Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 14, 2014

K. Kasamatsu
S. Kanno
NTT Software Corporation
T. Kobayashi
Y. Kawahara
NTT

January 10, 2014

Barreto-Naehrig Curves
draft-kasamatsu-bncurves-00

Abstract

Elliptic curves with pairing are useful tools for constructing cryptographic primitives. In this memo, we specify domain parameters of Barreto-Naehrig curve (BN-curve) [5]. 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 two 254-bit BN-curves [1] [2] which allow us to obtain efficient implementations and domain parameters of 224, 256, 384, and 512-bit BN-curves which are compliant with ISO/IEC 15946-5[3]. Furthermore, this memo organizes differences between types of elliptic curves specified in ISO document and often used in open source softwares, which are called M-type and D-type respectively[21].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 14, 2014.

Table of Contents

1. Introduction

Elliptic curves with a special map called a pairing or bilinear map allows cryptographic primitives to achieve functions or efficiency which cannot be realized by conventional mathmatical tools. There

are identity-based encryption (IBE), attribute-based encryption (ABE), ZSS signature, broadcast encryption (BE) as examples of these primitives. IBE realizes powerful management of public key 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 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 pairing were proposed in the IETF (e.g. [6], [7], and [8]) and used in some protocols (e.g. [9], [10], [11], [12], and [13]). 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 curves 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) [5]. The BN-curve allows us to achieve high security and efficiency with pairings due to an optimum embedding degree. This memo specifies domain parameters of two 254-bit BN-curves ([1] and [2]) because of these efficiencies. These BN-curves are known as efficient curves in academia and particularly provide efficient pairing which is generally slowest operation in pairing-based cryptography. There are optimized source codes of ([1] and [2]) as open source softwares ([19] and [20]), respectively. Furthermore, this memo specifies 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 specified in ISO document and used in open source softwares, which are called M-type and D-type respectively [21].

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 defintion of elliptic curve and bilinear map, notation used in this memo.

3.1. Elliptic Curve

Throughout this memo, let p > 3 be a prime and F_p be a finite field. The curve defined by the following equation E is called elliptic curve.

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

Solutions (x,y) for an elliptic curve E, as well as the point at infinity, are called F_p-rational points. The additive group is constructed by a well-defined operation in the set of F_p-rational points. Typically, the cyclic additive group with prime order q and base point G in E(F_p) 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_p): number of points on an elliptic curve E over F_p.

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

embedding degree k: minimum integer k such that r is a divisor of q^k - 1 and r^2 is not a divisor of q^k - 1

3.2. Bilinear Map

Let G_1 be an additive group of prime order p 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_q, we have the relation e(aS, bT) = e(S,T)^{ab}.

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

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

4. There exists an efficient, publicly computable isomorphism I: G_2 -> G_1 such that I(Q) = P.

For BN-curves, G_1 is a q-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 q-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 two 254-bit elliptic curves which allow us to efficiently compute the operation of a pairing at high levels of security and domain parameters for 224, 256, 384, and 512-bit elliptic curves which are compliant with the ISO document [3].

4.1. Notations for Domain Parameters and Types of Sextic Twists

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

Domain parameters of the elliptic curve E(F_p) and E(F_{p^12}) are needed for computation of the pairing. Barreto and Naehrig proposed a method of point and pairing compression by using output of a map I from a sextic twist E'(F_{p^2}) to E(F_{p^12}) instead of E(F_{p^12}). Generally, this method is used with BN-curves. Hence, this memo follows the method. For the details of the method, refer

to [5].

The pairing friendly curves are classified two types, which are called D-type and M-type respectively [21]. The D-type sextic twist curve is defined by equation y'^2 = x'^3 + b/s when elliptic curve E(F_p) is let to be y^2 = x^3 + b and represent of F_{p^12} is let 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}) -> E(F_{p^12}) is (x', y') -> (z^2 * x', z^3 * y').

The M-type sextic twist curve is defined by equation y'^2 = x'^3 + b * s when elliptic curve E(F_p) is let to be y^2 = x^3 + b and represent of F_{p^12} is let to be F_{p^2}[u]/(u^6 - s), where s is in F_{p^2}^*. The corresponding map I: E'(F_{p^2}) -> E(F_{p^12}) is (x', y') -> (x' * s^{-1} * z^4, y' * s^{-1} * z^3), with z^6 = s.

These domain parameters are described in the following way.

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

p_b is a prime specifying base field.

p_e is an irreducible polynomial specifying extension field.

For elliptic curve E

A and B are the coefficients of the equation y^2 = x^3 + A * x + 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.

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

h is the cofactor of G in E

For twist curve E'

A' and B' are the coefficients of the equation y^2 = x^3 + A' * x + 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.

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

h' is the cofactor of G' in E'

4.2. Efficient Domain Parameters for 254-Bit-Curves

In this section, this memo specifies the domain parameters for two 254-bit elliptic curves which are more efficient than parameters of ISO document with D-type.

4.2.1. Domain Parameters by Beuchat et al.

Here, we describe the domain parameters for 254-bit elliptic curve[1] with D-type.

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'. For the details of these parameters, refer to [1].

Curve-ID: Fp254BNa

p_b = 0x2370fb049d410fbe4e761a9886e502417d023f40180000017e80600000000001

A = 0

B = 5

x = 1

y = 0xd45589b158faaf6ab0e4ad38d998e9982e7ff63964ee1460342a592677cccb0

q = 0x2370fb049d410fbe4e761a9886e502411dc1af70120000017e806000000000001

h = 1

Curve-ID: Fp254n2BNa

p_b = 0x2370fb049d410fbe4e761a9886e502417d023f40180000017e80600000
000001

p_e = u^2 + 5 over p_b

A' = 0

B' = - u

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

y' = 0x17abd366ebbd65333e49c711a80a0cf6d24adf1b9b3990eedcc91731384
d2627 +
(0x0ee97d6de9902a27d00e952232a78700863bc9aa9be960C32f5bf9fd
0a32d345) u

q' = 0x2370fb049d410fbe4e761a9886e502411dc1af70120000017e806000000
00001

h' = 0x2370fb049d410fbe4e761a9886e50241dc42cf101e0000017e806000000
00001

4.2.2. Domain Parameters by Aranha et al.

Here, we describe the domain parameters for 254-bit elliptic curve [2] with D-type.

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'. For the details of these parameters, refer to [2].

Curve-ID: Fp254BNb

```
p_b = 0x2523648240000001ba344d8000000008612100000000013a700000000
000013

A = 0

B = 2

x = 0x2523648240000001ba344d8000000008612100000000013a70000000000
0012

y = 1

q = 0x2523648240000001ba344d8000000007ff9f800000000010a10000000000
000d

h = 1

Curve-ID: Fp254n2BNb

p_b = 0x2523648240000001ba344d8000000008612100000000013a700000000
000013

p_e = u^2 + 1 over p_b

A' = 0

B' = 1 + (0x2523648240000001ba344d8000000008612100000000013a70000
0000000012) u

x' = 0x061a10bb519eb62feb8d8c7e8c61edb6a4648bbb4898bf0d91ee4224c80
3fb2b +(0x0516aaf9ba737833310aa78c5982aa5b1f4d746bae3784b70d8c34c1
e7d54cf3)u

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

q' = 0x2523648240000001ba344d8000000007ff9f800000000010a1000000000
0000d

h' = 0x2523648240000001ba344d8000000008c2a2800000000016ad000000000
00019
```

4.3. Domain Parameters Based on ISO Document

Here, 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. 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[X]/(X^2 + 1), F_{p^12} = F_{p^2}[X]/(X^6 - s), s = 1 + X. We describe domain parameters of elliptic curves E. Detailed information on these domain parameters is given in [3].

4.3.1. Domain Parameters for 224-Bit Curves

Curve-ID: Fp224BN

p_b = 0xffffffffff107288ec29e602c4520db42180823bb907d1287127833

A = 0

B = 3

x = 1

y = 2

q = 0xffffffffff107288ec29e602c4420db4218082b36c2accff76c58ed

h = 1

4.3.2. Domain Parameters for 256-Bit Curves

Curve-ID: Fp256BN

p_b = 0xffffffffffcf0cd46e5f25eee71a49f0cdc65fb12980a82d3292ddbaed33013

A = 0

B = 3

x = 1

y = 2

q = 0xffffffffffcf0cd46e5f25eee71a49e0cdc65fb1299921af62d536cd10b500d

h = 1

4.3.3. Domain Parameters for 384-Bit Curves

Curve-ID: Fp384BN

p_b = 0xffffffffffffffffff2a96823d5920d2a127e3f6fbca024c8fbe29531
892c79534f9d306328261550a7cabd7cccd10b

A = 0

B = 3

x = 1

y = 2

q = 0xffffffffffffffffff2a96823d5920d2a127e3f6fbca023c8fbe2953189
2c795356487d8ac63e4f4db17384341a5775

h = 1

4.3.4. Domain Parameters for 512-Bit Curves

Curve-ID: Fp512BN

p_b = 0xffffffffffffffffffffffffff9ec7f01c60ba1d8cb5307c0bbe3c111
b0ef455146cf1eacbe98b8e48c65deab236fel916a55ce5f4c6467b4eb280922ad
ef33

A = 0

B = 3

x = 1

y = 2

q = 0xffffffffffffffffffffffffff9ec7f01c60ba1d8cb5307c0bbe3c111b0
ef445146cf1eacbe98b8e48c65deab2679a34a10313e04f9a2b406a64a5f519a09
ed

h = 1

4.3.5. Differences between D-Type and M-Type on ISO parameters

Although ISO document is based on M-type, open source softwares are often based on D-type. We need to be aware of the differences. Hence we also describe elliptic curve with D-type based on ISO document. The elliptic curve E(F_p) is defined by equation y^2 = x^3

+ 3 and the sextic twist E'(F_{p^2}) is defined by y'^2 = x'^3 + 3/s, where F_{p^2} = F_p[X]/(X^2 + 1), F_{p^12} = F_{p^2}[X]/(X^6 - s), 1/s = -8 + 8 * i, i = X^2 + 1. Detailed information on these domain parameters is given in [5].

5. Object Identifiers

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

Fp254BNa OBJECT IDENTIFIER ::= {TBD}

Fp254n2BNa OBJECT IDENTIFIER ::= {TBD}

Fp254BNb OBJECT IDENTIFIER ::= {TBD}

Fp254n2BNb OBJECT IDENTIFIER ::= {TBD}

Fp224BN OBJECT IDENTIFIER ::= {TBD}

Fp256BN OBJECT IDENTIFIER ::= {TBD}

Fp384BN OBJECT IDENTIFIER ::= {TBD}

Fp512BN OBJECT IDENTIFIER ::= {TBD}

6. Security Considerations

Elliptic curves which are specified in this memo have hardness of the problems below and enough security margin against the attacks below.

The elliptic curve that supports a bilinear map requires the hardness of solving following problems, since the security of pairing-based cryptographic primitives is based on hardness of these problems. (For details of problems, refer to section 2 of [14].)

The elliptic curve discrete logarithm problem (ECDLP)

The elliptic curve computational Diffie-Hellman problem (ECDHP)

The bilinear Diffie-Hellman problem (BDHP)

The elliptic curve discrete logarithm problem with auxiliary inputs (ECDLP with auxiliary inputs)

Algorithms to efficiently solve the problems above, aside from special cases, are unknown. When choosing elliptic curve domain

parameters we need to consider the Pollard-rho algorithm [16] and Menezes-Okamoto-Vanstone algorithm [15] as generic attacks against ECDLP. The Pollard-rho algorithm is believed to have the best performance against ECDLP at present. However, it is an exponential time algorithm. Menezes-Okamoto-Vanstone algorithm converts ECDLP into the discrete logarithm problem in a finite field F_{p^k}^*, the codomain of the bilinear map, where k is embedding number. This is a subexponential time algorithm.

The Smart, Semaev, and Sato-Araki algorithm [17], and Cheon algorithm [14] are main algorithms which improve efficiency in specific cases. The Smart-Semaev algorithm and Sato-Araki algorithm are polynotmial time algorithms against the ECDLP in the case where #E(F_{p}) equals to p. These algorithms are independently proposed. Cheon algorithm [14] is against the ECDLP with auxiliary inputs. It is prevented by satisfy the following condition, where n is order.

there is no divisor d of n - 1 s.t. (log n)^2 < d < n^{1/2} and there is no divisor e of n + 1 s.t. (log n)^2 < e < n^{1/2}

Table 1 shows the security level of elliptic curves described in this memo ([1], [2]). Schemes based on the elliptic curves must be combined with cryptographic primitives which have similar or greater security level than the scheme.

Curve-ID	Security Level (bits)
Fp224BN	112
Fp254BNa	128
Fp254BNb	128
Fp256BN	128
Fp384BN	128
Fp512BN	128

Table 1: security level of elliptic curve specified in this memo

7. Acknowledgements

This memo was inspired by the content and structure of [18].

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.

9.2. Informative References

[5] 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.

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

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

[8] Hitt, L., "ZSS Short Signature Scheme for BN Curves", 2013.

[9] 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.

[10] 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.

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

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

2012.

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

[14] Cheon, J., "Security Analysis of the Strong Diffie-Hellman Problem", Proceedings Lecture notes in computer sciences; 4004 in Advances in Cryptogoly -- Eurocrypt2006, 2006.

[15] Menezes, A., Okamoto, T., and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", Proceedings IEEE Transactions to Information Theroy 39, 1993.

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

[17] Satoh, T. and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves", Proceedings Comm. Math. UnivSancti Pauli 47, 1998.

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

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

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

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

Authors' Addresses

Kohei Kasamatsu
NTT Software Corporation

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

Satoru Kanno
NTT Software Corporation

EMail: kanno.satoru-at-po.ntts.co.jp

Tetsutaro Kobayashi
NTT

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

Yuto Kawahara
NTT

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