ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.024— 2019

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Параметры эллиптических кривых для криптографических алгоритмов и протоколов

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ Обществом с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)

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 15 мая 2019 г. № 190-ст

4 ВЗАМЕН Р 50.1.114— 2016

*Правила применения настоящих рекомендаций 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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2019

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Представление в канонической форме 1
3.1 Математическое описание 1
3.2 Параметры кривых 2
4 Представление в форме скрученных кривых Эдвардса 2
4.1 Математическое описание 2
4.2 Параметры кривых 3
Приложение А (обязательное) Значения параметров эллиптических кривых, представленных в канонической форме 4
Приложение Б (обязательное) Значения параметров эллиптических кривых, представленных в форме скрученных кривых Эдвардса 8

Введение

Настоящие рекомендации определяют параметры и идентификаторы эллиптических кривых ГОСТ Р 34.10 для случая эллиптических кривых в канонической форме с простыми модулями длины 256 и 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.

Настоящие рекомендации не отменяют использование иных параметров эллиптических кривых.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Параметры эллиптических кривых для криптографических алгоритмов и протоколов

Information technology. Cryptographic data security.
Elliptic curve parameters for the cryptographic algorithms and protocols

Дата введения — 2019—10—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 использована нормативная ссылка 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

3.1 Математическое описание

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

Издание официальное

$$y^2 \equiv x^3 + ax + b(\mathrm{mod}\ p), \quad (1)$$

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).

3.2 Параметры кривых

В соответствии с ГОСТ Р 34.10 предлагаются следующие параметры пяти 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-3410-2012-256-paramSetB, «1.2.643.7.1.2.1.1.2.»;

id-tc26-gost-3410-2012-256-paramSetC, «1.2.643.7.1.2.1.1.3.»;

id-tc26-gost-3410-2012-256-paramSetD, «1.2.643.7.1.2.1.1.4.»;

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.

4 Представление в форме скрученных кривых Эдвардса

4.1 Математическое описание

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

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

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:

$$a = s^2 - 3t^2,$$

$$b = 2t^3 - ts^2,$$

$$s = (e - d)/4, \quad (3)$$

$$t = (e + d)/6.$$

Преобразования координат при этом задаются следующими соотношениями:

$$(u,v)\to(x,y)=\left(\frac{s(1+v)}{1-v}+t,\frac{s(1+v)}{(1-v)u}\right),$$

$$(x,y)\to(u,v)=\left(\frac{x-t}{y},\frac{x-t-s}{x-t+s}\right). \quad (4)$$

4.2 Параметры кривых

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 Б.

Приложение А
(обязательное)

Значения параметров эллиптических кривых, представленных в канонической форме

Для каждой из пяти эллиптических кривых, представленных в 3.2 настоящих рекомендаций, приводятся значения параметров их структур.

А.1 Набор параметров id-tc26-gost-3410-2012-256-paramSetB

```
SEQUENCE
{
OBJECT IDENTIFIER
id-tc26-gost-3410-2012-256-paramSetB
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 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
  94
  INTEGER
  A6
  INTEGER
  00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  FF 6C 61 10 70 99 5A D1 00 45 84 1B 09 B7 61 B8
  93
  INTEGER
  00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  FF 6C 61 10 70 99 5A D1 00 45 84 1B 09 B7 61 B8
  93
  INTEGER
  01
  INTEGER
  00 8D 91 E4 71 E0 98 9C DA 27 DF 50 5A 45 3F 2B
  76 35 29 4F 2D DF 23 E3 B1 22 AC C9 9C 9E 9F 1E
  14
 }
}
```

А.2 Набор параметров id-tc26-gost-3410-2012-256-paramSetC

```
SEQUENCE
{
   OBJECT IDENTIFIER
   id-tc26-gost-3410-2012-256-paramSetC
   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 0C
    99
    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 0C
            96
            INTEGER
            3E 1A F4 19 A2 69 A5 F8 66 A7 D3 C2 5C 3D F8 0A
            E9 79 25 93 73 FF 2B 18 2F 49 D4 CE 7E 1B BC 8B
            INTEGER
            00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            01 5F 70 0C FF F1 A6 24 E5 E4 97 16 1B CC 8A 19
            8F
            INTEGER
            00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            01 5F 70 0C FF F1 A6 24 E5 E4 97 16 1B CC 8A 19
            8F
            INTEGER
            01
            INTEGER
            3F A8 12 43 59 F9 66 80 B8 3D 1C 3E B2 C0 70 E5
            C5 45 C9 85 8D 03 EC FB 74 4B F8 D7 17 71 7E FC
          }
}
```

A.3 Набор параметров id-tc26-gost-3410-2012-256-paramSetD

```
SEQUENCE
{
   OBJECT IDENTIFIER
   id-tc26-gost-3410-2012-256-paramSetD
   SEQUENCE
   {
    INTEGER
    00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
    AA CF 84 6E 86 78 90 51 D3 79 98 F7 B9 02 2D 75
    9B
    INTEGER
    00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
    AA CF 84 6E 86 78 90 51 D3 79 98 F7 B9 02 2D 75
    98
    INTEGER
    80 5A
    NTEGER
    00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
    AA 58 2C A3 51 1E DD FB 74 F0 2F 3A 65 98 98 0B
    B9
    NTEGER
    00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
    AA 58 2C A3 51 1E DD FB 74 F0 2F 3A 65 98 98 0B
    B9
    INTEGER
    00
    INTEGER
    41 EC E5 57 43 71 1A 8C 3C BF 37 83 CD 08 C0 EE
    4D 4D C4 40 D4 64 1A 8F 36 6E 55 0D FD B3 BB 67
   }
}
```

A.4 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
 NTEGER
 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
}
}
```

A.5 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
  }
}
```

Приложение Б
(обязательное)

Значения параметров эллиптических кривых, представленных в форме скрученных кривых Эдвардса

Для двух эллиптических кривых, представленных в 4.2 настоящих рекомендаций, приводятся значения параметров их структур.

Б.1 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
     }
}
```

Б.2 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
      }
    }
```

УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002

Ключевые слова: информационная технология, криптографическая защита информации, эллиптическая кривая, кривая Эдвардса, параметры

БЗ 5—2019/94

Редактор *Л.И. Нахимова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 16.05.2019 Подписано в печать 23.05.2019 Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,70.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru