ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

**Р 50.1.114—
2016**

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Параметры эллиптических кривых для криптографических алгоритмов и протоколов

Издание официальное

Москва
Стандартинформ
2016

Предисловие

1 РАЗРАБОТАНЫ подкомитетом № 1 Технического комитета по стандартизации ТК 26 «Криптографическая защита информации»

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 ноября 2016 г. № 1829-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (www.gost.ru)

Содержание

Введение

Настоящие рекомендации определяют параметры и идентификаторы эллиптических кривых стандарта ГОСТ Р 34.10 для случая эллиптических кривых в канонической форме с простыми модулями длины 512 бит, а также эллиптических кривых, имеющих представление в форме скрученных кривых Эдвардса, с простыми модулями длины 256 и 512 бит. Данные параметры рекомендуются для совместимых реализаций протоколов ключевого обмена и схем электронной подписи в соответствии с ГОСТ Р 34.10.

В случае эллиптических кривых в канонической форме с модулем p длины 256 бит предлагается использовать параметры, определенные в [1].

Настоящие рекомендации не отменяют использование иных параметров эллиптических кривых.

Примечание — Основная часть настоящих рекомендаций дополнена приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Параметры эллиптических кривых для криптографических алгоритмов и протоколов

Information technology. Cryptographic data security.
Parameters of elliptic curves for cryptographic algorithms and protocols

Дата введения — 2017—06—01

1 Область применения

Определяемые в настоящих рекомендациях параметры эллиптических кривых рекомендуется применять для использования совместно с алгоритмами формирования и проверки электронной цифровой подписи в соответствии с ГОСТ Р 34.10, а также с алгоритмами согласования ключей при защите информации, не содержащей сведений, составляющих государственную тайну.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующий стандарт:

ГОСТ Р 34.10—2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

Примечание — При пользовании настоящими рекомендациями 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 ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Представление в канонической форме

Канонической формой (формой Вейерштрасса) эллиптической кривой E, определенной над конечным простым полем F_p (где p простое, $p>3$), называется множество пар чисел (x,y), x, $y \in F_p$, удовлетворяющих тождеству

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

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

Данное представление используется в ГОСТ Р 34.10—2012 (раздел 5).

3.1 Спецификация

В соответствии с ГОСТ Р 34.10 предлагаются следующие параметры двух эллиптических кривых:

p — модуль эллиптической кривой;

a, b — коэффициенты уравнения эллиптической кривой в канонической форме;

m — порядок группы точек эллиптической кривой;

q — порядок циклической подгруппы группы точек эллиптической кривой;

(x, y) — координаты точки P (порождающего элемента подгруппы порядка q) на эллиптической кривой в канонической форме.

Данный набор параметров представляется в виде ASN структуры следующего вида:

```
SEQUENCE
{
    p    INTEGER,
    a    INTEGER,
    b    INTEGER,
    m    INTEGER,
    q    INTEGER,
    x    INTEGER,
    y    INTEGER
}
```

Наборы параметров имеют следующие идентификаторы:

- id-tc26-gost-3410-12-512-paramSetA, «1.2.643.7.1.2.1.2.1.»;
- id-tc26-gost-3410-12-512-paramSetB, «1.2.643.7.1.2.1.2.2.».

Значения параметров структуры для каждой эллиптической кривой представлены в приложении А настоящих рекомендаций.

4 Представление в форме скрученных кривых Эдвардса

Эллиптическая кривая представлена в форме скрученной кривой Эдвардса, определенной над конечным простым полем F_p (где p простое, $p>3$), если она описывается множеством пар чисел (u,v), u, $v \in F_p$, удовлетворяющих уравнению

$$eu^2+v^2 \equiv 1+du^2v^2 \ (mod\ p), \tag{2}$$

где $e,d \in F_p$, $ed(e-d)$ не сравнимо с нулем по модулю p.

Эллиптическая кривая, представленная в форме скрученной кривой Эдвардса, имеет эквивалентное представление в канонической форме, которая задается соответствующими параметрами a и b. Параметры a, b и e, d связаны следующими соотношениями:

$$\begin{aligned} a&=s^2-3t^2,\\ b&=2t^3-ts^2,\\ s&=(e-d)/4,\\ t&=(e+d)/6. \end{aligned} \tag{3}$$

Преобразования координат при этом задаются следующими соотношениями:

$$\begin{aligned} (u,v)\rightarrow(x,y)&=\left(\frac{s(1+v)}{1-v}+t,\frac{s(1+v)}{(1-v)u}\right),\\ (x,y)\rightarrow(u,v)&=\left(\frac{x-t}{y},\frac{x-t-s}{x-t+s}\right). \end{aligned} \tag{4}$$

4.1 Спецификация

Предлагаются следующие параметры двух эллиптических кривых в соответствии с ГОСТ Р 34.10, имеющих эквивалентное представление в форме скрученных кривых Эдвардса:

p — модуль эллиптической кривой;

a, b — коэффициенты уравнения эллиптической кривой в канонической форме;

e, d — коэффициенты уравнения эллиптической кривой в форме скрученных кривых Эдвардса;

m — порядок группы точек эллиптической кривой;

q — порядок циклической подгруппы группы точек эллиптической кривой;

(x, y) — координаты точки P (порождающего элемента подгруппы порядка q) на эллиптической кривой в канонической форме;

(u, v) — координаты точки P (порождающего элемента подгруппы порядка q) на скрученной кривой Эдвардса.

Данный набор параметров представляется в виде ASN-структуры следующего вида:

```
SEQUENCE
{
    p    INTEGER,
    a    INTEGER,
    b    INTEGER,
    e    INTEGER,
    d    INTEGER,
    m    INTEGER,
    q    INTEGER,
    x    INTEGER,
    y    INTEGER,
    u    INTEGER,
    v    INTEGER
}
```

Наборы параметров имеют следующие идентификаторы:

- id-tc26-gost-3410-2012-256-paramSetA, «1.2.643.7.1.2.1.1.1»;
- id-tc26-gost-3410-2012-512-paramSetC, «1.2.643.7.1.2.1.2.3».

Значения параметров структуры для каждой эллиптической кривой представлены в приложении А настоящих рекомендаций.

Приложение А
(обязательное)

Значения параметров эллиптических кривых

Для каждой из четырех эллиптических кривых, представленных в 3.1 и 4.1 настоящих рекомендаций, приводятся значения параметров их структур.

А.1 Набор параметров id-tc26-gost-3410-12-512-paramSetA

```
SEQUENCE
{
    OBJECT IDENTIFIER
    id-tc26-gost-3410-12-512-paramSetA
    SEQUENCE
    {
     INTEGER
     00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
     C7
     INTEGER
     00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
     C4
     INTEGER
     00 E8 C2 50 5D ED FC 86 DD C1 BD 0B 2B 66 67 F1
     DA 34 B8 25 74 76 1C B0 E8 79 BD 08 1C FD 0B 62
     65 EE 3C B0 90 F3 0D 27 61 4C B4 57 40 10 DA 90
     DD 86 2E F9 D4 EB EE 47 61 50 31 90 78 5A 71 C7
     60
     INTEGER
     00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF 27 E6 95 32 F4 8D 89 11 6F F2 2B 8D 4E 05 60
     60 9B 4B 38 AB FA D2 B8 5D CA CD B1 41 1F 10 B2
     75
     INTEGER
     00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF 27 E6 95 32 F4 8D 89 11 6F F2 2B 8D 4E 05 60
     60 9B 4B 38 AB FA D2 B8 5D CA CD B1 41 1F 10 B2
     75
     INTEGER
     03
     INTEGER
     75 03 CF E8 7A 83 6A E3 A6 1B 88 16 E2 54 50 E6
     CE 5E 1C 93 AC F1 AB C1 77 80 64 FD CB EF A9 21
     DF 16 26 BE 4F D0 36 E9 3D 75 E6 A5 0E 3A 41 E9
     80 28 FE 5F C2 35 F5 B8 89 A5 89 CB 52 15 F2 A4
    }
}
```

А.2 Набор параметров id-tc26-gost-3410-12-512-paramSetB

```
SEQUENCE
{
    OBJECT IDENTIFIER
    id-tc26-gost-3410-12-512-paramSetB
    SEQUENCE
    {
     INTEGER
     00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     6F
     INTEGER
     00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     6C
     INTEGER
     68 7D 1B 45 9D C8 41 45 7E 3E 06 CF 6F 5E 25 17
     B9 7C 7D 61 4A F1 38 BC BF 85 DC 80 6C 4B 28 9F
     3E 96 5D 2D B1 41 6D 21 7F 8B 27 6F AD 1A B6 9C
     50 F7 8B EE 1F A3 10 6E FB 8C CB C7 C5 14 01 16
     INTEGER
     00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     01 49 A1 EC 14 25 65 A5 45 AC FD B7 7B D9 D4 0C
     FA 8B 99 67 12 10 1B EA 0E C6 34 6C 54 37 4F 25
     BD
     INTEGER
     00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     01 49 A1 EC 14 25 65 A5 45 AC FD B7 7B D9 D4 0C
     FA 8B 99 67 12 10 1B EA 0E C6 34 6C 54 37 4F 25
     BD
     INTEGER
     02
     INTEGER
     1A 8F 7E DA 38 9B 09 4C 2C 07 1E 36 47 A8 94 0F
     3C 12 3B 69 75 78 C2 13 BE 6D D9 E6 C8 EC 73 35
     DC B2 28 FD 1E DF 4A 39 15 2C BC AA F8 C0 39 88
     28 04 10 55 F9 4C EE EC 7E 21 34 07 80 FE 41 BD
    }
```

А.3 Набор параметров id-tc26-gost-3410-2012-256-paramSetA

```
SEQUENCE
{
    OBJECT IDENTIFIER
    id-tc26-gost-3410-2012-256-paramSetA
    SEQUENCE
    {
        INTEGER
        00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
        97
        INTEGER
        00 C2 17 3F 15 13 98 16 73 AF 48 92 C2 30 35 A2
        7C E2 5E 20 13 BF 95 AA 33 B2 2C 65 6F 27 7E 73
        35
        INTEGER
```

```
        29 5F 9B AE 74 28 ED 9C CC 20 E7 C3 59 A9 D4 1A
        22 FC CD 91 08 E1 7B F7 BA 93 37 A6 F8 AE 95 13
        INTEGER
        01
        INTEGER
        06 05 F6 B7 C1 83 FA 81 57 8B C3 9C FA D5 18 13
        2B 9D F6 28 97 00 9A F7 E5 22 C3 2D 6D C7 BF FB
        INTEGER
        01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 3F 63 37 7F 21 ED 98 D7 04 56 BD 55 B0 D8 31
        9C
        INTEGER
        40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        0F D8 CD DF C8 7B 66 35 C1 15 AF 55 6C 36 0C 67
        INTEGER
        00 91 E3 84 43 A5 E8 2C 0D 88 09 23 42 57 12 B2
        BB 65 8B 91 96 93 2E 02 C7 8B 25 82 FE 74 2D AA
        28
        INTEGER
        32 87 94 23 AB 1A 03 75 89 57 86 C4 BB 46 E9 56
        5F DE 0B 53 44 76 67 40 AF 26 8A DB 32 32 2E 5C
        INTEGER
        0D
        INTEGER
        60 CA 1E 32 AA 47 5B 34 84 88 C3 8F AB 07 64 9C
        E7 EF 8D BE 87 F2 2E 81 F9 2B 25 92 DB A3 00 E7
    }
}
```

А.4 Набор параметров id-tc26-gost-3410-2012-512-paramSetC

```
SEQUENCE
{
    OBJECT IDENTIFIER
    id-tc26-gost-3410-2012-512-paramSetC
    SEQUENCE
    {
        INTEGER
        00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
        C7
        INTEGER
        00 DC 92 03 E5 14 A7 21 87 54 85 A5 29 D2 C7 22
        FB 18 7B C8 98 0E B8 66 64 4D E4 1C 68 E1 43 06
        45 46 E8 61 C0 E2 C9 ED D9 2A DE 71 F4 6F CF 50
        FF 2A D9 7F 95 1F DA 9F 2A 2E B6 54 6F 39 68 9B
        D3
        INTEGER
        00 B4 C4 EE 28 CE BC 6C 2C 8A C1 29 52 CF 37 F1
        6A C7 EF B6 A9 F6 9F 4B 57 FF DA 2E 4F 0D E5 AD
        E0 38 CB C2 FF F7 19 D2 C1 8D E0 28 4B 8B FE F3
        B5 2B 8C C7 A5 F5 BF 0A 3C 8D 23 19 A5 31 25 57
        E1
        INTEGER
        01
        INTEGER
        00 9E 4F 5D 8C 01 7D 8D 9F 13 A5 CF 3C DF 5B FE
        4D AB 40 2D 54 19 8E 31 EB DE 28 A0 62 10 50 43
        9C A6 B3 9E 0A 51 5C 06 B3 04 E2 CE 43 E7 9E 36
        9E 91 A0 CF C2 BC 2A 22 B4 CA 30 2D BB 33 EE 75
        50
```

```
        INTEGER
        00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        FF 26 33 6E 91 94 1A AC 01 30 CE A7 FD 45 1D 40
        B3 23 B6 A7 9E 9D A6 84 9A 51 88 F3 BD 1F C0 8F
        B4
        INTEGER
        3F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        C9 8C DB A4 65 06 AB 00 4C 33 A9 FF 51 47 50 2C
        C8 ED A9 E7 A7 69 A1 26 94 62 3C EF 47 F0 23 ED
        INTEGER
        00 E2 E3 1E DF C2 3D E7 BD EB E2 41 CE 59 3E F5
        DE 22 95 B7 A9 CB AE F0 21 D3 85 F7 07 4C EA 04
        3A A2 72 72 A7 AE 60 2B F2 A7 B9 03 3D B9 ED 36
        10 C6 FB 85 48 7E AE 97 AA C5 BC 79 28 C1 95 01
        48
        INTEGER
        00 F5 CE 40 D9 5B 5E B8 99 AB BC CF F5 91 1C B8
        57 79 39 80 4D 65 27 37 8B 8C 10 8C 3D 20 90 FF
        9B E1 8E 2D 33 E3 02 1E D2 EF 32 D8 58 22 42 3B
        63 04 F7 26 AA 85 4B AE 07 D0 39 6E 9A 9A DD C4
        0F
        INTEGER
        12
        INTEGER
        46 9A F7 9D 1F B1 F5 E1 6B 99 59 2B 77 A0 1E 2A
        0F DF B0 D0 17 94 36 8D 9A 56 11 7F 7B 38 66 95
        22 DD 4B 65 0C F7 89 EE BF 06 8C 5D 13 97 32 F0
        90 56 22 C0 4B 2B AA E7 60 03 03 EE 73 00 1A 3D
    }
}
```

Библиография

[1] RFC4357 В. Попов, И. Курепкин, С. Леонтьев «Дополнительные алгоритмы шифрования для использования с алгоритмами по ГОСТ 28147—89, ГОСТ Р 34.10—94, ГОСТ Р 34.10—2001 и ГОСТ Р 34.11—94» (Popov V., Kurepkin I. and S. Leontiev, Additional Cryptographic Algorithms for Use with GOST 28147—89, GOST R 34.10—94, GOST R 34.10—2001, and GOST R 34.11—94 Algorithms, Informational, IETF RFC 4357, January 2006)

УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002 П85

Ключевые слова: эллиптическая кривая, кривая Эдвардса

Редактор *Е.С. Смышляева*
Технический редактор *В.Ю. Фотиева*
Корректор *И.А. Королева*
Компьютерная верстка *А.С. Тыртышного*

Сдано в набор 05.12.2016. Подписано в печать 27.12.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 26 экз. Зак. 3316.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru