.$$

При этом кратная точка C = kP имеет координаты:

$$x_c = 248920447703134926507286464303214775366745131928213144402749863 73\\5761109281022179510187141292882371680595982870833028424365345308 53\\2200444244253415176146 2_{10},$$

$$x_c = 2F86FA60A081091A23DD795E1E3C689EE$$
$$512A3C82EE0DCC2643C78EEA8FCAC\\$$
$$D35492558486B20F1C9EC197C90699850260C9$$
$$3BCBCD9C5C3317E19344E173AE36_{16}.$$

$$y_c = 770173889928991836047844798780960441682062631876096137673946801 50\\2442229353276517652844283783245693642266254651370214816293307951 7\\0843005015210864150831 0_{10},$$

$$y_c = EB488140F7E2F4E35CF220BDBC75AE44F$$
$$26F9C7DF52E82436BDE80A91831DA27\\$$
$$C8100DAA876F9ADC0D28A82DD3826D4DC7$$
$$F92E471DA23E55E0EBB3927C85BD6_{16}.$$

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

$$r = 248920447703134926507286464303214775366745131928213144402749863 73\\5761109281022179510187141292882371680595982870833028424365345308 53\\2200444244253415176146 2_{10},$$

$$r = 2F86FA60A081091A23DD795E1E3C689EE$$
$$512A3C82EE0DCC2643C78EEA8FCAC\\$$
$$D35492558486B20F1C9EC197C90699850260C$$
$$93BCBCD9C5C3317E19344E173AE36_{16}.$$

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

$$s = 8645232217076695190388492973829369170$$
$$75023735848431579919598 7\backslash\backslash 99313385180564$$
$$74887719563967246017942176077089327 8030$$
$$956807690115\backslash\backslash 82270990385368283183515937 0_{10},$$

$$s = 1081B394696FFE8E6585E7A9362D26B6325$$
$$F56778AADBC081C0BFBE933D52FF58\backslash\backslash$$
$$23CE288E8C4F362526080DF7F70CE406A6EE$$
$$B1F56919CB92A9853BDE73E5B4A_{16}.$$

А.2.3. Процесс проверки цифровой подписи (алгоритм II)

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

$$e = 2897963881682868575562827278553865 0$$
$$491737451978718251995629 47\backslash\backslash 41904138895$$
$$097053666110955349995424873308871974 88$$
$$44538964641281654 4\backslash\backslash 635132969738277062720459 64_{10},$$

$$e = 3754F3CFACC9E0615C4F4A7C4D8DAB53$$
$$1B09B6F9C170C533A71D147035B0C591\backslash\backslash$$
$$7184EE536593F4414339976C647C5D5A407AD$$
$$EDB1D560C4FC6777D2972075B8C_{16}.$$

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

$$v = 2556942153946052222660740843164 0861$$
$$53877692234400783191146928 49\backslash\backslash 356194345$$
$$732344708924001925205698280688153534 00$$
$$41458212439906061 36\backslash\backslash 707223818593481596025267 1_{10},$$

$$v = 30D212A9E25D1A80A0F238532CADF3E64$$
$$D7EF4E782B6AD140AAF8BBD9BB4729\backslash\backslash$$
$$84595EEC87B2F3448A1999D5F0A6DE0E14A5$$
$$5AD875721EC8CFD504000B3A840FF_{16}.$$

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

$$z_1 = 32064708273367686296869071018734$$
$$75250343306448089030311214484\\$$
$$38587274320504518034520882655290100$$
$$34967329410497803577935419420 55\\$$
$$60008495619817370719790257 5_{10},$$

$$z_1 = 3D38E7262D69BB2AD24DD81EEA2F92$$
$$E6348D619FA45007B175837CF13B026079\\$$
$$051A48A1A379188F37BA46CE12F7207F2A8$$
$$345459FF960E1EBD5B4F2A34A6EEF_{16},$$

$$z_2 = 13667709118340031081429778480218 4$$
$$75973204553475356412734827\\320820470$$
$$28342168006031261814273230879203690 7$$
$$26448631222679743757 5\\61637266958056$$
$$805859603008203_{10},$$

$$z_2 = 1A18A31602E6EAC0A9888C01941082AE$$
$$FE296F840453D2603414C2A16EB6FC529\\$$
$$D8D8372E50DC49D6C612CE1FF65BD58E1D$$
$$2029F22690438CC36A76DDA444ACB_{16}.$$

Точка $C = z_1P + z_2Q$ имеет координаты:

$$x_c = 24892044770313492650728646430321 4$$
$$77536674513192821314440274986 37\\$$
$$35761109281022179510187141292882371 68$$
$$05959828708330284243653453085 3\\$$
$$22004442442534151761462_{10},$$

$$x_c = 2F86FA60A081091A23DD795E1E3C689$$
$$EE512A3C82EE0DCC2643C78EEA8FCAC\\$$
$$D35492558486B20F1C9EC197C90699850260$$
$$C93BCBCD9C5C3317E19344E173AE36_{16}.$$

$$y_c = 770173889928991836047844798780960441682062631876096137673946801502442229353276517652844283783245693642266254651370214816293307951701843005015210864150831010,$$

$$y_c = EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831DA27\\C8100DAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD616.$$

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

$$R = 248920447703134926507286464303214775366745131928213144402749861037357611092810221795101871412928823716805959828708330284243653453085\\32200444244253415176146210,$$

$$R = 2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE3616.$$

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

БИБЛИОГРАФИЯ <*>

<*> Оригиналы международных стандартов ИСО/МЭК находятся в ФГУП "Стандартинформ" Федерального агентства по техническому регулированию и метрологии.

[1] ИСО 2382-2:1976 — Системы обработки информации. Словарь. Часть 2. Арифметические и логические операции
(ISO 2382-2:1976) — (Data processing - Vocabulary - Part 2: Arithmetic and logic operations)
[2] ИСО/МЭК 9796-2:2010 — Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации
(ISO/IEC 9796-2:2010) — (Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms)

[3]	ИСО/МЭК 9796-3:2006	Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 3. Механизмы на основе дискретного логарифма
	(ISO/IEC 9796-3:2006)	(Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms)
[4]	ИСО/МЭК 14888-1:2008	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения
	(ISO/IEC 14888-1:2008)	(Information technology - Security techniques - Digital signatures with appendix - Part 1: General)
[5]	ИСО/МЭК 14888-2:2008	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы, основанные на разложении на множители
	(ISO/IEC 14888-2:2008)	(Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms)
[6]	ИСО/МЭК 14888-3:2006	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма
	(ISO/IEC 14888-3:2006)	(Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms)
[7]	ИСО/МЭК 14888-3:2006/Изм. 1:2010	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма. Изменение 1. Алгоритм русской цифровой подписи эллиптической кривой, алгоритм цифровой подписи Шнора, алгоритм цифровой подписи Шнора для эллиптической кривой и полный алгоритм цифровой подписи Шнора для эллиптической кривой
	(ISO/IEC 14888-3:2006/Amd 1:2010)	(Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms. Ammendment 1. Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm)
[8]	ИСО/МЭК 10118-1:2000	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 1. Общие положения
	(ISO/IEC 10118-1:2000)	(Information technology - Security techniques - Hash-functions - Part 1: General)
[9]	ИСО/МЭК 10118-2:2010	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 2. Хэш-функции с использованием алгоритма шифрования n-битными блоками
	(ISO/IEC 10118-2:2010)	(Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher)

[10] ИСО/МЭК 10118-3:2004	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 3. Выделенные хэш-функции
(ISO/IEC 10118-3:2004)	(Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions)
[11] ИСО/МЭК 10118-4:1998	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 4. Хэш-функции с применением арифметики в остаточных классах
(ISO/IEC 10118-4:1998)	(Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic)