Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 7, 2016

K. Kasamatsu
A. Kato
NTT Software Corporation
M. Scott
CertiVox
T. Kobayashi
Y. Kawahara
NTT
July 6, 2015

Barreto-Naehrig Curves
draft-kasamatsu-bncurves-01

Abstract

Elliptic curves with pairings are useful tools for constructing cryptographic primitives. In this memo, we specify domain parameters of Barreto-Naehrig curves (BN-curves) [8]. The BN-curve is an elliptic curve suitable for pairings and allows us to achieve high security and efficiency of cryptographic schemes. This memo specifies domain parameters of four 254-bit BN-curves [1] [2] [5] which allow us to obtain efficient implementations.

Table of Contents

1. Introduction

Elliptic curves with a special map called a pairing or bilinear map allow cryptographic primitives to achieve functions or efficiency which cannot be realized by conventional mathematical tools. There are identity-based encryption (IBE), attribute-based encryption (ABE), ZSS signature, broadcast encryption (BE) as examples of such primitives. IBE realizes powerful management of public keys by allowing us to use a trusted identifier as a public key. ABE

provides a rich decryption condition based on boolean functions and attributes corresponding to a secret key or a ciphertext. The ZSS signature gives a shorter size of signature than that of ECDSA. BE provides an efficient encryption procedure in a broadcast setting.

Some of these cryptographic schemes based on elliptic curves with pairings were proposed in the IETF (e.g. [9], [10], and [11]) and used in some protocols (e.g. [12], [13], [14], [15], and [16]). These cryptographic primitives will be used actively more in the IETF due to their functions or efficiency.

We need to choose an appropriate type of elliptic curve and parameters for the pairing-based cryptographic schemes, because the choice has great impact on security and efficiency of these schemes. However, an RFC on elliptic curves with pairings has not yet been provided in the IETF.

In this memo, we specify domain parameters of Barreto-Naehrig curve (BN-curve) [8]. The BN-curve allows us to achieve high security and efficiency with pairings due to an optimum embedding degree for 128-bit security. This memo specifies domain parameters of four 254-bit BN-curves ([1] and [2]) because of these efficiencies ([5]). These BN-curves are known as efficient curves in academia and particularly provide efficient pairing computation which is generally slowest operation in pairing-based cryptography. There are optimized source codes of ([1] and [2]) as open source software ([20] , [21], and [23]), respectively. This memo describes domain parameters of 224, 256, 384, and 512-bit curves which are compliant with ISO document [3] and organizes differences between types of elliptic curves which are compliant with ISO document [3] in Appendix A.

2. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this memo are to be interpreted as described in [4].

3. Preliminaries

In this section, we introduce the definition of elliptic curve and bilinear map, notation used in this memo.

3.1. Elliptic Curve

Throughout this memo, let $p > 3$ be a prime, $q = p^n$, and n be a natural number. Also, let F_q be a finite field. The curve defined by the following equation E is called an elliptic curve.

```
E : y^2 = x^3 + A * x + B such that A, B are in F_q,
          4 * A^3 + 27 * B^2 != 0 mod F_q
```

Solutions (x, y) for an elliptic curve E, as well as the point at infinity, are called F_q-rational points. The additive group is constructed by a well-defined operation in the set of F_q-rational points. Typically, the cyclic additive group with prime order r and the base point G in its group is used for the cryptographic applications. Furthermore, we define terminology used in this memo as follows.

O_E: the point at infinity over elliptic curve E.

#E(F_q): number of points on an elliptic curve E over F_q.

cofactor h: h = #E(F_p)/r.

embedding degree k: minimum integer k such that r is a divisor of q^k - 1

3.2. Bilinear Map

Let G_1 be an additive group of prime order r and let G_2 and G_T be additive and multiplicative groups, respectively, of the same order. Let P, Q be generators of G_1, G_2 respectively. We say that (G_1, G_2, G_T) are asymmetric bilinear map groups if there exists a bilinear map e: (G_1, G_2) -> G_T satisfying the following properties:

1. Bilinearity: for any S in G_1, for any T in G_2, for any a, b in Z_r, we have the relation e([a]S, [b]T) = e(S, T)^{a * b}.

2. Non-degeneracy: for any T in G_2, e(S, T) = 1 if and only if S = O_E. Similarly, for any S in G_1, e(S, T) = 1 if and only if T = O_E.

3. Computability: for any S in G_1, for any T in G_2, the bilinear map is efficiently computable.

For BN-curves, G_1 is a r-order cyclic subgroup of E(F_p) and G_2 is a subgroup of E(F_{p^k}), where k is the embedding degree of the curve. The group G_T is the set of r-th roots of unity in the finite field F_{p^k}.

4. Domain Parameter Specification

In this section, this memo specifies the domain parameters for four 254-bit elliptic curves which allow us to efficiently compute the operation of a pairing at high levels of security.

4.1. Notation for Domain Parameters and Types of Sextic Twists

Here, we define notations for specifying domain parameters and explain types of pairing friendly curves.

The BN-curves E over F_p satisfy following equation.

$$y^2 = x^3 + B \text{ for } B \text{ in } F_p$$

The values p and r are computed from a suitable integer t.

p is a characteristic of a prime field F_p: $p = 36 * t^4 + 36 * t^3 + 24 * t^2 + 6 * t + 1$.

r is order of group E over F_p: $r = 36 * t^4 + 36 * t^3 + 18 * t^2 + 6 * t + 1$.

Also, the value b in the constant of the irreducible field polynomial $u^2 + b$ in F_{p^2}.

Domain parameters of the elliptic curve $E(F_p)$ and $E(F_{p^{12}})$ are needed for computation of the pairing. In the pairing over BN-curves, we usually use a sextic twist curve group $E'(F_{p^2})$ and a map I from the sextic twist $E'(F_{p^2})$ to $E(F_{p^{12}})$ instead of $E(F_{p^{12}})$. Hence, this memo follows the group and the map. For the details of the group and the map, refer to [8].

The sextic twist curves are classified in two types, which are called D-type and M-type respectively [22]. The D-type sextic twist curve is defined by equation E': $y'^2 = x'^3 + B/s$ when elliptic curve $E(F_p)$ is set to be $y^2 = x^3 + B$ and represent of $F_{p^{12}}$ is set to be $F_{p^2}[u]/(u^6 - s)$, where s is in $F_{p^2}^*$. Let z be a root of $u^6 - s$, where z is in $F_{p^{12}}$. The corresponding map I: $E'(F_{p^2}) \rightarrow E(F_{p^{12}})$ is $(x', y') \rightarrow (z^2 * x', z^3 * y')$. The M-type sextic twist curve is defined by equation E': $y^2 = x^3 + B * s$ when elliptic curve $E(F_p)$ is set to be $y^2 = x^3 + B$ and represent of $F_{p^{12}}$ is set to be $F_{p^2}[u]/(u^6 - s)$, where s is in $F_{p^2}^*$. The corresponding map I: $E'(F_{p^2}) \rightarrow E(F_{p^{12}})$ is $(x', y') \rightarrow (x' * s^{-1} * z^4, y' * s^{-1} * z^3)$, with $z^6 = s$.

For the pairing, the group G_1 is defined as the subgroup of order r in $E(F_p)$. Then, the group G_2 is defined as the subgroup of order r

in E'(F_{p^2}). The group G_T is subgroup of order r in the multiplicative group F_{p^12}^*. The output of pairing is an element on G_T. The order of F_{p^12}^* can be decomposed into (p^12 - 1) = (p^6 - 1) * (p^2 + 1) * (p^4 - p^2 + 1)/r. Let the cofactor h'' of r on F_{p^12} be h''_1 * h''_2, where h''_1 = (p^4 - p^2 + 1)/r and h''_2 = (p^6 - 1) * (p^2 + 1).

These domain parameters are described in the following way.

For elliptic curve E(F_p)

G1-Curve-ID is an identifier of the G_1 curve with which the curve can be referenced.

p_b is a prime specifying a base field F_p.

B is the coefficient of the equation y^2 = x^3 + B mod p defining E.

G = (x, y) is the base point, i.e., a point with x and y being its x- and y-coordinates in E, respectively.

r is the prime order of the group generated by G.

h is the cofactor of G in E(F_p)

For twisted curve E'(F_{p^2})

G2-Curve-ID is an identifier of the G_2 curve with which the curve can be referenced.

p_b is a prime specifying a base field.

e2 is the constant of an irreducible polynomial specifying extension field F_{p^2} = F_p[u]/(u^2 - e2).

B' is the coefficient of the equation y'^2 = x'^3 + B' mod F_p^2 defining E'.

G' = (x', y') is the base point, i.e., a point with x' and y' being its x'- and y'-coordinates in E', respectively.

r' is the prime order of the group generated by G'.

h' is the cofactor of r' in #E'(F_{p^2})

For F_{p^12}^*

GT-Field-ID is an identifier of the F_{p^12}^*.

p_b is a prime specifying base field.

r'' is the prime order of the group.

e2 is the constant of the irreducible polynomial of F_{p^2} = F_p [u]/(u^2 - e2).

e6 is the constant of the irreducible polynomial of F_{p^6} = F_{p^2}[v]/(v^3 - e6).

e12 is the constant of the irreducible polynomial of F_{p^12} = F_{p^6}[w]/(w^2 - e12).

h'' is the cofactor of r in F_{p^12}^* s.t. h'' = h''_1 * h''_2

h''_1 is the part of cofactor of r in F_{p^12}^* s.t. h''_1 = (p^4 - p^2 + 1)/r

h''_2 is the part of cofactor of r in F_{p^12}^* s.t. h''_2 = (p^6 - 1) * (p^2 + 1)

For the definition of the pairing parameter

Pairing-Param-ID is the set of the identifiers G1-Curve-ID, G2-Curve-ID and GT-Field-ID.

4.2. Efficient Domain Parameters for 254-Bit-Curves

This section specifies the domain parameters for four 254-bit elliptic curves. All twisted domain parameters specified in this section are D-type.

4.2.1. Domain Parameters by Beuchat et al.

The domain parameters by Beuchat et al. [1] generated by t = 3fc0100000000000.

The domain parameters described in this subsection are defined by elliptic curve E(F_p) : y^2 = x^3 + 5 and sextic twist E'(F_{p^2}) : x'^3 + 5/s = x'^3 - u, where F_{p^2} = F_p[u]/(u^2 + 5), F_{p^6} = F_{p^2}[v]/(v^3 - u), F_{p^12} = F_{p^6}[w]/(w^2 - v), s = - 5/u. We describe domain parameters of elliptic curves E and E'. The parameter p_b is 1 mod 8. For the details of these parameters, refer to [1].

G1-Curve-ID: Fp254BNa

p_b = 0x2370fb049d410fbe4e761a9886e502417d023f40180000017e80600000
000001

x = 1

y = 0xd45589b158faaf6ab0e4ad38d998e9982e7ff63964ee1460342a592677cc
cb0

r = 0x2370fb049d410fbe4e761a9886e502411dc1af70120000017e8060000000
0001

h = 1

G2-Curve-ID: Fp254n2BNa

p_b = 0x2370fb049d410fbe4e761a9886e502417d023f40180000017e80600000
000001

e2 = -5 in F_p

B' = -u

x' = 0x19b0bea4afe4c330da93cc3533da38a9f430b471c6f8a536e81962ed967
909b5 + (0xa1cf585585a61c6e9880b1f2a5c539f7d906fff238fa6341e1de1a2
e45c3f72) u

y' = 0x17abd366ebbd65333e49c711a80a0cf6d24adf1b9b3990eedcc91731384
d2627 + (0x0ee97d6de9902a27d00e952232a78700863bc9aa9be960C32f5bf9f
d0a32d345) u

r' = r

h' = 0x2370fb049d410fbe4e761a9886e50241dc42cf101e0000017e806000000
00001

GT-Field-ID: Fp254n12a

p_b = 0x2370fb049d410fbe4e761a9886e502417d023f40180000017e80600000
000001

r'' = r

e2 = -5 in F_p

e6 = u in F_{p^2}

e12 = v in F_{p^6}

```
h'' = 0x189b459262d16204423a54bb8427aba5530e63254675b78cca28b1f810
476f6b3c53ed0eec245d3ffa0db96f3d713f434a4870545018ff4ea2c361c594bb
b978ce81c80fd1d1cc16cdde274c80f3345359b79069f453e128c1502c0939bbc7
c5cd822ab539b98c5bd283a3377cf7638d91a123a167c510e55bbf53609af49c01
b9c0678c1c10f11cc862018f8fca977741390b5093031edcef806a7301b263b23c
97ea03430da6512a4d5f6df97e761baaf604e724be4f5aafd48fe75994131f2c78
5e364e09256e04dbd1c5eb89733e8ad5a1dacfbb082f399a0d0ea0ab73d6478a96
4221656337a971792a7a42902fcce7c32eb12ab7225b55bf4c7c56d697e0481cb6
23808f99ac23c352660bfd238ab5347121765223970ad69ad7343393718708bd0f
613e4596afede064f7eea9f73082070596e8c495b49fab1bed21ac7b33b5d084c7
ed91d1ae8c38a69d0fa48b8000011ee04800000000000

h''_1 = 0xade56cf7e1002629c65ca37294ca9149f129ccbb50212575b3d18098
dac4072302eae88c14b40564d9b21719304c9efd7c907850461e1ce3a37da6d40b
e2032e03c8c76238b30af10d6da963854a4aca504a90ae0000017e806000000000
01

h''_2 = 0x24396d2e7daaf102f72fc17484da5601e50a8e4fe4101271d84f0639
930313fae7dbbc4b6f64a48a9bbc8b65632eea8295222ece92adb1fdad8a57b84b
13025fd1c64ebe9b3daa6b9be21c2330e997025161babcc1d0eb55d93939c5fd02
e02f1c269f16c3785aef71f0ef1c256be2bf9de36925b42004c3d390638c802e46
f220bf63cc039d8ab7e73ad426b32f383084672ea9f0fe34d053a6184768d21c52
cfd50313acaeed74538e4cd07c1827e7e9a8f14eac8401482fefa2e06ec810f407
882b548ea549c760b3e2013b5a299a6cd7395bbd58ebd04400e5e193fcae081e0b
e4dae5650bb8707a73b116f9fa887c708000011ee04800000000000

Pairing-Param-ID: Beuchat = {
    G1-Curve-ID: Fp254BNa
    G2-Curve-ID: Fp254n2BNa
    GT-Field-ID: Fp254n12a
}
```

4.2.2. Domain Parameters by Nogami et al. / Aranha et al.

The domain parameters by Nogami et al. [2] generated by t = -0x4080000000000001. Aranha et al. presented an open source library of the pairing using this parameter [2].

The domain parameters described in this subsection are defined by elliptic curve E(F_p) : y^2 = x^3 + 2 and sextic twist E'(F_{p^2}) : x'^3 + 2/s = x'^3 + 1 - u, where F_{p^2} = F_p[u]/(u^2 + 1), F_{p^6} = F_{p^2}[v]/(v^3 - (1 + u)), F_{p^12} = F_{p^6}[w]/(w^2 - v), 1/s = 1/(1 + u). We describes domain parameters of elliptic curves E and E'. The parameter p_b is 3 mod 4. For the details of these parameters, refer to [2].

```
G1-Curve-ID: Fp254BNb
```

```
p_b = 0x2523648240000001ba344d80000000086121000000000013a700000000
000013

B = 2

x = 0x2523648240000001ba344d80000000086121000000000013a70000000000
0012

y = 1

r = 0x2523648240000001ba344d8000000007ff9f800000000010a10000000000
000d

h = 1

G2-Curve-ID: Fp254BNb

p_b = 0x2523648240000001ba344d80000000086121000000000013a700000000
000013

e2 = -1 in F_p

B' = 1 + (-1) u

x' = 0x061a10bb519eb62feb8d8c7e8c61edb6a4648bbb4898bf0d91ee4224c80
3fb2b + (0x0516aaf9ba737833310aa78c5982aa5b1f4d746bae3784b70d8c34c
1e7d54cf3) u

y' = 0x021897a06baf93439a90e096698c822329bd0ae6bdbe09bd19f0e07891c
d2b9a + (0x0ebb2b0e7c8b15268f6d4456f5f38d37b09006ffd739c9578a2d1ae
c6b3ace9b) u

r' = r

h' = 0x2523648240000001ba344d8000000008c2a2800000000016ad000000000
00019

GT-Field-ID: Fp254n12b

p_b = 0x2523648240000001ba344d80000000086121000000000013a700000000
000013

r'' = r

e2 = -1 in F_p

e6 = 1 + u in F_{p^2}
```

```
e12 = v in F_{p^6}

h'' = 0x2928fbb36b391596ee3fe4cbe857330da83e46fedf04d235a4a8daf5ff
9f6eabcb4e3f20aa06f0a0d96b24f9af0cbbce750d61627dcbf5fec9139b8f1c46
c86b49b4f8a202af26e4504f2c0f56570e9bd5b94c403f385d1908556486e24b39
6ddc2cdf13d06542f84fe8e82ccbad7b7423fc1ef4e8cc73d605e3e867c0a75f45
ea7f6356d9846ce35d5a34f30396938818ad41914b97b99c289a7259b5d2e09477
a77bd3c409b19f19e893f8ade90b0aed1b5fc8a07a3cebb41d4e9eee96b21a832d
db1e93e113edfb704fa532848c18593cd0ee90444a1b3499a800177ea38bdec62e
c5191f2b6bbee449722f98d2173ad33077545c2ad10347e125a56fb40f086e9a4e
62ad336a72c8b202ac3c1473d73b93d93dc0795ca0ca39226e7b4c1bb92f99248e
c0806e0ad70744e9f2238736790f5185ea4c70808442a7d530c6ccd56b55a69738
67ec6c73599bbd020bbe105da9c6b5c009ad8946cd6f0

h''_1 = 0xc816ed457c4f0cbba598fbf85278d6a283736855af2828a32ad1c29a
144223e6281b946847fdfeb69c50d19a04e83b02b9108347fe83011a78b30ec3c0
4f5235bd893d800083e82c022780000099261da2800000006fd671000000000027
0d

h''_2 = 0x34a94d3d1f0dc12947911459f9c97e1cafcb74609938a7cd37a11adf
6b9bd9bba488c257f6684b18eaf5e67df52cac7666c59efee0438bd28494fdda8d
885b39a9fcdc9ec6fccae4176a422f3f96db68ff3d696b0842dfed0d2ba7e853d9
cb6ea2194a2457251fa44e714cea395c60ea4852c28305971c9405144476d3cad8
a7fdcb78a53125d893e87ac3969ecf74ddd99f9e6ba4fc7d0d8c6b607840f2b9a2
5cf964bff87e6160db1954275f370301029b0b18e809ac493883635763bd991d19
19680457071767d197dfed87a2112b74feaec3e7e276b2c884552cc2543491bfb5
420df1026219e849c1f94a4d35e0020c9d8849b5c000003f71a76b0



Pairing-Param-ID: Nogami-Aranha = {
    G1-Curve-ID: Fp254BNb
    G2-Curve-ID: Fp254n2BNb
    GT-Field-ID: Fp254n12b
}
```

4.2.3. Domain Parameters Scott

The domain parameters by Scott generated by t = -0x4000806000004081 [6].

The domain parameters described in this subsection are defined by elliptic curve E(F_p) : y^2 = x^3 + 2 and sextic twist E'(F_{p^2}) : x'^3 + 2/s = x'^3 + 1 - u, where F_{p^2} = F_p[u]/(u^2 + 1), F_{p^6} = F_{p^2}[v]/(v^3 - (1 + u)), F_{p^12} = F_{p^6}[w]/(w^2 - v), 1/s = 1/(1 + u). We describes domain parameters of elliptic curves E and E'. The parameter p_b is 3 mod 4. For the details of these parameters, refer to [2].

G1-Curve-ID: Fp254BNc

p_b = 0x240120db6517014efa0bab3696f8d5f06e8a555614f464babe9dbbfeee
b4a713

B = 2

x = 0x240120db6517014efa0bab3696f8d5f06e8a555614f464babe9dbbfeeeb4
a712

y = 1

r = 0x240120db6517014efa0bab3696f8d5f00e88d43492b2cb363a75777e8d30
210d

h = 1

G2-Curve-ID: Fp254n2BNc

p_b = 0x240120db6517014efa0bab3696f8d5f06e8a555614f464babe9dbbfeee
b4a713

e2 = -1 in F_p

B' = 1 + (-1) u

r' = r

x' = 0x0571af2ea9666eb2a53f3fb837172bdd809c03a95c5870f34a8cb340220
bf9c0 + (0x0f71abb712a9e6e12c07b58bc01f2f994c3b5a1531cf96609b838e5
ccf05bc71) u

y' = 0x0b88822fe134c1695b21419bb1ab9732f707701046a2e6ff3ad10f3c702
84b93 + (0x1659b723676b5af5231fb045b3d822c0de6fcaab171bad9c8951afc
800a26775) u

h' = 0x240120db6517014efa0bab3696f8d5f0ce8bd6779735fe3f42c6007f503
92d19

GT-Field-ID: Fp254n12c

p_b = 0x240120db6517014efa0bab3696f8d5f06e8a555614f464babe9dbbfeee
b4a713

r'' = r

e2 = -1 in F_p

```
e6 = 1 + u in F_{p^2}

e12 = v in F_{p^6}

h'' = 0x1d43e8fcd92a8e7d54f5820d5a3701e694bad5ec9021a8a58128e0908b
cb1747bc941f92c7713cf91dc9a015614324e892b37c0bbcc7873897da12bded8e
e32461e008c9b2e43e5a5d6498bb1b44874b164fc2f8cb2e02847eb2550ef4fb67
ebba59d2dc7b7fa6b348d432b00916f8fafd5ec31daed9dc0c9790d7640fd2085e
d6bf6796b5634709896c13aabbc8ad817ce596a31e581258e2d88985978f27e6b4
b5daadbe327cb2dfc0220f0dfb61a1fe9dc7f88e061d67a0c1f6dac9b1d839e046
ecbd957bb030322f4ab982f624f1aa8c1d8f97661f7d6fe0f01660b845948d1ca4
db92203ccb50779ccb981ba37248a67f2f5f7201dd03efbadd98232ffec54f723b
583c0df642183ad006819a33e938fd763efee80a64a5aa7092ce5e4bf7f40c9442
5a83e47b6f0e685bf5a801c864f76637225082c61c7fda904ac0d5fc90ee608f9c
b5f79b6e69c217097de370e7a0f22ae9afbb992f232f0

h''_1 = 0xb651238d914d6ec916c6f4c59202389fb75a267e7c7feabf4a5ee9ef
5aa0b588f60d6f5d737b92988f3253f3d3c8aa439f0743d28102d47dc7e0b0ff07
f71e282739c9d5a3236579d81733eaf9269bb184134d7ac2c082e05ea6e634f918
0d

h''_2 = 0x2917c05fa90fae306d470d8d5d3f04e9265a173b6c281349dab6abff
e85c4b6129d208e97f9d6240137b86473a62a611475435473877667 77a255874c9
16f826d23df531380749423add88352eb9838833969e3fcc2b61bbfa62ab642308
509c7ef4dddc267f1f9ab38047837b4618a6d477a9c3067cd2d5711c450915e9a6
fd49ee049860c56da205aaf066dfab99472a91a225abcaa4051b77ee0f8c811889
384be038871765c7e4ade3fe391232d04f4397c94f1273cf057a6552123e1c30d6
e0dd4536a32d372a3d426d1d9046f5da0ffdfe53ab2d4a4fa6604b6c224c04e916
90d605d0bd8be366a4bd78b4bfeafb9c7face675844fd40ed13d2b0

Pairing-Param-ID: Scott = {
    G1-Curve-ID: Fp254BNc
    G2-Curve-ID: Fp254n2BNc
    GT-Field-ID: Fp254n12c
}
```

4.2.4. Domain Parameters by BCMNPZ

The domain parameters by BCMNPZ generated by t = -0x4000020100608205 [7].

The domain parameters described in this subsection are defined by elliptic curve E(F_p) : y^2 = x^3 + 2 and sextic twist E'(F_{p^2}) : x'^3 + 2/s = x'^3 + 1 - u, where F_{p^2} = F_p[u]/(u^2 + 1), F_{p^6} = F_{p^2}[v]/(v^3 - (1 + u)), F_{p^12} = F_{p^6}[w]/(w^2 - v), 1/s = 1/(1 + u). We describes domain parameters of elliptic curves E and E'. The parameter p_b is 3 mod 4. For the details of these parameters, refer to [2].

```
G1-Curve-ID: Fp254BNd

p_b = 0x24000482410f5aadb74e200f3b89d00081cf93e428f0d651e8b2dc2bb4
60a48b

x = 0x24000482410f5aadb74e200f3b89d00081cf93e428f0d651e8b2dc2bb460
a48a

y = 1

B = 2

r = 0x24000482410f5aadb74e200f3b89d00021cf8de127b73833d7fb71a511aa
2bf5

h = 1

G2-Curve-ID: Fp254BNd

p_b = 0x24000482410f5aadb74e200f3b89d00081cf93e428f0d651e8b2dc2bb4
60a48b

e2 = -1 in F_p

B' = 1 + (-1) u

r' = r

x' = 0x20cfe8b965fc444008a21b12cd2a55f843c1dd68ba12a8bb1f1dde3533b
91a32 + (0x0176f822a5ee7ada449f8f876ee001508dd43b5413e03c8f4ad3e3b
38dadaf51) u

y' = 0x02b27f22c2920fee3b4af218b6d92421780a9bdc66155142fecef3af7f5
8e872 + (0x14e9c62a36ebce710810576b5401fdf0b28126ad2d563bf5043be33
47646dfb4) u

h' = 0x24000482410f5aadb74e200f3b89d000e1cf99e72a2a746ff96a46b2571
71d21

GT-Field-ID: Fp254n12d

p_b = 0x24000482410f5aadb74e200f3b89d00081cf93e428f0d651e8b2dc2bb4
60a48b

r'' = r

e2 = -1 in F_p
```

```
e6 = 1 + u in F_{p^2}

e12 = v in F_{p^6}

h'' = 0x1d39fc2421c459d1f0de7cde7c1285648918cd045a503063f111e3aaba
83df215962969c6fceb6f999c374d7c0fb36eb380701566be2e2b206368ba4f04e
ebcdf9c008c23935547b5a46e37a5f1f6e26745bf3219c8b4456c4fbc261596000
4d5f42547d6b9a867244929fd958b2f962fb35d58f0225a524e4199f3e961c67e9
b1618141cbe93892841e90040854c324d828bcabba01c45b1c8d62829192d22d2f
a7281370c28fe7449df33a45af6bf04c8fc54e271bd28c671b5ef06591044fce06
13d7a0fb7a9f4467428dcdf071e85f86bf6097ec6dd14b974aa94a1d189b2227ae
75851160753faac94c2bcb2c15fd5be5e68fc316683ac92cf07b7030c91b25e4dd
40f8a6fc9c128f52b060f4be0c33dd22007c9df38874bf6ce8f21736b6ce5b2d0a
69d802b0efe5d3a05fe0fa939f27bdb66812f89bfef4c3852044c18aa3059d5b63
505ec878753497904916ce2ede9dd267ccd69fcf26c50

h''_1 = 0xb640447a44acc2b50912a1528832c5f4358315c85cd27dc4629b83ad
23ca6447537784d1adc703cf92a32bf736604c22f7fc113e08bd1a0f4061cc8a1c
c42f380317a331d6cb9e0fbbb55404de8fbd905999f354e0c0a9d80c9dbebc66ca
35

h''_2 = 0x290d9d32167d7406812204488b22639b77897f44694c058dd022c218
16fc3e82f03b87223ac3b8fba7a347184422c7278b0d501d0de0374429d873e7ef
5c86ca749bc6bc55607d2f6dc47fc8fa1abf770d4341041836d6de95ffa72e2cee
6b0ace366bdd8d94be2d4c7c4a4f2312b12932ca02c795a69a53467ce26ae7afb2
f5d99e43aec676bc1564aad101c07a096650986516e4680683384113fcb842d1d4
b6dc261a852b3e85e2b39d159189a82de7794fe53d10feec08ec3521b110b1cfc4
d9d49204f248f9d162489f3bb2c5c0725a1e6da1e0b7df86f8464cc6df13439cd2
5d90d220d3514c1824b5917c5713a224dcd44c8e2c08fbe2e9fc510

Pairing-Param-ID: BCMNPZ = {
    G1-Curve-ID: Fp254BNd
    G2-Curve-ID: Fp254n2BNd
    GT-Field-ID: Fp254n12d
}
```

5. Object Identifiers

We need to define the following object identifiers. Which organization is suitable for the allotment of these object identifiers?

```
Beuchat OBJECT IDENTIFIER ::= {TBD}

Nogami-Aranha OBJECT IDENTIFIER ::= {TBD}

Scott OBJECT IDENTIFIER ::= {TBD}
```

    BCMNPZ OBJECT IDENTIFIER ::= {TBD}

6. Security Considerations

For above sections, G_1 is a r-order cyclic subgroup of E(F_p) and G_2 is a subgroup of E'(F_{p^2}), where k is the embedding degree of the curve and the group G_T is the set of r-th roots of unity in the finite field F_{p^12}^*. In this section, G_1, G_2 and G_T imply E(F_p), E'(F_{p^2}) and F_{p^12}^* respectively.

Pairing-based cryptographic primitives are often based on the hardness of the following problems, so when the elliptic curves from this document are used in such schemes, these problems would apply.

The elliptic curve discrete logarithm problem in G_1 and G_2 (ECDLP)

The finite field discrete logarithm problem in G_T (FFDLP)

The elliptic curve computational Diffie-Hellman (CDH) problem in G_1 and G_2

The elliptic curve computational co-Diffie-Hellman problem in G_1 and G_2

The elliptic curve decisional Diffie-Hellman (DDH) problem in G_1

The bilinear Diffie-Hellman (BDH) problem

Algorithms to efficiently solve the problems above, aside from special cases, are unknown. Mainly, there are Pollard-rho algorithm [18] against point of an elliptic curve G_1 and G_2, and Number Field Sieve method [17] against G_T which is output of pairing as generic attacks against elliptic curve with pairing .

G_T to be larger than G_1 and G_2, because FFDLP can be computed more efficiently than ECDLP in most cases. Security level of schemes based on pairing depends most weak level for each problems. Thus implementors should necessary to ensure adequate security level for both of problems.

Table 1 shows the security level of elliptic curves described in this memo Schemes based on the elliptic curves (i.e. G_1 and G_2) and the finite fields (i.e. G_T) must be combined with cryptographic primitives which have similar or greater security level than the scheme.

Pairing-Param-ID	Security Level for ECDLP in G_1, G_2 (bits)	Security Level for FFDLP in G_T (bits)
Beuchat	128	128
Nogami-Aranha	128	128
Scott	128	128
BCMNPZ	128	128

Table 1: security level of elliptic curves and finite field specified in this memo

6.1. Subgroup Security (OPTIONAL requirement)

For BN-curves, G_1 is cryptographic group of large prime order and cofactor h is always 1. On the other hand, G_2, G_T are consisted of subgroup of order h' and h'' that are not equal to 1 in addition to subgroup of order r , resp. Thus implementors who provided groups in G_2 and G_T, MUST check element of those groups included in subgroup of order r (see [7]) .

The order check of G_T can be performed by exponentiation of h''_1 and h''_2. The exponentiation of h''_2 can be easily computed by using Frobenius map. Whereas the exponentiation of h''_1 is complicated.

For simplification of the order check which is the smallest prime factor of h' and h''_1 will be greater than r, of element, we define OPTIONAL security G_2-strong and G_T-strong security. G_2-strong and G_T-strong means those order of cryptographic group MUST have the smallest prime factor greater than r. Therefore implementors could not check of order, G_2-strong and G_T-strong cryptographic group will not be insecure

Table 2 shows the G_2, G_T-strong security of parameters described in this memo.

Pairing-Param-ID	Have G_2-Strong?	Have G_T-Strong?
Beuchat	no	no
Nogami-Aranha	no	no
Scott	no	yes
BCMNPZ	yes	yes

Table 2: G2, G3-strong security

7. Acknowledgements

This memo was inspired by the content and structure of [19].

8. Change log

NOTE TO RFC EDITOR: Please remove this section in before final RFC publication.

9. References

9.1. Normative References

[1] Beuchat, J., Gonzalez-Diaz, J., Mitsunari, S., Okamoto, E., Rodriguez-Henriquez, F., and T. Teruya, "High-Speed Software Implementation of the Optimal Ate Pairing over Barreto-Naehrig Curves", Proceedings Lecture notes in computer sciences; Pairing-Based Cryptography --Pairing2010, 2010.

[2] Aranha, D., Karabina, K., Longa, P., Gebotys, C., Rodriguez-Henriquez, F., and J. Lopez, "Faster Explicit Formulas for Computing Pairings over Ordinary Curves", Proceedings Lecture notes in computer sciences; EUROCRYPT --EUROCRYPT2011, 2011.

[3] International Organization for Standardization, "Information Technology - Security Techniques -- Cryptographic techniques based on elliptic curves . Part 5: Elliptic curve generation", ISO/IEC 15946-5, 2009.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[5] Nogami, Y., Akane, M., Sakemi, Y., Kato, H., and Y. Morikawa, "Integer Variable \chi Based Ate Pairing", Proceedings Pairing 2008, LNCS 5209, pp. 178.191, Springer-Verlag , 2008.

9.2. Informative References

[6] Scott, M., "Unbalancing Pairing-Based Key Exchange Protocols", ePrint http://eprint.iacr.org/2013/688.pdf, 2013.

[7] Barreto, P., Costello, C., Misoczki, R., Naehrig, M., Pereira, G., and G. Zanon, "Subgroup security in pairing-based cryptography", ePrint http://eprint.iacr.org/2015/247.pdf, 2015.

[8] Barreto, P. and M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order", Proceedings Lecture notes in computer sciences; 3897 in Selected Areas in Cryptgraphy -- SAC2005, 2006.

[9] Boyen, X. and L. Martin, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, December 2007.

[10] Groves, M., "Sakai-Kasahara Key Encryption (SAKKE)", RFC 6508, February 2012.

[11] Hitt, L., "ZSS Short Signature Scheme for Supersingular and BN Curves", draft-irtf-cfrg-zss-02 (work in progress), 2013.

[12] Martin, L. and M. Schertler, "Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS)", RFC 5409, January 2009.

[13] Cakulev, V. and G. Sundaram, "MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)", RFC 6267, June 2011.

[14] Groves, M., "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)", RFC 6507, February 2012.

[15] Groves, M., "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)", RFC 6509, February 2012.

[16] Cakulev, V., Sundaram, G., and I. Broustis, "IBAKE: Identity-Based Authenticated Key Exchange", RFC 6539, March 2012.

[17] Joux, A., Lercier, R., Smart, P., and F. Vercauteren, "The number field sieve in the medium prime case", Proceedings Lecture notes in computer sciences; 4117 in Comput. Sci. -- CRYPTO2006, 2006.

[18] Pollard, J., "Monte Carlo Methods for Index Computation (mod p)", Proceedings Mathematics of Computation, Vol.32, 1978.

[19] Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, March 2010.

[20] "University of Tsukuba Elliptic Curve and Pairing Library", 2013, <http://www.cipher.risk.tsukuba.ac.jp/tepla/index_e.html>.

[21] Aranha, D. and C. Gouv, "RELIC is an Efficient LIbrary for Cryptography", 2013, <https://code.google.com/p/relic-toolkit/>.

[22] Aranha, D., Barreto, P., Longa, P., and J. Rocardini, "The Realm of the Pairings", SAC 2013, to appear, 2013.

[23] Scott, M., "The MIRACL IoT Multi-Lingual Crypto Library", 2015, <https://github.com/CertiVox/MiotCL.git>.

Appendix A. Domain Parameters Based on ISO Document

We describe the domain parameters for 224, 256, 384, and 512-bit elliptic curves which are compliant with the ISO document and are based on M-type twisted curve. The domain parameters described in below subsections are defined by Elliptic curve E(F_p): y^2 = x^3 + 3 and sextic twist E'(F_{p^2}): y'^2 = x'^3 + 3 * s, where F_{p^2} = F_p[u]/(u^2 + 1), F_{p^12} = F_{p^2}[w]/(w^6 - s), s = 1 + u. We describe domain parameters of elliptic curves E. Detailed information on these domain parameters is given in [3].

A.1. Specific ISO domain parameters

A.1.1. Domain Parameters for 224-Bit Curves

```
G1-Curve-ID: Fp224BN

p_b = 0xfffffffffff107288ec29e602c4520db42180823bb907d1287127833

B = 3

x = 1

y = 2

r = 0xfffffffffff107288ec29e602c4420db4218082b36c2accff76c58ed

h = 1
```

A.1.2. Domain Parameters for 256-Bit Curves

```
G1-Curve-ID: Fp256BN

p_b = 0xfffffffffffcf0cd46e5f25eee71a49f0cdc65fb12980a82d3292ddbae
d33013

B = 3

x = 1

y = 2

r = 0xfffffffffffcf0cd46e5f25eee71a49e0cdc65fb1299921af62d536cd10b
500d

h = 1
```

A.1.3. Domain Parameters for 384-Bit Curves

G1-Curve-ID: Fp384BN

p_b = 0xfffffffffffffffffff2a96823d5920d2a127e3f6fbca024c8fbe29531
892c79534f9d306328261550a7cabd7cccd10b

B = 3

x = 1

y = 2

r = 0xfffffffffffffffffff2a96823d5920d2a127e3f6fbca023c8fbe2953189
2c795356487d8ac63e4f4db17384341a5775

h = 1

A.1.4. Domain Parameters for 512-Bit Curves

G1-Curve-ID: Fp512BN

p_b = 0xfffffffffffffffffffffffffff9ec7f01c60ba1d8cb5307c0bbe3c111
b0ef455146cf1eacbe98b8e48c65deab236fel916a55ce5f4c6467b4eb280922ad
ef33

B = 3

x = 1

y = 2

r = 0xfffffffffffffffffffffffffff9ec7f01c60ba1d8cb5307c0bbe3c111b0
ef445146cf1eacbe98b8e48c65deab2679a34a10313e04f9a2b406a64a5f519a09
ed

h = 1

A.1.5. Security of ISO curves

In this section, this memo describes ECDLP on G_1 and G_2, FFDLP on G_T and subgroup security over G_2 and G_T, for ISO curves.

Table 3 shows the security level of ISO curves.

Pairing-Param-ID	Security Level for ECDLP in G_1, G_2 (bits)	Security Level for FFDLP in G_T (bits)
ISO-Fp224	112	112
ISO-Fp256	128	128
ISO-Fp384	192	128
ISO-Fp512	256	128

Table 3: security level of ISO elliptic curves and finite field specified in this memo

Table 4 shows the G_2, G_T-strong security of ISO curves.

Pairing-Param-ID	Have G_2-Strong?	Have G_T-Strong?
ISO-Fp224	no	no
ISO-Fp256	no	no
ISO-Fp384	no	no
ISO-Fp512	no	no

Table 4: G2, G3-strong security of ISO curves

Authors' Addresses

Kohei Kasamatsu
NTT Software Corporation

EMail: kasamatsu.kohei-at-po.ntts.co.jp

Akihiro Kato
NTT Software Corporation

EMail: kato.akihiro-at-po.ntts.co.jp

Michael Scott
CertiVox

EMail: mike.scott-at-certivox.com

Tetsutaro Kobayashi
NTT

EMail: kobayashi.tetsutaro-at-lab.ntt.co.jp

Yuto Kawahara
NTT

EMail: kawahara.yuto-at-lab.ntt.co.jp