ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(РОССТАНДАРТ)

Технический комитет 026

«Криптографическая защита информации»

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

ЗАДАНИЕ ПАРАМЕТРОВ СКРУЧЕННЫХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ЭДВАРДСА В СООТВЕТСТВИИ С ГОСТ Р 34.10-2012

Москва
2014

Содержание

1. Введение

Документ определяет параметры эллиптических кривых стандарта **ГОСТ Р 34.10-2012**, имеющих эквивалентное представление в форме скрученных кривых Эдвардса, с простыми модулями p длины 256 и 512 бит, а также их идентификаторы.

Известно, что некоторые классы эллиптических кривых обладают бирационально эквивалентными представлениями, допускающими более эффективную реализацию групповых операций по сравнению с формой Вейерштрасса. Как показывают теоретические исследования и результаты экспериментов, при реализации схемы электронной цифровой подписи в соответствии с **ГОСТ Р 34.10-2012** и алгоритма выработки общего ключа преимуществами по эффективности обладают скрученные эллиптические кривые в форме Эдвардса. Использование вводимых в данном документе параметров позволяет получать более эффективные программные и аппаратные реализации соответствующих процедур по сравнению с использованием эллиптических кривых в форме Вейерштрасса.

Данный документ не отменяет использование иных параметров эллиптических кривых.

2. Область применения

Определяемые в настоящем документе параметры эллиптических кривых предназначены для использования совместно с алгоритмами формирования и проверки электронной цифровой подписи в соответствии с **ГОСТ Р 34.10-2012**, а также с алгоритмами согласования ключей VKO_GOST3410_2012_256 и VKO_GOST3410_2012_512 в соответствии с **ТК26АЛГ** при защите информации, не содержащей сведений, составляющих государственную тайну.

3. Нормативные ссылки

Указанные в этом разделе ссылочные документы являются обязательными для их применения. Для датированных ссылок используют только указанное здесь издание. Для недатированных ссылок – последнее и актуальное издание со всеми изменениями и дополнениями.

ГОСТ Р 34.10-2012 — Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации, Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ТК26АЛГ — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет №26. Рекомендации по стандартизации. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Москва, 2014.

4. Спецификация

Предлагаются параметры двух эллиптических кривых в соответствии с **ГОСТ Р 34.10-2012**, имеющих эквивалентное представление в форме скрученных кривых Эдвардса.

Наборы параметров имеют следующие идентификаторы:

I) id-tc26-gost-3410-2012-256-paramSetA, «1.2.643.7.1.2.1.1.1»

II) id-tc26-gost-3410-2012-512-paramSetC, «1.2.643.7.1.2.1.2.3»

Для каждой эллиптической кривой представлены значения следующих параметров (значения приведены в виде чисел в десятичной и шестнадцатеричной системах счисления):

p – характеристика простого поля, над которым определяется эллиптическая кривая;

a, **b** – коэффициенты эллиптической кривой в форме Вейерштрасса;

e, d – коэффициенты эквивалентной скрученной эллиптической кривой в форме Эдвардса;

m – порядок группы точек эллиптической кривой;

q – порядок подгруппы простого порядка группы точек эллиптической кривой;

(x,y) – координаты точки P (порождающего элемента подгруппы простого порядка) на кривой в форме Вейерштрасса;

(u,v) – координаты точки P при эквивалентном представлении в форме скрученной кривой Эдвардса.

4.1 Набор параметров id-tc26-gost-3410-2012-256-paramSetA

p = 2^{256}-617

p = $FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD97_{16}$

a = $8778976548588580879336975129440684117161458992519345690985596216650501812715 7_{10}$

a = $C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335_{16}$

b = $1871375173701540376389050345731859656045986779616983027916251146174490100251 5_{10}$

b = $295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513_{16}$

e = 1_{10}

e = 1_{16}

d = $2724414110474605931834268501164757645998726878473076809432604223414351675387_{10}$

d = $605F6B7C183FA81578BC39CFAD518132B9DF62897009AF7E522C32D6DC7BFFB_{16}$

m = $1157920892373161954235709850086879078533542411923690137700486136351421214355 48_{10}$

m = 1000000000000000000000000000000003F63377F21ED98D70456BD55B0D8319C$_{16}$

q = 28948022309329048855892746252171976963338560298092253442512153408785530358887$_{10}$

q = 400000000000000000000000000000000FD8CDDFC87B6635C115AF556C360C67$_{16}$

x = 659873501825845607903086406195868347121055451262697593654067689624532983260 56$_{10}$

x = 91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28$_{16}$

y = 228551892029849628704214025041103992931522353829081057417499874057213204352 92$_{10}$

y = 32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C$_{16}$

u = 13$_{10}$

u = D$_{16}$

v =43779144989398987843428779166090436406934195821915183574454224403186176950503$_{10}$

v = 60CA1E32AA475B348488C38FAB07649CE7EF8DBE87F22E81F92B2592DBA300E7$_{16}$

4.2 Набор параметров id-tc26-gost-3410-2012-512-paramSetC

p = 2^{512}-569

p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDC7$_{16}$

a = 1155220774172662408138485443175427045341999095815853654745363047275328427985602901303342173019597777291248497056097705489756374945796698516542818228427873 9$_{10}$

a = DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3$_{16}$

b = 946765431497423936484977989349793599761654668089364237723598186874105121565103244

$6828994750528267630604306101610711521055955290148577159125187794668181473_{10}$

b = B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C1
8DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1_{16}

e = 1_{10}

e = 1_{16}

d = 829136858254039175995632559944969625017173783865124128958599794055705870368261198
327693382131572427326245697949078360228402539959900787061306101057076974$4_{10}$

d = 9E4F5D8C017D8D9F13A5CF3CDF5BFE4DAB402D54198E31EBDE28A0621050439CA6B39E0A515C06B
304E2CE43E79E369E91A0CFC2BC2A22B4CA302DBB33EE7550$_{16}$

m = 1340780792994259709957402499820584612747936582059239337772356144372176403007344846
347320033739688509767539282340336658205886846512763738374217385971709125$2_{10}$

m = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF26336E91941AAC0130CEA
7FD451D40B323B6A79E9DA6849A5188F3BD1FC08FB4_{16}

q = 335195198248564927489350624955146153186984145514809834443089036093044100751836211
586830008434922127441884820585084164551471711628190934593554346492927281$3_{10}$

q = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC98CDBA46506AB004C33A9
FF5147502CC8EDA9E7A769A12694623CEF47F023ED$_{16}$

x = 1188304634094941753595925361103163743848612198935774824796358501545516705356508594
2161130870937622596747831459979590245849590330315393322885186213222089032$_{10}$

x = E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF
2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148_{16}

y = 1287388791229141876216321917489924902778890935496427956104470458407989428328693568
8639587101137346765264237830933785897290140286858111689735138773336704015$_{10}$

y = F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2

EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F$_{16}$

u = 18$_{10}$

u = 12$_{16}$

v = 3697901750350036466195501370680965130892925445528794106515700685530527913038331015106382234398842797314774264061702328469726236276369898526828850803907133$_{10}$

v = 469AF79D1FB1F5E16B99592B77A01E2A0FDFB0D01794368D9A56117F7B38669522DD4B650CF789EEBF068C5D139732F0905622C04B2BAAE7600303EE73001A3D$_{16}$

5. Приложение

В данном разделе параметры каждой эллиптической кривой представлены в виде структур следующего типа:

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

5.1 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
  }
}
```

5.2 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
  }
}
```