Internet Engineering Task Force (IETF)
Request for Comments: 6932
Category: Informational
ISSN: 2070-1721

D. Harkins, Ed.
Aruba Networks

May 2013

Brainpool Elliptic Curves for the Internet Key Exchange (IKE) Group Description Registry

Abstract

This memo allocates code points for four new elliptic curve domain parameter sets over finite prime fields into a registry that was established by the Internet Key Exchange (IKE) but is used by other protocols.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6932.

Table of Contents

1. Introduction

[RFC5639] defines new elliptic curve domain parameters for curves over a number of different prime fields, each with a "twisted" variant. These curves have a number of interesting security properties (as described in [EBP]) that make them desirable to use.

IANA maintains a registry for [RFC2409] to map complete domain parameter sets into easily referenced numbers. While [RFC2409] is deprecated, other protocols, for example [IEEE802.11] and [RFC5931], refer to this registry for its convenience. Therefore, this memo instructs IANA to allocate new code points for the Brainpool curves defined in [RFC5639] to the registry established by [RFC2409] for use by other protocols.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Brainpool Elliptic Curves

[RFC5639] defines several elliptic curves over finite prime fields (ECP, in the parlance of [RFC2409]). The domain parameter sets for each of the elliptic curves defined in [RFC5639] are copied here for convenient reference.

The equation for all elliptic curves defined here is:

$$y^2 = x^3 + ax + b \pmod{p}$$

Domain parameter sets consist of:

- p: the prime
- a, b: parameters to the equation of the curve
- x, y: the coordinates of the generator for the group, G
- q: the order of the group formed by the generator G
- h: the co-factor
- z: the "twist" (for conversion into twisted curves)

[RFC5639] defines elliptic curves over seven (7) prime fields with a random and a "twisted" variety for each, for a total of fourteen (14) distinct curves. However, some of those curves are not particularly useful: the 160-bit curves provide only 80 bits of strength and that is too small to be of use in current cryptographic applications, and there is no standard hash function to use with the 196-bit and 320-bit curves -- it would make more sense to use the 224-bit and 384-bit curves, respectively, instead. For this reason, the curves defined over 160-bit, 192-bit, and 320-bit primes are not being added to the registry created by [RFC2409].

The twisted curves in [RFC5639] are isomorphic to the random curves of the same length. The curve parameter "a" for the twisted curves equals -3 mod p, and there are certain arithmetical advantages to using such curves. It is possible to convert a point from a random curve (x,y) into a point on the twisted curve (x', y') and back again using this equation:

$$(x',y') = (x*z^2, y*z^3)$$

This would allow an implementation to internally use the twisted version of the curve, taking full advantage of the arithmetical advantages, while exchanging points on the random versions of the curve with peers.

Therefore, the twisted curves are not being added to the registry created by [RFC2409]. Implementations that desire to use the twisted curves internally MUST refer to [RFC5639] for the complete domain parameter sets, only the "twist" is defined here.

2.1. Domain Parameters for the 224-Bit Curve

Curve-ID: brainpoolP224r1

p = D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF

A = 68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43

B = 2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B

x = 0D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D

y = 58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD

q = D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

z = 2DF271E14427A346910CF7A2E6CFA7B3F484E5C2CCE1C8B730E28B3F

h = 1

2.2. Domain Parameters for the 256-Bit Curve

Curve-ID: brainpoolP256r1

p = A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377

A = 7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9

B = 26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

x = 8BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262

y = 547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997

q = A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7

z = 3E2D4BD9597B58639AE7AA669CAB9837CF5CF20A2C852D10F655668DFC150EF0

h = 1

2.3. Domain Parameters for the 384-Bit Curve

Curve-ID: brainpoolP384r1

p = 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB711
23ACD3A729901D1A71874700133107EC53

A = 7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F9
0F8AA5814A503AD4EB04A8C7DD22CE2826

B = 04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62
D57CB4390295DBC9943AB78696FA504C11

x = 1D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10
E8E826E03436D646AAEF87B2E247D4AF1E

y = 8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129
280E4646217791811142820341263C5315

q = 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425
A7CF3AB6AF6B7FC3103B883202E9046565

z = 41DFE8DD399331F7166A66076734A89CD0D2BCDB7D068E44E1F378F41ECBAE
97D2D63DBC87BCCDDCCC5DA39E8589291C

h = 1

2.4. Domain Parameters for the 512-Bit Curve

Curve-ID: brainpoolP512r1

p = AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308
717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A
48F3

A = 7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863
BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC
94CA

B = 3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117
A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016
F723

x = 81AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D009
8EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9
F822

y = 7DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F81
11B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD8
0892

q = AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308
70553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA9
0069

z = 12EE58E6764838B69782136F0F2D3BA06E27695716054092E60A80BEDB212B
64E585D90BCE13761F85C3F1D2A64E3BE8FEA2220F01EBA5EEB0F35DBD29D9
22AB

h = 1

3. IANA Considerations

IANA has assigned four values from the unassigned portion of the "Group Description" component of the [IANA-IKE] registry and updated the registry by appending Table 1 to the registry table.

Value	Group Description	Reference	Note
27	224-bit Brainpool ECP group	RFC 6932, Section 2.1	Not for RFC 2409
28	256-bit Brainpool ECP group	RFC 6932, Section 2.2	Not for RFC 2409
29	384-bit Brainpool ECP group	RFC 6932, Section 2.3	Not for RFC 2409
30	512-bit Brainpool ECP group	RFC 6932, Section 2.4	Not for RFC 2409

Table 1: Group Description Updates

4. Security Considerations

[EBP] describes the security properties of the curves referenced here. The curves support security levels of 112 (Section 2.1), 128 (Section 2.2), 192 (Section 2.3), and 256 (Section 2.4). These security levels assume that when these elliptic curves are used with discrete logarithm cryptography, for example elliptic curve Diffie-Hellman, that the private key used is a uniformly random number in the range [1..(q-1)], where q is the order from the curve’s domain parameter set. In order to achieve system security commensurate with

the security level of a particular elliptic curve, it is incumbent upon an implementation to choose key derivation functions, hash functions, pseudo-random functions, and ciphers according to the recommendations from [SP800-57].

5. Use of Brainpool Curves

The notes in Table 1 are an administrative prohibition, not a technical one. The notes are there because, although [RFC2409] has been deprecated, it is still widely used. There is a desire among some in the IETF to not do anything that would prolong the use of [RFC2409], and the addition of these curves was perceived as doing just that. The registry could not have been updated without including notes to indicate that these curves are not for use with [RFC2409] and not updating the [RFC2409] registry would have a detrimental affect on the other protocols that use it.

6. References

6.1. Normative References

[IANA-IKE] IANA, "Internet Key Exchange (IKE) Attributes", Registry Name: Group Description (Value 4), <http://www.iana.org/assignments/ipsec-registry>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5639] Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, March 2010.

6.2. Informative References

[EBP] The Brainpool Workgroup, "ECC Brainpool Standard Curves and Curve Generation", October 2005, <http://www.ecc-brainpool.org/download/Domain-parameters.pdf>.

[IEEE802.11] IEEE, "Telecommunications and information exchange between systems Local and metropolitan area networks--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2012, 2012.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC5931] Harkins, D. and G. Zorn, "Extensible Authentication Protocol (EAP) Authentication Using Only a Password", RFC 5931, August 2010.

[SP800-57] National Institute of Standards and Technology, "Recommendation for Key Management - Part 1: General (Revised)", NIST Special Publication 800-57, March 2007.

Appendix A. Test Data

This section provides some test vectors for example Diffie-Hellman key exchanges using each of the curves defined in Section 2. The following notation is used in subsequent sections:

- dA: the secret key of party A
- x_qA: the x-coordinate of the public key of party A
- y_qA: the y-coordinate of the public key of party A
- dB: the secret key of party B
- x_qB: the x-coordinate of the public key of party B
- y_qB: the y-coordinate of the public key of party B
- x_Z: the x-coordinate of the shared secret that results from completion of the Diffie-Hellman computation
- y_Z: the y-coordinate of the shared secret that results from completion of the Diffie-Hellman computation

A.1. Test Vector for brainpoolP224r1

dA =
7C4B7A2C 8A4BAD1F BB7D79CC 0955DB7C 6A4660CA 64CC4778
159B495E

x_qA =
B104A67A 6F6E85E1 4EC1825E 1539E8EC DBBF5849 22367DD8
8C6BDCF2
y_qA =
46D782E7 FDB5F60C D8404301 AC5949C5 8EDB26BC 68BA0769
5B750A94

dB =
63976D4A AE6CD0F6 DD18DEFE F55D9656 9D0507C0 3E74D648
6FFA28FB

x_qB =
2A97089A 9296147B 71B21A4B 574E1278 245B536F 14D8C2B9
D07A874E
y_qB =
9B900D7C 77A709A7 97276B8C A1BA61BB 95B546FC 29F862E4
4D59D25B

```
x_Z =
312DFD98 783F9FB7 7B970494 5A73BEB6 DCCBE3B6 5D0F967D
CAB574EB
y_Z =
6F800811 D64114B1 C48C621A B3357CF9 3F496E42 38696A2A
012B3C98
```

A.2. Test Vector for brainpoolP256r1

```
dA =
041EB8B1 E2BC681B CE8E3996 3B2E9FC4 15B05283 313DD1A8
BCC055F1 1AE49699

x_qA =
78028496 B5ECAAB3 C8B6C12E 45DB1E02 C9E4D26B 4113BC4F
015F60C5 CCC0D206
y_qA =
A2AE1762 A3831C1D 20F03F8D 1E3C0C39 AFE6F09B 4D44BBE8
0CD10098 7B05F92B

dB =
06F5240E ACDB9837 BC96D482 74C8AA83 4B6C87BA 9CC3EEDD
81F99A16 B8D804D3

x_qB =
8E07E219 BA588916 C5B06AA3 0A2F464C 2F2ACFC1 610A3BE2
FB240B63 5341F0DB
y_qB =
148EA1D7 D1E7E54B 9555B6C9 AC90629C 18B63BEE 5D7AA694
9EBBF47B 24FDE40D

x_Z =
05E94091 5549E9F6 A4A75693 716E3746 6ABA79B4 BF291987
7A16DD2C C2E23708
y_Z =
6BC23B67 02BC5A01 9438CEEA 107DAAD8 B94232FF BBC350F3
B137628F E6FD134C
```

A.3. Test Vector for brainpoolP384r1

```
dA =
014EC075 5B78594B A47FB0A5 6F617304 5B4331E7 4BA1A6F4
7322E70D 79D828D9 7E095884 CA72B73F DABD5910 DF0FA76A
```

```
x_qA =
45CB26E4 384DAF6F B7768853 07B9A38B 7AD1B5C6 92E0C32F
01253327 78F3B8D3 F50CA358 099B30DE B5EE69A9 5C058B4E
y_qA =
8173A1C5 4AFFA7E7 81D0E1E1 D12C0DC2 B74F4DF5 8E4A4E3A
F7026C5D 32DC530A 2CD89C85 9BB4B4B7 68497F49 AB8CC859

dB =
6B461CB7 9BD0EA51 9A87D682 8815D8CE 7CD9B3CA A0B5A826
2CBCD550 A015C900 95B976F3 52995750 6E1224A8 61711D54

x_qB =
01BF92A9 2EE4BE8D ED1A9111 25C209B0 3F99E316 1CFCC986
DC771138 3FC30AF9 CE28CA33 86D59E2C 8D72CE1E 7B4666E8
y_qB =
3289C4A3 A4FEE035 E39BDB88 5D509D22 4A142FF9 FBCC5CFE
5CCBB302 68EE4748 7ED80448 58D31D84 8F7A95C6 35A347AC

x_Z =
04CC4FF3 DCCCB07A F24E0ACC 529955B3 6D7C8077 72B92FCB
E48F3AFE 9A2F370A 1F98D3FA 73FD0C07 47C632E1 2F1423EC
y_Z =
7F465F90 BD69AFB8 F828A214 EB9716D6 6ABC59F1 7AF7C75E
E7F1DE22 AB5D0508 5F5A01A9 382D05BF 72D96698 FE3FF64E
```

A.4. Test Vector for brainpoolP512r1

```
dA =
636B6BE0 482A6C1C 41AA7AE7 B245E983 392DB94C ECEA2660
A379CFE1 59559E35 75818253 91175FC1 95D28BAC 0CF03A78
41A383B9 5C262B98 3782874C CE6FE333

x_qA =
0562E68B 9AF7CBFD 5565C6B1 6883B777 FF11C199 161ECC42
7A39D17E C2166499 389571D6 A994977C 56AD8252 658BA8A1
B72AE42F 4FB75321 51AFC3EF 0971CCDA
y_qA =
A7CA2D81 91E21776 A89860AF BC1F582F AA308D55 1C1DC613
3AF9F9C3 CAD59998 D7007954 8140B90B 1F311AFB 378AA81F
51B275B2 BE6B7DEE 978EFC73 43EA642E

dB =
0AF4E7F6 D52EDD52 907BB8DB AB3992A0 BB696EC1 0DF11892
FF205B66 D381ECE7 2314E6A6 EA079CEA 06961DBA 5AE6422E
F2E9EE80 3A1F236F B96A1799 B86E5C8B
```

```
x_qB =
5A7954E3 2663DFF1 1AE24712 D87419F2 6B708AC2 B92877D6
BFEE2BFC 43714D89 BBDB6D24 D807BBD3 AEB7F0C3 25F862E8
BADE4F74 636B97EA ACE739E1 1720D323
y_qB =
96D14621 A9283A1B ED84DE8D D64836B2 C0758B11 441179DC
0C54C0D4 9A47C038 07D171DD 544B72CA AEF7B7CE 01C7753E
2CAD1A86 1ECA55A7 1954EE1B A35E04BE

x_Z =
1EE8321A 4BBF93B9 CF8921AB 209850EC 9B7066D1 984EF08C
2BB72323 6208AC8F 1A483E79 461A00E0 D5F6921C E9D36050
2F85C812 BEDEE23A C5B210E5 811B191E
y_Z =
2632095B 7B936174 B41FD2FA F369B1D1 8DCADEED 7E410A7E
251F0831 097C50D0 2CFED026 07B6A2D5 ADB4C000 60085622
08631875 B58B54EC DA5A4F9F E9EAABA6
```

Author's Address

Dan Harkins (editor)
Aruba Networks
1322 Crossman avenue
Sunnyvale , California 94089
United States of America

Phone: +1 408 227 4500
EMail: dharkins@arubanetworks.com