Standards for Efficient Cryptography

SEC 2: Recommended Elliptic Curve Domain Parameters

Certicom Research

Contact: Daniel R. L. Brown (dbrown@certicom.com)

Working Draft
September 27, 2005
Version 1.5

Contents

List of Tables

1 Introduction

1.1 Overview

This document lists example elliptic curve domain parameters at commonly required security levels for use by implementers of SEC 1 [SEC00] and other ECC standards like ANSI X9.62 [ANS98], ANSI X9.63 [ANS01], and IEEE P1363 [IEE99].

It is strongly recommended that implementers select parameters from among the example parameters listed in this document when they deploy ECC-based products in order to encourage the deployment of interoperable ECC-based solutions.

1.2 Compliance

Implementations may claim compliance with the recommended parameters specified in this document provided some subset of the recommended parameters are used by the cryptographic schemes based on elliptic curve cryptography included in the implementation.

It is envisioned that implementations choosing to comply with this document will typically choose also to comply with its companion document, SEC 1 [SEC00].

It is intended to make a validation system available so that implementors can check compliance with this document - see the SECG website, www.secg.org, for further information.

1.3 Document Evolution

This document will be reviewed every five years to ensure it remains up to date with cryptographic advances. The next scheduled review will therefore take place in September 2005.

Additional intermittent reviews may also be performed from time-to-time as deemed necessary by the Standards for Efficient Cryptography Group.

1.4 Intellectual Property

The reader's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder(s) may have filed with the SECG a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Additional details may be obtained from the patent holder and from the SECG website, www.secg.org.

1.5 Organization

This document is organized as follows.

The main body of the document focuses on the specification of recommended elliptic curve domain parameters. Section 2 describes recommended elliptic curve domain parameters over $\mathbb{F}_p$, and Section 3 describes recommended elliptic curve domain parameters over $\mathbb{F}_{2^m}$.

The appendices to the document provide additional relevant material. Appendix A provides reference ASN.1 syntax for implementations to use to identify the parameters. Appendix B lists the references cited in the document.

2 Recommended Elliptic Curve Domain Parameters over $\mathbb{F}_p$

This section specifies the elliptic curve domain parameters over $\mathbb{F}_p$ recommended in this document.

The section is organized as follows. First Section 2.1 describes relevant properties of the recommended parameters over $\mathbb{F}_p$. Then Section 2.2 specifies recommended 192-bit elliptic curve domain parameters over $\mathbb{F}_p$, Section 2.3 specifies recommended 224-bit elliptic curve domain parameters over $\mathbb{F}_p$, Section 2.4 specifies recommended 256-bit elliptic curve domain parameters over $\mathbb{F}_p$, Section 2.5 specifies recommended 384-bit elliptic curve domain parameters over $\mathbb{F}_p$, Section 2.6 specifies recommended 521-bit elliptic curve domain parameters over $\mathbb{F}_p$,

2.1 Properties of Elliptic Curve Domain Parameters over $\mathbb{F}_p$

Following SEC 1 [SEC00], elliptic curve domain parameters over $\mathbb{F}_p$ are a sextuple:

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

consisting of an integer p specifying the finite field $\mathbb{F}_p$, two elements $a, b \in \mathbb{F}_p$ specifying an elliptic curve $E(\mathbb{F}_p)$ defined by the equation:

$$E : \; y^2 \equiv x^3 + a.x + b \pmod{p},$$

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

When elliptic curve domain parameters are specified in this document, each component of this sextuple is represented as an octet string converted using the conventions specified in SEC 1 [SEC00].

Again following SEC 1 [SEC00], elliptic curve domain parameters over $\mathbb{F}_p$ must have:

$$\lceil \log_2 p \rceil \in \{192, 224, 256, 384, 521\}.$$

This restriction is designed to encourage interoperability while allowing implementers to supply commonly required security levels — recall that elliptic curve domain parameters over $\mathbb{F}_p$ with $\lceil \log_2 p \rceil = 2t$ supply approximately t bits of security — meaning that solving the logarithm problem on the associated elliptic curve is believed to take approximately 2^t operations.

Here recommended elliptic curve domain parameters are supplied at each of the sizes allowed in SEC 1.

All the recommended elliptic curve domain parameters over $\mathbb{F}_p$ use special form primes for their field order p. These special form primes facilitate especially efficient implementations like those described in [NIS99]. Recommended elliptic curve domain parameters over $\mathbb{F}_p$ which use random primes for their field order p may be added later if commercial demand for such parameters increases.

The elliptic curve domain parameters over $\mathbb{F}_p$ supplied at each security level typically consist of examples of two different types of parameters — one type being parameters associated with a Koblitz curve and the other type being parameters chosen verifiably at random — although only verifiably random parameters are supplied at export strength and at extremely high strength.

Parameters associated with a Koblitz curve admit especially efficient implementation. The name Koblitz curve is best-known when used to describe binary anomalous curves over $\mathbb{F}_{2^m}$ which have $a, b \in \{0, 1\}$ [Kob92]. Here it is generalized to refer also to curves over $\mathbb{F}_p$ which possess an efficiently computable endomorphism [?]. The recommended parameters associated with a Koblitz curve were chosen by repeatedly selecting parameters admitting an efficiently computable endomorphism until a prime order curve was found.

Verifiably random parameters offer some additional conservative features. These parameters are chosen from a seed using SHA-1 as specified in ANSI X9.62 [ANS98]. 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.

Here verifiably random parameters have been chosen either so that the associated elliptic curve has prime order, or so that scalar multiplication of points on the associated elliptic curve can be accelerated using Montgomery's method [?]. The recommended verifiably random parameters were chosen by repeatedly selecting a random seed and counting the number of points on the corresponding curve until appropriate parameters were found. Typically the parameters were chosen so that $a = p - 3$ because such parameters admit efficient implementation. For a given p, approximately half the isomorphism classes of elliptic curves over $\mathbb{F}_p$ contain a curve with $a = p - 3$.

See SEC 1 [SEC00] for further guidance on the selection of elliptic curve domain parameters over $\mathbb{F}_p$.

Parameters	Section	Strength	Size	RSA/DSA	Koblitz or random
secp192k1	2.2.1	96	192	1536	k
secp192r1	2.2.2	96	192	1536	r
secp224k1	2.3.1	112	224	2048	k
secp224r1	2.3.2	112	224	2048	r
secp256k1	2.4.1	128	256	3072	k
secp256r1	2.4.2	128	256	3072	r
secp384r1	2.5.1	192	384	7680	r
secp521r1	2.6.1	256	521	15360	r

Table 1: Properties of Recommended Elliptic Curve Domain Parameters over $\mathbb{F}_p$

The recommended elliptic curve domain parameters over $\mathbb{F}_p$ 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 a `p` to denote parameters over

$\mathbb{F}_p$, followed by a number denoting the length in bits of the field size p, followed by a `k` to denote parameters associated with a Koblitz curve or an `r` to denote verifiably random parameters, followed by a sequence number.

Table 1 summarizes salient properties of the recommended elliptic curve domain parameters over $\mathbb{F}_p$.

Information is represented in Table 1 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 length in bits of the field order. The column labelled 'RSA/DSA' gives the approximate size of an RSA or DSA modulus at comparable strength. (See SEC 1 [SEC00] 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'.

Parameters	Section	ANSI X9.62	ANSI X9.63	echeck	IEEE P1363	IPSec	NIST	WAP
secp192k1	2.2.1	c	r	c	c	c	-	c
secp192r1	2.2.2	r	r	c	c	c	r	c
secp224k1	2.3.1	c	r	c	c	c	-	c
secp224r1	2.3.2	c	r	c	c	c	r	c
secp256k1	2.4.1	c	r	c	c	c	-	c
secp256r1	2.4.2	r	r	c	c	c	r	c
secp384r1	2.5.1	c	r	c	c	c	r	c
secp521r1	2.6.1	c	r	c	c	c	r	c

Table 2: Status of Recommended Elliptic Curve Domain Parameters over $\mathbb{F}_p$

Table 2 summarizes the status of the recommended elliptic curve domain parameters over $\mathbb{F}_p$ with respect to their alignment with other standards.

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 remaining columns give the status of the parameters with respect to various other standards which specify mechanisms based on elliptic curve cryptography: 'ANSI X9.62' refers to the ANSI X9.62 standard [ANS98], 'ANSI X9.63' refers to the draft ANSI X9.63 standard [ANS01], 'echeck' refers to the draft FSML standard [Fin99], 'IEEE P1363' refers to the draft IEEE P1363 standard [IEE99], 'IPSec' refers to the recent internet draft related to ECC [?] submitted to the IETF's IPSec working group, 'NIST' refers to the list of recommended parameters recently released by the U.S. government [NIS99], and 'WAP' refers to the Wireless Application Forum's WTLS standard [WAP99]. In these columns, a '-' denotes parameters non-conformant with the standard, a 'c' denotes parameters conformant with the standard, and an 'r' denotes parameters explicitly recommended in the standard.

Note that ANSI X9.62 is currently being updated. The set of recommended parameters in the proposed ANSI X9.62-1 [?] is identical to the set of recommended parameters in this document.

2.2 Recommended 192-bit Elliptic Curve Domain Parameters over $\mathbb{F}_p$

This section specifies the two recommended 192-bit elliptic curve domain parameters over $\mathbb{F}_p$ in this document: parameters `secp192k1` associated with a Koblitz curve, and verifiably random parameters `secp192r1`.

Section 2.2.1 specifies the elliptic curve domain parameters `secp192k1`, and Section 2.2.2 specifies the elliptic curve domain parameters `secp192r1`.

2.2.1 Recommended Parameters secp192k1

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp192k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

$$p = \texttt{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFEE37}$$
$$= 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$$

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

$$a = \texttt{00000000 00000000 00000000 00000000 00000000 00000000}$$
$$b = \texttt{00000000 00000000 00000000 00000000 00000000 00000003}$$

The base point G in compressed form is:

$$G = \texttt{03 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D}$$

and in uncompressed form is:

$$G = \texttt{04 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D}$$
$$\texttt{9B2F2F6D 9C5628A7 844163D0 15BE8634 4082AA88 D95E2F9D}$$

Finally the order n of G and the cofactor are:

$$n = \texttt{FFFFFFFF FFFFFFFF FFFFFFFE 26F2FC17 0F69466A 74DEFD8D}$$
$$h = \texttt{01}$$

2.2.2 Recommended Parameters secp192r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_p$ `secp192r1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF
$= 2^{192} - 2^{64} - 1$

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

a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFC

b = 64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1

E was chosen verifiably at random as specified in ANSI X9.62 [ANS98] from the seed:

S = 3045AE6F C8422F64 ED579528 D38120EA E12196D5

The base point G in compressed form is:

G = 03 188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012

and in uncompressed form is:

G = 04 188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012
07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811

Finally the order n of G and the cofactor are:

n = FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831

h = 01

2.3 Recommended 224-bit Elliptic Curve Domain Parameters over $\mathbb{F}_p$

This section specifies the two recommended 224-bit elliptic curve domain parameters over $\mathbb{F}_p$ in this document: parameters `secp224k1` associated with a Koblitz curve, and verifiably random parameters `secp224r1`.

Section 2.3.1 specifies the elliptic curve domain parameters `secp224k1`, and Section 2.3.2 specifies the elliptic curve domain parameters `secp224r1`.

2.3.1 Recommended Parameters secp224k1

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp224k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFE56D
$= 2^{224} - 2^{32} - 2^{12} - 2^{11} - 2^9 - 2^7 - 2^4 - 2 - 1$

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

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000000 00000005

The base point G in compressed form is:

G = 03 A1455B33 4DF099DF 30FC28A1 69A467E9 E47075A9 0F7E650E
B6B7A45C

and in uncompressed form is:

G = 04 A1455B33 4DF099DF 30FC28A1 69A467E9 E47075A9 0F7E650E
B6B7A45C 7E089FED 7FBA3442 82CAFBD6 F7E319F7 C0B0BD59 E2CA4BDB
556D61A5

Finally the order n of G and the cofactor are:

n = 01 00000000 00000000 00000000 0001DCE8 D2EC6184 CAF0A971
769FB1F7

h = 01

2.3.2 Recommended Parameters secp224r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_p$ `secp224r1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 00000000 00000001
$= 2^{224} - 2^{96} + 1$

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

a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFE

b = B4050A85 0C04B3AB F5413256 5044B0B7 D7BFD8BA 270B3943 2355FFB4

E was chosen verifiably at random as specified in ANSI X9.62 [ANS98] from the seed:

S = BD713447 99D5C7FC DC45B59F A3B9AB8F 6A948BC5

The base point G in compressed form is:

G = 02 B70E0CBD 6BB4BF7F 321390B9 4A03C1D3 56C21122 343280D6
115C1D21

and in uncompressed form is:

G = 04 B70E0CBD 6BB4BF7F 321390B9 4A03C1D3 56C21122 343280D6
115C1D21 BD376388 B5F723FB 4C22DFE6 CD4375A0 5A074764 44D58199
85007E34

Finally the order n of G and the cofactor are:

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D

h = 01

2.4 Recommended 256-bit Elliptic Curve Domain Parameters over $\mathbb{F}_p$

This section specifies the two recommended 256-bit elliptic curve domain parameters over $\mathbb{F}_p$ in this document: parameters `secp256k1` associated with a Koblitz curve, and verifiably random parameters `secp256r1`.

Section 2.4.1 specifies the elliptic curve domain parameters `secp256k1`, and Section 2.4.2 specifies the elliptic curve domain parameters `secp256r1`.

2.4.1 Recommended Parameters secp256k1

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp256k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = `FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F`

$= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

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

a = `00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000`

b = `00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007`

The base point G in compressed form is:

G = `02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798`

and in uncompressed form is:

G = `04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8`

Finally the order n of G and the cofactor are:

n = `FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141`

h = `01`

2.4.2 Recommended Parameters secp256r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_p$ `secp256r1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF

$= 2^{224}(2^{32} - 1) + 2^{192} + 2^{96} - 1$

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

a = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC

b = 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B

E was chosen verifiably at random as specified in ANSI X9.62 [ANS98] from the seed:

S = C49D3608 86E70493 6A6678E1 139D26B7 819F7E90

The base point G in compressed form is:

G = 03 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296

and in uncompressed form is:

G = 04 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5

Finally the order n of G and the cofactor are:

n = FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

h = 01

2.5 Recommended 384-bit Elliptic Curve Domain Parameters over $\mathbb{F}_p$

This section specifies the recommended 384-bit elliptic curve domain parameters over $\mathbb{F}_p$ in this document: verifiably random parameters `secp384r1`.

Section 2.5.1 specifies the elliptic curve domain parameters `secp384r1`.

2.5.1 Recommended Parameters secp384r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_p$ `secp384r1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = `FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF`
`FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFF`
$= 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$

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

a = `FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF`
`FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFC`

b = `B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F`
`5013875A C656398D 8A2ED19D 2A85C8ED D3EC2AEF`

E was chosen verifiably at random as specified in ANSI X9.62 [ANS98] from the seed:

S = `A335926A A319A27A 1D00896A 6773A482 7ACDAC73`

The base point G in compressed form is:

G = `03 AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98`
`59F741E0 82542A38 5502F25D BF55296C 3A545E38 72760AB7`

and in uncompressed form is:

G = `04 AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98`
`59F741E0 82542A38 5502F25D BF55296C 3A545E38 72760AB7 3617DE4A`
`96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C E9DA3113 B5F0B8C0`
`0A60B1CE 1D7E819D 7A431D7C 90EA0E5F`

Finally the order n of G and the cofactor are:

n = `FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81`
`F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973`

h = `01`

2.6 Recommended 521-bit Elliptic Curve Domain Parameters over $\mathbb{F}_p$

This section specifies the recommended 521-bit elliptic curve domain parameters over $\mathbb{F}_p$ in this document: verifiably random parameters `secp521r1`.

Section 2.6.1 specifies the elliptic curve domain parameters `secp521r1`.

2.6.1 Recommended Parameters secp521r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_p$ `secp521r1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = 01FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF
= $2^{521} - 1$

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

a = 01FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFC

b = 0051 953EB961 8E1C9A1F 929A21A0 B68540EE A2DA725B 99B315F3
B8B48991 8EF109E1 56193951 EC7E937B 1652C0BD 3BB1BF07 3573DF88
3D2C34F1 EF451FD4 6B503F00

E was chosen verifiably at random as specified in ANSI X9.62 [ANS98] from the seed:

S = D09E8800 291CB853 96CC6717 393284AA A0DA64BA

The base point G in compressed form is:

G = 0200C6 858E06B7 0404E9CD 9E3ECB66 2395B442 9C648139 053FB521
F828AF60 6B4D3DBA A14B5E77 EFE75928 FE1DC127 A2FFA8DE 3348B3C1
856A429B F97E7E31 C2E5BD66

and in uncompressed form is:

G = 04 00C6858E 06B70404 E9CD9E3E CB662395 B4429C64 8139053F
B521F828 AF606B4D 3DBAA14B 5E77EFE7 5928FE1D C127A2FF A8DE3348
B3C1856A 429BF97E 7E31C2E5 BD660118 39296A78 9A3BC004 5C8A5FB4
2C7D1BD9 98F54449 579B4468 17AFBD17 273E662C 97EE7299 5EF42640
C550B901 3FAD0761 353C7086 A272C240 88BE9476 9FD16650

Finally the order n of G and the cofactor are:

n = 01FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFA 51868783 BF2F966B 7FCC0148 F709A5D0 3BB5C9B8
899C47AE BB6FB71E 91386409

h = 01

3 Recommended Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

This section specifies the elliptic curve domain parameters over $\mathbb{F}_{2^m}$ recommended in this document.

The section is organized as follows. First Section 3.1 describes relevant properties of the recommended parameters over $\mathbb{F}_{2^m}$. Then Section 3.2 specifies recommended 163-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$, Section 3.3 specifies recommended 233-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$, Section 3.4 specifies recommended 239-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$, Section 3.5 specifies recommended 283-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$, Section 3.6 specifies recommended 409-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$, and Section 3.7 specifies recommended 571-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$.

3.1 Properties of Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

Following SEC 1 [SEC00], elliptic curve domain parameters over $\mathbb{F}_{2^m}$ are a septuple:

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

consisting of an integer m specifying the finite field $\mathbb{F}_{2^m}$, an irreducible binary polynomial $f(x)$ of degree m specifying the polynomial basis representation of $\mathbb{F}_{2^m}$, two elements $a, b \in \mathbb{F}_{2^m}$ specifying an elliptic curve $E(\mathbb{F}_{2^m})$ defined by the equation:

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

a base point $G = (x_G, y_G)$ on $E(\mathbb{F}_{2^m})$, a prime n which is the order of G, and an integer h which is the cofactor $h = \#E(\mathbb{F}_{2^m})/n$.

When elliptic curve domain parameters over $\mathbb{F}_{2^m}$ are specified in this document, m is represented directly as an integer, $f(x)$ is represented directly as a polynomial, and the remaining components are represented as octet strings converted using the conventions specified in SEC 1 [SEC00].

Again following SEC 1 [SEC00], elliptic curve domain parameters over $\mathbb{F}_{2^m}$ must have:

$$m \in \{163, 233, 239, 283, 409, 571\}.$$

Furthermore elliptic curve domain parameters over $\mathbb{F}_{2^m}$ must use the reduction polynomials listed in Table 3 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 1.

The elliptic curve domain parameters over $\mathbb{F}_{2^m}$ supplied at each security level typically consist of examples of two different types of parameters — one type being parameters associated with a Koblitz curve and the other type being parameters chosen verifiably at random — although only verifiably random parameters are supplied at export strength.

Field	Reduction Polynomial(s)
$\mathbb{F}_{2^{163}}$	$f(x) = x^{163} + x^7 + x^6 + x^3 + 1$
$\mathbb{F}_{2^{233}}$	$f(x) = x^{233} + x^{74} + 1$
$\mathbb{F}_{2^{239}}$	$f(x) = x^{239} + x^{36} + 1$ or $x^{239} + x^{158} + 1$
$\mathbb{F}_{2^{283}}$	$f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$
$\mathbb{F}_{2^{409}}$	$f(x) = x^{409} + x^{87} + 1$
$\mathbb{F}_{2^{571}}$	$f(x) = x^{571} + x^{10} + x^5 + x^2 + 1$

Table 3: Representations of $\mathbb{F}_{2^m}$

Parameters associated with a Koblitz curve admit especially efficient implementation. Koblitz curves over $\mathbb{F}_{2^m}$ are binary anomalous curves which have $a, b \in \{0, 1\}$ [Kob92].

Verifiably random parameters offer some additional conservative features. These parameters are chosen from a seed using SHA-1 as specified in ANSI X9.62 [ANS98]. 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.

The recommended verifiably random parameters were chosen by repeatedly selecting a random seed and counting the points on the corresponding curve using Schoof's algorithm until appropriate parameters were found. The parameters were chosen so that either a is random or $a = 1$. For a given m, approximately half the isomorphism classes of elliptic curves over $\mathbb{F}_{2^m}$ contain a curve with $a = 1$.

See SEC 1 [SEC00] for further guidance on the selection of elliptic curve domain parameters over $\mathbb{F}_{2^m}$.

The example elliptic curve domain parameters over $\mathbb{F}_{2^m}$ 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 a `t` to denote parameters over $\mathbb{F}_{2^m}$, followed by a number denoting the field size m, followed by a `k` to denote parameters associated with a Koblitz curve or an `r` to denote verifiably random parameters, followed by a sequence number.

Table 4 summarizes salient properties of the recommended elliptic curve domain parameters over $\mathbb{F}_{2^m}$.

Information is represented in Table 4 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 m. The column labelled 'RSA/DSA' gives the approximate size of an RSA or DSA modulus at comparable strength. (See SEC 1 [SEC00] for precise technical guidance on the strength

Parameters	Section	Strength	Size	RSA/DSA	Koblitz or random
sect163k1	3.2.1	80	163	1024	k
sect163r1	3.2.2	80	163	1024	r
sect163r2	3.2.3	80	163	1024	r
sect233k1	3.3.1	112	233	2240	k
sect233r1	3.3.2	112	233	2240	r
sect239k1	3.4.1	115	239	2304	k
sect283k1	3.5.1	128	283	3456	k
sect283r1	3.5.2	128	283	3456	r
sect409k1	3.6.1	192	409	7680	k
sect409r1	3.6.2	192	409	7680	r
sect571k1	3.7.1	256	571	15360	k
sect571r1	3.7.2	256	571	15360	r

Table 4: Properties of Recommended Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

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'.

Parameters	Section	ANSI X9.62	ANSI X9.63	echeck	IEEE P1363	IPSec	NIST	WAP
sect163k1	3.2.1	c	r	r	c	r	r	r
sect163r1	3.2.2	c	c	r	c	r	-	c
sect163r2	3.2.3	c	r	r	c	c	r	c
sect233k1	3.3.1	c	r	c	c	c	r	c
sect233r1	3.3.2	c	r	c	c	c	r	c
sect239k1	3.4.1	c	c	c	c	c	-	c
sect283k1	3.5.1	c	r	r	c	r	r	c
sect283r1	3.5.2	c	r	r	c	r	r	c
sect409k1	3.6.1	c	r	c	c	c	r	c
sect409r1	3.6.2	c	r	c	c	c	r	c
sect571k1	3.7.1	c	r	c	c	c	r	c
sect571r1	3.7.2	c	r	c	c	c	r	c

Table 5: Status of Recommended Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

Table 5 summarizes the status of the recommended elliptic curve domain parameters over $\mathbb{F}_{2^m}$ with respect to their alignment with other standards.

Information is represented in Table 5 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 remaining columns give the status of the parameters with respect to various other standards which specify mechanisms based on elliptic curve cryptography: 'ANSI X9.62' refers to the ANSI X9.62 standard [ANS98], 'ANSI X9.63' refers to the draft ANSI X9.63 standard [ANS01], 'echeck' refers to the draft FSML standard [Fin99], 'IEEE P1363' refers to the draft IEEE P1363 standard [IEE99], 'IPSec' refers to the recent internet draft related to ECC [?] submitted to the IETF's IPSec working group, 'NIST' refers to the list of recommended parameters recently released by the U.S. government [NIS99], and 'WAP' refers to the Wireless Application Forum's WTLS standard [WAP99]. In these columns, a '-' denotes parameters non-conformant with the standard, a 'c' denotes parameters conformant with the standard, and an 'r' denotes parameters explicitly recommended in the standard.

Note that ANSI X9.62 is currently being updated. The set of recommended parameters in the proposed ANSI X9.62-1 [?] is identical to the set of recommended parameters in this document.

3.2 Recommended 163-bit Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

This section specifies the three recommended 163-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$ in this document: parameters `sect163k1` associated with a Koblitz curve, verifiably random parameters `sect163r1`, and verifiably random parameters `sect163r2`.

Section 3.2.1 specifies the elliptic curve domain parameters `sect163k1`, Section 3.2.2 specifies the elliptic curve domain parameters `sect163r1`, and Section 3.2.3 specifies the elliptic curve domain parameters `sect163r2`.

3.2.1 Recommended Parameters sect163k1

The elliptic curve domain parameters over $\mathbb{F}_{2^m}$ associated with a Koblitz curve `sect163k1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 163$ and the representation of $\mathbb{F}_{2^{163}}$ is defined by:

$$f(x) = x^{163} + x^7 + x^6 + x^3 + 1$$

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

a = `00 00000000 00000000 00000000 00000000 00000001`

b = `00 00000000 00000000 00000000 00000000 00000001`

The base point G in compressed form is:

G = `0302 FE13C053 7BBC11AC AA07D793 DE4E6D5E 5C94EEE8`

and in uncompressed form is:

G = `0402FE 13C0537B BC11ACAA 07D793DE 4E6D5E5C 94EEE802 89070FB0 5D38FF58 321F2E80 0536D538 CCDAA3D9`

Finally the order n of G and the cofactor are:

n = `04 00000000 00000000 00020108 A2E0CC0D 99F8A5EF`

h = `02`

3.2.2 Recommended Parameters sect163r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_{2^m}$ `sect163r1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 163$ and the representation of $\mathbb{F}_{2^{163}}$ is defined by:

$$f(x) = x^{163} + x^7 + x^6 + x^3 + 1$$

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

a = `07 B6882CAA EFA84F95 54FF8428 BD88E246 D2782AE2`

b = `07 13612DCD DCB40AAB 946BDA29 CA91F73A F958AFD9`

E was chosen verifiably at random from the seed:

S = 24B7B137 C8A14D69 6E676875 6151756F D0DA2E5C

However for historical reasons the method used to generate E from S differs slightly from the method described in ANSI X9.62 [ANS98]. Specifically the coefficient b produced from S is the reverse of the coefficient that would have been produced by the method described in ANSI X9.62.

The base point G in compressed form is:

G = 0303 69979697 AB438977 89566789 567F787A 7876A654

and in uncompressed form is:

G = 040369 979697AB 43897789 56678956 7F787A78 76A65400 435EDB42 EFAFB298 9D51FEFC E3C80988 F41FF883

Finally the order n of G and the cofactor are:

n = 03 FFFFFFFF FFFFFFFF FFFF48AA B689C29C A710279B

h = 02

3.2.3 Recommended Parameters sect163r2

The verifiably random elliptic curve domain parameters over $\mathbb{F}_{2^m}$ `sect163r2` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 163$ and the representation of $\mathbb{F}_{2^{163}}$ is defined by:

$$f(x) = x^{163} + x^7 + x^6 + x^3 + 1$$

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

a = 00 00000000 00000000 00000000 00000000 00000001

b = 02 0A601907 B8C953CA 1481EB10 512F7874 4A3205FD

E was chosen verifiably at random from the seed:

S = 85E25BFE 5C86226C DB12016F 7553F9D0 E693A268

E was selected from S as specified in ANSI X9.62 [ANS98] in normal basis representation and converted into polynomial basis representation.

The base point G in compressed form is:

G = 0303 F0EBA162 86A2D57E A0991168 D4994637 E8343E36

and in uncompressed form is:

G = 0403F0 EBA16286 A2D57EA0 991168D4 994637E8 343E3600 D51FBC6C 71A0094F A2CDD545 B11C5C0C 797324F1

Finally the order n of G and the cofactor are:

n = 04 00000000 00000000 000292FE 77E70C12 A4234C33

h = 02

3.3 Recommended 233-bit Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

This section specifies the two recommended 233-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$ in this document: parameters `sect233k1` associated with a Koblitz curve, and verifiably random parameters `sect233r1`.

Section 3.3.1 specifies the elliptic curve domain parameters `sect233k1`, and Section 3.3.2 specifies the elliptic curve domain parameters `sect233r1`.

3.3.1 Recommended Parameters sect233k1

The elliptic curve domain parameters over $\mathbb{F}_{2^m}$ associated with a Koblitz curve `sect233k1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 233$ and the representation of $\mathbb{F}_{2^{233}}$ is defined by:

$$f(x) = x^{233} + x^{74} + 1$$

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

a = 0000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 0000 00000000 00000000 00000000 00000000 00000000 00000000 00000001

The base point G in compressed form is:

G = 020172 32BA853A 7E731AF1 29F22FF4 149563A4 19C26BF5 0A4C9D6E EFAD6126

and in uncompressed form is:

G = 04 017232BA 853A7E73 1AF129F2 2FF41495 63A419C2 6BF50A4C 9D6EEFAD 612601DB 537DECE8 19B7F70F 555A67C4 27A8CD9B F18AEB9B 56E0C11056FAE6A3

Finally the order n of G and the cofactor are:

n = 80 00000000 00000000 00000000 00069D5B B915BCD4 6EFB1AD5 F173ABDF

h = 04

3.3.2 Recommended Parameters sect233r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_{2^m}$ `sect233r1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 233$ and the representation of $\mathbb{F}_{2^{233}}$ is defined by:

$$f(x) = x^{233} + x^{74} + 1$$

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

a = `0000 00000000 00000000 00000000 00000000 00000000 00000000 00000001`

b = `0066 647EDE6C 332C7F8C 0923BB58 213B333B 20E9CE42 81FE115F 7D8F90AD`

E was chosen verifiably at random from the seed:

S = `74D59FF0 7F6B413D 0EA14B34 4B20A2DB 049B50C3`

E was selected from S as specified in ANSI X9.62 [ANS98] in normal basis representation and converted into polynomial basis representation.

The base point G in compressed form is:

G = `0300FA C9DFCBAC 8313BB21 39F1BB75 5FEF65BC 391F8B36 F8F8EB73 71FD558B`

and in uncompressed form is:

G = `04 00FAC9DF CBAC8313 BB2139F1 BB755FEF 65BC391F 8B36F8F8 EB7371FD 558B0100 6A08A419 03350678 E58528BE BF8A0BEF F867A7CA 36716F7E 01F81052`

Finally the order n of G and the cofactor are:

n = `0100 00000000 00000000 00000000 0013E974 E72F8A69 22031D26 03CFE0D7`

h = `02`

3.4 Recommended 239-bit Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

This section specifies the recommended 239-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$ in this document: parameters `sect239k1` associated with a Koblitz curve.

Section 3.4.1 specifies the elliptic curve domain parameters `sect239k1`.

3.4.1 Recommended Parameters sect239k1

The elliptic curve domain parameters over $\mathbb{F}_{2^m}$ associated with a Koblitz curve `sect239k1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 239$ and the representation of $\mathbb{F}_{2^{239}}$ is defined by:

$$f(x) = x^{239} + x^{158} + 1$$

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

a = 0000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 0000 00000000 00000000 00000000 00000000 00000000 00000000 00000001

The base point G in compressed form is:

G = 0329A0 B6A887A9 83E97309 88A68727 A8B2D126 C44CC2CC 7B2A6555 193035DC

and in uncompressed form is:

G = 04 29A0B6A8 87A983E9 730988A6 8727A8B2 D126C44C C2CC7B2A 65551930 35DC7631 0804F12E 549BDB01 1C103089 E73510AC B275FC31 2A5DC6B7 6553F0CA

Finally the order n of G and the cofactor are:

n = 2000 00000000 00000000 00000000 005A79FE C67CB6E9 1F1C1DA8 00E478A5

h = 04

3.5 Recommended 283-bit Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

This section specifies the two recommended 283-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$ in this document: parameters `sect283k1` associated with a Koblitz curve, and verifiably random parameters `sect283r1`.

Section 3.5.1 specifies the elliptic curve domain parameters `sect283k1`, and Section 3.5.2 specifies the elliptic curve domain parameters `sect283r1`.

3.5.1 Recommended Parameters sect283k1

The elliptic curve domain parameters over $\mathbb{F}_{2^m}$ associated with a Koblitz curve `sect283k1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 283$ and the representation of $\mathbb{F}_{2^{283}}$ is defined by:

$$f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$$

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

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001

The base point G in compressed form is:

G = 02 0503213F 78CA4488 3F1A3B81 62F188E5 53CD265F 23C1567A 16876913 B0C2AC24 58492836

and in uncompressed form is:

G = 04 0503213F 78CA4488 3F1A3B81 62F188E5 53CD265F 23C1567A 16876913 B0C2AC24 58492836 01CCDA38 0F1C9E31 8D90F95D 07E5426F E87E45C0 E8184698 E4596236 4E341161 77DD2259

Finally the order n of G and the cofactor are:

n = 01FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFE9AE 2ED07577 265DFF7F 94451E06 1E163C61

h = 04

3.5.2 Recommended Parameters sect283r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_{2^m}$ `sect283r1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 283$ and the representation of $\mathbb{F}_{2^{283}}$ is defined by:

$$f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$$

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

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001

b = 027B680A C8B8596D A5A4AF8A 19A0303F CA97FD76 45309FA2 A581485A F6263E31 3B79A2F5

E was chosen verifiably at random from the seed:

S = 77E2B073 70EB0F83 2A6DD5B6 2DFC88CD 06BB84BE

E was selected from S as specified in ANSI X9.62 [ANS98] in normal basis representation and converted into polynomial basis representation.

The base point G in compressed form is:

G = 03 05F93925 8DB7DD90 E1934F8C 70B0DFEC 2EED25B8 557EAC9C 80E2E198 F8CDBECD 86B12053

and in uncompressed form is:

G = 04 05F93925 8DB7DD90 E1934F8C 70B0DFEC 2EED25B8 557EAC9C 80E2E198 F8CDBECD 86B12053 03676854 FE24141C B98FE6D4 B20D02B4 516FF702 350EDDB0 826779C8 13F0DF45 BE8112F4

Finally the order n of G and the cofactor are:

n = 03FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFEF90 399660FC 938A9016
5B042A7C EFADB307

h = 02

3.6 Recommended 409-bit Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

This section specifies the two recommended 409-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$ in this document: parameters `sect409k1` associated with a Koblitz curve, and verifiably random parameters `sect409r1`.

Section 3.6.1 specifies the elliptic curve domain parameters `sect409k1`, and Section 3.6.2 specifies the elliptic curve domain parameters `sect409r1`.

3.6.1 Recommended Parameters sect409k1

The elliptic curve domain parameters over $\mathbb{F}_{2^m}$ associated with a Koblitz curve `sect409k1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 409$ and the representation of $\mathbb{F}_{2^{409}}$ is defined by:

$$f(x) = x^{409} + x^{87} + 1$$

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

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000001

The base point G in compressed form is:

G = 03 0060F05F 658F49C1 AD3AB189 0F718421 0EFD0987 E307C84C
27ACCFB8 F9F67CC2 C460189E B5AAAA62 EE222EB1 B35540CF E9023746

and in uncompressed form is:

G = 04 0060F05F 658F49C1 AD3AB189 0F718421 0EFD0987 E307C84C
27ACCFB8 F9F67CC2 C460189E B5AAAA62 EE222EB1 B35540CF E9023746
01E36905 0B7C4E42 ACBA1DAC BF04299C 3460782F 918EA427 E6325165
E9EA10E3 DA5F6C42 E9C55215 AA9CA27A 5863EC48 D8E0286B

Finally the order n of G and the cofactor are:

n = 7FFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFE5F
83B2D4EA 20400EC4 557D5ED3 E3E7CA5B 4B5C83B8 E01E5FCF

h = 04

3.6.2 Recommended Parameters sect409r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_{2^m}$ `sect409r1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 409$ and the representation of $\mathbb{F}_{2^{409}}$ is defined by:

$$f(x) = x^{409} + x^{87} + 1$$

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

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000001

b = 0021A5C2 C8EE9FEB 5C4B9A75 3B7B476B 7FD6422E F1F3DD67 4761FA99
D6AC27C8 A9A197B2 72822F6C D57A55AA 4F50AE31 7B13545F

E was chosen verifiably at random from the seed:

S = 4099B5A4 57F9D69F 79213D09 4C4BCD4D 4262210B

E was selected from S as specified in ANSI X9.62 [ANS98] in normal basis representation and converted into polynomial basis representation.

The base point G in compressed form is:

G = 03 015D4860 D088DDB3 496B0C60 64756260 441CDE4A F1771D4D
B01FFE5B 34E59703 DC255A86 8A118051 5603AEAB 60794E54 BB7996A7

and in uncompressed form is:

G = 04 015D4860 D088DDB3 496B0C60 64756260 441CDE4A F1771D4D
B01FFE5B 34E59703 DC255A86 8A118051 5603AEAB 60794E54 BB7996A7
0061B1CF AB6BE5F3 2BBFA783 24ED106A 7636B9C5 A7BD198D 0158AA4F
5488D08F 38514F1F DF4B4F40 D2181B36 81C364BA 0273C706

Finally the order n of G and the cofactor are:

n = 01000000 00000000 00000000 00000000 00000000 00000000 000001E2
AAD6A612 F33307BE 5FA47C3C 9E052F83 8164CD37 D9A21173

h = 02

3.7 Recommended 571-bit Elliptic Curve Domain Parameters over $\mathbb{F}_{2^m}$

This section specifies the two recommended 571-bit elliptic curve domain parameters over $\mathbb{F}_{2^m}$ in this document: parameters `sect571k1` associated with a Koblitz curve, and verifiably random parameters `sect571r1`.

Section 3.7.1 specifies the elliptic curve domain parameters `sect571k1`, and Section 3.7.2 specifies the elliptic curve domain parameters `sect571r1`.

3.7.1 Recommended Parameters sect571k1

The elliptic curve domain parameters over $\mathbb{F}_{2^m}$ associated with a Koblitz curve `sect571k1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 571$ and the representation of $\mathbb{F}_{2^{571}}$ is defined by:

$$f(x) = x^{571} + x^{10} + x^5 + x^2 + 1$$

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

```
a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000001
```

The base point G in compressed form is:

```
G =       02 026EB7A8 59923FBC 82189631 F8103FE4 AC9CA297 0012D5D4
    60248048 01841CA4 43709584 93B205E6 47DA304D B4CEB08C BBD1BA39
    494776FB 988B4717 4DCA88C7 E2945283 A01C8972
```

and in uncompressed form is:

```
G =       04 026EB7A8 59923FBC 82189631 F8103FE4 AC9CA297 0012D5D4
    60248048 01841CA4 43709584 93B205E6 47DA304D B4CEB08C BBD1BA39
    494776FB 988B4717 4DCA88C7 E2945283 A01C8972 0349DC80 7F4FBF37
    4F4AEADE 3BCA9531 4DD58CEC 9F307A54 FFC61EFC 006D8A2C 9D4979C0
    AC44AEA7 4FBEBBB9 F772AEDC B620B01A 7BA7AF1B 320430C8 591984F6
    01CD4C14 3EF1C7A3
```

Finally the order n of G and the cofactor are:

n = 02000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 131850E1 F19A63E4 B391A8DB 917F4138 B630D84B
E5D63938 1E91DEB4 5CFE778F 637C1001

h = 04

3.7.2 Recommended Parameters sect571r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_{2^m}$ `sect571r1` are specified by the septuple $T = (m, f(x), a, b, G, n, h)$ where $m = 571$ and the representation of $\mathbb{F}_{2^{571}}$ is defined by:

$$f(x) = x^{571} + x^{10} + x^5 + x^2 + 1$$

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

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000001

b = 02F40E7E 2221F295 DE297117 B7F3D62F 5C6A97FF CB8CEFF1 CD6BA8CE
4A9A18AD 84FFABBD 8EFA5933 2BE7AD67 56A66E29 4AFD185A 78FF12AA
520E4DE7 39BACA0C 7FFEFF7F 2955727A

E was chosen verifiably at random from the seed:

S = 2AA058F7 3A0E33AB 486B0F61 0410C53A 7F132310

E was selected from S as specified in ANSI X9.62 [ANS98] in normal basis representation and converted into polynomial basis representation.

The base point G in compressed form is:

G = 03 0303001D 34B85629 6C16C0D4 0D3CD775 0A93D1D2 955FA80A
A5F40FC8 DB7B2ABD BDE53950 F4C0D293 CDD711A3 5B67FB14 99AE6003
8614F139 4ABFA3B4 C850D927 E1E7769C 8EEC2D19

and in uncompressed form is:

G = 04 0303001D 34B85629 6C16C0D4 0D3CD775 0A93D1D2 955FA80A
A5F40FC8 DB7B2ABD BDE53950 F4C0D293 CDD711A3 5B67FB14 99AE6003
8614F139 4ABFA3B4 C850D927 E1E7769C 8EEC2D19 037BF273 42DA639B
6DCCFFFE B73D69D7 8C6C27A6 009CBBCA 1980F853 3921E8A6 84423E43
BAB08A57 6291AF8F 461BB2A8 B3531D2F 0485C19B 16E2F151 6E23DD3C
1A4827AF 1B8AC15B

Finally the order n of G and the cofactor are:

n = 03FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF E661CE18 FF559873 08059B18 6823851E C7DD9CA1
161DE93D 5174D66E 8382E9BB 2FE84E47

h = 02

A ASN.1 Syntax

This section discusses the representation of elliptic curve domain parameters using ASN.1 syntax and specifies ASN.1 object identifiers for the elliptic curve domain parameters recommended in this document.

A.1 Syntax for Elliptic Curve Domain Parameters

There are a number of ways of representing elliptic curve domain parameters using ASN.1 syntax. The following syntax is recommended in SEC 1 [SEC00] for use in X.509 certificates and elsewhere (following [?]).

```
Parameters{CURVES:IOSet} ::= CHOICE {
     ecParameters ECParameters,
     namedCurve CURVES.&id({IOSet}),
     implicitCA NULL
}
```

where

- ecParameters of type ECParameters indicates that the full elliptic curve domain parameters are given,
- namedCurve of type CURVES indicates that a named curve from the set delimited by CurveNames is to be used, and
- implicitCA of type NULL indicates that the curve is known implicitly, that is, the actual curve is known to both parties by other means.

The following syntax is then used to describe explicit representations of elliptic curve domain parameters, if need be.

```
ECParameters ::= SEQUENCE {
     version INTEGER { ecpVer1(1) } (ecpVer1),
     fieldID FieldID {{FieldTypes}},
     curve Curve,
     base ECPoint,
     order INTEGER,
     cofactor INTEGER OPTIONAL,
     ...
}
```

See SEC 1 [SEC00] for more details on the explicit representation of elliptic curve domain parameters.

A.2 Object Identifiers for Recommended Parameters

This section specifies object identifiers for the elliptic curve domain parameters recommended in this document. These object identifiers may be used, for example, to represent parameters using the `namedCurve` syntax described in the previous section.

Parameters that have not previously been assigned object identifiers appear in the tree whose root is designated by the object identifier `certicom-arc`. It has the following value.

```
certicom-arc OBJECT IDENTIFIER ::= {
     iso(1) identified-organization(3) certicom(132)
}
```

Parameters that are given as examples in ANSI X9.62 [ANS98] appear in the tree whose root is designated by the object identifier `ansi-X9-62`. It has the following value.

```
ansi-X9-62 OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) 10045
}
```

The values of the object identifiers of parameters given in ANSI X9.62 are duplicated here for convenience.

To reduce the encoded lengths, the parameters under `certicom-arc` appear just below the main node. The object identifier `ellipticCurve` represents the root of the tree containing all such parameters in this document and has the following value.

```
ellipticCurve OBJECT IDENTIFIER ::= { certicom-arc curve(0) }
```

The actual parameters appear immediately below this; their object identifiers may be found in the following sections. Section A.2.1 specifies object identifiers for the parameters over $\mathbb{F}_p$, and Section A.2.2 specifies object identifiers for the parameters over $\mathbb{F}_{2^m}$.

A.2.1 OIDs for Recommended Parameters over $\mathbb{F}_p$

The object identifiers for the recommended parameters over $\mathbb{F}_p$ have the following values. The names of the identifiers agree with the nicknames given to the parameters in this document. In ANSI X9.62 [ANS98], the curve `secp192r1` is designated `prime192v1`, and the curve `secp256r1` is designated `prime256v1`.

```
--
-- Curves over prime-order fields:
--
secp192k1 OBJECT IDENTIFIER ::= { ellipticCurve 31 }
secp192r1 OBJECT IDENTIFIER ::= { ansi-X9-62 curves(3) prime(1) 1 }

secp224k1 OBJECT IDENTIFIER ::= { ellipticCurve 32 }
secp224r1 OBJECT IDENTIFIER ::= { ellipticCurve 33 }
```

```
secp256k1 OBJECT IDENTIFIER ::= { ellipticCurve 10 }
secp256r1 OBJECT IDENTIFIER ::= { ansi-X9-62 curves(3) prime(1) 7 }

secp384r1 OBJECT IDENTIFIER ::= { ellipticCurve 34 }

secp521r1 OBJECT IDENTIFIER ::= { ellipticCurve 35 }
```

A.2.2 OIDs for Recommended Parameters over $\mathbb{F}_{2^m}$

The object identifiers for the recommended parameters over $\mathbb{F}_{2^m}$ have the following values. The names of the identifiers agree with the nicknames given to the parameters in this document.

```
--
-- Curves over characteristic 2 fields.
--
sect163k1 OBJECT IDENTIFIER ::= { ellipticCurve 1 }
sect163r1 OBJECT IDENTIFIER ::= { ellipticCurve 2 }
sect163r2 OBJECT IDENTIFIER ::= { ellipticCurve 15 }

sect233k1 OBJECT IDENTIFIER ::= { ellipticCurve 26 }
sect233r1 OBJECT IDENTIFIER ::= { ellipticCurve 27 }

sect239k1 OBJECT IDENTIFIER ::= { ellipticCurve 3 }

sect283k1 OBJECT IDENTIFIER ::= { ellipticCurve 16 }
sect283r1 OBJECT IDENTIFIER ::= { ellipticCurve 17 }

sect409k1 OBJECT IDENTIFIER ::= { ellipticCurve 36 }
sect409r1 OBJECT IDENTIFIER ::= { ellipticCurve 37 }

sect571k1 OBJECT IDENTIFIER ::= { ellipticCurve 38 }
sect571r1 OBJECT IDENTIFIER ::= { ellipticCurve 39 }
```

A.2.3 The Information Object Set `SECGCurveNames`

The following information object set `SECGCurveNames` of class `CURVES` may be used to delineate the use of a curve recommended in this document. When it is used to govern the component `namedCurve` of `Parameters` (defined in section A.1), the value of `namedCurve` must be one of the values of the set.

```
SECGCurveNames CURVES ::= {
    -- Curves over prime-order fields:
    { ID secp192k1 } |
```

```
    { ID secp192r1 } |
    { ID secp224k1 } |
    { ID secp224r1 } |
    { ID secp256k1 } |
    { ID secp256r1 } |
    { ID secp384r1 } |
    { ID secp521r1 } |
    -- Curves over characteristic 2 fields:
    { ID sect163k1 } |
    { ID sect163r1 } |
    { ID sect163r2 } |
    { ID sect233k1 } |
    { ID sect233r1 } |
    { ID sect239k1 } |
    { ID sect283k1 } |
    { ID sect283r1 } |
    { ID sect409k1 } |
    { ID sect409r1 } |
    { ID sect571k1 } |
    { ID sect571r1 } ,
    ...
    }
```

The type CURVES used above is defined below.

```
CURVES ::= CLASS {
    &curve-id OBJECT IDENTIFIER UNIQUE
} WITH SYNTAX { ID &curve-id }
```

B References

[ANS98] *ANS X9.62-1998: Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA)*, 1998, Revision scheduled for 2005. `webstore.ansi.org/ansidocstore/default.asp`.

[ANS01] *ANS X9.63-2001: Public-key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography*, 2001, `webstore.ansi.org/ansidocstore/default.asp`.

[Fin99] Financial Services Technology Consortium, *Financial services markup language*, August 1999, Working Draft.

[IEE99] *IEEE P1363: Standard for public-key cryptography*, July 11 1999, Working Draft.

[Kob92] N. Koblitz, *CM-curves with good cryptographic properties*, Advances in Cryptology — CRYPTO '91 (J. Feigenbaum, ed.), LNCS 576, IACR, Springer, 1992, pp. 279–287.

[NIS99] NIST, *Recommended elliptic curves for federal government use*, July 1999, `csrc.nist.gov/encryption`.

[SEC00] *SEC 1: Elliptic curve cryptography*, September 2000, Version 1.0. Document proposed for revision. `www.secg.org`.

[WAP99] *WAP WTLS: Wireless application protocol wireless transport layer security specification*, February 1999.