Specification of Curve Selection and Supported Curve Parameters in MSR ECCLib

Joppe W. Bos[1], Craig Costello[2], Patrick Longa[2], and Michael Naehrig[2]

[1] NXP Semiconductors
[2] Microsoft Research

This document explains the details of the curve generation algorithms and provides the parameters for the NUMS (Nothing Up My Sleeve) curves, which are supported in the MSR Elliptic Curve Cryptography Library (a.k.a. MSR ECCLib). For more details on curve selection and curve properties, see [1] and [2].

1 Notation

The following notation is used in this document.

s	Denotes the target security level in bits, here $s \in \{128, 192, 256\}$.
p	Denotes a prime number.
c	A positive integer used in the representation of the prime p as $p = 2^{2s} - c$.
$\mathbb{F}_p$	The finite field with p elements.
b	An element in the finite field $\mathbb{F}_p$, $b \neq \pm 2$.
E_b	The elliptic curve $E_b/\mathbb{F}_p : y^2 = x^3 - 3x + b$ in short Weierstrass form, defined over $\mathbb{F}_p$ by the parameter $b \neq \pm 2$.
r_b	The prime order $r_b = \#E_b(\mathbb{F}_p)$ of the group of $\mathbb{F}_p$-rational points on E_b.
t_b	The trace of Frobenius $t_b = p + 1 - r_b$ of E_b.
r'_b	The prime order $r'_b = \#E'_b(\mathbb{F}_p) = p + 1 + t_b$ of the group of $\mathbb{F}_p$-rational points on the quadratic twist E'_b.
d	An element in the finite field $\mathbb{F}_p$, $d \notin \{1, 0\}$.
$\mathcal{E}_d$	The elliptic curve $\mathcal{E}_d/\mathbb{F}_p : x^2 + y^2 = 1 + dx^2y^2$ in Edwards form, defined over $\mathbb{F}_p$ by the parameter $d \notin \{0, 1\}$.
r_d	The prime subgroup order such that $4r_d = \#\mathcal{E}_d(\mathbb{F}_p)$ is the order of the group of $\mathbb{F}_p$-rational points on $\mathcal{E}_d$.
t_d	The trace of Frobenius $t_d = p + 1 - 4r_d$ of $\mathcal{E}_d$.
r'_d	The prime subgroup order such that $4r'_d = \#\mathcal{E}'_d(\mathbb{F}_p) = p + 1 + t_d$ is the order of the group of $\mathbb{F}_p$-rational points on the quadratic twist $\mathcal{E}'_d$.
P	A generator point defined over $\mathbb{F}_p$ either of prime order r_b on the Weierstrass curve E_b, or of prime order r_d on the Edwards curve $\mathcal{E}_d$.
$X(P)$	The x-coordinate of the elliptic curve point P.
$Y(P)$	The y-coordinate of the elliptic curve point P.

2 Selection of the prime p.

For each given security level $s \in \{128, 192, 256\}$, a prime p is selected as a pseudo-Mersenne prime of the form $p = 2^{2s} - c$ for a positive integer c. Each prime is determined by the smallest positive integer c such that $p = 2^{2s} - c$ is prime. For the three values of s above, the resulting primes satisfy $p \equiv 3 \pmod 4$.

3 Selection of Weierstrass curves E_b

Given a security level $s \in \{128, 192, 256\}$ and a corresponding prime $p = 2^{2s} - c$ selected according to Section 2, the elliptic curve E_b in short Weierstrass form is determined by the element $b \in \mathbb{F}_p$, $b \neq \pm 2$ with smallest absolute value (when represented as an integer in the interval $[-(p-1)/2, (p-1)/2]$) such that both group orders r_b and r'_b are prime and $r_b < r'_b$.

4 Selection of Edwards curves $\mathcal{E}_d$

Given a security level $s \in \{128, 192, 256\}$ and a corresponding prime $p = 2^{2s} - c$ selected according to Section 2, the elliptic curve $\mathcal{E}_d$ in Edwards form is determined by the element $d \in \mathbb{F}_p$, $d \notin \{0, 1\}$ with smallest absolute value (when represented as an integer in the interval $[-(p-1)/2, (p-1)/2]$) such that both subgroup orders r_d and r'_d are prime.

5 Curve parameters for short Weierstrass curves.

The following curves in short Weierstrass form $y^2 = x^3 - 3x + b$ over $\mathbb{F}_p$ were generated according to Section 3.

Curve ID: numsp256d1, prime $p = 2^{256} - 189$

p :	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF43
b :	0x25581
r_b :	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE43C8275EA265C6020AB20294751A825
$X(P)$:	0xBC9ED6B65AAADB61297A95A04F42CB0983579B0903D4C73ABC52EE1EB21AACB1
$Y(P)$:	0xD08FC0F13399B6A673448BF77E04E035C955C3D115310FBB80B5B9CB2184DE9F
cofactor :	0x01

Curve ID: numsp384d1, prime $p = 2^{384} - 317$

p :	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFEC3
b :	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFF77BB
r_b :	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD61EAF1EEB5D6881 BEDA9D3D4C37E27A604D81F67B0E61B9
$X(P)$:	0x757956F0B16F181C4880CA224105F1A60225C1CDFB81F9F4F3BD291B2A6CC742 522EED100F61C47BEB9CBA042098152A
$Y(P)$:	0xACDEE368E19B8E38D7E33D300584CF7EB0046977F87F739CB920837D121A837E BCD6B4DBBFF4AD265C74B8EC66180716
cofactor :	0x01

Curve ID: numsp512d1, prime $p = 2^{512} - 569$

p :	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDC7
b :	0x1D99B
r_b :	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF 5B3CA4FB94E7831B4FC258ED97D0BDC63B568B36607CD243CE153F390433555D
$X(P)$:	0x3AC03447141D0A93DA2B7002A03D3B5298CAD83BB501F6854506E0C25306D9F9 5021A151076B359E93794286255615831D5D60137D6F5DE2DC8287958CABAE57
$Y(P)$:	0x943A54CA29AD56B3CE0EEEDC63EBB1004B97DBDEABBCBB8C8F4B260C7BD14F14 A28415DA8B0EEDE9C121A840B25A5602CF2B5C1E4CFD0FE923A08760383527A6
cofactor :	0x01

6 Curve parameters for Edwards curves.

The following curves in Edwards form $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbb{F}_p$ were generated according to Section 4.

Curve ID: numsp256t1, prime $p = 2^{256} - 189$

p : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF43

d : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC355

r_d : 0x40000000000000000000000000000000041955AA52F59439B1A47B190EEDD4AF5

$X(P)$: 0x8A7514FB6AEA237DCD1E3D5F69209BD60C398A0EE3083586A0DEC0902EED13DA

$Y(P)$: 0x44D53E9FD9D925C7CE9665D9A64B8010715F61D810856ED32FA616E7798A89E6

cofactor : 0x04

Curve ID: numsp384t1, prime $p = 2^{384} - 317$

p : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFEC3

d : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFD19F

r_d : 0x3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE2471A1CB46BE1CF
61E4555AAB35C87920B9DCC4E6A3897D

$X(P)$: 0x61B111FB45A9266CC0B6A2129AE55DB5B30BF446E5BE4C005763FFA8F3316340
6FF292B16545941350D540E46C206BDE

$Y(P)$: 0x82983E67B9A6EEB08738B1A423B10DD716AD8274F1425F56830F98F7F645964B
0072B0F946EC48DC9D8D03E1F0729392

cofactor : 0x04

Curve ID: numsp512t1, prime $p = 2^{512} - 569$

p : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDC7

d : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFECBEF

r_d : 0x3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
B4F0636D2FCF91BA9E3FD8C970B686F52A4605786DEFECFF67468CF51BEED46D

$X(P)$: 0xDF8E316D128DB69C7A18CB7888D3C5332FD1E79F4DC4A38227A17EBE273B8147
4621C14EEE46730F78BDC992568904AD0FE525427CC4F015C5B9AB2999EC57FE

$Y(P)$: 0x6D09BFF39D49CA7198B0F577A82A256EE476F726D8259D22A92B6B95909E8341
20CA53F2E9963562601A06862AECC1FD0266D38A9BF1D01F326DDEC0C1E2F5E1

cofactor : 0x04

References

1. Joppe W. Bos, Craig Costello, Patrick Longa, and Michael Naehrig. Selecting elliptic curves for cryptography: An efficiency and security analysis. *J. Cryptographic Engineering*, 2015. http://dx.doi.org/10.1007/s13389-015-0097-y.
2. Craig Costello, Patrick Longa, and Michael Naehrig. A brief discussion on selecting new elliptic curves. Technical Report MSR-TR-2015-46, June 2015.