

STANDARDS FOR EFFICIENT CRYPTOGRAPHY

SEC X.2: Recommended Elliptic Curve Domain Parameters

Nippon Telephone and Telegraph Corporation
Contact: Kazumaro Aoki, Tetsutaro Kobayashi, and Akira Nagai
(publickey@lab.ntt.co.jp)

Working Draft
August 6, 2008
Version 0.6

©NTT 2008

1 Recommended Elliptic Curve Domain Parameters over \mathbb{F}_{p^m}

This section specifies the elliptic curve domain parameters over \mathbb{F}_{p^m} recommended in this document. The section is organized as follows. First Section 1.1 describes relevant properties of the recommended parameters over \mathbb{F}_{p^m} . Then Section 1.2 specifies recommended 305-bit elliptic curve domain parameters over \mathbb{F}_{p^m} , Section 1.3 specifies recommended 427-bit elliptic curve domain parameters over \mathbb{F}_{p^m} , Section 1.4 specifies recommended 671-bit elliptic curve domain parameters over \mathbb{F}_{p^m} ,

1.1 Properties of Elliptic Curve Domain Parameters over \mathbb{F}_{p^m}

Following SEC X.1 [1], elliptic curve domain parameters over \mathbb{F}_{p^m} are an octuple:

$$T = (p, m, f(x), a, b, G, n, h)$$

consisting of an integer p and m specifying the finite field \mathbb{F}_{p^m} , an irreducible polynomial $f(x)$ of degree m specifying the polynomial basis representation of \mathbb{F}_{p^m} , two elements $a, b \in \mathbb{F}_{p^m}$ specifying an elliptic curve $E_{\mathbb{F}_{p^m}}$ defined by the equation:

$$E : y^2 = x^3 + ax + b \text{ in } \mathbb{F}_{p^m}$$

a base point $G = (x_G, y_G)$ on $E(\mathbb{F}_{p^m})$, a prime n which is the order of G , and an integer h which is the cofactor $h = \#E(\mathbb{F}_{p^m})/n$.

When elliptic curve domain parameters are specified in this document, each component of this octuple is represented as an octet string converted using the conventions specified in SEC X.1 [1].

Again following SEC X.1 [1], elliptic curve domain parameters over $E(\mathbb{F}_{p^m})$ must have:

$$(p, m) \in \{(2^{61} - 1, 5), (2^{61} - 1, 7), (2^{61} - 1, 11)\}$$

This restriction is designed to encourage interoperability while allowing implementers to supply commonly required security levels. For a Koblitz curve, domain parameters over $E(\mathbb{F}_{p^m})$ with $\lceil \log_2 p^m \rceil = 2t$ supply approximately t bits of security. Meanwhile, for the verifiably random elliptic curve, domain parameters over $E(\mathbb{F}_{p^m})$ with $\lceil \log_2 p^{m-1} \rceil = 2t$ supply approximately t bits of security. This means that solving the logarithm problem on the associated elliptic curve is believed to take approximately 2^t operations.

Furthermore elliptic curve domain parameters over \mathbb{F}_{p^m} must use the reduction polynomials listed in Table 1 below.

This restriction is designed to encourage interoperability while allowing implementers to supply efficient implementations at commonly required security levels.

Here recommended elliptic curve domain parameters are supplied at each of the sizes allowed by SEC X.1 [1].

The elliptic curve domain parameters over \mathbb{F}_{p^m} supplied at the field size consist of examples of two

Field	Reduction Polynomial(s)
$F_{(2^{61}-1)^5}$	$f(x) = x^5 - 3$
$F_{(2^{61}-1)^7}$	$f(x) = x^7 - 3$
$F_{(2^{61}-1)^{11}}$	$f(x) = x^{11} - 3$

Table 1: Representations of \mathbb{F}_{p^m}

different types of parameters. Concretely speaking, one type being parameters associated with a Koblitz curve and the other type being parameters chosen verifiably at random.

Verifiably random parameters offer some additional conservative features. These parameters are chosen from a seed using SHA-1 as specified in SEC X.1 [1]. This process ensures that the parameters cannot be predetermined. The parameters are therefore extremely unlikely to be susceptible to future special-purpose attacks, and no trapdoors can have been placed in the parameters during their generation. When elliptic curve domain parameters are chosen verifiably at random, the seed S used to generate the parameters may optionally be stored along with the parameters so that users can verify the parameters were chosen verifiably at random.

See SEC X.1 [1] for further guidance on the selection of elliptic curve domain parameters over \mathbb{F}_{p^m} .

The example elliptic curve domain parameters over \mathbb{F}_{p^m} have been given nicknames to enable them to be easily identified. The nicknames were chosen as follows. Each name begins with **sec** to denote ‘Standards for Efficient Cryptography’, followed by an **o** to denote parameters over \mathbb{F}_{p^m} , followed by a number denoting the field size n , followed by a **k** to denote parameters associated with Koblitz curves or an **r** to denote random parameters, followed by a sequence number.

Table 2 summarizes salient properties of the recommended elliptic curve domain parameters over \mathbb{F}_{p^m} . Information is represented in Table 2 as follows. The column labelled ‘parameters’ gives the nickname of the elliptic curve domain parameters. The column labelled ‘section’ refers to the section of this document where the parameters are specified. The column labelled ‘strength’ gives the approximate number of bits of security the parameters offer. The column labelled ‘size’ gives the field size. The column labelled ‘RSA/DSA’ gives the approximate size of an RSA or DSA modulus at comparable strength. (See SEC 1 [2] for precise technical guidance on the strength of elliptic curve domain parameters.) Finally the column labelled ‘Koblitz or random’ indicates whether the parameters are associated with a Koblitz curve — ‘k’ — or were chosen verifiably at random — ‘r’.

1.2 Recommended 305-bit Elliptic Curve Domain Parameters over an odd characteristic extension field \mathbb{F}_{p^m}

This section specifies the two recommended 305-bit elliptic curve domain parameters over \mathbb{F}_{p^m} in this document: parameters **seco305k** associated with a Koblitz curve, and verifiably random parameters **seco305r**.

Section 1.2.1 specifies the elliptic curve domain parameters **seco305k**, and Section 1.2.2 specifies

Parameters	Section	Strength	Size	RSA/DSA	Koblitz or random
seco305k	1.2.1	112	305	2048	k
seco305r	1.2.2	128	305	3072	r
seco427k	1.3.1	160	427	3072	k
seco427r	1.3.2	192	427	7680	r
seco671k	1.4.1	256	671	15360	k
seco671r	1.4.2	256	671	15360	r

Table 2: Properties of Recommended Elliptic Curve Domain Parameters over an odd characteristic extension field \mathbb{F}_{p^m}

the elliptic curve domain parameters **seco305r**.

1.2.1 Recommended Parameters **seco305k**

The elliptic curve domain parameters over \mathbb{F}_{p^m} associated with a Koblitz curve **seco305k** are specified by the octuple $T = (p, m, f(x), a, b, G, n, h)$ where $p = 2^{61} - 1$, $m = 5$ and the representation of \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} p &= 2^{61} - 1 \\ &= \text{1FFFFFF FFFFFFF} \end{aligned}$$

$$f(x) = x^5 - 3$$

The curve E: $y^2 = x^3 + ax + b$ over \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} a &= \text{000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 1FFFFFFF FFFFFFFC} \\ b &= \text{000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 0FE3A248 499DD27E} \end{aligned}$$

E was chosen verifiably at random from the seed:

$$S = \text{4E545420 436F7270 6F726174 696F6E00 04A90700}$$

E was selected from S as specified in SEC X.1 [1] in section 3.1.3.1.

The base point G in compressed form is:

$$\begin{aligned} G &= \text{0300595E EA64AD0D 9495D3AC CC43EEBE E2DD7E75 DDA8E143 08EC3E80} \\ &\quad \text{C68B117C C51D0B73 19455C8B} \end{aligned}$$

and in uncompressed form is:

$$\begin{aligned} G &= \text{040059 5EEA64AD 0D9495D3 ACCC43EE BEE2DD7E 75DDA8E1 4308EC3E} \\ &\quad \text{80C68B11 7CC51D0B 7319455C 8B0129D3 6A8F0366 C35FED32 C256A940} \\ &\quad \text{65F0B440 E504DE2A E86E7586 C4658836 F1D7FD89 9E59288F} \end{aligned}$$

G was selected from S as specified in SEC X.1 [1] in section 3.1.3.2.
Finally the order n of G and the cofactor are:

```
n = 100000 00012E8C BC001659 05BE2A45 1CE16B8A 290B3477 AE30812C
    3C2D0183
h = 1FFFFFFF FDA2E683
```

1.2.2 Recommended Parameters seco305r

The verifiably random elliptic curve domain parameters over \mathbb{F}_{p^m} **seco305r** are specified by the octuple $T = (p, m, f(x), a, b, G, n, h)$ where $p = 2^{61} - 1$, $m = 5$ and the representation of \mathbb{F}_{p^m} is defined by:

```
p = 261 - 1
    = 1FFFFFFF FFFFFFFF
f(x) = x5 - 3
```

The curve E: $y^2 = x^3 + ax + b$ over \mathbb{F}_{p^m} is defined by:

```
a = 000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 1FFFFFFF FFFFFFFC
b = 00CE6A C542EE65 694530D7 770BF7DA 97B0B987 1FD7E363 5F312903
    79A295C4 7407C791 6C5490A9
```

E was chosen verifiably at random from the seed:

```
S = 4E545420 436F7270 6F726174 696F6E00 03EB0100
```

E was selected from S as specified in SEC X.1 [1] in section 3.1.3.1.
The base point G in compressed form is:

```
G = 02000000 00000000 00000000 00000000 00000000 36A8C2E2 137228E0
    9A4D8A2C A664293E 1FDE3D99
```

and in uncompressed form is:

```
G = 020000 00000000 00000000 00000000 00000000 0036A8C2 E2137228
    E09A4D8A 2CA66429 3E1FDE3D 99003F79 D371C332 AEDB593A 79AF160B
    C75FCA4D 37FD3D10 EA05D658 BAD0B23F A3BF7EBC C239EA30
```

G was selected from S as specified in SEC X.1 [1] in section 3.1.3.2.
Finally the order n of G and the cofactor are:

```
n = 1FFFF FFFFFFFF FFB00000 00000000 04FFFFFF FFCB2305 2FF95755
    191DFC31 0D16E689 24D05D97
h = 01
```

1.3 Recommended 427-bit Elliptic Curve Domain Parameters over an odd characteristic extension field \mathbb{F}_{p^m}

This section specifies the two recommended 427-bit elliptic curve domain parameters over \mathbb{F}_{p^m} in this document: parameters `seco427k` associated with a Koblitz curve, and verifiably random parameters `seco427r`.

Section 1.3.1 specifies the elliptic curve domain parameters `seco427k`, and Section 1.3.2 specifies the elliptic curve domain parameters `seco427r`.

1.3.1 Recommended Parameters `seco427k`

The elliptic curve domain parameters over \mathbb{F}_{p^m} associated with a Koblitz curve `seco427k` are specified by the octuple $T = (p, m, f(x), a, b, G, n, h)$ where $p = 2^{61} - 1$, $m = 7$ and the representation of \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} p &= 2^{61} - 1 \\ &= \text{1FFFFFF FFFFFFF} \end{aligned}$$

$$f(x) = x^7 - 3$$

The curve E: $y^2 = x^3 + ax + b$ over \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} a &= \quad 0000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \\ &\quad 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 1FFFFFFF \ FFFFFFFC \\ b &= \quad 0000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \\ &\quad 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 02ADD02E \ 768A202C \end{aligned}$$

E was chosen verifiably at random from the seed:

$$S = \text{4E545420 436F7270 6F726174 696F6E00 07006400}$$

E was selected from S as specified in SEC X.1 [1] in section 3.1.3.1.

The base point G in compressed form is:

$$\begin{aligned} G &= \quad 020363 \ 0C3DBA08 \ 22C233D0 \ D60BF2C8 \ 51FB907B \ 32DA9960 \ 0B1608F2 \\ &\quad 56FC5D09 \ 963501EF \ 135D35D6 \ 5C02A14D \ BAFD5065 \ C3DD7403 \ 68EF6F2B \end{aligned}$$

and in uncompressed form is:

$$\begin{aligned} G &= \quad 04 \ 03630C3D \ BA0822C2 \ 33D0D60B \ F2C851FB \ 907B32DA \ 99600B16 \\ &\quad 08F256FC \ 5D099635 \ 01EF135D \ 35D65C02 \ A14DBAFD \ 5065C3DD \ 740368EF \\ &\quad 6F2B0732 \ 9DD20851 \ CBF0648C \ A866E706 \ B4F9EDF5 \ 4B01B380 \ 2D0BD08D \\ &\quad 82B90C5E \ 7DC39032 \ BC6E7E5A \ DDC8F05B \ 0431B135 \ 611F2008 \ 271C2502 \end{aligned}$$

G was selected from S as specified in SEC X.1 [1] in section 3.1.3.2.

Finally the order n of G and the cofactor are:

$$\begin{aligned} n &= \quad 3FFF \ FFFF295D \ 7D42CFD0 \ 66D2958D \ 0A0A4A6C \ 1FF5C071 \ 2E26C0D2 \\ &\quad 5F864565 \ 81E78118 \ 14207946 \ E4FBC329 \ 32B1872D \\ h &= \ 20000000 \ 6B514159 \end{aligned}$$

1.3.2 Recommended Parameters `seco427r`

The verifiably random elliptic curve domain parameters over \mathbb{F}_{p^m} `seco427r` are specified by the octuple $T = (p, m, f(x), a, b, G, n, h)$ where $p = 2^{61} - 1$, $m = 7$ and the representation of \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} p &= 2^{61} - 1 \\ &= \text{1FFFFFFF FFFFFFFF} \\ f(x) &= x^7 - 3 \end{aligned}$$

The curve E: $y^2 = x^3 + ax + b$ over \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} a &= \quad 0000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \\ &\quad 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 1FFFFFFF \ FFFFFFFC \\ b &= \quad 4DFF \ B7A2CEC7 \ D877A2F1 \ 416033A6 \ CCE84DD \ 9301FA23 \ 6A254818 \\ &\quad 8DA1C1CB \ 1DE92903 \ EB3E9372 \ 76E5240C \ 11A15F48 \ E8B36379 \ FA5B579F \end{aligned}$$

E was chosen verifiably at random from the seed:

$$S = \text{4E545420 436F7270 6F726174 696F6E00 06BABA00}$$

E was selected from S as specified in SEC X.1 [1] in section 3.1.3.1.

$$\begin{aligned} G &= \quad 020000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \\ &\quad 00000000 \ 00000000 \ 25A0F41E \ 124C90C2 \ E3AE8FB8 \ EE228EAC \ 1BEAF72A \end{aligned}$$

and in uncompressed form is:

$$\begin{aligned} G &= \quad 04 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \ 00000000 \\ &\quad 00000000 \ 00000000 \ 000025A0 \ F41E124C \ 90C2E3AE \ 8FB8EE22 \ 8EAC1BEA \\ &\quad F72A042F \ 38ACC12B \ DC9C5CE5 \ 7251C039 \ 81863365 \ A9C80199 \ 0F0AB1CE \\ &\quad 462C2538 \ 6D34ACC5 \ 24F20452 \ 6D6C79FC \ 065FF797 \ F426C4D9 \ 66B92113 \end{aligned}$$

G was selected from S as specified in SEC X.1 [1] in section 3.1.3.2.

Finally the order n of G and the cofactor are:

$$\begin{aligned} n &= \quad 7FF \ FFFFFFFF \ FFFE4000 \ 00000000 \ 0029FFFF \ FFFFFFFF \ FDCFFFFFFF \\ &\quad FFED95A5 \ B02D31FF \ FB2115C1 \ AB3D0D3B \ D4477989 \ A552CAB0 \ 60D8C4AF \\ h &= \quad 01 \end{aligned}$$

1.4 Recommended 671-bit Elliptic Curve Domain Parameters over an odd characteristic extension field \mathbb{F}_{p^m}

This section specifies the two recommended 610-bit elliptic curve domain parameters over \mathbb{F}_{p^m} in this document: parameters `seco671k` associated with a Koblitz curve, and verifiably random parameters `seco671r`.

Section 1.4.1 specifies the elliptic curve domain parameters `seco671k`, and Section 1.4.2 specifies the elliptic curve domain parameters `seco671r`.

1.4.1 Recommended Parameters seco671k

The elliptic curve domain parameters over \mathbb{F}_{p^m} associated with a Koblitz curve **seco671k** are specified by the octuple $T = (p, m, f(x), a, b, G, n, h)$ where $p = 2^{61} - 1$, $m = 11$ and the representation of \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} p &= 2^{61} - 1 \\ &= \text{1FFFFFFF FFFFFFFF} \\ f(x) &= x^{11} - 3 \end{aligned}$$

The curve E: $y^2 = x^3 + ax + b$ over \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} a &= \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 00000000 00000000 00000000 00000000 1FFFFFFF FFFFFFFC} \\ b &= \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 00000000 00000000 00000000 00000000 07D5B59B 5A5E5429} \end{aligned}$$

E was chosen verifiably at random from the seed:

$$S = \text{4E545420 436F7270 6F726174 696F6E00 06BC1300}$$

E was selected from S as specified section 3.1.3.1 in SEC X.1 [1] in section 3.1.3.1.

The base point G in compressed form is:

$$\begin{aligned} G &= \quad \text{03 24293b96 4B416E53 BDAB2713 33AE270B 014EDB71 3C6947A5} \\ &\quad \text{E747BD9B 276C4F0D 5A95649C AF96C63E 34304E22 04E1DD2B DAFEF27C} \\ &\quad \text{C2C3B321 C931E182 34DB653D 216610EC DF661912 33E3AD13 0123B520} \\ &\quad \text{52CD0C0A} \end{aligned}$$

and in uncompressed form is:

$$\begin{aligned} G &= \quad \text{04 24293b96 4B416E53 BDAB2713 33AE270B 014EDB71 3C6947A5} \\ &\quad \text{E747BD9B 276C4F0D 5A95649C AF96C63E 34304E22 04E1DD2B DAFEF27C} \\ &\quad \text{C2C3B321 C931E182 34DB653D 216610EC DF661912 33E3AD13 0123B520} \\ &\quad \text{52CD0C0A 6BF67DFB B9AF89C3 2EFDD5B0 7E4349D7 ODD57C57 99C7D06B} \\ &\quad \text{735BA461 F1241B7D 2A98CB83 621FB1A3 5BCED502 687C7648 2925BF20} \\ &\quad \text{7A61075E 655F0CD8 962703BB CC239D54 6F3D4C59 286B4030 53DA73E7} \\ &\quad \text{A039AE5F} \end{aligned}$$

G was selected from S as specified in SEC X.1 [1] in section 3.1.3.2.

Finally the order n of G and the cofactor are:

$$\begin{aligned} n &= \quad \text{03 FFFFFFFF1 8C568094 36B2E5E4 78B92E0A 117C2B3E F36B0E42} \\ &\quad \text{57FA68EF DB9F9E62 EE411700 5C737B6B 7FC9989E EE472ACB 99927E19} \\ &\quad \text{9CEE7135 DB0E5499 6BFAE625 D90B03E1 FF5BA546 8798E6F7} \\ h &= \text{20000000 739D4BF2} \end{aligned}$$

1.4.2 Recommended Parameters `seco671r`

The elliptic curve domain parameters over \mathbb{F}_{p^m} associated with a Koblitz curve `seco671r` are specified by the octuple $T = (p, m, f(x), a, b, G, n, h)$ where $p = 2^{61} - 1$, $m = 11$ and the representation of \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} p &= 2^{61} - 1 \\ &= \text{1FFFFFFF FFFFFFFF} \end{aligned}$$

$$f(x) = x^{11} - 3$$

The curve E: $y^2 = x^3 + ax + b$ over \mathbb{F}_{p^m} is defined by:

$$\begin{aligned} a &= \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000 00000000 00000000 00000000 00000000 1FFFFFFF FFFFFFFC} \end{aligned}$$

E was chosen verifiably at random from the seed:

$$S = \text{4E545420 436F7270 6F726174 696F6E00 ??????00}$$

E was selected from S as specified in SEC X.1 [1] in section 3.1.3.1.

to be completed . . .

References

- [1] SEC X.1 Supplemental Document for Odd Characteristic Extension Fields. Nippon Telephone and Telegraph Corporation, June, 2008.
- [2] SEC 1. Elliptic Curve Cryptography. Standards for Efficient Cryptography Group, September, 2000. Working Draft. Available from: <http://www.secg.org/>